CA API Gateway
Secure Installation Guide

Contents

Introduction

This guide describes how to configure the CA API Gateway v9.2 for secure installation, to support the following conformance claims:

- Common Criteria (CC) 3.1, Revision 4, September 2012
- CC Part 2 extended
- CC Part 3 conformant
- Exact conformance to:
  - Standard Protection Profile for Enterprise Security Management Policy Management v2.1, October 2013 (shortened to "ESM Policy Manager PP" for the remainder of this document)
  - Standard Protection Profile for Enterprise Security Management Access Control v2.1, October 2013 (shortened to "ESM Access Control PP" for the remainder of this document)

Notes: (1) The CA API Gateway documentation referenced within this document is available online at: https://docops.ca.com/gateway (2) The "ESM" abbreviation is also used to refer to the CA API Gateway – Enterprise Service Manager product. Do not confuse "ESM Policy Manager" with the ESM product or the Policy Manager administrative client for the CA API Gateway.

Prerequisites

A correctly configured CA API Gateway already largely conforms to the evaluated configuration. The remainder of this document describes the remaining adjustments necessary.

Before you begin, ensure that:

- A CA API Gateway v9.2 is set up and configured as described under "Configure the Appliance Gateway" in the CA API Gateway online documentation.

- You have installed the *CA_API_nShieldUpdate_64bit_v12.30.00.L7P* patch onto your Gateway. For information on obtaining and installing this patch, see "Patch an Appliance Gateway" in the CA API Gateway online documentation.
- You have applied all recent monthly platform updates to the CA API Gateway. For more information, see the following topics in the CA API Gateway online documentation:
    - Understand Gateway Patches
    - Patch an Appliance Gateway

Evaluated Configuration

The evaluated configuration assumes a CA API Gateway v9.2 configured according to the Gateway online documentation.

Note the following:

- **Load Balancer:** Load balancers are not included in the evaluated configuration.
- **Identity Providers:** The evaluated configuration supports the Internal Identity Provider, LDAP Identity Provider, and Federated Identity Providers with a X.509 credential source. Not supported are:
    - Federated Identity Providers with a SAML credential source
    - Custom identity solutions
- **Identity Server:** The Policy Manager requires a LDAP 3.0 directory server. The evaluated configuration specifies the Microsoft Active Directory. The LDAP connections must be over TLS (LDAPS).
- **FIPS Mode:** The Gateway must be configured to use FIPS mode. This is enabled by setting the *security.fips.enabled* cluster property to "true". For more information, see "Miscellaneous Cluster Properties" in the CA API Gateway online documentation.
- **Hardware Security Modules:** The CA API Gateway supports an optional hardware security module (HSM) for cryptographic operations. Hardware Appliance form factors of the evaluated configuration must be configured to use the Thales nShield F3 6000+ (Model: nC4433E-6K0) HSM. The HSM must be configured to be compliant with FIPS 140-2 Level 3.

  The HSM is optional for Virtual Appliance form factors.

  For information on configuring your HSM, see "Configure the nShield Solo+" in the CA API Gateway online documentation. Specifically, follow the steps under "Manually Programmed Security Worlds". Be sure to include the "-F" option to enable FIPS 140-2 level 3 compliance.

- **Management:** The CA API Gateway can be managed by a number of different interfaces. These interfaces are included in the evaluated configuration:
  - Policy Manager standard client
  - Gateway main menu

  These interfaces are excluded from the evaluated configuration:
  - Policy Manager web client
  - Enterprise Service Manager
- Policy Manager Environment:
  - Microsoft Windows 7
  - Java Virtual Machine JRE 8u102

  Other operating systems are supported, but are not included in the scope of evaluation.

Identification

To ensure that you have the correct evaluated system, verify the following information against your system:

➢ *To verify the Gateway version:*

1. Connect to the Gateway as the *ssgconfig* user.
2. From the main menu, open a privileged shell (option 3).
3. At the command prompt, type:

   ```
   # rpm –q ssg
   ```

   The Gateway should report "ssg-9.2.00-6904.noarch".

➢ *To verify the Policy Manager version:*

- In the Policy Manager, select **Help > About > Info** tab. You should see "Version: 9.2 build 6904".

Security Functions

This section describes the security functions provided by the CA API Gateway that are included in the evaluated configuration.

Access Control Policy Definition

The Policy Manager is used to create detailed policies that control access to SOAP Web services. There are many assertions predefined in the Policy Manager, *but only those listed below have been evaluated*.

For information about the assertions, refer to the CA API Gateway online documentation. Any additional information related to the evaluated configuration is noted below.

Access Control Assertions

The evaluated configuration includes the following assertions from the Access Control palette.

- *Authenticate User or Group Assertion*
- *Authenticate Against Identity Provider Assertion.* Only these providers are included in the evaluated configuration:
  - Internal Identity Provider
  - Federated Identity Provider with X.509 credentials
- *Require HTTP Basic Credential Assertion.* Should be used in conjunction with the *Require SSL or TLS Assertion*.
- *Require SAML Token Profile:* The evaluated configuration requires the following settings:
  - *SAML Version:* SAML v2
  - *SAML Statement Type:* Authentication
  - *Authentication Methods:* Password, Password Protected Transport, SSL/TLS Client Certificate authentication, X.509 Public Key, XML Digital Signature
  - *Authorization Statement:* Not applicable
  - *Attribute Statement:* Not applicable
  - *Subject Confirmation:* Sender Vouches (SV) or Holder-of-Key (HoK)
  - *Name Identifier:* Any
  - *Conditions:* Check Assertion Validity Period
- *Require SSL or TLS Transport with Client Authentication:* This assertion appears in two different palettes. (In the “Transport Layer Security” palette, it is named *Require SSL or TLS Transport Assertion* and does not have the “Require Client Certificate Authentication” check box selected by default.)
- *Require WS-Security Signature Credentials:* The evaluated configuration requires the following settings:
  - *Allow multiple signatures:* Disabled (check box unselected)
  - *Signature Element Variable:* Any
  - *Signature Reference Element Variable:* Any

Transport Layer Security Assertion

- *Require SSL or TLS Transport:* This assertion is the same as the *Require SSL or TLS Transport with Client Authentication* assertion under the "Access Control" palette, except the "Require Client Certificate Authentication" check box is not selected by default.

Service Availability Assertions

The evaluated configuration includes the following assertions from the Service Availability palette:

- *Limit Availability to Time/Days*
- *Restrict Access to IP Address Range*

Policy Logic Assertions

The evaluated configuration includes the following assertions from the Policy Logic palette:

- *All Assertions Must Evaluate to True*
- *At Least One Assertion Must Evaluate to True*

Access Control Policy Enforcement

The CA API Gateway enforces the policies defined by the Policy Manager. The Gateway inspects messages sent between service clients and service endpoints to evaluate and enforce compliance with the defined policies.

For information about how the Gateway resolves the service endpoint, see "Gateway Service Resolution Process" in the CA API Gateway online documentation.

WS-Security Processing

- **For the request:** The Gateway decrypts the encrypted sections in the request and verifies the WS-Security signatures.

  In the evaluated configuration, only signature verification is applicable when SAML envelope signatures are in use (the decrypting is not supported).

- **For the response:** The Gateway applies the following to the response message:
  - A default security header
  - The signatures specified by the policy (this only applies to SAML envelope signatures)
  - Encryption specified by the policy (this feature has not been evaluated)

Gateway Confirmation of Policy Versions

When a policy is edited and saved in the Policy Manager, it is saved directly to the CA API Gateway database.

The following audits are generated within 30 seconds of policy save and can be viewed using the Gateway Audit Events window. These serve as confirmations from the Gateway that a policy has been saved.

Audit generated when a policy is saved:

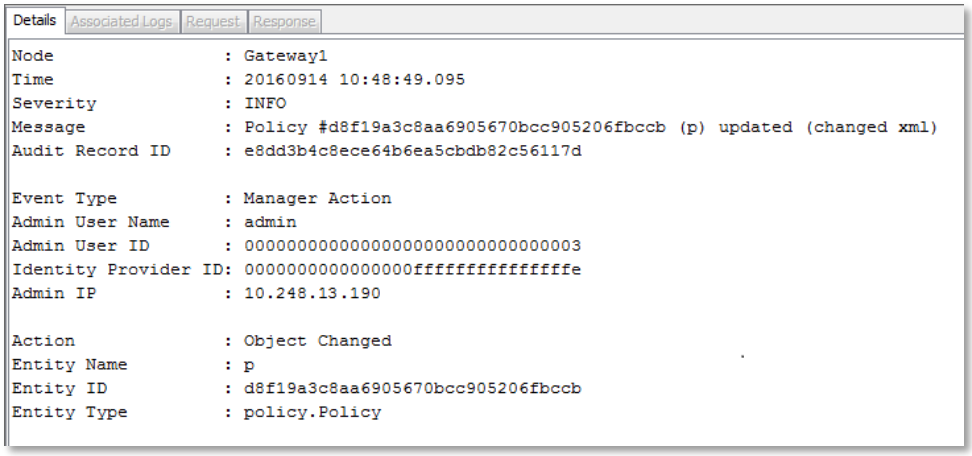

Figure 1: Policy save audit

Audit generated when a policy is saved and the version is incremented:

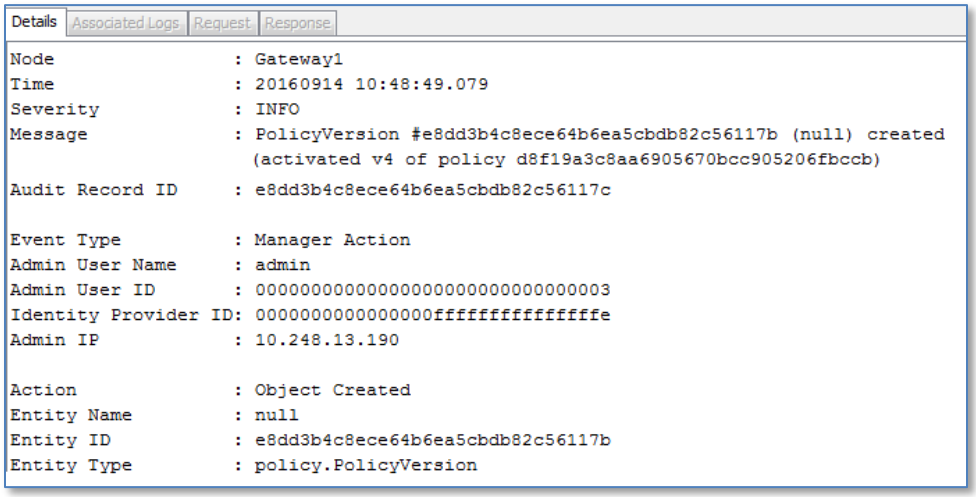

Figure 2: Policy saved and version incremented audit

System Monitoring

The Gateway maintains an audit/log trail to provide administrative insight into system management and operation. The following policy assertions are used to support system monitoring:

Audit Message in Policy Assertion
Add Audit Detail Assertion
Customize SOAP Fault Response Assertion

See also these topics for additional information about auditing:

About Message Auditing
View Gateway Audit Events
View Logs for the Gateway
Configure the Gateway Audit Functionality
Configure the Gateway Logging Functionality

These topics are contained in the CA API Gateway online documentation.

Secure Administration

The CA API Gateway employs role-based access control to restrict administrative access. It can also enforce an administrator-defined password policy. For details, see these topics in the CA API Gateway online documentation:

Manage Roles
Manage Administrative User Account Policy
Manage Password Policy

The *ssgconfig* user can also perform administration tasks using the Gateway main menu (see the "Gateway Main Menu (Appliance)" topic).

Messages can be communicated to the user during log in by using message banners. For details, see "Message Banners" on page 16.

Continuity of Enforcement

The Policy Manager saves directly to the Gateway database. If communication between the CA API Gateway and the Policy Manager is lost, the Gateway denies all requests and continues to enforce the last policy received. (FPT_FLS_EXT.1)

When the connection is lost, the Policy Manager prompts the user to either save or discard:

- If the user chooses to save, the policy is saved to an XML file with a name of the user's choosing. The default save location is: *C:\Users\[userDirectory]\.l7tech\policy.templates*.
- If the user chooses to discard, the policy changes are lost.

When the connection is restored, the user will reload the policy (which by default will load the latest in the revision history). This is the version that was in effect prior to the connection loss. At this point, the user can import and activate the saved policy. For more information, see "Importing a Policy from a File" in the CA API Gateway online documentation.

This designed behavior ensures that the Gateway always has access to the latest policy version during and after a connection loss.

Security Objectives

This section describes the security objectives and any additional steps you must take to achieve these objectives. The referenced topics are located in the CA API Gateway online documentation.

Objectives for Operational Environment

Table 1: Operational environment objectives (ESM Policy Manager PP)

Identifier	Description	Specific configuration required?
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the CA API Gateway.	None. Assigning administrators to the operational environment is covered by the topics "Managing Roles" and "Add a User or Group to a Role".
OE.CRYPTO	The Operational Environment will provide cryptographic primitives that can be used by the CA API Gateway to provide services such as ensuring the confidentiality and integrity of communications.	None.
OE.INSTAL	Those responsible for the Gateway shall ensure that the Gateway is delivered, installed, managed, and operated in a secure manner.	None.
OE.PERSON	Personnel working as Gateway administrators shall be carefully selected and trained for proper operation of the Gateway.	None.
OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.	None.
OE.SYSTIME	The Operational Environment will provide reliable time data to the Gateway.	None, provided that the network and system time have been set up as part of the normal Gateway configuration. For more information, see "Option 1 – Configure Network and System Time Settings".

Identifier	Description	Specific configuration required?
OE.USERID	The Operational Environment shall be able to identify a user requesting access to the TOE.	None. Logging in to the Gateway is described in the topic "Start the Policy Manager" (under "Connect to the Gateway").

Table 2: Operational environment objectives (ESM Access Control PP)

Identifier	Description	Specific configuration required?
OE.CRYPTO	The Operational Environment will provide cryptographic primitives that can be used by the Gateway to provide services such as ensuring the confidentiality and integrity of communications.	None.
OE.INSTALL	Those responsible for the Gateway must ensure that the Gateway is delivered, installed, managed, and operated in a manner that is consistent with IT security.	None.
OE.POLICY	The Operational Environment will provide a policy that the Gateway will enforce	None. Configuring policies is described in the topic "Configure a Service Policy".
OE.PROTECT	The Operational Environment will protect the Gateway from unauthorized modifications and access to its functions and data.	None. The roles functionality ensures that only authorized users have access.
OE.USERID	The Operational Environment shall be able to identity a user requesting access to protected resources.	None. User is validated when logging into the Gateway—see topic "Start the Policy Manager" (under "Connect to the Gateway").

Objectives for the CA API Gateway

Table 3: Security objectives (ESM Policy Manager PP)

Identifier	Description	Specific configuration required?
O.ACCESSID	The Gateway will contain the ability to validate the identity of other ESM products prior to distributing data to them.	None.
O.AUDIT	The Gateway will provide measures for generating and recording security relevant events that will detect access attempts to Gateway-protected resources by users.	None. The Gateway contains a comprehensive audit/log subsystem that records all security events. For more information, see these topics in the CA API Gateway online

Identifier	Description	Specific configuration required?
		documentation: • View Gateway Audit Events • Manage Log/Audit Sinks • Configure the Log Message Format • Configure the Gateway Audit Functionality
O.AUTH	The Gateway will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the Gateway's security functions.	None. Logging in to the Gateway is described in the topic "Start the Policy Manager" (under "Connect to the Gateway").
O.BANNER	The Gateway will display an advisory warning regarding use of the Gateway.	Configure a message banner to display the warning. This is described under "Message Banners" on page 16.
O.CONSISTENT	The Gateway will provide a mechanism to identify and rectify contradictory policy data.	None, provided that the Policy Validation window is visible and that policy validation has not been disabled in the Preferences. For more information, see "Validate a Policy" in the in the CA API Gateway online documentation.
O.DISTRIB	The Gateway will provide the ability to distribute policies to trusted IT products using secure channels.	None
O.INTEGRITY	The Gateway will contain the ability to assert the integrity of policy data.	None
O.MANAGE	The Gateway will provide the ability to manage the behavior of trusted IT products using secure channels.	None
O.POLICY	The Gateway will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.	None
O.PROTCOMMS	The Gateway will provide protected communication channels or administrators, other parts of a distributed TOE, and authorized IT entities.	None

Identifier	Description	Specific configuration required?
O.ROBUST	The Gateway will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	None
O.SELFID	The Gateway will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.	None

Table 4: Security objectives (ESM Access Control PP)

Identifier	Description	Specific configuration required?
O.DATAPROT	The Gateway will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.	None. Refer to the following topics in the Gateway online documentation to create an access control policy: • Thinking in Policy • Configure a Service Policy
O.INTEGRITY	The Gateway will contain the ability to verify the integrity of transferred data from Operational Environment components.	None
O.MAINTAIN	The Gateway will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy.	None. See "Continuity of Enforcement" on page 8 for details.
O.MNGRID	The Gateway will be able to identify and authorize a Policy Management product prior to accepting policy data from it.	None
O.MONITOR	The Gateway will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).	None. Use the Gateway Audit Viewer to inspect all the events.
O.OFLOWS	The Gateway will be able to recognize and discard invalid or malicious input provided by users.	Ensure that the appropriate policy assertions (for example, XML Security or Threat Protection) are present in the access control policy.
O.PROTCOMMS	The Gateway will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	None

Identifier	Description	Specific configuration required?
O.SELFID	The Gateway will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.	None

Security Requirements

This section describes any additional configuration required to meet the security requirements for Common Criteria.

Access Control

The Gateway policy language allows users to create service policies that control and restrict access to objects. (FDP_ACF.1, FMT_MSA.3)

For more information, refer to these topics in the CA API Gateway online documentation:

Understanding Services and Policies on the Gateway
Configure a Service Policy
Access Control Assertions

Administrative User Account Configuration

Configure the password requirements as necessary using the Manage Password Policy task. The minimum password length is **16**.

Configure various other user account settings such as maximum login attempts, lockout duration, and session expiry period using the Manage Administrative User Account Policy task. (FTA_SSL_EXT.1.1)

Users may initiate termination of the session by using the “Disconnect” button on the Policy Manager (FTA_SSL.4).

For more information, refer to the following topics in the CA API Gateway online documentation:

Manage Password Policy
Manage Administrative User Account Policy
Policy Manager Interface

Antivirus

The Gateway is capable of sending message attachments to an external server for virus checking. This capability is not evaluated.

Auditing

The Gateway displays an event in the Gateway Audit Viewer whenever a user is added or removed from management roles (see Appendix A on page 22). (FAU_GEN.1)

The Gateway audits changes to password policies. When the password policy is altered from the default 'STIG' settings, the following audits are generated and are available in the Gateway Audit Events window:

```
Node           : Gateway1
Time           : 20161217 09:49:41.463
Severity       : WARNING
Message        : Password requirements are below STIG minimum for
Internal Identity Provider
Audit Record ID: 8d2eb19dcd9926170dc3e349f775707b

Event Type     : System Message
Node IP        : 10.255.13.186
Action         : Password Policy Validation
Component      : SecureSpan Gateway: Server: Password Policy
Service
Entity name    : Password Policy Service
```

By default, the CA API Gateway records all audit events of severity INFO, WARNING, and SEVERE. Using the Policy Manager, it is possible to restrict the recording to only SEVERE events or to expand the recording to include audit events below INFO. **Note:** SEVERE events are always recorded and cannot be disabled. (FAU_SEL.1, FAU_SEL_EXT.1)

For more information, refer to the following topics in the CA API Gateway online documentation:

About Message Auditing
Audit Messages in Policy Assertion
Audit Cluster Properties (specifically *audit.messageThreshold*).

Information about all logged audit events (including the stopping and starting of the Audit System) can be viewed in the Gateway Audit Events window (see "View Gateway Audit Events" in the CA API Gateway online documentation). (FAU_GEN.1.1, FAU_GEN.1.2, FCO_NRR.2)

Audit events are recorded until a predefined percentage of the database hard disk space is consumed. Once the threshold is reached, all message processing ceases until the log size drops below the threshold. The threshold is defined in the *audit.archiverShutdownThreshold* cluster property and is 90% by default.

Older audit records (non-SEVERE events older than 7 days) can be purged using the Gateway Audit Events windows. The deletion of audit records is restricted only to those who have the Administrator or Gateway Maintenance roles[1]. (FAU_STG.1.1)

When connection to a repository is lost, the Gateway stops writing to the Syslog. When connection is restored, the Gateway resumes writing to the Syslog. For brief outages, the logged information is cached on the Gateway until connection is restored. (FAU_STG_EXT.1)

Audits can also be archived using the FTP Audit Archiver feature. For more information, refer to the following topics in the CA API Gateway online documentation:

FTP Audit Archiver
Audit Archiver Cluster Properties (used to configure thresholds, etc.)

Audit events may be logged to an internal Gateway database file or to an external Syslog server. For information on how to configure this, see "Manage Log/Audit Sinks" in the CA API Gateway online documentation. (FAU_STG_EXT.1.1)

Audits for Changes to Password Policies

When a password policy is changed, the following audits are recorded to the log:

```
INFO      IdentityProviderPasswordPolicy
#0000000000000000ffffffffffffffe updated (changed
serializedProps)
Log:
INFO    1655        com.l7tech.server.admin:
IdentityProviderPasswordPolicy #0000000000000000ffffffffffffffe
updated (changed serializedProps)

Upon changing password policy if password policy is below STIG
Requirement (doesn't matter if before the change whether the
policy is STIG or not):
WARNING          Password requirements are below STIG minimum
for Internal Identity Provider
Log:
WARNING          59          com.l7tech.server: Password
requirements are below STIG minimum for Internal Identity
Provider
```

Note that the numbers next to the severity levels are line numbers, not audit code numbers, and may be subject to change.

Cryptographic Suites

The CA API Gateway supports many different cipher suites. The evaluated configuration must include this cipher suite: (FCS_SSH_EXT.1.4, FCS_TLS_EXT.1.1)

TLS_RSA_WITH_AES_128_CBC_SHA

The following cipher suites are optional:

[1]Note that the "Gateway Maintenance" role on its own will not allow this—a user needs other roles that allow node information to be read, such as "Manage <*name*> Service" or "Operator".

TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

For more information, refer to "Selecting Cipher Suites" in the CA API Gateway online documentation.

Enterprise Authentication/Identification

The Gateway Identity Providers define all the users and groups capable of accessing the Gateway or appearing in message traffic. When connecting to the Gateway using the Policy Manager, users are authenticated by username/password or client certificate. (ESM_EAU.2, ESM_EID.2)

The following identity providers are supported in the evaluated configuration:

Internal Identity Provider
Federated Identity Provider with X.509 credentials

For more information, refer to these topics in the in the CA API Gateway online documentation:

Identity Providers
Internal Identity Provider
Federated Identity Providers
Start the Policy Manager

Identity Servers and Credential Sources

The Gateway has a built-in Internal Identity Provider and can also be configured to use a Federated Identity Provider.

When using a Federated Identity Provider, a trusted Certificate Authority (CA) capable of signing X.509 certificates for use by service clients must be available.

The following identity providers are not supported in the evaluated configuration:

- LDAP Identity Providers (including Simple LDAP Identity Providers)
- Federated Identity Providers using a SAML credential source

Message Banners

The CA API Gateway can display a message banner upon connecting to the Gateway. By default, a message banner is not displayed. (FTA_TAB.1)

➢ *To configure the message banner on the Gateway:*

1. Log in to the Gateway as *ssgconfig* and open a privileged command shell.
2. Change the permission of the script file to be edited:

```
# chmod u+w /opt/SecureSpan/Gateway/runtime/bin/samples/fix_banner.sh
```

3. Open the *fix_banner.sh* file in a text editor and edit the message as appropriate. Be sure to only modify the text between the "cat" and "EOF" lines.

   This file is preloaded with sample text specific to U.S. Government clients.

4. Save and exit the script, then execute it.
5. Restart all the Gateway nodes. The updated banner will be displayed during the next connection to the Gateway.

Tip: If SSH is not currently configured to use a banner, see the instructions at the end of the *fix_banner.sh* file on how to enable it.

The Policy Manager can display a warning banner after login, forcing the user to accept the warning or be disconnected.

➢ *To configure the warning banner on the Policy Manager:*

- Define the warning banner in the *logon.warningBanner* cluster property.

  For more information, see "Administrative Account Cluster Properties" in the CA API Gateway online documentation.

Policy Validation

The Policy Manager provides real time and on-demand validation of a policy, via messages and on-screen visual cues (red underscore). (FMT_MSA_EXT.5)

Policy validation is enabled by default and must not be disabled in the preferences.

For more information, see the following topics in the CA API Gateway online documentation:

Validate a Policy
Preferences

Replay Detection

The Gateway is protected against message replay attacks adding the "Protect Against Message Replay Assertion" to a service policy. (FPT_RPL.1)

Security Roles

The Gateway has built-in predefined roles that you can assign to users to control access to the system. (FIA_USB.1, FMT_MOF.1, FMT_MSA.1, FMT_SMR.1)

You can create custom roles to control access to audits, log sinks, and service policies. Only authorized personnel shall have access to these objects.

For more information, refer to these topics in the CA API Gateway online documentation:

Manage Roles
Predefined Roles and Permissions

Note: Be especially careful about which users get the roles Administrator and Operator. These roles have the ability to query the entire system. (FMT_MOF_EXT.1)

Secure Transport via TLS

To ensure transport-level confidentiality and integrity, include the *Require SSL or TLS Transport* assertion in your policy.

For more information, see "Require SSL or TLS Transport Assertion" in the CA API Gateway online documentation. (FTP_ITC.1.1(1))

SSH Support

The CA API Gateway Implements SSHv2. The evaluated configuration supports the OpenSSH client; be sure to use this client when connecting to the Gateway via SSH.

The following SSH encryption algorithms are supported:

AES-CBC-256
AES-CBC-128

In FIPS mode, the Gateway supports the following SSH data integrity algorithms:

HMAC-SHA1-96
HMAC-SHA1

The Gateway is configured to negotiate the above algorithms in order of preference. If a connecting client does not support the listed algorithms, the connection is refused.

To configure the CA API Gateway to support only the algorithms listed above, refer to "Selecting Cipher Suites" in the CA API Gateway online documentation.

SSH Support in Evaluated Configuration

The evaluated configuration requires the following modifications to enable only the supported algorithms:

1. Open the following file in a text editor:

   ```
   # /etc/ssh/sshd_config
   ```

2. Modify the list of algorithms to include only the supported algorithms:

   ```
   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
   ```

3. Add the following line:

   ```
   KexAlgorithms diffie-hellman-group14-sha1
   ```

   By default, the CA API Gateway supports Diffie-Hellman group 14 for key exchange as well as other less secure algorithms. The evaluated configuration requires that *only* DH group 14 be supported.

4. Save and exit the file and then restart the service:

   ```
   # service sshd restart
   ```

FIPS Mode for OpenSSL

The evaluated configuration requires the following modification to make RHEL 6 (OpenSSL) FIPS 140-2 compliant.

Tip:: For more information, refer to these resources:

http://www.inetservices.com/knowledgebase/make-rhel-6-fips-140-2-compliant/

https://access.redhat.com/solutions/137833

➢ *To make OpenSSL FIPS compliant:*

1. Check whether the prelink package is installed and disable prelinking if it is (each command is a single line).

   ```
   # rpm -q prelink && sed -i '/^PRELINKING/s,yes,no,'
   /etc/sysconfig/prelink
   ```

   ```
   # rpm -q prelink && prelink -uav
   ```

2. Install *dracut-fips:*

   ```
   #  yum install dracut-fips
   ```

3. Install *dracut-fips-aesni:*

   ```
   # yum install dracut-fips-aesni
   ```

4. Back up the existing *infitramfs:*

   ```
   # cp /boot/initramfs-2.6.32-642.11.1.el6.x86_64.img /boot/initramfs-
   nofips-2.6.32-642.11.1.el6.x86_64.img
   ```

5. Run *dracut* to rebuild *initramfs:*

   ```
   # dracut
   ```

6. Edit kernel command-line to include the fips=1 argument:

   ```
   # grubby --update-kernel=DEFAULT --args=fips=1
   ```

7. Next, you need to add the kernel parameter “boot=<*partition of /boot* >”. Run this command to find the boot parameter:

   ```
   #  df /boot
   ```

   Make a note of the returned results.

8. Locate and open the */etc/grub.conf* file in a text editor.

9. Append the results noted in step 7 to the *kernel* line in */etc/grub.conf*. The following is an example of the line after appending:

   " kernel /vmlinuz quiet rhgb ... fips=1 boot=/dev/sda1"

10. Reboot with this command:

    # reboot

➢ *To verify that FIPS is enabled:*

1. Run the following command to check that FIPS is enabled:

   # sysctl crypto.fips_enabled

   You should see the following:

   crypto.fips_enabled = 1

2. Run the following tests to verify that OpenSSL is operating under FIPS mode. First, try the following command with any file for *"<testFile>"*:

   # openssl md5 *<testFile>*

   This command should fail with *"Error setting digest md5"*. Reason: MD5 is not a FIPS-approved Hash Standard.

   Next, try the command with a FIPS-approved standard:

   # openssl sha1 *<testFile>*

   You should see a success message similar to:

   SHA1(*<testFile>*)= a94a8fe5ccb19ba61c4c0873d391e987982fbbd3

Stored Credentials and Keys

The Gateway can securely store passwords and plain text PEM private keys in its internal database, where they can be selected in situations where a password is required. The actual password is never displayed in the clear in the normal interface. (FPT_APW_EXT.1)

The Gateway stores private keys in its own internal database (as PKCS#12 files) or in the Thales nShield F3 6000+ Hardware Security Module. (FPT_SKP_EXT.1)

For more information, see the following topics in the CA API Gateway online documentation:

Manage Stored Passwords
Manage Private Keys

User Authentication/Identification

To authenticate and identity a user in a policy, insert one of the following authentication assertions into the policy:

Authenticate Against Identity Provider Assertion
Authenticate User or Group Assertion

For more information about these assertions, see the CA API Gateway online documentation.

Unevaluated Features

The following security-related features of the CA API Gateway have not been evaluated:

Access to Non-SOAP Web Services
Authentication of service clients against Identity Providers[2]
Federated Identity Providers using SAML credential source
Gateway Appliance Firewall (IP Tables)
Gateway Backup and Restore
Gateway Patch Management
Global Policy Fragments
LDAP Identity Providers
Policy Manager Audit Alerts
Salesforce Integration
Security Zones
SFTP Polling Listeners
UDDI Registries
Using the Gateway as an HTTP Proxy
Windows Domain Login
Working with CA Single Sign-On

[2] Evaluation only includes ensuring that authentication has occurred, but does not include evaluating the authentication itself.

Appendix A:
Audits for Management Role Changes

The Gateway logs the following audits whenever a user is added to or removed from a management role. These audits are visible in the Gateway Audit Event window. (FAU_GEN.1)

Table 5: Audits for management role changes

Role	Audit when user added to role	Audit when user removed from role
Administrator	INFO Role #0000000000000000ffffffffffffff9c (Administrator) updated	INFO Role #0000000000000000ffffffffffffff9c (Administrator) updated
Operator	INFO Role #0000000000000000ffffffffffffff6a (Operator) updated	INFO Role #0000000000000000ffffffffffffff6a (Operator) updated
Gateway Maintenance	INFO Role #0000000000000000ffffffffffffcae (Gateway Maintenance) updated	INFO Role #0000000000000000ffffffffffffcae (Gateway Maintenance) updated
Invoke Audit Viewer Policy	INFO Role #0000000000000000ffffffffffffb50 (Invoke Audit Viewer Policy) updated	INFO Role #0000000000000000ffffffffffffb50 (Invoke Audit Viewer Policy) updated
Manage [name] Folder	INFO Role #5726551c1ab368126cc8ff60dd10a345 (Manage <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a345 (Manage <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated
Manage [name] Identity Provider	INFO Role #5726551c1ab368126cc8ff60dd10a385 (Manage <IP Name> Identity Provider (#5726551c1ab368126cc8ff60dd10a383)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a385 (Manage <IP Name> Identity Provider (#5726551c1ab368126cc8ff60dd10a383)) updated
Manage [name] Policy	INFO Role #44c5f7b1aac091ea118908b01154ebee (Manage <policy name> Policy (#44c5f7b1aac091ea118908b01154ebea)) updated	INFO Role #44c5f7b1aac091ea118908b01154ebee (Manage <policy name> Policy (#44c5f7b1aac091ea118908b01154ebea)) updated
Manage [name] Service	INFO Role #5726551c1ab368126cc8ff60dd10a1b7 (Manage <Service name> Service (#5726551c1ab368126cc8ff60dd10a1b0)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a1b7 (Manage <Service name> Service (#5726551c1ab368126cc8ff60dd10a1b0)) updated
Manage Administrative Accounts Configuration	INFO Role #0000000000000000ffffffffffffb1e (Manage Administrative Accounts Configuration) updated	INFO Role #0000000000000000ffffffffffffb1e (Manage Administrative Accounts Configuration) updated

Role	Audit when user added to role	Audit when user removed from role
Manage Certificates	INFO Role #0000000000000000ffffffffffffda8 (Manage Certificates (truststore)) updated	INFO Role #0000000000000000ffffffffffffda8 (Manage Certificates (truststore)) updated
Manage Cluster Properties	INFO Role #0000000000000000ffffffffffffd44 (Manage Cluster Properties) updated	INFO Role #0000000000000000ffffffffffffd44 (Manage Cluster Properties) updated
Manage Cluster Status	INFO Role #0000000000000000ffffffffffffdda (Manage Cluster Status) updated	INFO Role #0000000000000000ffffffffffffdda (Manage Cluster Status) updated
Manage Custom Key Value Store	INFO Role #0000000000000000ffffffffffffa56 (Manage Custom Key Value Store) updated	INFO Role #0000000000000000ffffffffffffa56 (Manage Custom Key Value Store) updated
Manage Email Listeners	INFO Role #0000000000000000ffffffffffffc7c (Manage Email Listeners) updated	INFO Role #0000000000000000ffffffffffffc7c (Manage Email Listeners) updated
Manage Firewall Rules	INFO Role #0000000000000000ffffffffffffa88 (Manage Firewall Rules) updated	INFO Role #0000000000000000ffffffffffffa88 (Manage Firewall Rules) updated
Manage Internal Users and Groups	INFO Role #0000000000000000fffffffffffff38 (Manage Internal Users and Groups) updated	INFO Role #0000000000000000fffffffffffff38 (Manage Internal Users and Groups) updated
Manage JDBC Connections	INFO Role #0000000000000000ffffffffffffc4a (Manage JDBC Connections) updated	INFO Role #0000000000000000ffffffffffffc4a (Manage JDBC Connections) updated
Manage Listen Ports	INFO Role #0000000000000000ffffffffffffd12 (Manage Listen Ports) updated	INFO Role #0000000000000000ffffffffffffd12 (Manage Listen Ports) updated
Manage Log Sinks	INFO Role #0000000000000000ffffffffffffce0 (Manage Log Sinks) updated	INFO Role #0000000000000000ffffffffffffce0 (Manage Log Sinks) updated
Manage Message Destinations	INFO Role #0000000000000000ffffffffffffd76 (Manage Message Destinations) updated	INFO Role #0000000000000000ffffffffffffd76 (Manage Message Destinations) updated
Manage Password Policies	INFO Role #0000000000000000ffffffffffffb82 (Manage Password Policies) updated	INFO Role #0000000000000000ffffffffffffb82 (Manage Password Policies) updated
Manage Private Keys	INFO Role #0000000000000000ffffffffffffbb4 (Manage Private Keys) updated	INFO Role #0000000000000000ffffffffffffbb4 (Manage Private Keys) updated
Manage Secure Passwords	INFO Role #0000000000000000ffffffffffffbe6 (Manage Secure Passwords) updated	INFO Role #0000000000000000ffffffffffffbe6 (Manage Secure Passwords) updated

Role	Audit when user added to role	Audit when user removed from role
Manage UDDI Registries[3]	INFO Role #0000000000000000ffffffffffffffc18 (Manage UDDI Registries) updated	INFO Role #0000000000000000ffffffffffffffc18 (Manage UDDI Registries) updated
Manage CA Single Sign-On Configuration	INFO Role #0000000000000000ffffffffffffffa24 (Manage CA Single Sign-On Configuration) updated	INFO Role #0000000000000000ffffffffffffffa24 (Manage CA Single Sign-On Configuration) updated
Manage Web Services	INFO Role #0000000000000000ffffffffffffffe70 (Manage Webservices) updated	INFO Role #0000000000000000ffffffffffffffe70 (Manage Webservices) updated
Publish External Identity Providers	INFO Role #0000000000000000ffffffffffffff06 (Publish External Identity Providers) updated	INFO Role #0000000000000000ffffffffffffff06 (Publish External Identity Providers) updated
Publish Web Services	INFO Role #0000000000000000ffffffffffffffea2 (Publish Webservices) updated	INFO Role #0000000000000000ffffffffffffffea2 (Publish Webservices) updated
Search Users and Groups	INFO Role #0000000000000000ffffffffffffffed4 (Search Users and Groups) updated	INFO Role #0000000000000000ffffffffffffffed4 (Search Users and Groups) updated
View [name] Folder	INFO Role #5726551c1ab368126cc8ff60dd10a36b (View <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a36b (View <folder name> Folder (#5726551c1ab368126cc8ff60dd10a343)) updated
View [name] Log Sink	INFO Role #5726551c1ab368126cc8ff60dd10a3f8 (View <log sink name> Log Sink (#5726551c1ab368126cc8ff60dd10a3f6)) updated	INFO Role #5726551c1ab368126cc8ff60dd10a3f8 (View <log sink name> Log Sink (#5726551c1ab368126cc8ff60dd10a3f6)) updated
View Audit Records	INFO Role #0000000000000000ffffffffffffffe3e (View Audit Records) updated	INFO Role #0000000000000000ffffffffffffffe3e (View Audit Records) updated
View Service Metrics	INFO Role #0000000000000000ffffffffffffffe0c (View Service Metrics) updated	INFO Role #0000000000000000ffffffffffffffe0c (View Service Metrics) updated

Additional information is displayed about the audit when viewed in the Gateway Audit Event window. The following illustration is an example:

[3] UDDI is not included in the evaluated configuration. Role listed here for completeness.

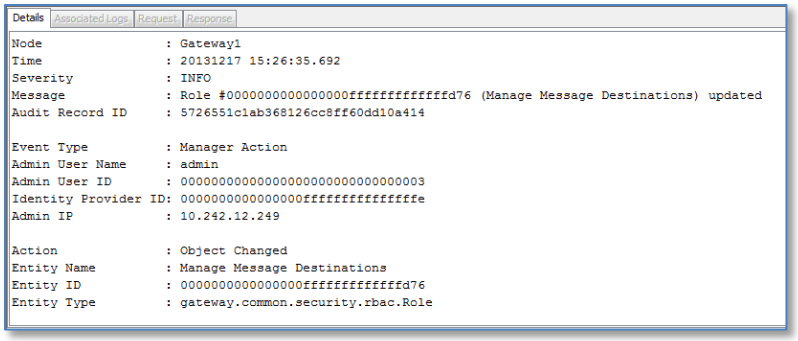

Figure 3: Example audit in Gateway Audit Events window

Appendix B:
Scope of Evaluated Policy Assertions

The CA API Gateway uses policy assertions to define and enforce policies for SOAP Web services. All available assertions are described under "Assertion Palette" in the CA API Gateway online documentation. Note that the evaluated configuration includes only a subset of the available assertions.

Table 4 lists all the assertions included with the Gateway and breaks them down into the following categories:

- **Enforcing.** Assertions that enforce the security policy used by the Gateway and have been evaluated.
- **Unevaluated Functional.** Assertions that are not security related and have not been evaluated, but may be present in the evaluated configuration. These assertions facilitate product functionality and do not interfere with the security functions of the Gateway.
- **Unevaluated Security.** Assertions that are security related but have not been evaluated.

Table 6: Evaluated policy assertions

Assertion	Enforcing	Unevaluated Functional	Unevaluated Security
Access Control Assertions			
Authenticate User or Group Assertion	X		
Authenticate Against Identity Provider Assertion	X		
Require HTTP Basic Credentials Assertion	X		
Require SAML Token Profile Assertion	X		
Require SSL or TLS Transport Assertion with Client Authentication (same as the Transport Layer Security assertion "Require SSL or TLS Transport Assertion")	X		
Authenticate Against CA Single Sign-On Assertion			X
Authorize via CA Single Sign-On Assertion			X
Check Protected Resource Against CA Single Sign-On Assertion			X

Assertion	Enforcing	Unevaluated Functional	Unevaluated Security
Exchange Credentials using WS-Trust Assertion			X
Extract Attributes from Certificate Assertion			X
Extract Attributes for Authenticated User Assertion			X
Perform JDBC Query Assertion			X
Query LDAP Assertion			X
Require Encrypted Username Token Profile Credentials Assertion			X
Require FTP Credentials Assertion			X
Require HTTP Cookie Assertion			X
Require Remote Domain Identity Assertion			X
Require NTLM Authentication Credentials Assertion			X
Require SSH Credentials Assertion			X
Require Windows Integrated Authentication Credentials Assertion			X
Require WS-Secure Conversation Assertion			X
Require WS-Security Kerberos Token Profile Credentials Assertion			X
Require WS-Security Password Digest Credentials Assertion			X
Require WS-Security Signature Credentials Assertion	X		
Require WS-Security UsernameToken Profile Credentials Assertion			X
Require XPath Credentials Assertion			X
Retrieve Credentials from Context Variable Assertion			X
Retrieve Kerberos Authentication Credentials Assertion			X
Retrieve SAML Browser Artifact Assertion			X
Use WS-Federation Credential Assertion			X

Assertion	Enforcing	Unevaluated Functional	Unevaluated Security
Transport Layer Security Assertions			
Require SSL or TLS Transport (same as Access Control assertion: *Require SSL or TLS Transport Assertion with Client Authentication*)	X		
XML Security Assertions			X
Message Validation / Transformation Assertions		X	
Message Routing Assertions			
Add Header Assertion		X	
Configure Message Streaming Assertion		X	
Copy Request Message to Response Assertion		X	
Execute Salesforce Operation Assertion		X	
Return Template Response to Requestor Assertion		X	
Route via FTP(S) Assertion – Configured with FTP		X	
Route via FTP(S) Assertion – Configured with FTPS			X
Route via HTTP(S) Assertion – Configured with HTTP		X	
Route via HTTP(S) Assertion – Configured with HTTPS			X
Route via JMS Assertion		X	
Route via MQ Native Assertion		X	
Route via Raw TCP Assertion		X	
Route via SecureSpan Bridge Assertion			X
Route via SSH2 Assertion			X
Close XMPP Session Assertion		X	
Get XMPP Session ID Assertion		X	
Start TLS on XMPP Session Assertion			X
XMPP Open Server Connection Assertion		X	

Assertion	Enforcing	Unevaluated Functional	Unevaluated Security
XMPP Associate Sessions Assertion		X	
Service Availability Assertions			
Limit Availability to Time/Days Assertion	X		
Restrict Access to IP Address Range Assertion	X		
Apply Rate Limit Assertion		X	
Apply Throughput Quota Assertion		X	
Look Up in Cache Assertion		X	
Query Rate Limit Assertion		X	
Query Throughput Quota Assertion		X	
Resolve Service Assertion		X	
Store to Cache Assertion		X	
Logging, Auditing, and Alerts Assertions			
Add Audit Detail Assertion	X		
Audit Messages in Policy Assertion	X		
Capture Identity of Requestor Assertion		X	
Customize Error Response Assertion		X	
Customize SOAP Fault Response Assertion	X		
Send Email Alert Assertion			X
Send SNMP Trap Assertion		X	
Policy Logic Assertions			
Add Comment to Policy Assertion		X	
All Assertions Must Evaluate to True Assertion	X		
At Least One Assertion Must Evaluate to True Assertion	X		
Compare Expression Assertion			X

Assertion	Enforcing	Unevaluated Functional	Unevaluated Security
Continue Processing Assertion			X
Create Routing Strategy Assertion			X
Execute Routing Strategy Assertion			X
Export Variables from Fragment Assertion			X
Generate UUID Assertion			X
Include Policy Fragment Assertion			X
Join Variable Assertion			X
Look Up Context Variable			X
Look Up Item by Value Assertion			X
Look Up Item by Index Position Assertion			X
Manipulate Multivalued Variable Assertion			X
Map Value Assertion			X
Process Routing Strategy Result Assertion			X
Run All Assertions Concurrently Assertion			X
Run Assertions for Each Item Assertion			X
Set Context Variable Assertion			X
Split Variable Assertion			X
Stop Processing Assertion			X
Threat Protection Assertions			X
Internal Assertions		X	
Custom Assertions			X