Management Center - 3.0
## Table of Contents

- Get Started with Management Center .......................................................... 15
  - Management Center Overview ...................................................................... 15
  - About this Documentation .............................................................................. 16
- Web Console Overview .................................................................................... 17
  - Verify Web Console Access ........................................................................... 20
  - Log into the Web Console ............................................................................... 21
  - Navigate the Web Console .............................................................................. 21
  - Move Items .................................................................................................. 22
- Required Ports, Protocols, and Services ......................................................... 24
- Encrypt Sensitive System Data ......................................................................... 27
- Special Character Replacement .......................................................................... 28
- Management Center Terminology ...................................................................... 29
- Set HTTPS Server Certificate Hostname for Secure Device Communication ....... 31
- Initial Configuration Guide For Virtual Appliances ........................................... 32
  - Management Center Initial Configuration .................................................... 32
  - Complete Pre-Installation Tasks .................................................................... 33
    - Pre-Installation Planning and Verification .................................................... 33
    - Register With Broadcom Support ................................................................. 33
  - Deploy Management Center as a VM ........................................................... 33
    - VMware Requirements ................................................................................ 34
    - ESX Deployment Notes ................................................................................. 34
    - Create the VMware Virtual Appliance ......................................................... 34
    - Enter the Serial Number: VMWare ................................................................. 35
    - KVM System Requirements .......................................................................... 35
    - Set Up the KVM Environment ....................................................................... 36
    - Create and Launch the Management Center KVM Instance ...................... 37
    - Enter the Serial Number - KVM ................................................................... 38
    - Configure Access to the Management Center KVM Instance .................... 38
  - Deploy Management Center on AWS ............................................................ 40
    - Prepare for AWS Deployment ...................................................................... 40
    - Step 1: Generate AWS User Data File ....................................................... 41
    - Step 2: Import and Register an AMI ............................................................ 42
Configure Users, Roles, and Attributes .......................................................... 71
Management Center Solutions ..................................................................................70
Federal Information Processing Standards (FIPS) Mode .............................................................. 67
Management Center Security Best Practices ................................................................................63
Management Center Solutions ..................................................................................70

Step 3: Deploy the Instance .......................................................................................... 44
Step 4: Verify the Instance ............................................................................................ 45
Step 5: Disassociate User Data from the Instance ......................................................... 46
Step 6: Back up and Restore an Instance of Management Center ...................................... 46
Troubleshoot Management Center on AWS ...........................................................................47

Hyper-V Hypervisor Requirements .................................................................................. 49
Create a Virtual Switch ................................................................................................. 50
Import a Management Center Hyper-V VA ........................................................................ 51
Power on the Management Center Hyper-V VA .............................................................. 54
Enter the Serial Number: Hyper-V .................................................................................. 54

Perform the Initial Configuration .................................................................................... 55
Prepare for VA Initial Configuration ................................................................................. 55
Configure the Virtual Appliance ....................................................................................... 56
(Optional) Configure Explicit Proxy .................................................................................. 57
Verify the Web Console ..................................................................................................... 57
Update the Management Center License ............................................................................. 57
Prevent Licensing Issues on Management Center Virtual Appliances ......................... 57
Retrieve and Install the License from the CLI ................................................................. 58
Stop or Restart Services ................................................................................................... 59

References ....................................................................................................................... 59
Virtual Machine Sizing Guidelines ...................................................................................... 59
Required Ports, Protocols, and Services ............................................................................ 59

Management Center Security Best Practices ................................................................. 63

Federal Information Processing Standards (FIPS) Mode .......................................................... 67

What Happens When FIPS Mode is Enabled in Management Center 2.1.1.2 ......................... 67
FIPS Cryptographic Algorithms for Management Center 2.1.1.2 ........................................ 68
Enable FIPS Mode on Management Center ........................................................................... 69
What Happens When FIPS Mode is Disabled in Management Center 2.1.1.2 ......................... 69

Configure Users, Roles, and Attributes ............................................................................ 71

Manage Management Center Users .................................................................................. 71
Add Users and Grant Permissions .................................................................................... 71
Use Specific Attribute Values to Control Access to Policy .................................................. 73
Add Local Users ............................................................................................................... 73
View All Users and Associated Roles and Permissions ....................................................... 75
Add Users from an Existing Directory or Service ............................................................... 77
  Authenticate Users Against LDAP .................................................................................... 78
  Authenticate Users Against Active Directory LDAP ....................................................... 80
  Authenticate Users Against RADIUS .............................................................................. 82
View Policy.................................................................352
View Policy Versions.........................................................352
View Existing Policy Information.................................355
View Deployed Policy for each Device Slot.................356
View Devices Associated with Policy.............................356
Configure Policy..........................................................357
Manage Attributes.........................................................357
Receive Notification When Policy Changes..................363
Compare Different Versions of the Same Policy.............364
Export Policy or Shared Objects to Local Disk...............365
Restore a Version of Policy.............................................366
Check Consistency between Policy and Devices............366
Add or Remove Devices Associated with Policy.............368
Import External Policy...................................................370
Distribute ProxySG Policy to Multiple Devices.............372
Create Job to Check Consistency of Policy.....................372
About Universal Policy Enforcement..............................373
Filter by Attributes and Keyword Search......................374
Create and Manage Jobs................................................376
Add a Job........................................................................376
Add Job That Includes Multiple Jobs (Multistep Job)......377
Add Job That Includes Multiple Operations (Multistep Device).............378
Job Scheduling Options...............................................380
Change Device Health and Statistics Monitoring State........381
Collect Sysinfo...............................................................383
Restore Device to Factory Defaults..............................384
Schedule Device Restart...............................................385
Save Device Configurations..........................................386
Schedule Reporter Reports..........................................388
Schedule Summary Report Job.....................................389
Job Operations.............................................................390
Share a Job With Another Management Center Appliance (Export/Import).........................................................393
Monitor Jobs.................................................................396
Edit a Job.......................................................................396
View Current Jobs.........................................................396
Cancel a Currently Running Job.................................397
View and Manage Job History......................................397
Organize Jobs with Folders............................................399
View Archived Files......................................................400
Management Center Reports........................................................................................................401

View Consolidated Reports.....................................................................................................401

Integrate Reporter into Management Center.........................................................................402
  View a Reporter Report.......................................................................................................403
  Create Geovisual Reporter Reports...................................................................................409
  Run a Summary Report......................................................................................................410
  View Reporter Report Details............................................................................................411
  Schedule SWG-VR Data Collection....................................................................................412
  Run a Reporter Report in the Background (Or to Archive)................................................413

Reference: Report Descriptions............................................................................................414

How Many Open Reports Can I Have?................................................................................425

Search for Specific Report Data (Search and Forensic Report)............................................425

Reporter Graph Types and Views........................................................................................428

Create a Custom Reporter Report.........................................................................................429
  Edit Custom Reporter Reports............................................................................................434
  Customize Reporter Report Options..................................................................................436
  Create Custom Report Groups..........................................................................................439
  Set Time Zone for Reporter Reports................................................................................440

Determine Why A Reporter Database Does Not Display......................................................441

View Statistics Monitoring Reports.....................................................................................442

Reference: Statistics Monitoring Reports in Management Center........................................443

Modify Options for Statistics Monitoring Reports...............................................................447

Change the Scope of a Statistics Monitoring Report............................................................449

Display a Full Statistics Monitoring Report..........................................................................450

Statistics Monitoring Graph Types.......................................................................................451

Schedule Statistics Monitoring Reports................................................................................451

Remove Orphan Device Count in Statistics Monitoring Dashboard....................................452

Statistics Monitoring Over HTTPS.......................................................................................452

Work with Reports................................................................................................................453

Create a Shared Statistics Monitoring or Reporter Custom Report......................................453

Add a Custom Logo to Downloaded Reports.......................................................................455

Filter and Keyword Search....................................................................................................456

About Database Filtering to Restrict Report Data.................................................................458

Use a Database Filter to Restrict Report Data.....................................................................458

Date Filters............................................................................................................................460

Customize Report Widgets..................................................................................................460

View Raw Report Data..........................................................................................................462

Modify Display of Table Data...............................................................................................462

Reports: Save as PDF............................................................................................................463

Monitor Device Health..........................................................................................................463
Troubleshoot and Resolve Issues ........................................................................................................... 528

"Multi-tenant policy support is not enabled for this device" when installing policy ........................................ 528
User has "access denied" error when running a job ......................................................................................... 528
User has "does not support" error when adding target device to edited policy ................................................ 529
A Device is Unassigned to a Device Group .................................................................................................. 529
"Local Changes Detected" error when installing policy .................................................................................. 529
"Import batch contains duplicate device name violation" when importing multiple devices ................................. 529
"Could not enable statistics collection due to unexpected server failure" when activating a device ...................... 529
Can't Connect to Device After Upgrading to 2.x ............................................................................................ 530
Read Messages and Alerts ............................................................................................................................. 530
Configure Diagnostics Logging ....................................................................................................................... 531
Determine Which Management Center Version You are Using ...................................................................... 531
# service .......................................................................................................................................................... 532
Configure Management Center to Trust Its Image Store .................................................................................. 534
Install Management Center Certificates on Content Analysis to Establish SSL Trust ....................................... 536
Stop or Restart Services ................................................................................................................................... 539
Test Network Connectivity ............................................................................................................................... 539
Upload System Diagnostics ............................................................................................................................. 539
View Hardware Diagnostics and Memory Resources ........................................................................................ 540
Reference: Understanding Job Permissions ........................................................................................................ 541
Reference: Permissions Interdependencies ........................................................................................................ 542
Tips and Use Cases ........................................................................................................................................ 551
Restrict Access Only to a Specific Object Included in a VPM Layer .................................................................... 551
Management Center REST API ........................................................................................................................ 555
CLI Command Reference ................................................................................................................................... 556
Command Line Overview ..................................................................................................................................... 556
Access the Management Center Command Line Interface (CLI)................................................................. 558
CLI URL Syntax.................................................................................................................................................. 559
CLI Output Processing...................................................................................................................................... 559
Configure Mode Commands........................................................................................................................... 567
acl...................................................................................................................................................................... 567
appliance-name.............................................................................................................................................. 568
device-communication................................................................................................................................. 569
dns.................................................................................................................................................................... 570
installed-systems........................................................................................................................................... 570
interface........................................................................................................................................................... 572
ip....................................................................................................................................................................... 573
ipv6................................................................................................................................................................. 574
login-banner................................................................................................................................................. 574
licensing.......................................................................................................................................................... 575
ntp.................................................................................................................................................................... 577
password-policy............................................................................................................................................. 578
proxy-settings.............................................................................................................................................. 580
security............................................................................................................................................................. 581
# service-action............................................................................................................................................ 583
shutdown....................................................................................................................................................... 585
snmp.................................................................................................................................................................. 585
    snmp agent............................................................................................................................................. 585
    snmp community................................................................................................................................. 586
    snmp system......................................................................................................................................... 587
    snmp usm local................................................................................................................................. 587
    snmp usm remote............................................................................................................................ 588
    snmp vacm group access................................................................................................................. 588
    snmp vacm group member................................................................................................................ 588
splunkforwarder........................................................................................................................................... 589
ssh-console.................................................................................................................................................... 589
ssl.................................................................................................................................................................... 590
    ssl create.............................................................................................................................................. 591
    ssl delete........................................................................................................................................... 592
    ssl edit................................................................................................................................................. 593
    ssl inline............................................................................................................................................. 594
    ssl view............................................................................................................................................... 595
statistics-monitoring................................................................................................................................. 597
timezone........................................................................................................................................................... 598
upload............................................................................................................................................................... 599
virtual-ip.......................................................................................................................................................... 599

Enable Mode Commands

- authentication
- backup
- clock
- configure
- diagnostic-systems
- diagnostics
- disable
- display-level
- event-log
- exit
- failover
- fips-mode
- halt
- health-monitoring
- history
- logout
- pcap
- ping
- restart
- restore-defaults
- send
- shutdown
- subscription
- system-services

Standard Mode Commands

- show
  - show raid
- help
- enable
- quit
Get Started with Management Center

Choose a topic to get started:

- Management Center Solutions - Look at what you can do with Management Center.
- Add a Device
- Distribute ProxySG Policy to Multiple Devices
- Schedule the Execution of a Configuration Script
- Management Center REST API - Use the API to perform Management Center operations.
- Required Ports, Protocols, and Services - Helpful information for Management Center deployment.
- Verify VMware Requirements - Verify system requirements for running a Management Center virtual appliance.
- Administrate Management Center - Manage your appliance.

Other References:

- Overview — Features and benefits of using Management Center.
- Using the Help System WebGuide - Learn how to use this WebGuide.
- Management Center Terminology — A glossary of terms used in Management Center.
- Web Console Overview - Become acquainted with the Management Center web console's user interface.

Management Center Overview

Management Center centrally manages and monitors the Symantec devices in your organization. You can organize devices into hierarchical groups, monitor device health, install policies to ProxySG devices, back up device configurations, and produce consolidated reports. In addition, you can control access to Management Center and devices by adding system users manually or authenticating through an existing directory or service, such as RADIUS.

The following table summarizes some of the features and benefits of using Management Center.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Center provides centralized management for up to 1000 devices.</td>
<td>Eliminate the need to manage each remote device manually, reducing management costs.</td>
</tr>
<tr>
<td>Groups devices based on location, department, purpose, and other attributes that you specify.</td>
<td>Delegate administrative duties and deploy policies for specific groups. Enables administrators to assign attributes for managed devices that have different purposes within their network.</td>
</tr>
<tr>
<td>Roles have greater flexibility, enabling user groups with the same permissions to access and manage policies and devices within their specific organization.</td>
<td>User Groups with the same permissions access, manage, and can report on devices within their management area without overlapping job duties and wasting time and resources. Apply roles to user groups that you need to have homogenous results (for example user groups that are in specific locations or have a specific job function).</td>
</tr>
<tr>
<td>Manages internal and external user accounts for Management Center.</td>
<td>Users only access the functional areas and perform tasks required for their jobs.</td>
</tr>
<tr>
<td>Facilitates creating and deploying policy to multiple devices simultaneously. Includes Visual Policy Manager and consistency checking between policies and devices</td>
<td>Ensure consistency amongst devices that have the same purpose or require standardized policy. Administrators can manage policy using the Visual Policy Manager on managed devices from within the Management Center web console.</td>
</tr>
</tbody>
</table>

NOTE
You can also view a list of Management Center solutions.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage attributes for devices, device groups, policy and device scripts</td>
<td>Use attributes to define custom metadata for devices, device groups, policy and device scripts. Filter on attributes to refine searches for all objects.</td>
</tr>
<tr>
<td>Create, edit and execute scripts. Includes the ability to compare script versions and to import a script from a managed device</td>
<td>Administrators can create and edit scripts as well as execute scripts on managed devices. Variable replacement is supported, as well as the ability to check versions of a saved script and to import a script from a device.</td>
</tr>
<tr>
<td>Audit log records user and system event history</td>
<td>Be aware of all user actions in the system and support organizational accountability.</td>
</tr>
</tbody>
</table>
| Default Reporting (Reports on device performance) | Management Center provides centralized reporting for managed devices. Statistics Monitoring reports are included by default and include:  
• Devices  
• WAN Optimization Reports  
For advanced reporting features, you can add a Reporter Enterprise Server as a managed device. After adding Reporter, four groups of reports are available for viewing data:  
• Security reports  
• Web Application reports  
• User Behavior reports  
• Bandwidth Usage reports  
Advanced Reporting provides visibility and a control point between employees of your organization and the cloud services and SaaS applications that users access (e.g., Box, Dropbox, Google Drive, Office 365, Salesforce, Facebook, etc.). Using full Reporter integration enables the discovery of all of the web applications in use, enabling you maximum visibility into all risky users, web sites and potential threats. See how trends of risky users and sites affect your company over time. |
| Advanced Reporting (Reporter 10.x integration) |  |
| Storing device backups on an external server | Enables administrators to export backups to external servers using any of the following 4 protocols: FTP, HTTP, HTTPS, or SCP |
| Job scheduling to automate repetitive tasks | Administrators can set up jobs to automate tasks that recur or are otherwise inefficient to perform manually. Additional permissions are required to perform some jobs. |
| Hardware appliance support | Hardware diagnostics information is available in the web console, such as System Metrics, Storage Usage, Temperature, Voltage, RPM and other sensors. From the CLI you can run hardware diagnostics, power off the appliance and restore the appliance to factory defaults. |

**About this Documentation**

This describes how to use Management Center to set up, monitor, and manage Symantec devices, and is intended for administrators. Delegated administrators might not be able to perform all of the tasks described in this guide.

Refer to the following topics to learn about this guide and other Management Center documentation.

- Using the Help System WebGuide
- Terminology
**Recommended Reading**

Before you start using Management Center, Symantec recommends that you review the following documentation:

- **VMware Documentation**, for assistance with setting up your virtual environment: [http://www.vmware.com/support/pubs/](http://www.vmware.com/support/pubs/)
- **Management Center Release Notes**, which contains information on third-party requirements, known issues, and other important information for setting up Management Center. [Access Management Center Software Downloads and Documentation](#)
- **Symantec Knowledge Base**, that includes support articles and cases pertaining to Management Center: [https://support.symantec.com](https://support.symantec.com)

**Web Console Overview**

The web console is the user interface for Management Center.

**NOTE**

Depending on a user's permissions, not all of the tabs may be visible to a particular user. See Reference: Permissions Interdependencies for more information.

**Banner**

The banner is the area at the top of the Management Center web console; look for the title Management Center. The banner is visible regardless of which tab or menu item you select. It provides you with a view of device health status and alert messages, access to your profile, global settings, and more. The following are options in the banner, from left to right (excluding the title):

- **Task Menu**
  
  contains device management operations.

- **Device Status Totals** indicate the number of devices and colors indicate device health. See the table below for web console color details.

- **Messages** display when you or other users complete certain tasks in Management Center. See Read Alerts.

- **– System Menu**
  
  contains the following options:

**Tabs**

Management Center divides functionality into tabs.

**Dashboard**

When you log in to Management Center, the web console displays the **Home** dashboard by default. From here, you can **Manage Dashboards** and customize the data that you want to monitor for managed devices. See Change the Dashboard Layout, Dashboards and Widgets, and Add the Bookmarked Devices Widget.

**Network**

**Network** displays all managed devices in your hierarchy. For each device, you can view device overview information (such as platform, OS and serial number), device health, system metrics, and the backups for each device. See Add and Monitor Devices.
Configuration
ProxySG configurations can be updated using Policy or Scripts. To create and manage policy or create and execute scripts, see Distribute Configurations to Devices.

Jobs
The Jobs tab enables you to create and run jobs, view the progress of any currently running job, and provides a way to schedule recurring jobs. You can also see the entire job history for each device. Manage Jobs.

Reports
Management Center provides centralized reporting for managed devices. Statistics Monitoring includes reports on the following categories:

• Devices
• WAN Optimization (requires a Proxy or MACH5 Edition license)

For advanced reporting features, you can add a Reporter Enterprise Server as a managed device. After adding Reporter, four groups of reports are available for viewing data about ProxySG devices:

• Security reports
• Web Application reports
• User Behavior reports
• Bandwidth Usage reports
• Log Detail

Administration
About Color-Coded Status Indicators
Colors represent the status of significant events in several areas in the web console:

• Alert colors
  In alerts that pop up in the web console and are listed in the Messages list, colors indicate the severity level of the event. If you have unread alerts, the Messages label in the banner displays the status of the message with the highest severity level. For example, if you have an unread Message-level alert and an unread Error alert, the Messages label displays a red Error status. See Read Alerts for more information.

• Banner
  On the web console banner, the Device Status Totals icons represent not only health status but the number of each devices. Click a number to view the devices in the Network tab.

• Dashboard
  Colors in the Device Health and Top Problem widgets indicate a device's health status. Select any part of the display color in the Device Health widget to display the devices in the Network tab.

• Example

• Network
  From the Network tab, a device's color indicates its health status. The colors of groups and hierarchies indicate the health status of the devices with the highest-severity status. See Monitor Device Health and View Device Backups, Exports and Restore.

• Jobs
  When viewing a currently running job, the status of the job is displayed. If you are viewing the Job History, all jobs are displayed with the completed job status. View Current Jobs.
The following table lists the statuses in Management Center, the colors associated with them, and descriptions of each status.

<table>
<thead>
<tr>
<th>Status</th>
<th>Color</th>
<th>How it applies to devices</th>
<th>How it applies to alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>red</td>
<td>A component on the device is failing, or is far outside normal parameters, and requires immediate attention. The job has not completed or has completed with errors. Red is also used for jobs that are running with errors. See View Current Jobs.</td>
<td>An error occurred, preventing an event from completing. Example: During the device registration process, the connection test failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: The ProxySG appliance's Subscription Communication Status metric is in critical state.</td>
</tr>
<tr>
<td>Warning</td>
<td>yellow</td>
<td>A component on the device is outside normal operating parameters and might require attention. Yellow is also used to show that an attribute on a device is in a warning state. See Monitor Device Health and Backups.</td>
<td>An error might occur if you do not take preventative action. Example: The Management Center license will expire in 15 days or fewer. If you do not renew the license within 15 days, Error alerts display.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: The ProxySG appliance's SGOS Base License Expiration is in warning state.</td>
<td></td>
</tr>
<tr>
<td>OK (device) Message (alert)</td>
<td>green</td>
<td>Components on the device are operating within normal parameters. The job has completed successfully. See View Job History.</td>
<td>A task was completed or a change was made. Example: A user account was added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: The monitored device has no health warnings or errors.</td>
<td></td>
</tr>
<tr>
<td>Inactive</td>
<td>gray</td>
<td>The device is pre-deployment or deactivated. See About Pre-deployed and Deactivated Devices for information.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

**Dashboard**

When you log in to Management Center, the web console displays the Home dashboard by default. From here, you can Manage Dashboards and customize the data that you want to monitor for managed devices. See Change the Dashboard Layout, Dashboards and Widgets, and Add the Bookmarked Devices Widget.
Management Center - 3.0

Network

Network displays all managed devices in your hierarchy. For each device, you can view device overview information (such as platform, OS and serial number), device health, system metrics, and the backups for each device. See Add and Monitor Devices.

Configuration

ProxySG configurations can be updated using Policy or Scripts. To create and manage policy or create and execute scripts, see Distribute Configurations to Devices.

Jobs

The Jobs tab enables you to create and run jobs, view the progress of any currently running job, and provides a way to schedule recurring jobs. You can also see the entire job history for each device. Manage Jobs.

Reports

Management Center provides centralized reporting for managed devices. Statistics Monitoring includes reports on the following categories:

- Devices
- WAN Optimization (requires a Proxy or MACH5 Edition license)

For advanced reporting features, you can add a Reporter Enterprise Server as a managed device. After adding Reporter, four groups of reports are available for viewing data about ProxySG devices:

- Security reports
- Web Application reports
- User Behavior reports
- Bandwidth Usage reports
- Log Detail

Administration

Example

Verify Web Console Access

After you install a new license or update an existing license, verify that you can access the web console. Refer to the Release Notes for a list of supported browsers.

NOTE
If you are creating a Management Center KVM instance, you must complete Configure Access to the Management Center KVM Instance before trying to verify web console access.

NOTE
TLS 1.0 and TLS 1.1 are disabled on Management Center. To securely connect to the Management Center web interface using Internet Explorer 10 or later, you must enable TLS 1.1 and 1.2 on the browser. In the browser, select Internet Options > Advanced, and enable Use TLS 1.1 and Use TLS 1.2.

1. Open a web browser.
2. In the address bar, enter the URL.
   https://<ip_address>:8082
NOTE
You cannot change the port number.
The web browser displays the login screen.
If the web console does not load, run the # licensing view CLI command to determine if the license was installed and is valid.

Log into the Web Console

Log into Management Center web console using a supported browser. For a list of supported browsers, refer to the Management Center Release Notes.

NOTE
TLS 1.0 and TLS 1.1 are disabled on Management Center. To securely connect to the Management Center web interface using Internet Explorer 10 or later, you must enable TLS 1.1 and 1.2 on the browser. In the browser, select Internet Options > Advanced, and enable Use TLS 1.1 and Use TLS 1.2.

1. In the web browser, enter one of the following URLs:
   – http://IP_address:8080
   – https://IP_address:8082
   The browser displays the login screen.
   **TIP**
   When enabled, the consent banner page displays before the login screen. If the user recognizes both the text and image, the user confirms that the system will be used for the purpose shown, by clicking Accept. Configure Consent Banner.

2. Enter your username and password, and click log in.
   **TIP**
   To restore the default admin password, see Reset or Restore Admin Account Passwords.

3. You can request a password reset. Click Reset Password. For more information, see Reset Password. For added access control, administrators should enable password reset settings for users with the correct permissions. See Enable Reset Password Settings.

4. Upon successful login, Management Center displays the main Dashboard. See Customize the Web Console and Dashboards and Widgets.

Navigate the Web Console

Refer to the following for an overview of navigational tools in the web console interface.

**Tabs**
The web console organizes information on tabs in a side bar. The functional grouping of tabs that include the Dashboards, Network, Configuration, Jobs, Reports, and Administration tabs are organized for managing devices from Management Center.
• Functional areas in the web console are divided into tabs on the left side of the interface. Hover over an icon to view information about that tab. Each tab is logically organized to perform specific tasks. For example, click **Network** to manage your devices.

• In **Dashboards**, you can see the **Home** and **Statistics Monitoring** dashboards. To close a report, click the **X** on the tab.

The **Administration** tab has numerous sections that are specific to managing Management Center itself.

**Split Screens**

In some areas of the web console, split bars divide screens into panes:

• From the **Network** tab, you can manage all devices in your network. The screens are divided into a left pane and a right pane with a filters pane on the right. The top pane displays the filters and a search field if the **Details** drop-down list has **Details** (rather than **Tiles**) selected.

If a split bar has an arrow on it, you can click the arrow to collapse or expand the split screen.

You can also move a split bar to resize panes: hover over the split bar until the pointer changes to divider. Then, drag the bar to a new location.

**Information on Multiple Pages**

In the following areas of the web console, items display on multiple pages if more than 50 items exist:

• Logs in **Auditing**

• Policy and Script Objects in **Configuration**

• Device search results in **Network**

Use the following features of the navigation bar at the bottom of a page to navigate pages:

• Click **< >** to move back or forward one page at a time.

• Click **<< >>** to go to the first page or the last page of results.

• Enter a page number in the **Page** field.

The right side of the navigation bar indicates which items are displayed and the total number of items in the list:

**Move Items**

To complete some tasks in the web console, you move items from one area or container to another. For example, you move items to add devices to groups, associate devices with policy, remove users from groups, and remove roles from users.

The following example shows the Edit User dialog, where you can add or remove roles to a user:
If the list of items is long, you can scroll down to locate the item to move. You can also search using the search field above it.

The web console allows several ways to move items.

**Drag an Item From One Area to Another**

For example, to add a role to a user, select the role under Available Roles. Click and hold; the pointer turns into a hand cursor.

Drag the role to Assigned Roles. The dialog displays a green line under Assigned Roles and the pointer turns into a pointer cursor, indicating that the role can be moved there.

Release the mouse button to move the role.

**Drag a Selected Device to a Device Group**

1. Click the Network tab. In the left pane, click Unassigned Devices. Unassigned devices display on the right pane. See Ensure Devices Belong to Device Groups.
2. Selected the saved device.
3. To assign the device to a group, select the device and drag it into the device group into the tree on the left.
4. Drop the device into the device group. Confirm the move. Click OK.
Required Ports, Protocols, and Services

Management Center uses the following ports while operating. Ensure that you allow these ports when setting up Management Center.

Important Notice

As of Saturday, April 11, 2020, The following Symantec licensing services IP address changes take effect.

<table>
<thead>
<tr>
<th>Service Host</th>
<th>Symantec IP Address (Old)</th>
<th>Broadcom IP Address (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>validation.es.bluecoat.com</td>
<td>155.64.49.136</td>
<td>192.19.237.101</td>
</tr>
<tr>
<td>bto-services.es.bluecoat.com</td>
<td>155.64.49.131</td>
<td>192.19.237.99</td>
</tr>
<tr>
<td>device-services.es.bluecoat.com</td>
<td>155.64.49.132</td>
<td>192.19.237.100</td>
</tr>
<tr>
<td>download.bluecoat.com</td>
<td>155.64.49.133</td>
<td>192.19.237.102</td>
</tr>
<tr>
<td>services.bluecoat.com</td>
<td>155.64.49.135</td>
<td>192.19.237.103</td>
</tr>
<tr>
<td>abrca.bluecoat.com</td>
<td>155.64.49.137</td>
<td>192.19.237.69</td>
</tr>
</tbody>
</table>

Inbound Connections to Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web UI</td>
<td>8080</td>
<td>TCP</td>
<td>No</td>
<td>User's client</td>
<td>Management Center web console.*</td>
</tr>
<tr>
<td>Web UI</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>User's client</td>
<td>Management Center CLI shell access</td>
</tr>
<tr>
<td>Web API</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>User's client</td>
<td>Management Center API using HTTPS</td>
</tr>
<tr>
<td>Statistics Collector</td>
<td>9009</td>
<td>TCP</td>
<td>No</td>
<td>Blue Coat ProxySG appliance/Advanced Secure Gateway/SSL Visibility</td>
<td>Performance Statistics data that is sent by monitoring assets using HTTP.*</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Configurable?</td>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------</td>
<td>----------</td>
<td>---------------</td>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Statistics Collector</td>
<td>9010</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance/ Advanced Secure Gateway/ SSL Visibility</td>
<td>Performance Statistics data that is sent by monitoring assets using HTTPS.*</td>
</tr>
<tr>
<td>Management Center Failover</td>
<td>2025</td>
<td>TCP</td>
<td>No</td>
<td>Alternate Management Center appliance in a failover cluster.</td>
<td>Used to transmit state and other pertinent information between primary and secondary Management Center appliances in a failover pair.</td>
</tr>
</tbody>
</table>

*Ports 8080 and 9009 are disabled by default on new deployments. If you upgrade from version 1.x to version 2.x and ports 8080 and 9009 were previously enabled in version 1.x (with the `security http enable` command), they will remain open after the upgrade to 2.x.

### Outbound Connections from Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP LDAPS</td>
<td>10389 389 636</td>
<td>TCP</td>
<td>Yes</td>
<td>LDAP server</td>
<td>Authentication</td>
</tr>
<tr>
<td>Active Directory</td>
<td>10389 389 636</td>
<td>TCP</td>
<td>Yes</td>
<td>Active Directory server</td>
<td>Authentication</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1812</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Authentication</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1813</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Accounting</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>TCP</td>
<td>Yes</td>
<td>SMTP server</td>
<td>SMTP alerts</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>162</td>
<td>UDP</td>
<td>Yes</td>
<td>Trap receiver</td>
<td>SNMP traps</td>
</tr>
<tr>
<td>HTTP Proxy</td>
<td>8080</td>
<td>TCP</td>
<td>Yes</td>
<td>HTTP Proxy</td>
<td>Updates</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
<td>UDP/TCP</td>
<td>No</td>
<td>NTP server list</td>
<td>Time sync to customer-configured NTP time server</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>No</td>
<td>Symantec</td>
<td><a href="https://support.symantec.com">https://support.symantec.com</a> License activation, the latest release information, and documentation</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Symantec</td>
<td><a href="https://support.symantec.com">https://support.symantec.com</a> License activation, Web Application Firewall (WAF) subscription, the latest release information, and documentation</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Configurable?</td>
<td>Destination</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------</td>
<td>----------</td>
<td>---------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP/TCP</td>
<td>No</td>
<td>DNS server</td>
<td>FQDN lookups</td>
</tr>
<tr>
<td>ProxySG/ASG</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance/Advanced Secure Gateway</td>
<td>ProxySG appliance monitoring and management</td>
</tr>
<tr>
<td>ProxySG/ASG</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance/Advanced Secure Gateway</td>
<td>System image upload</td>
</tr>
<tr>
<td>SSH access to managed devices</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>All managed devices</td>
<td>Device scripts support for appliances with SSH access, CLI shell.</td>
</tr>
<tr>
<td>SCP access to external servers</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>All managed devices and other hosts Management Center exports data to.</td>
<td>Importing and exporting data —Management Center and device backups, diagnostics, PCAP transfer</td>
</tr>
<tr>
<td>MA</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Malware Analysis</td>
<td>Health monitoring and backup</td>
</tr>
<tr>
<td>PacketShaper</td>
<td>80/443</td>
<td>TCP</td>
<td>No</td>
<td>PacketShaper</td>
<td>Health Monitoring (unencrypted/encrypted)</td>
</tr>
<tr>
<td>Reporter</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Reporter</td>
<td>Reporter API (unencrypted/encrypted)</td>
</tr>
<tr>
<td>Management Center</td>
<td>2025</td>
<td>TCP</td>
<td>No</td>
<td>Alternate Management Center appliance in a failover cluster.</td>
<td>Used to transmit state and other pertinent information between primary and secondary Management Center appliances in a failover pair.</td>
</tr>
<tr>
<td>CA</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Content Analysis</td>
<td>Health Monitoring (unencrypted/encrypted)</td>
</tr>
<tr>
<td>SSL Visibility</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>SSL Visibility</td>
<td>Health monitoring and configuration sync.</td>
</tr>
</tbody>
</table>
### Required IP Addresses and URLs

Ensure connectivity from Management Center to the following URLs.

<table>
<thead>
<tr>
<th>URL</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://telemetry.broadcom.com">https://telemetry.broadcom.com</a></td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Sends appliance usage data to Broadcom. The option must be explicitly enabled but PLA customers are required to enable it. Personally Identifiable Information that is covered under GDPR is never transmitted.</td>
</tr>
<tr>
<td>validation.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Validates the license every 5 minutes. After successful validation, validation occurs every hour.</td>
</tr>
<tr>
<td>bto-services.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Validates the license.</td>
</tr>
<tr>
<td>device-services.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>services.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>abrca.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Symantec CA.</td>
</tr>
<tr>
<td>appliance.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Trust package downloads.</td>
</tr>
<tr>
<td>subscription.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Subscription services.</td>
</tr>
<tr>
<td>upload.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Upload diagnostic reports to Symantec support.</td>
</tr>
<tr>
<td>sgapi.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Universal VPM policy.</td>
</tr>
</tbody>
</table>

### Encrypt Sensitive System Data

In 1.6 and later, each Management Center appliance (hardware or virtual) has a unique encryption key that is used to encrypt data in the system. The administrator generates this key in the Administration > Data Protection page. When the key is generated, a recovery key is also generated in case you later need to restore the encryption key. Make sure to save the recovery key in a safe place.

#### Caution: Potential Data Loss

- As part of this process, you should keep the recovery key in a safe place in the event that you need to restore the encryption key later. **DO NOT LOSE THE KEY.** If you lose the key, you will not be able to recover your encrypted data.
- You should not recover a key unless you are certain that you need to. If you use the **Restore previous key** feature and the current data in the database was not encrypted with that key, that data will not be able to be decrypted and you will have to reenter all of the device passwords.
- If the current passwords for the device were not encrypted with the previous key, you will not be able to access the information with the current passwords. You will need to reenter the device passwords before accessing the backup information.

### New Management Center Appliance Recommendations
Upon receiving a new appliance, you should do the following:

1. Select **Administration > Data Protection**.
2. Click **Generate Key**.
   A new encryption key is created and a recovery key is displayed.
3. Record the recovery key and secure it in a safe location.
4. Click **Restart System**.
5. Configure the appliance.
6. Run a Management Center backup. See **Back Up the Configuration**.

This process ensures that you can restore your configuration as necessary.

**Upgrade Recommendations**

If you are upgrading Management Center, Symantec recommends regenerating a new key and then taking a new backup. Doing so will ensure that you have the latest protection schemes and a valid backup that can be restored to the device if necessary.

1. Select **Administration > Data Protection**.
2. Click **Generate Key**.
   A new encryption key is created and a recovery key is displayed.
3. Record the recovery key and secure it in a safe location.
4. Click **Restart System**.
5. Run a Management Center backup. See **Back Up the Configuration**.

This process ensures that you will be able to restore the previous configuration if the upgrade fails.

**Special Character Replacement**

Management Center intentionally replaces some non-displayable characters, quotes, and so on, to normalize file names. This is done to create a consistent download behavior for systems receiving the files. Management Center could preserve these characters but they would not be accepted by the receiving system.

<table>
<thead>
<tr>
<th>Special Character</th>
<th>Replacement Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>_</td>
</tr>
<tr>
<td>\n</td>
<td>None. Removed.</td>
</tr>
<tr>
<td>\r</td>
<td>None. Removed.</td>
</tr>
<tr>
<td>\t</td>
<td>None. Removed.</td>
</tr>
<tr>
<td>\0</td>
<td>None. Removed.</td>
</tr>
<tr>
<td>\f</td>
<td>None. Removed.</td>
</tr>
<tr>
<td>`</td>
<td>None. Removed.</td>
</tr>
<tr>
<td>?</td>
<td>_</td>
</tr>
<tr>
<td>*</td>
<td>_</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;</td>
<td>_</td>
</tr>
<tr>
<td>&gt;</td>
<td>_</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>'</td>
<td>None. Removed.</td>
</tr>
<tr>
<td>&quot;</td>
<td>None. Removed.</td>
</tr>
</tbody>
</table>
Management Center Terminology

Important terms used in Management Center are listed alphabetically in the following table.

In some cases, this guide uses abbreviations instead of expanded forms. While using this guide, refer to this table to determine the meaning or expanded form of a term.

<table>
<thead>
<tr>
<th>Term (Abbreviation, when applicable)</th>
<th>Description and Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>This tab in the upper right of the web console where administrators can configure settings and view data specific to Management Center.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Attributes are additional metadata that you can define and apply to devices, device groups, policy and device scripts.</td>
</tr>
<tr>
<td>Command Line Interface (CLI)</td>
<td>One of two ways to access Management Center; a command line tool where you can configure Management Center and execute administrative commands. Set up the CLI admin account and password during the initial creation of your appliance. See Log on to the CLI.</td>
</tr>
<tr>
<td>Content Policy Language (CPL)</td>
<td>The language in which ProxySG appliance policy is written. Policies can be customized to an organization’s specific set of users and unique enforcement needs.</td>
</tr>
<tr>
<td>CPL Fragment</td>
<td>Policy fragments are reusable building blocks of CPL policy. Because fragments are not complete CPL policy, you do not deploy them to devices but include them within policy that you deploy to devices.</td>
</tr>
<tr>
<td>Dashboard</td>
<td>A page providing a simplified view of important information and statistics in widgets. Dashboards display in two prominent areas in the web console. Dashboards provide real-time monitoring of devices. By default, the Device Health and the Top Problem Devices widget is displayed after login.</td>
</tr>
<tr>
<td>Management Information Base (MIB)</td>
<td>MIBs are required for configuring SNMP for Management Center alerts. Download MIBs using the procedure described in Access Management Center Software Downloads and Documentation.</td>
</tr>
<tr>
<td>Metadata</td>
<td>Data about some user-defined and system-defined data in Management Center, such as the date and time of creation, the purpose of the data creation, and the user who created it. Policy objects and policy versions have metadata.</td>
</tr>
<tr>
<td>Broadcom Support</td>
<td>Website where you obtain your license for Management Center: <a href="https://support.broadcom.com/security">https://support.broadcom.com/security</a></td>
</tr>
<tr>
<td>Open Virtualized Format (OVF)</td>
<td>A format for packaging and distributing virtual machines. The OVF file in the VAP is an XML text file that defines the attributes of the specific virtual machine package.</td>
</tr>
<tr>
<td>Policy Editor</td>
<td>The area in Management Center where you write policy and create policy sections. To go to the Policy Editor, click Policy, select an object, and click Edit.</td>
</tr>
<tr>
<td>Pinned</td>
<td>The pinned item marks the item so that the item is not deleted automatically when the system attempts to recover space.</td>
</tr>
<tr>
<td>Term (Abbreviation, when applicable)</td>
<td>Description and Usage</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Prune</td>
<td>Pruning items attempts to recover storage by deleting old backup images.</td>
</tr>
<tr>
<td>Scripts</td>
<td>Commonly used configuration can be scripted. Scripts can be run on a device to configure that device. Administrators can create a script, list them, and filter scripts by attributes. The script itself is not directly associated to any device, but when you execute a script, you can select from the available devices to execute the script. Scripts are not written in a &quot;scripting&quot; language. Rather, scripts are sequentially run CLI commands. Scripts can be imported from a device.</td>
</tr>
<tr>
<td>Security Profile</td>
<td>A WAF Security Profile is a shared object that defines the Web Application Firewall settings for the associated WAF application object. You associate the WAF Security Profile with a WAF Application object to define the security rules for that object. You can create as many WAF Security Profiles as you need but a WAF Application object can be associated with only one security profile.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>A string of numbers that uniquely identify an appliance. When you first power on an appliance, you must enter the serial number before beginning initial configuration. You can verify your serial number in the web console by clicking the ? and selecting About.</td>
</tr>
<tr>
<td>SGOS</td>
<td>Operating system that runs on the ProxySG appliance.</td>
</tr>
<tr>
<td>Support case</td>
<td>A request for information or assistance with Symantec Support. To open a support case, you require a valid support entitlement with Symantec.</td>
</tr>
<tr>
<td>Tenant</td>
<td>Tenants are administrative entities defined on ProxySG appliances. Each request is routed through a tenant, whose policy is evaluated for that transaction. When no specific tenant is determined for a request, the default tenant policy is used.</td>
</tr>
<tr>
<td>Variable Substitution</td>
<td>When enabled, the replacement of substitution variables occurs when policy, policy fragments or script variables associated with a device are substituted with a specific value. Management Center attempts to replace variables with the values associated with the device where the policy is being installed or the script is being executed.</td>
</tr>
<tr>
<td>VPM Editor</td>
<td>Visual Policy Manager Editor enables you to create policy and edit policy.</td>
</tr>
<tr>
<td>Virtual Appliance (VA)</td>
<td>The virtual machine image.</td>
</tr>
<tr>
<td>Virtual Appliance Package (VAP)</td>
<td>The zip file that contains the OVF file and the virtual disk files (.vmdk) required for creating the Management Center VA.</td>
</tr>
<tr>
<td>Virtual Machine (VM)</td>
<td>An instance of an operating system and one or more applications that run in an isolated partition of a vmware server.</td>
</tr>
<tr>
<td>VMware client</td>
<td>The virtualization software used to create and/or host the virtual appliance. For simplicity, this document uses the term &quot;VMware client&quot; in all instances; substitute it with the supported ESX host you are using.</td>
</tr>
<tr>
<td>Vendor-Specific Attribute (VSA)</td>
<td>RADIUS attribute type that allows Symantec to specify its own attributes. Symantec's dictionary is available with the image download on the Symantec Support site and includes VSAs required to configure RADIUS authentication in Management Center.</td>
</tr>
<tr>
<td>Term (Abbreviation, when applicable)</td>
<td>Description and Usage</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>WAF Application Object</td>
<td>A WAF Application Object represents a web application (or group of applications) and its associated WAF security settings. The WAF application object is associated with a specific tenant and WAF Security Policy. You install this policy on ProxySG appliances to configure WAF settings.</td>
</tr>
<tr>
<td>Web Console (Management Center UI)</td>
<td>One of two ways to access Management Center; you display the web interface in a browser window, and it is the main point of access for performing tasks in Management Center. The web console comes with a default admin account and password.</td>
</tr>
<tr>
<td>Widget</td>
<td>A graphical representation of information, designed to provide you with a quick overview of statistics or other important information. Widgets display on dashboards in Management Center.</td>
</tr>
</tbody>
</table>

**Set HTTPS Server Certificate Hostname for Secure Device Communication**

This page refers to the hostname option on the **Administration > Settings > Device Communications** page.

When devices communicate with Management Center over secure channels, certificate information is exchanged. To qualify as legitimate, the hostname used by devices to communicate with Management Center should match the Common Name (CN) field of a PEM certificate, or one of the Subject Alternative Name fields. Define that hostname here.

If no value is provided for device communication, managed assets use the first IP address configured on the Management Center appliance.

**CAUTION**

If you are using PDM data collection, it is strongly recommended that you specify a hostname. If no hostname is specified, PDM data collection may fail.

**Set a Hostname**

1. Identify the hostname used in Management Center’s HTTPS server certificate, and enter it in the field on the **Administration > Settings > Device Communications** page.
2. Click **Activate** to save your changes.

This value can also be applied from the command line interface. See device-communication in the Management Center Command Line Interface reference.
Initial Configuration Guide For Virtual Appliances

Management Center Initial Configuration

Symantec® Management Center unifies management and reporting across Symantec products under a single operating environment and single pane of glass. Powerful central policy tools allow you to deploy effective web access security and governance across your entire organization. Management Center simplifies your tasks by providing inventory and health monitoring for the spectrum of supported Symantec Products:

- Blue Coat ProxySG appliance
- Content Analysis System
- SSL Visibility appliance
- Malware Analysis appliance
- PacketShaper appliance

About this Guide

This deployment guide is intended to help administrators set up and run Management Center in the following environments:

- VMware ESX
- Kernel-based Virtual Machine (KVM)
- Amazon Web Services (AWS)
- Microsoft Hyper-V Hypervisor

This document provides information on the requirements and instructions for creating and configuring a virtual Management Center appliance. This guide assumes that you are familiar with the administration of these environments.

TIP

Because KVM, ESX, AWS, and Hyper-V are outside of the Symantec network, you must upload an ISO image of the VAP file to a location accessible to your ESX, KVM, AWS, or Hyper-V instance.

The following table provides an overview of the deployment tasks.

<table>
<thead>
<tr>
<th>Deployment Step</th>
<th>Document Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete pre-installation tasks.</td>
<td>Complete Pre-Installation Tasks</td>
</tr>
<tr>
<td>Review ESX, KVM, AWS, or Hyper-V system requirements.</td>
<td>• Deploy Management Center on VMware ESX&lt;br&gt;• Deploy Management Center on KVM&lt;br&gt;• Deploy Management Center on AWS&lt;br&gt;• Deploy Management Center on Hyper-V</td>
</tr>
<tr>
<td>Create and launch the ESX, KVM, AWS, or Hyper-V virtual appliance.</td>
<td>• Deploy Management Center on VMware ESX&lt;br&gt;• Deploy Management Center on KVM&lt;br&gt;• Deploy Management Center on AWS&lt;br&gt;• Deploy Management Center on Hyper-V</td>
</tr>
<tr>
<td>Configure the Management Center virtual appliance.</td>
<td>Perform the Initial Configuration</td>
</tr>
<tr>
<td>Refer to these sections to resolve deployment issues.</td>
<td>Troubleshoot and Resolve Issues References</td>
</tr>
</tbody>
</table>
Complete Pre-Installation Tasks

Complete the following tasks before beginning the Management Center installation. These tasks apply to all deployments. If you are planning to deploy your virtual appliance in FIPS mode, see Federal Information Processing Standards (FIPS) Mode

Pre-Installation Planning and Verification

Before deploying on ESX, KVM, or AWS complete the following tasks.

Prepare and Verify Your Environment, Including Firewall Configuration

Examine the Required Ports, Protocols, and Services document to determine which ports you will need to permit to your VM-deployed.

Verify VA Configuration Requirements

Symantec recommends the following configuration as a base for your virtual appliance:

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Number of CPU Cores</th>
<th>Virtual Memory (GB)</th>
<th>Number of Virtual Drives</th>
<th>Storage Space per Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 50</td>
<td>2</td>
<td>8</td>
<td>2</td>
<td>4 GB/100 GB</td>
</tr>
<tr>
<td>51 - 250</td>
<td>4</td>
<td>16</td>
<td>2</td>
<td>4 GB/400 GB</td>
</tr>
<tr>
<td>251 - 500</td>
<td>8</td>
<td>32</td>
<td>2</td>
<td>4 GB/600 GB</td>
</tr>
<tr>
<td>501 - 1000</td>
<td>8</td>
<td>32</td>
<td>2</td>
<td>4 GB/1000 GB</td>
</tr>
</tbody>
</table>

NOTE

If Management Center is collecting statistics from ProxySG appliances configured with tenant policy, you will need to significantly increase the space requirements on Management Center. Every 1024 tenants require an extra 20 GB disk space on VM's Disk 2 storage. If, for example, each of the 10 managed devices has 2048 tenants configured (bringing the total number of tenants to 20480), the space requirement on Disk 2 is increased by an additional 400 GB.

Register With Broadcom Support

Obtain or confirm your Broadcom credentials. In addition to retrieving appliance serial numbers, these credentials are required for obtaining the ISO, OVF, or VHD image. Refer to the following content for more information:

- Symantec Getting Started
- Download Symantec Software and Tools

Deploy Management Center as a VM

The next sections provide all the steps you'll need to deploy Management Center virtually.

- Deploy Management Center on VMware ESX
- Deploy Management Center on KVM
- Deploy Management Center on AWS
- Deploy on Hyper-V
Deploy Management Center on VMware ESX

Complete the following tasks to deploy Management Center on ESX. VMware Requirements

1. VMware Requirements
2. ESX Deployment Notes
3. Create the VMware Virtual Appliance
4. Enter the Serial Number: VMWare

VMware Requirements

ESX Deployment Notes

The following describes special deployment considerations for ESX. These are not mandatory.

Create the VMware Virtual Appliance

After you extract the OVF file, create the Management Center VA.

1. Log into the VMware client.
2. Select File > Deploy OVF Template. The VMware client displays a wizard.
3. In the Source dialog, click Browse and browse to where you extracted the OVF file; click Next.
4. Verify the details for OVF template and click Next.
5. Specify a name for the VA and the inventory location; click Next.
6. Select where to put the VA (host or cluster); click Next.
7. Select where to store the virtual machine's files; click Next.
8. Specify thick or thin provisioning for the disk format and click Next.
   - If you select thin provisioning, VMware allocates only the required amount of virtual disk space for the VA. Thick provisioning could result in slightly better performance, but it is not required. Refer to VMware documentation if you require more information on virtual disk provisioning.
9. Select a network to map to and click Next.
10. On the Ready to Complete dialog, review your settings.
11. (Optional) At the bottom of the dialog, select Power on after deployment to power on the VA after deployment. If you do not select it, you can power on the VA later.
   - **NOTE**
     - Do not power on the virtual appliance if you need to adjust the resource allocation for the virtual machine.
     - See Virtual Machine Sizing Guidelines.
12. Click Finish. The VMware client displays a Deploying name message with a progress bar. When deployment is complete, close the message. The inventory on the left displays the VA.

Power On the VA

If you did not power on the VA in step 12 of the previous procedure, power it on now.

1. Locate the VA in the inventory, select it, and right-click. Select Power > Power On.
2. Verify that the VA is powered on. If it is powered on, its icon should look similar to the following:

You can also select the VA and right-click. If the VA is already powered on, the Power > Power On option should be unavailable.
Enter Your Serial Number.

Enter the Serial Number: VMWare
To activate your Virtual Appliance, enter the serial number that was provided in the eFulfillment e-mail from Symantec. After your serial number is validated, you can enter the Management Center CLI console.

1. In the VMWare client, in the inventory on the left, right-click the VA.
2. Select Open Console. The client displays the console. The console prompts you to enter the serial number.
3. Type in your serial number and press Enter.
4. If the serial number is not valid, check the number and try again. If the serial number is not accepted, do not proceed to the next steps; contact Symantec Support. See the Symantec Support web page for information: https://support.symantec.com/en_US/contact-support.html If the serial number is valid, the console prompts you to press Enter three times.
5. Press Enter three times. The console displays two options:
   – Command Line Interface
   – Setup Console
6. Press 2, to access the Initial Configuration Wizard.

Deploy Management Center on KVM
Complete the following tasks to deploy Management Center on KVM:

NOTE
Before beginning this procedure you should have completed all pre-Installation planning and verification tasks.

1. Read and understand the KVM requirements.
2. Set up the KVM environment.
3. Create and launch the Management Center KVM instance.
4. Configure the virtual appliance.
5. Configure access to the Management Center KVM instance.
6. Verify that Management Center has been configured correctly.

KVM System Requirements

KVM version
- KVM 1.5.3

OS Support
Management Center on KVM supports the following Linux-based operating system:
- CentOS 7.3

The operating system must be running kernel version 3.10 or later. Refer to the CentOS documentation as needed:
- CentOS 7.3: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/

Required Software
Confirm access to the following in your virtualization environment:
• KVM
• QEMU 2.0 or later
• Libvirt API
• Virsh tool

Set Up the KVM Environment

Before you can create the Management Center KVM instance, you need to configure the KVM environment.

Prerequisites

Before you begin, make sure you have done the following:

• Complied with the KVM System Requirements.
• Verified that your CPU has virtualization support, vmx (Intel) or svm (AMD).
• Installed CentOS 7.3 and KVM 1.5.3.
• Completed the pre-installation tasks.
• Verified that you have root/sudo permission on CentOS.
• Created a main partition with enough drive space allocated.

NOTE
See the Virtual Machine Sizing Guidelines to determine the correct parameters for your deployment.

• Placed the ISO file in a directory that be accessed by the QEMU user. Symantec recommends the following directory:
  var/lib/libvirt/images/
• Installed the qemu-kvm-ev stack from the CentOS Virtualization Special Interest Group. To install this version of qemu-kvm, use the following commands:
  # yum install centos-release-qemu-ev
  # yum install qemu-kvm-ev

Prepare for Management Center KVM Installation

Configure the KVM environment for the Management Center VA.

1. Install the required KVM packages:

   # yum install qemu-kvm libvirt libvirt-python libguestfs-tools virt-install

2. Enter the following command to verify that the following kernel modules are loaded:

   # lsmod | grep kvm

   kvm 461126 1 kvm_intel

3. Set the permissions in libvirtd:

   a.  # vi /etc/libvirt/qemu.conf
   b. Uncomment the user="root" and group="root" lines in the file.
c. Save your changes and exit vi.

4. Restart libvirt daemon:
   
   ```
   # systemctl restart libvirtd
   ```

5. Add UEFI boot support in KVM:
   a. # yum install wget
   b. # cd /etc/yum.repos.d/ && wget http://www.kraxel.org/repos/firmware.repo
   c. # yum install edk2.git-ovmf-x64 -y
   d. Append the following lines to the end of /etc/libvirt/qemu.conf file:

   ```
   nvram = [ "/usr/share/edk2.git/ovmf-x64/OVMF_CODE-pure-efi.fd:/usr/share/edk2.git/ovmf-x64/OVMF_VARS-pure-efi.fd" ]
   ```

6. Restart libvirt daemon:
   
   ```
   # systemctl restart libvirtd
   ```

### Create and Launch the Management Center KVM Instance

After you Download and Extract the VAP File and Set Up the KVM Environment, create the Management Center VA.

1. Verify that you have downloaded the .iso file to a directory for which you have full privileges. Symantec recommends the following directory:
   `var/lib/libvirt/images/`

2. Enter the following command to verify that the following kernel modules are loaded:
   ```
   # lsmod | grep kvm
   kvm                  461126  1 kvm_intel
   ```

3. Enter the following command to create and launch the KVM instance:
   
   ```
   NOTE
   The sizing provided in this example is for illustration purposes only. To determine the correct parameters for your deployment, see the Virtual Machine Sizing Guidelines.
   ```

   ```
   #
   --ram 8192 \n   --vcpus 2 \n   --disk path=va_storage_path1,bus=virtio,size=4 \n   --disk path=va_storage_path2,bus=virtio,size=100 \n   --boot uefi \n   --cdrom downloaded_iso_path \
   ```
The following example uses an Management Center KVM instance named `MC2-1-test` that will be created from an `.iso` file located in `/var/lib/libvirt/images/`:

```bash
# virt-install --name MC2-1-test 
--ram 8192 
--vcpus 2 
--disk path=/var/lib/libvirt/images/MC2-2-test1.img,bus=virtio,size=4 
--disk path=/var/lib/libvirt/images/MC2-2-test2.img,bus=virtio,size=100 
--boot uefi / 
--cdrom /var/lib.Libvirt/images/bccm_main-230197-live-install.debug.iso 
--graphics vnc,listen=127.0.0.1 
--network bridge=kvm-br0,model=virtio
```

4. Enter the following command to open the console on the Management Center KVM instance:
   ```bash
   # virsh console mc_vm_name
   ```

5. At this point, you will enter the Management Center serial number that was provided in the eFulfillment e-mail, and then configure the Management Center VA. After configuring the Management Center VA, you will need to Configure Access to the Management Center KVM Instance.

---

**Enter the Serial Number - KVM**

To activate your Virtual Appliance, enter the serial number that was provided in the eFulfillment e-mail from Symantec. After your serial number is validated, you can enter the Management Center CLI console.

1. In the KVM server, enter the following command to identify the VM name or ID of the Management Center instance:
   ```bash
   # virsh list --all
   ```

2. Enter the following command to open console to the Management Center instance:
   ```bash
   # virsh console mc_vm_name
   ```

3. Type in your serial number and press Enter.
   
   **NOTE**
   
   You might need to press Enter a few times before the system displays the CLI prompt. When it displays, the system prompts you for the serial number.

4. If the serial number is not valid, check the number and try again. If the serial number is not accepted, do not proceed to the next steps; contact Symantec Support. See the Symantec Support web page for information: [https://www.ca.com/us/services-support/ca-support/contact-support.html](https://www.ca.com/us/services-support/ca-support/contact-support.html)
   
   If the serial number is valid, the console prompts you to press Enter three times.

5. Press Enter three times. The console displays two options:
   - Command Line Interface
   - Setup Console

6. Press 2 to access the Initial Configuration Wizard.

---

**Configure Access to the Management Center KVM Instance**

This topic describes how to configure access so that users can access the Management Center KVM instance CLI shell or user interface.
NOTE
Configure your KVM virtual appliance before starting this procedure. See Deploy Management Center on KVM for a high-level list of the KVM configuration steps.

Prerequisites
Complete the following before configuring access:

• Start the firewalld service and enable it to run at boot:
  
  # sudo systemctl start firewalld
  
  # sudo systemctl enable firewalld

Configure SSH and GUI Access

1. Ensure that you have completed all prerequisites.
2. List the Management Center KVM instances to find the instance name:
   
   # virsh list --all

3. Identify the active network:
   
   # virsh net-list

4. Ensure the KVM Management Center instance is using the active network:
   
   # virsh domiflist kvm_mc_name

If the KVM Management Center instance is not using the active network, enter the following command to edit your KVM instance:

   # virsh edit kvm_instance_name

Now, edit the network name in the <interface type='network'> block. Edit the highlighted line to include the active network.

   <interface type='network'>
   <mac address='mc_mac_address'/>
   <model type='virtio'/>
   <source network='default'/>
   <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
   </interface>

5. Verify that the libvirtd service is running:
   
   # systemctl status libvirtd

6. Enable port forwarding on the firewall:

   outputclass="code"># firewall-cmd --add-masquerade --permanent

7. Add port forwarding rules to redirect traffic to the Management Center KVM instance:

   SSH:
   
   # firewall-cmd --add-forward-port=port=custom_ssh_port:proto=tcp:toport=22:toaddr=mc_ip_address --permanent

   GUI:
   
   # firewall-cmd --add-forward-port=port=8082:proto=tcp:toport=8082:toaddr=mc_ip_address --permanent

   NOTE
   The port for the Management Center GUI must be 8082 only. You cannot use other ports.

8. Reload the firewalld service to pick up your changes:
9. Update the `iptables` utility to enable SSH port forwarding:
   ```
   # firewall-cmd --reload
   # iptables -F
   # iptables -P INPUT ACCEPT
   # iptables -P FORWARD ACCEPT
   # iptables -P OUTPUT ACCEPT
   ```
   **NOTE**
   The `iptables` configuration is lost if there is a port forwarding reset or a system reboot. In those cases, you will have to re-run the preceding commands.

10. Access the SSH or GUI client.
    In the following examples the Management Center KVM instance's IP address is 198.51.100.20, the SSH port forwarding is 8111, and the GUI port forwarding is 8082.
    **SSH example**
    ```
    # ssh admin@198.51.100.20 -p 8111
    ```
    **GUI example**
    ```
    https://198.51.100.20:8082
    ```
    See [Access the Management Center Command Line Interface (CLI)] and [Verify Web Console Access] for more information.

**Proceed to the next step**

## Deploy Management Center on AWS

This section provides instructions for deploying a Symantec Management Center (MC) virtual appliance running on Xen Hypervisor in Amazon Web Services (AWS).

**NOTE**
For details beyond the scope of Management Center documentation, refer to AWS documentation: [https://aws.amazon.com/documentation/](https://aws.amazon.com/documentation/)

Complete the following tasks to install and perform initial Management Center configuration.

**Prepare for AWS Deployment**

- **Step 1: Generate AWS User Data File**
- **Step 2: Import and Register an AMI**
- **Step 3: Deploy the Instance**
- **Step 4: Verify the Instance**
- **Step 5: Disassociate User Data from the Instance**
- **Step 6: Back up and Restore an Instance of Management Center**

**Prepare for AWS Deployment**

Before deploying AWS, complete the pre-installation tasks and consider the following AWS deployment information:
• You have two ways to manage Management Center instances:
  – Using an SSH client to access the CLI.
  – Using a web browser to access the Management Console.
    You cannot access a serial or VGA console to a virtual machine.
• You cannot downgrade the MC VA image lower than version 2.0.x.
• This release does not support AWS Marketplace for third-party AMIs.

Proceed to Step 1: Generate AWS User Data File.

Step 1: Generate AWS User Data File

Complete the following steps to generate the user data file.

1. Ensure you have completed the pre-installation tasks.
2. Set up your preferred CLI:
   – AWS CLI
     [link to AWS CLI documentation]
3. Make note of or confirm the following information:
   – The username for the administrator account will always be admin.
   – The virtual appliance serial number (which you retrieved when you downloaded the VHD from Broadcom)
   – The intended password for the administrator account
   – The intended enable password for the appliance
     **NOTE**
     Make sure that the passwords are strong.
   You require these details to generate the user data file.
4. Generate the user data file:
   a. Log into https://support.broadcom.com using your Broadcom Support username and password.
     The page displays the key generator.
   c. Select Management Center.
     a. Enter the following:
        • Hostname: The appliance name to be used.
        • Serial Number: The appliance serial number.
        • Console Password: The administrative password.
        • Enable Password: The enable password.
        **TIP**
        Be sure to create strong, complex passwords.
   d. Click Generate User Data. The browser displays the user data, obfuscated by the key generator as shown in the following example:

```json
{
  "password": "\\5\\8acabdbc4fd6\\oqeer1gX.sFNfsuSYaFWl4.hELzxf6iImJsQz/2e4",
  "enable_password": \\5\2bcabd6c4fd6\\ogMjrBcIgX.ss9wwusSYaFWl4.hELzxf6iImJsQz/2e4",
  "hostname": "ManagementCenterMain",
  "serial_number": "0000000009"
}
```
Management Center - 3.0

5. (If necessary) Create an S3 bucket for the region from which you intend to launch EC2 instances.

Using the AWS dashboard:

a. Log in to the AWS dashboard.

The URL is https://console.aws.amazon.com/s3/home?region=<region_name>#

where <region_name> is the ID of the region from which you will launch EC2 instances.

b. In the list of AWS services, in the Storage & Content Delivery section, select S3.

c. If there are no existing S3 buckets, or if you want to use a new bucket for importing the image, click Create Bucket. Follow the prompts to create the bucket.

Alternatively, you can use an existing bucket for importing the image.

Using the AWS CLI:

a. Issue the following command:

```
$ aws s3 mb s3://bucket_name --region region_name
```

where region_name is the ID of the region from which you will launch EC2 instances.

Example:

```
$ aws s3 mb s3://HQ-Lab-1 --region us-east-1
```

The following output indicates that the bucket was created:

```
make_bucket: s3://HQ-Lab-1
```

**NOTE**
You cannot use EC2 CLI to create a bucket because it does not have the functionality to interact with S3.

Proceed to Step 2: Import and Register an AMI.

### Step 2: Import and Register an AMI

This section describes the CLI commands and required parameters you use to import and register an AMI. Refer to the instructions for your preferred CLI tools—either EC2 or AWS.

**Import and Register Using AWS CLI**

1. Upload the MC VHD file to the appropriate S3 bucket:

```
$ aws s3 cp local_path_to_vhd S3_URI
```

Example:

```
$ aws s3 cp C://My_VHDs/MCAWS_193348.vhd s3://mc-image
```

2. After the upload is complete, create a snapshot of the VHD file specifying the S3 bucket and VHD file from the previous step:

```
$ aws ec2 import-snapshot --description "MC Snapshot Import" --disk-container "{ \"Description\": \"MC Snapshot Import\", \"UserBucket\":{ \"S3Bucket\":\"S3_bucket\", \"S3Key\":\"VHD_name\" } }"
```

Example:

```
$ aws ec2 import-snapshot --description "Management Center Snapshot Import" --disk-container "{ \"Description\":\"MC Snapshot Import Task\", \"UserBucket\":{ \"S3Bucket\":\"mc-images\", \"S3Key\":\"MC_AWS_193348.vhd\" } }"
```

JSON output such as the following indicates successful snapshot creation:

```
{
    "SnapshotTaskDetail": {
```
"Status": "active",
"Description": "Management Center Snapshot Import",
"DiskImageSize": 0.0,
"Progress": "3",
"UserBucket": {
  "S3Bucket": "MC-images",
  "S3Key": "MC_AWS_193348.vhd"
},
"StatusMessage": "pending"
},
"Description": "Management Center Snapshot Import",
"ImportTaskId": "import-snap-fgxcnc3v"
}

Wait for the snapshot to be created. To view its progress, use the `describe-import-snapshot-tasks` command:

```bash
$ aws ec2 describe-import-snapshot-tasks --import-task-ids
```

where `SNAPSHOT_IMPORT_TASK_ID` is the identifier that AWS uses to track the snapshot creation task; look for the `ImportTaskId` key in the output. In this example, the identifier is `import-snap-fgxcnc3v`.

Example:

```bash
$ aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-fgxcnc3v
```

3. Confirm that the snapshot is created. Look for the `Status` key in the output; it should read "completed", as in the following example:

```json
{
  "ImportSnapshotTasks": [
    {
      "SnapshotTaskDetail": {
        "Status": "completed",
        "Description": "Management Center Snapshot Import",
        "Format": "VHD",
        "DiskImageSize": 430756352.0,
        "SnapshotId": "snap-87af1b61",
        "UserBucket": {
          "S3Bucket": "MC-images",
          "S3Key": "MC_AWS_193348.vhd"
        }
      },
      "Description": "Management Center Snapshot Import",
      "ImportTaskId": "import-snap-fgxcnc3v"
    }
  ]
}
```

4. Register the snapshot as the AMI you will use to launch EC2 instances:

```bash
$ aws ec2 register-image --name "AMI_NAME" --description "VHD_NAME" --architecture x86_64 --root-device-name "/dev/sda1" --virtualization-type hvm --block-device-mappings "{{"DeviceName": "/dev/sda1","Ebs":{{"SnapshotId":"SNAPSHOT_ID \"","VolumeSize":100,"DeleteOnTermination":true,"VolumeType":"io1","Iops":300}}}"
```

where `AMI_NAME` is the AMI name. Create user-friendly, memorable AMI names to help identify the AMI if you use the AWS web console to launch your EC2 instances.
Example:
```bash
$ aws ec2 register-image --name "Lab_1" --description "MC_AWS_193348.vhd" --architecture x86_64 --root-device-name "/dev/sda1" --virtualization-type hvm --block-device-mappings "["DeviceName": "/dev/sda1", "Ebs": {"SnapshotId": "snap-87af1b61", "VolumeSize": 100, "DeleteOnTermination": true, "VolumeType": "io1", "Iops": 300}]
```

The block device mappings specify the default EBS volume to be used as the root volume. You can change the volume type when you create and launch the EC2 instance.

When the snapshot is registered successfully, the CLI returns the AMI identifier:

```json
{"ImageId": "ami-8ba466e6"
}
```

Proceed to Step 3: Deploy the Instance.

### Step 3: Deploy the Instance

After you import and register the AMI, deploy the instance through the AWS Management Console.

**NOTE**

To complete this step, you require the user data file.

1. Log in to the AWS Management Console:
   a. Open a web browser window/tab.
   b. Go to the following URL: [https://console.aws.amazon.com](https://console.aws.amazon.com).
      The browser displays the AWS Management Console.
2. In the AWS Management Console, select Services > EC2.
   The browser displays the EC2 Dashboard.
3. In the Create Instance section, click Launch Instance.
   The browser opens a wizard to guide you through the import process.
4. On the left menu on the EC2 dashboard, select My AMIs.
   a. Select the AMI and click Select.
   b. Choose a supported instance type. Review the table in Prerequisite Tasks for reference.
      Click Next: Configure Instance Details.
   c. Specify networks/subnets in your AWS region and assign the instance to a placement group.
      (Required) Expand the Advanced Details section. In the User data field, select As file. Browse to the location where you saved the user data file that you created and select it.
      ▼ Advanced Details

Do not select Input is already base64 encoded.

Click Next: Add Storage.

d. Specify storage settings:
   • For the default Root volume, specify a single EBS volume 100 GiB in size.
   • For Volume Type, select Magnetic or Provisioned IOPS SSD (io1) for Volume Type. Symantec recommends that if you select Provisioned IOPS, set the IOPS to 300.
   Click Next: Tag Instance.

e. Provide the necessary tags for the instance in accordance with your corporate policy. Symantec recommends that you use a unique name as an identifier to make it easier to locate this VM for later reference.
Click **Next: Configure Security Group**.

f. Create a new security group or select an existing one. Security groups allow you to control the inbound connections to, and outbound connections from, your EC2 instance. See **Required Ports, Protocols, and Services** for more information. Typical Management Center deployments require ports 8082 (HTTPS management), 22 (SSH Management), 9010 (statistical data input from SSLV and ProxySG devices), and 2025 (failover with another MC instance).

Click **Review and Launch**.

g. Review the instance settings. Make corrections as needed.

5. Launch the instance using your preferred method:

   a. In the Management Console, click **Launch** to launch the instance.
   
   The browser displays the Launch Status page.

   b. Using AWS CLI:
      

6. In the “Your instances are now launching” message box, click the link to the instance.

   The browser displays the Instances page.

7. Under Instance State, look for a status icon and an indication of the number of checks passed. If the instance launched successfully, you should see a green icon and "2/2 checks passed".

   If fewer than two checks passed (as follows), refer to the tabs at the bottom of the page.

   ![Status Checks](image)

   Click **Status Checks** to determine which check(s) failed, and troubleshoot the problem(s) as suggested. In the following example, the Instance Status Checks report a failure and provide a link for troubleshooting.

   ![Instance Status Checks](image)

8. Repeat the previous steps as needed to set up additional instances.

   Proceed to **Step 4: Verify the Instance**.

**Step 4: Verify the Instance**

After you create the instance, verify that you can access it through SSH and the web-based Management Console.

**NOTE**

To complete this step, you require the private key (PEM file) and/or the login credentials that you used to generate the user data file.

1. On the EC2 Dashboard, select **Instances > Instances**. Locate the instance.

2. Make sure that the Instance State says "running" and that Status Checks says "2/2 checks passed".

   If fewer than two checks passed, refer to the **Status Checks** tab to determine which check(s) failed, and troubleshoot the problem(s) as suggested.

3. Select the instance, right-click, and click **Connect**.

   Connect to the instance using a standalone SSH client, such as PuTTY and enter the login command as follows: `ssh admin@ec2-hostname`
4. Access the Management Center's web-based Management Console using the instance’s AWS-assigned private IP or public IP address (depending on your security group settings) and your login credentials. With the instance selected, click the **Description** tab to determine the AWS-assigned network settings. See [Verify Web Console Access](#) for more information.

5. Go to **Configure the Virtual Appliance**.

**Step 5: Disassociate User Data from the Instance**

After verifying that the instance boots successfully, configuring Management Center, and updating the license, Symantec recommends that you dissociate the user data from the instance for security considerations.

1. Stop the instance. In the **Instances** list, select an instance and right click. On the menu, select **Instance State > Stop**.
2. Verify the instance state. In the Instance State column, look for a red icon and the status "stopped".
3. Select the instance again and right click. On the menu, select **Instance Settings > View/Change User Data**.

    On the dialog that appears, replace the contents of the User Data field with two sets of quotation marks, as follows: ""

    **NOTE**

    Deleting the contents of the User Data field does not disassociate user data from the instance; it only reverts to the user data that was associated with the instance when it was first launched.

4. Click **Save** to save your changes.
5. Restart the instance. Select the instance again and right click. On the menu, select **Instance State > Start**.


For details on changing usernames and passwords in Management Center, refer to the Management Center Configuration and Management Guide, and the Command Line Interface Reference.

**Step 6: Back up and Restore an Instance of Management Center**

In case you need to revert or restore your Management Center instance to an earlier state, you should create a snapshot of your instance. When you create a snapshot in an AWS environment, the AWS environment saves the snapshot to S3, which backs up the contents of your Amazon Elastic Book Store (EBS) volume.

**CAUTION**

Snapshots are incremental; that is, subsequent snapshots include only contents that differ from previous snapshots.

**Create a Snapshot to Back up Your Management Center Instance**

This section provides steps for creating a snapshot of your instance using your AWS console or preferred CLI tool.

To create a snapshot of your Management Center instance from your AWS console:

1. In the EC2 Dashboard, under Elastic Block Store, select **Snapshots**.
2. Click **Create Snapshot**.
3. In the Create Snapshot dialog:
   a. Select the volume for which you want to create the snapshot
   b. Enter a name and description for the snapshot.
   c. Click **Create**.

To create a snapshot using your preferred CLI tool:

- In the EC2 CLI: `ec2-create-snapshot`
- In the AWS CLI: `create-snapshot`


**Restore an Instance of Management Center from a Snapshot**

This section provides the steps for reverting or restoring an instance from a snapshot using your AWS console or preferred CLI tool.

To revert or restore an instance:

1. Create an AMI from a snapshot of an Management Center instance.
2. Deploy the newly registered AMI.

**Create an AMI from a Snapshot of an Management Center Instance**

This section provides steps for creating an AMI from a snapshot using your AWS console or preferred CLI tool.

To create an AMI from a snapshot from your AWS console:

1. In the EC2 Dashboard, under Elastic Block Store, click **Snapshots**.
2. In the list of snapshots, select the snapshot you want to create an AMI from.
3. Click **Actions > Create Image**.
4. In the Create Image from EBS Snapshot dialog, enter information in the following fields:
   a. **Architecture**: Select x86_64 for 64-bit.
   b. **Root device name**: Enter the name for the root volume.
   c. **RAM disk ID**: Use the default.
   d. **Virtualization**: Select Hardware-assisted virtualization.
   e. **Kernel ID**: Use the default.
   f. **(Optional) Block Device Mappings**: You can add new volumes or expand the size of the root volume for your AMI.
5. Click **Create**.

To create an AMI from a snapshot using your preferred CLI tool:


**Deploy the Newly Registered AMI**

You deploy snapshots the same way that you deploy new instances. For the full steps on deploying an instance, see Step 3: Deploy the Instance.

**Troubleshoot Management Center on AWS**

If you experience errors or issues using Management Center on AWS, and have already checked the Management Center Release Notes, refer to the following troubleshooting steps.
**General Troubleshooting Steps**

<table>
<thead>
<tr>
<th>Possible Troubleshooting Step</th>
<th>Details</th>
</tr>
</thead>
</table>
| Monitor instance health checks. | Look for problems under Status Checks:  
1. In the EC2 Dashboard, under Instances, select **Instances**. The page displays all instances.  
2. For the instance you are troubleshooting, under Instance State, look for a status icon and an indication of the number of checks passed. If there are no issues, you should see a green icon and "2/2 checks passed".  
3. If fewer than two checks passed, refer to the tabs at the bottom of the Instances page for details. Click **Status Checks** to determine which check(s) failed, and troubleshoot the problem(s) as suggested. |
| Take screenshots of the instance console. | AWS does not provide serial or VGA access to instances, but it allows you to generate console screenshots. To help diagnose issues, you can take these screenshots at any time while the instance is running.  
1. In the EC2 Dashboard, under Instances, select **Instances**. The page displays all instances.  
2. Select the instance and right click.  
3. On the menu, select **Instance Settings > Get Instance Screenshot**. The browser opens a new page with a static image of the console.  
4. While troubleshooting, you can:  
   - Click **Refresh** to generate newer console screenshots.  
   - Right click and save screenshot images to save the information. |
| Check the AWS security group settings and group membership for the affected instance. | Security group settings should allow communication with Symantec servers, including the licensing server. Refer to AWS documentation for details on security groups.  
Change security group membership:  
1. In the EC2 Dashboard, under Instances, select **Instances**. The page displays all instances.  
2. Select the instance and right click.  
3. On the menu, select **Networking > Change Security Groups**.  
4. On the dialog that appears, select or clear security groups as needed.  
5. Click **Assign Security Groups**.  
Edit security group settings:  
1. In the EC2 Dashboard, under Network & Security, select **Security Groups**.  
2. Select the security group, right click, and select **Edit inbound rules** or **Edit outbound rules**.  
3. On the dialog that appears, add, remove, or configure rules as needed.  
4. Click **Save**. |
# Troubleshoot Licensing Errors

<table>
<thead>
<tr>
<th>Possible Troubleshooting Step</th>
<th>Details</th>
</tr>
</thead>
</table>
| Make sure that a supported instance type is selected. | Verify that a supported instance type is selected:  
1. In the EC2 Dashboard, under Instances, select **Instances**. The page displays all instances.  
2. Select the instance and right click.  
3. On the menu, select **Instance Settings > Change Instance Type**.  
4. On the dialog that appears, make sure that a supported instance type is selected.  
5. If the selected instance type is not one that Management Center on AWS supports:  
   a. Stop the instance. In the Instances list, select an instance and right click. On the menu, select **Instance State > Stop**.  
   b. Verify the instance state. In the Instance State column, look for a red icon and the status "stopped".  
   c. Select the instance and right click. On the menu, select **Settings > Change Instance Type**.  
   d. On the dialog, select a supported type.  
   e. Click **Apply** to save your changes.  
   f. Restart the instance. Select the instance again and right click. On the menu, select **Instance State > Start**. |
| Check the AWS security group settings and group membership for the affected instance. | Security group settings should allow communication with Symantec servers, including the licensing server. Refer to AWS documentation for details on security groups.  
Change security group membership:  
1. In the EC2 Dashboard, under Instances, select **Instances**. The page displays all instances.  
2. Select the instance and right click.  
3. On the menu, select **Networking > Change Security Groups**.  
4. On the dialog that appears, select or clear security groups as needed.  
5. Click **Assign Security Groups**.  
Edit security group settings:  
1. In the EC2 Dashboard, under Network & Security, select **Security Groups**.  
2. Select the security group, right click, and select **Edit inbound rules** or **Edit outbound rules**.  
3. On the dialog that appears, add, remove, or configure rules as needed.  
4. Click **Save**. |

## Hyper-V Hypervisor Requirements

### Review Hypervisor Compatibility
Management Center is compatible with the Hyper-V hypervisor on the following operating system:  
- Microsoft Windows Server 2016 configured with GPT partition
Management Center does not support suspend and resume operations, or the creation of watchpoints.

**Verify Resource Availability**

Because all virtual appliances use a hardware resource pool that can be shared and assigned as needed, you must verify that the Hyper-V hypervisor meets the minimum hardware requirements for the Management Center model that you have purchased.

The following instructions describe how to verify system resources on the Hyper-V hypervisor using the Hyper-V Manager.

1. Access the Windows Server Manager > Local Server.
2. In the **Properties** panel, note the total amount of memory and CPU resources available on the server.
3. Access the Hyper-V Manager.
4. In the **Virtual Machines** panel, note the total amount of memory and CPU resources that are allocated to existing virtual machines.
5. Verify adequate resource availability. For Management Center VA resource requirements, see Virtual Machine Sizing Guidelines.

**About the Virtual Appliance Package (VAP)**

The VAP is a zip file that contains the following files:

- Management Center VA Hyper-V configuration folder, containing all files necessary to import the VA.
- The VHD file containing the `mc-hyper-v-install.ps1` installation script
- A PDF of this document

**Obtain the VAP**

The VAP file is located in the Management Center software download area of the Broadcom support site. Refer to the following content for more information:

- Symantec Getting Started
- Download Symantec Software and Tools

**Notes**

- Extract and store the contents of the .zip file within the same folder. Do not rename the files.
- The Management Center Hyper-V VM zip package might be blocked by a global setting in the Windows Attachment Manager. To unblock the zip file, edit the file properties or execute `Unblock#File myzipfile` in PowerShell.

**Create a Virtual Switch**

A virtual machine has virtual network interfaces that are not physically cabled to a network interface card (NIC) on the Hyper-V hypervisor host. To provide network access, a virtual switch (VMSwitch) is required. The virtual switch logically connects the virtual network interface on the virtual machine to a physical NIC on the Hyper-V hypervisor host.

Management Center supports only one virtual network interface.

If your network topology requires an extra interface for handling management traffic to Management Center, you can:

- Create a virtual switch for the interface.
- Use an existing virtual switch that provides the connectivity you require.

If you use VLANs for segregating traffic within the Hyper-V hypervisor or across your network, you must enable VLAN trunking on all interconnecting devices such as switches or routers. This guide does not include information on VLAN configurations.
If needed, follow these steps to create a virtual switch:

1. Start a PowerShell or cmd prompt and type `ipconfig /all`. From this step, note the description field of the physical NIC that you want to connect to. For example:
   
   Ethernet adapter NIC3:
   
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet #7

2. In the Hyper-V Manager’s Actions panel, click Virtual Switch Manager.

3. Choose External, and click Create Virtual Switch.

4. Name the switch and select the physical NIC to use with this switch. For the example, select 'Broadcom NetXtreme® Gigabit Ethernet #7' from the External network list.

**Import a Management Center Hyper-V VA**

**Prerequisites**

- Windows Server 2016 configured with:
  - GPT partition style
  - Hyper-V role
  - External switch
- Hyper-V Manager
- Management Center installation archive containing the following items:
  - Hyper-V VHD installation image
  - PowerShell script
  - This installation document

The Management Center Hyper-V Virtual Machine is supported on the Windows Server 2016 configured with the Hyper-V role. The server should be installed with the GPT partition style to support the full-sized virtual disks allowed by your Management Center license. A Hyper-V external switch is also required to allow Management Center to validate its license periodically and obtain dynamic application data. Nested virtualization may succeed, but is not supported.

**Creating a Management Center Hyper-V VM with PowerShell Script**

The Management Center VM is launched from a VHD image file. The Management Center VM requires virtual VHD boot and data disks. A PowerShell script is provided to simplify the VM installation. The script must have administrative privileges. Open and run the PowerShell as administrator.

**Consider vhdxtool.exe to Ease Installation**

By default, Hyper-V attempts to zero out every byte in a new data disk file. Depending on your hardware I/O performance, it can take many hours to zero out every byte on a large data file. During this time, disk usage may stay near 100 percent and Windows performance may suffer dramatically for any other I/O usage on that drive. However, the vhdxtool.exe tool can ease installation. Using vhdxtool.exe, the system can create Management Center’s multi-TB virtual data disk file in only seconds because it does not zero out every byte in the new file.

The vhdxtool.exe tool can be obtained from various third parties. For example:

[https://www.systola.com/obj/Files/static/vhdxtool.exe](https://www.systola.com/obj/Files/static/vhdxtool.exe)
WARNING
vhdxtool.exe and similar tools are optional third-party software. Use at your own risk. Symantec does not assume responsibility for supporting such tools. IN NO EVENT SHALL SYMANTEC BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The script optionally checks to see if vhdxtool.exe is available. If it is not available, you see the following warning.

```plaintext
==== Management Center Hyper-V Installation ====
Warning: Installing without Vhdtool.exe

Continue without vhdxtool.exe

? [Y/N]:
```

If you desire a fully zeroed-out data file, enter Y. To reduce the installation time, enter N, download a copy of the vhdxtool.exe tool into the same folder as the script (ensure it is named vhdxtool.exe), and run the script again.

**Required Installation Information**

During installation, you must provide the following information:

- Size of the Management Center VM
- Name
- Location on disk
- External switch

If you desire a non-standard size, a custom option is provided. At run time, your Management Center license restricts maximum usable disk size, regardless of the configured size.

**Installation Path**

The Hyper-V role uses a common path to store virtual disk files for VMs. Typically, this path is:

```
C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
```

You may choose a different path during installation. Network paths are not supported unless they are configured as persistent mapped drives.

**NOTE**

The script installs the Management Center VM into a folder that is named by the VM. Although you can stop and delete any VM with Hyper-V Manager, the manager does not delete the virtual disks on the VM. To make sure you have enough space, you might need to delete obsolete folders and files. Use caution and make sure to preserve data for current VMs.

The following output is an example of a typical Management Center Hyper-V VM installation.

**Step 1: Select the Devices Option**

```
H:\Install MC> .\mc-hyper-v-install.ps1

==== Management Center Hyper-V Installation ====
```

```plaintext
Host Name: DESKTOP-BFNLBKG
Physical CPUs: 1
Logical CPUs: 8
Total RAM: 64 GB
```
Free RAM: 60 GB

<table>
<thead>
<tr>
<th>NumberOfDevices</th>
<th>CPU</th>
<th>RAM GB</th>
<th>Boot GB</th>
<th>Data GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. up to 50</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>100</td>
</tr>
<tr>
<td>2. 51 - 250</td>
<td>4</td>
<td>16</td>
<td>4</td>
<td>400</td>
</tr>
<tr>
<td>3. 251- 500</td>
<td>8</td>
<td>32</td>
<td>4</td>
<td>600</td>
</tr>
<tr>
<td>4. 501-1000</td>
<td>8</td>
<td>32</td>
<td>4</td>
<td>1000</td>
</tr>
<tr>
<td>5. Custom</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Quit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Select the number of devices your MC will support:

**Step 2: Enter the VM Details**

Enter the VM name, installation location, and specify virtual switch details.

Select the number of devices your MC will support: 1

Processors: 2
Memory: 8 GB
Boot Disk: 4 GB
Data Disk: 100 GB

Use this size? [Y/N]: y

Enter the new VM name: MC-VM

Common Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
Enter the new VM location: T:\VM

Path: T:\VM\MC-VM
Type: Local Disk
Volume: T
Total Disk: 129 GB
Free Disk: 120 GB (16 GB after install)

Use this path? [Y/N]: y

1. Test-Switch
Select the network adapter: 1

----- Management Center Hyper-V Installation -----
Adapter: Test-Switch  
Boot Disk: 4 GB  
Data Disk: 100 GB  
Path: T:\VM\MC-VM  
Type: Local Disk  
Volume: T  
Total Disk: 129 GB  
Free Disk: 120 GB (16 GB after install) 

Create this VM? [Y/N]: y 

**Step 3: Finalize Installation**

Create this VM? [Y/N]: y 

Info: Creating new VM MC-VM.  
Info: Creating 4 GB boot file.  
Info: Creating 100 GB data file.  
Info: Adding boot disk.  
Info: Adding data disk.  
Info: Connecting network adapter. 

Info: Successfully created new VM MC-VM. 

Now use Hyper-V Manager to:  
1. Start your new Management Center VM.  
2. Connect to its console. 

Then use the console to:  
3. Assign the serial number.  
4. Setup the network configuration. 

**Power on the Management Center Hyper-V VA**

1. Log in to the Hyper-V Manager.  
2. Select the Management Center VA.  
3. Right click and select **Start**. 
4. When the Management Center VA is powered on, the State changes to **Running** in the Hyper-V Manager. 

**Enter the Serial Number: Hyper-V**

1. Open the Hyper-V Manager and select the specific VM. 
2. Right click the Hyper-V instance and click **Connect**.  
The client displays the console. The console prompts you to enter the serial number. 
3. Type in your serial number and press Enter. 

If the serial number is not valid, check the number and try again. If the serial number is not accepted, do not proceed to the next steps; contact Key defintion for "CompanyName" not found in the DITA map. Support. See the Key defintion for "CompanyName" not found in the DITA map. Support web page for information: [https://](https://)
support.symantec.com/en_US/contact-support.html If the serial number is valid, the console prompts you to press Enter three times.

4. Press Enter three times.
   The console displays two options:
   • Command Line Interface
   • Setup Console

5. Press 2, to access the Initial Configuration Wizard.

**Perform the Initial Configuration**

Complete the following tasks to install and perform initial Management Center configuration.

• Prepare for VA Initial Configuration
• Configure the Virtual Appliance
• (Optional) Configure Explicit Proxy
• Verify Web Console Access
• Update the Management Center License
• Prevent Licensing Issues on Management Center Virtual Appliances
• Retrieve and Install the License from the CLI
• Access the Management Center Command Line Interface (CLI)
• Stop or Restart Services

**Prepare for VA Initial Configuration**

The virtual appliance initial configuration wizard prompts you to configure basic network settings. Obtain and record the information specific to your deployment in this table, and then use your notes for reference when you go through the installation process.

**NOTE**
Print this page for reference

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>My values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance serial number</td>
<td>The serial number from Broadcom Support. See Download Symantec Software and Tools.</td>
<td></td>
</tr>
</tbody>
</table>
| Interface configuration   | • IP address
   When initially configuring Management Center in a KVM environment, you must assign an IP address and subnet that matches KVM's default network IP address range. That range can be seen by viewing the `/etc/libvirt/qemu/networks/default.xml` file. It should be a range between 192.168.122.2 and 192.168.122.254, with a subnet mask of 255.255.255.0.
   • Subnet mask |           |
Proceed to **Configure the Virtual Appliance**.

**Configure the Virtual Appliance**

After your serial number is validated, the system displays the initial configuration wizard. Follow the prompts to complete initial configuration of Management Center; refer to your notes in **Prepare for Initial Configuration**.

You can change these settings at any time after initial configuration. When you change the IP address, consider the following:

- The web console can take a while to load; if the browser displays an error after you change the IP address, try connecting to the web console again in a few moments.
- The SSL certificate is regenerated; you do not have to do it manually. If a new certificate is required after Management Center is already configured, use the CLI command `(config)# ssl regenerate certificate default` to regenerate it.

**Run the Initial Configuration Wizard**

1. In the initial configuration wizard, enter the following details, and press **Enter** after each entry:
   - IP address (you will use this IP address for the web console)
     When initially configuring Management Center in a KVM environment, you must assign an IP address and subnet that matches KVM's default network IP address range. That range can be seen by viewing the `/etc/libvirt/qemu/networks/default.xml` file. It should be a range between 192.168.122.2 and 192.168.122.254, with a subnet mask of 255.255.255.0.
   - Subnet mask
   - IP address for the default gateway
   - IP address for the primary DNS server
   - The **admin** account password; the wizard prompts you to enter the password again for confirmation
   - An enable mode password; different from the admin password, used to access elevated permission areas of the CLI.
   - A setup password that secures the initial configuration wizard.

Make sure that the password is not easily guessed. If the password is not valid (for example, it is fewer than six characters, or is a dictionary word), the wizard prompts you to enter another password. Use an alphanumeric password that is at least 8 characters long.

When setup is complete, the CLI displays the welcome banner:

```
Welcome to the Symantec Virtual Series Appliance Serial Console Version: Blue Coat Management Center 2.0.1.1, Release id: 218800 64-bit Production
--------------------MENU--------------------
1) Command Line Interface
2) Setup Console
-----------------------------
Enter option:
```

2. **Perform one of the following to close the console:**
   - **ESX:**
     - Press **Ctrl+Alt** to release the cursor from the Console.
   - **KVM:** When using the `virsh` console in KVM, you must press **Ctrl+J** to exit out of the console and revert back to the KVM host.
NOTE
You can only reset the admin account if you access the Initial Configuration Wizard via the serial console.

Proceed to the next step

KVM: Go to Configure Access to the Management Center KVM Instance.

ESX: Verify that Management Center has been configured correctly. Go to Verify Web Console Access, then Update the Management Center License.

AWS: Go to Verify Web Console Access, then Update the Management Center License.

(Optional) Configure Explicit Proxy

NOTE
Perform these steps only if you have an explicit proxy deployment that requires traffic from all hosts to traverse the proxy.

If your Management Center is deployed behind a ProxySG appliance, you may have to configure proxy settings before Management Center can reach the Internet to verify your or install your appliance's license.

1. Log on to the CLI and enter enable mode. See Access the Management Center CLI for instructions.
2. To enable use of the proxy server, issue the following commands:
   
   ```
   #configure t <cr>
   (config)# proxy-settings <cr>
   (config-proxy-settings)# host <proxy_ip_address_or_hostname>
   (config-proxy-settings)# port <explicit_proxy_port>
   (config-proxy-settings)#
   ```

3. (Optional) If your explicit proxy configuration requires authentication:
   ```
   (config-proxy-settings)# username:<proxy_username>
   (config-proxy-settings)# password:<proxy_password>
   ```

4. Enable the explicit proxy settings:
   ```
   (config-proxy-settings)# enable <cr>
   ```

5. Verify your explicit proxy configuration:
   ```
   (config-proxy-settings)# view
   ```

For more information on configuring proxy settings in the web console, refer to the Management Center Configuration Guide. To configure proxy settings using the CLI, refer to the ProxySG CLI Reference Guide.

Verify the Web Console

For more information, see Verify Web Console Access.

Update the Management Center License

For more information, see Update the Management Center License.

Prevent Licensing Issues on Management Center Virtual Appliances

To prevent licensing issues, ensure that the Virtual Appliance (VA) is permitted to access to the license validation server at https://validation.es.bluecoat.com through your infrastructure. See Verify Web Console Access.
If communication with the server fails, the license may be suspended. Unless you have purchased a VA offline license, constant Internet connection is required for Management Center to communicate regularly with the license validation server to confirm that the serial number is valid.

**Duplicate Serial Numbers**

If any of your virtual appliances are deployed with the same serial number, Symantec will record a violation, and that license may be invalidated. Verify your license in the Broadcom Support site and contact Support if you continue to have problems.

**Expiring Licenses**

Management Center health goes into a Warning state when the license is 30 days from expiring. For example, if the license will expire on January 30th, the Messages option in the web console banner displays Warning-level alerts, such as the following, starting on January 1st.

![License Alert]

The web console banner displays an alert for each licensed component.

Once a license expires, Management Center goes into an Error state and remains in that state for another 15 days or until the license is updated (whichever occurs first). Once the license is renewed, the warning is marked as complete and removed from the Alerts page. See Manage Alerts for more information.

If you do not renew the license within 15 days after the expiration date, you will be unable to load the web console. You must renew the license through the CLI using `licensing load` or see #licensing in the Configuration Management Guide for more information.

**Retrieve and Install the License from the CLI**

The Management Center license contains data that is used to uniquely identify the VA as a Symantec appliance.

**NOTE**

Make sure that Management Center is connected to the Internet while performing this procedure, and that it can reach https://bto-services.es.bluecoat.com.

**IMPORTANT!**

- The appliance time must be correct for the appliance to be successfully licensed. Symantec recommends that you enable NTP time synchronization.
- HTTPS connections from Management Center to Symantec servers should not be decrypted by intermediary SSL decryption devices.
- If your deployment sends all traffic through a proxy:
  - You must manually check the clock and set it to proper UTC time before attempting to download the license.
  - Create proxy policy to tunnel all Management Center traffic.

**Install License**

1. Log on to the CLI. See Access the Management Center CLI for instructions.
2. Enter privileged mode from standard mode by using the `enable` command. The prompt changes from a > to a #, indicating that you are in privileged mode.
3. At the `#` command prompt, enter the following command to either retrieve or paste the license into the CLI to install manually:
   a. (config)# licensing load to retrieve the license from MySymantec.
   b. (config)# licensing inline eof <cr> <license text> eof

   **NOTE**
   Your Management Center license can be obtained from https://mysymantec.force.com/customer/s.

   **TIP**
   For more information, refer to licensing in the Management Center Configuration Guide.

1. Restart the Management Center services with the `#restart` command.
2. Go to the Management Center web console in a web browser. See Verify Web Console Access.

   **CAUTION**
   If a license is not installed and the VA is powered on, users will be unable to load the Management Center web console. Additionally, once installed, connectivity to the license validation server must be maintained unless you have purchased a VA Offline license. The VA Offline license requires the use of a passphrase. When you use the offline license installation process, enter the same passphrase used to generate the Offline VA license. See Update the Management Center License for more information.

### Stop or Restart Services
For more information, see Stop or Restart Services.

### References
Refer to the following topics:
- Virtual Machine Sizing Guidelines
- Required Ports, Protocols, and Services
- Job Permissions

#### Virtual Machine Sizing Guidelines

### Required Ports, Protocols, and Services
Management Center uses the following ports while operating. Ensure that you allow these ports when setting up Management Center.

**Important Notice**
As of Saturday, April 11, 2020, The following Symantec licensing services IP address changes take effect.

<table>
<thead>
<tr>
<th>Service Host</th>
<th>Symantec IP Address (Old)</th>
<th>Broadcom IP Address (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>validation.es.bluecoat.com</td>
<td>155.64.49.136</td>
<td>192.19.237.101</td>
</tr>
<tr>
<td>bto-services.es.bluecoat.com</td>
<td>155.64.49.131</td>
<td>192.19.237.99</td>
</tr>
<tr>
<td>device-services.es.bluecoat.com</td>
<td>155.64.49.132</td>
<td>192.19.237.100</td>
</tr>
<tr>
<td>download.bluecoat.com</td>
<td>155.64.49.133</td>
<td>192.19.237.102</td>
</tr>
<tr>
<td>services.bluecoat.com</td>
<td>155.64.49.135</td>
<td>192.19.237.103</td>
</tr>
<tr>
<td>abrca.bluecoat.com</td>
<td>155.64.49.137</td>
<td>192.19.237.69</td>
</tr>
</tbody>
</table>
### Inbound Connections to Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web UI</td>
<td>8080 8082</td>
<td>TCP</td>
<td>No</td>
<td>User's client</td>
<td>Management Center web console.*</td>
</tr>
<tr>
<td>CLI</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>User's client</td>
<td>Management Center CLI shell access</td>
</tr>
<tr>
<td>Web API</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>User's client</td>
<td>Management Center API using HTTPS</td>
</tr>
<tr>
<td>Statistics Collector</td>
<td>9009</td>
<td>TCP</td>
<td>No</td>
<td>Blue Coat ProxySG appliance/Advanced Secure Gateway/SSL Visibility</td>
<td>Performance Statistics data that is sent by monitoring assets using HTTP.*</td>
</tr>
<tr>
<td>Statistics Collector</td>
<td>9010</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance/Advanced Secure Gateway/SSL Visibility</td>
<td>Performance Statistics data that is sent by monitoring assets using HTTPS.*</td>
</tr>
<tr>
<td>Management Center Failover</td>
<td>2025</td>
<td>TCP</td>
<td>No</td>
<td>Alternate Management Center appliance in a failover cluster.</td>
<td>Used to transmit state and other pertinent information between primary and secondary Management Center appliances in a failover pair.</td>
</tr>
</tbody>
</table>

*Ports 8080 and 9009 are disabled by default on new deployments. If you upgrade from version 1.x to version 2.x and ports 8080 and 9009 were previously enabled in version 1.x (with the `security http enable` command), they will remain open after the upgrade to 2.x.

### Outbound Connections from Management Center

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP LDAPS</td>
<td>10389 389</td>
<td>TCP 636</td>
<td>Yes</td>
<td>LDAP server</td>
<td>Authentication</td>
</tr>
<tr>
<td>Active Directory</td>
<td>10389 389</td>
<td>TCP 636</td>
<td>Yes</td>
<td>Active Directory server</td>
<td>Authentication</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1812</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Authentication</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1813</td>
<td>UDP/TCP</td>
<td>Yes</td>
<td>RADIUS server</td>
<td>Accounting</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>TCP</td>
<td>Yes</td>
<td>SMTP server</td>
<td>SMTP alerts</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>162</td>
<td>UDP</td>
<td>Yes</td>
<td>Trap receiver</td>
<td>SNMP traps</td>
</tr>
<tr>
<td>HTTP Proxy</td>
<td>8080</td>
<td>TCP</td>
<td>Yes</td>
<td>HTTP Proxy</td>
<td>Updates</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
<td>UDP/TCP</td>
<td>No</td>
<td>NTP server list</td>
<td>Time sync to customer-configured NTP time server</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Configurable?</td>
<td>Destination</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------</td>
<td>----------</td>
<td>---------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>No</td>
<td>Symantec</td>
<td><a href="https://support.symantec.com">https://support.symantec.com</a> License activation, the latest release information, and documentation</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Symantec</td>
<td><a href="https://support.symantec.com">https://support.symantec.com</a> License activation, Web Application Firewall (WAF) subscription, the latest release information, and documentation</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP/TCP</td>
<td>No</td>
<td>DNS server</td>
<td>FQDN lookups</td>
</tr>
<tr>
<td>ProxySG/ASG</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance/ Advanced Secure Gateway</td>
<td>ProxySG appliance monitoring and management</td>
</tr>
<tr>
<td>ProxySG/ASG</td>
<td>8082</td>
<td>TCP</td>
<td>No</td>
<td>ProxySG appliance/ Advanced Secure Gateway</td>
<td>System image upload</td>
</tr>
<tr>
<td>SSH access to managed devices</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>All managed devices</td>
<td>Device scripts support for appliances with SSH access, CLI shell.</td>
</tr>
<tr>
<td>SCP access to external servers</td>
<td>22</td>
<td>TCP</td>
<td>No</td>
<td>All managed devices and other hosts Management Center exports data to.</td>
<td>Importing and exporting data —Management Center and device backups, diagnostics, PCAP transfer</td>
</tr>
<tr>
<td>MA</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>Malware Analysis</td>
<td>Health monitoring and backup</td>
</tr>
<tr>
<td>PacketShaper</td>
<td>80/443</td>
<td>TCP</td>
<td>No</td>
<td>PacketShaper</td>
<td>Health Monitoring (unencrypted/ encrypted)</td>
</tr>
<tr>
<td>Reporter</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Reporter</td>
<td>Reporter API (unencrypted/ encrypted)</td>
</tr>
</tbody>
</table>
### Service Port Protocol Configurable? Destination Description

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Configurable?</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Center</td>
<td>2025</td>
<td>TCP</td>
<td>No</td>
<td>Alternate</td>
<td>Used to transmit state and other pertinent information between primary and secondary Management Center appliances in a failover pair.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Management Center appliance in a failover cluster.</td>
<td></td>
</tr>
<tr>
<td>CA</td>
<td>8080/8082</td>
<td>TCP</td>
<td>No</td>
<td>Content Analysis</td>
<td>Health Monitoring (unencrypted/encrypted)</td>
</tr>
<tr>
<td>SSL Visibility</td>
<td>443</td>
<td>TCP</td>
<td>No</td>
<td>SSL Visibility</td>
<td>Health monitoring and configuration sync.</td>
</tr>
</tbody>
</table>

### Required IP Addresses and URLs

Ensure connectivity from Management Center to the following URLs.

<table>
<thead>
<tr>
<th>URL</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://telemetry.broadcom.com">https://telemetry.broadcom.com</a></td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Sends appliance usage data to Broadcom. The option must be explicitly enabled but PLA customers are required to enable it. Personally Identifiable Information that is covered under GDPR is never transmitted.</td>
</tr>
<tr>
<td>validation.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Validates the license every 5 minutes. After successful validation, validation occurs every hour.</td>
</tr>
<tr>
<td>bto-services.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Validates the license.</td>
</tr>
<tr>
<td>device-services.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>services.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>License related.</td>
</tr>
<tr>
<td>abrca.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Symantec CA.</td>
</tr>
<tr>
<td>appliance.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Trust package downloads.</td>
</tr>
<tr>
<td>subscription.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Subscription services.</td>
</tr>
<tr>
<td>upload.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Upload diagnostic reports to Symantec support.</td>
</tr>
<tr>
<td>sgapi.es.bluecoat.com</td>
<td>HTTPS TCP</td>
<td>443</td>
<td>Universal VPM policy.</td>
</tr>
</tbody>
</table>
Management Center Security Best Practices

Your Management Center appliance attaches to other devices on your network, so it is important that you manage it in a secure fashion. The items listed here represent best-effort security considerations. Consult the security requirements of your organization when deploying Management Center in your environment.

Physical Location and Networking

- **Secure the physical location where Management Center is deployed.**
  Make sure that access is limited to a few top-level administrators. Wherever possible, monitor their access.

- **Avoid deploying Management Center with a direct connection to the Internet.**
  Wherever possible, Management Center should be behind a firewall, proxy, and or other security appliance to protect it from internet-based attacks. Note: VA instances of Management Center require access to the Internet so it is important that you provide internet access to the VA.

- **Configure the management interfaces on the appliance in unique, non-congruent subnets.**
  Configuring the interfaces in this way reduces the vectors available to an attacker.

- **Ensure that your network infrastructure is prepared for the connections to and from your Management Center appliance.**
  Refer to Required Ports, Protocols, and Services for a list of URLs and ports used by Management Center.

- **Enable TLS 1.2 for browser connecting to Management Center.**
  By default, Management Center does not allow access to the UI using SSL or TLS versions less than 1.2. Make sure you enable TLS 1.2 on some older browsers.

- **Use the ssl-context CLI command to configure device connection security.**
  An SSL context is a collection of ciphers, protocol versions, trusted certificates, and other TLS options. The `ssl-context` CLI command enables you to configure a global SSL context that applies to all devices, or to assign a context on a per-device basis. This command is available in Management Center 2.1.x and later.

- **Use only high-strength security ciphers and protocols.**
  Regardless of the default values, Symantec encourages Management Center administrators to be aware of the security landscape, and only use ciphers and protocols that are known to be highly secure.

  **NOTE**
  Do not use SSLv3, TLSv1, or TLSv1.1. Avoid using CBC ciphers.
  Although Management Center 2.1.x and later use only TLS 1.2 by default, previous TLS settings may be retained on upgrade from Management Center 2.0.x. To delete the older TLS protocols, you will explicitly have to disable TLSv1 and TLSv1.1 after upgrading.

Check Current Settings

```
# ssl view ssl-context default

Name:           default
Keyring:        default
CCL:            browser-trusted
Protocols:      tlsv1.2 tlsv1.1 tlsv1

(config)# ssl edit ssl-context default

(config ssl-context default)# protocols view
```
Management Center - 3.0

tls1.2 tls1.1 tls1
(config ssl-context default)# protocols remove tls1

ok
(config ssl-context default)# protocols remove tls1.1

ok

- **Do not rely on the self-signed certificate.**
  Symantec recommends that you replace the built-in self-signed certificate with one signed by a public Certificate Authority (CA) or your organizations private CAB, before deploying your Management Center appliance. This certificate should be generated with a 2048 bit or higher RSA key, and should use the SHA2 hashing algorithm. While Management Center does not provide a facility to generate a Certificate Signing Request (CSR), you can generate one externally using OpenSSL or from the website of your Certificate Authority. The instructions to install a CA-signed certificate are detailed here: # security

**Administering and Monitoring the Appliance**

- **Immediately change the default password.**
  On initial deployments of Management Center version 2.0 and earlier, a default password is provided for user interface access. Symantec recommends that you change the default password as soon as possible. To increase security, include at least one number and one or more special characters. Do not use colons.

- **Strengthen default password policy.**
  Symantec recommends that you change the default password policy to make it stronger. Consider the following best practices:
  - Require that passwords have a minimum of eight characters.
  - Do not allow easily guessed passwords, such as 12345678, or common words.
  - Require that all passwords contain characters from at least three character classes: letters (upper and lower case), numbers, and special or meta characters. (Do not use colons.)

- **Maintain security patches.**
  Most attacks exploit known vulnerabilities. Make sure your Management Center appliance is updated with the latest available software version.

- **Web browsers that are used by Management Center administrators accessing the web management console of the appliance should not have access to the Internet.**
  This action ensures that no web applications can glean login or other details that are used in your connection to Management Center management console.

- **Do not enable HTTP web management.**
  By default, only HTTPS web administration is enabled. Symantec does not recommend that you enable the HTTP management console for any reason.

- **Enable HTTP Strict Transport Security (HSTS).**
  - HSTS should be enabled and left enabled.
    (config)# security hsts enable
  - Set the age of the HSTS token to a value greater than 120 days:
    (config)# security hsts set-age 130
  - You should only use HSTS with a valid, signed certificate for Management Center.
  - Do not use the default self-signed certificate with Management Center as the browser blocks or ignores the HSTS headers.
NOTE
HSTS is supported only on management interface (port 8082). The Statistics Collector on port 9010 is exempt due to how devices supporting PDM Export communicate with Management Center.

- **Specify the hosts that can access Management Center.**
  Use the `security allowed-hosts` command to specify the IP addresses or hostnames that are allowed to access Management Center.

- **Ensure that connections to your mail server are encrypted.**
  Encrypt all connections to the mail server that Management Center uses to send alerts that are related to users of the system, for example, password resets. Encrypt all connections to other servers when possible.

- **Configure Management Center not to return 404 errors.**
  When users request a non-existent page, send them to a site map, search page, or authentication page instead or returning a 404 error.

- **Keep the UI inactivity timeout set to the default value (30 minutes).**
  Refer to Configure General System Settings for more information. Only use the timeout exclusion list for specific accounts requiring it. For example, use a timeout exclusion for a NOC account that might have the display up in an operations center for long periods. When using a timeout exclusion, the account should be configured so the role is set to read only for all operations.

- **Ensure that the primary administrator account (admin) details are known only to a select few administrators.**
  Set the primary admin password to use twelve or more characters, and include a mix of case and special characters. Save the details in a secure location.

- **Set a unique enable password, different from the password of the built-in admin account.**
  Set the enable password to use twelve or more characters, and include a mix of case and special characters. Save the details in a secure location.

- **Make sure that every Management Center administrator has their own account.**

- **Do not share admin accounts.** Wherever possible, use LDAPS (Secure LDAP) authentication or AD, instead of local authentication or standard LDAP or RADIUS authentication.

- **Do not use local authentication for high secure environments.**
  The local authentication mechanism does not support auto lockout after a user fails to authenticate n times. For this reason, Symantec does not recommend using local users where this feature is required.

- **Set the Management Center Audit Log to remote output syslog.**
  Management Center sends all audit records to the syslog. Symantec recommends that you enable remote syslog so that you can detect an abnormal behavior as quickly as possible. Make sure to protect this channel as it is not encrypted.

- **Enable all email and other alerts.**
  Direct them to addresses and services that can be viewed by multiple administrators. Refer to Receive Error Notifications for more information.

- **Review system logs regularly.**
  Symantec recommends that administrators frequently examine the system regularly. Specifically, review System logs for errors, anomalies, or unexpected events, and review the Audit logs for unauthorized access attempts or suspicious activities. You can find information on Management Center logs here: Preview or Download Logs

- **Change passwords on regular basis.**
  Symantec recommends that you change console, enable mode and users passwords on regular basis.

- **Set max failed attempts for external authentication services.**
  Set a limit for the number of failed access attempts on any external authentication service you are using(LDAP, AD, or Radius). If you do use the local internal user store, make sure you monitor for failed authentication requests in the audit logs.
Management Center provides a REST API that you can use to automate common operations. Use a separate role and user account for accessing the API. Doing so provides better auditing and security.
Federal Information Processing Standards (FIPS) Mode

The Federal Information Processing Standards (FIPS) mode puts Management Center into a mode that is compliant with the publicly announced standards developed by the United States federal government. You can put Management Center into FIPS mode if you are running 2.1.x or later.

You use the `fips-mode` CLI command to enable or disable FIPS mode.

NOTE
In Management Center 2.2.x and later, when the appliance is in FIPS mode, you must specify a setup password to secure the initial configuration wizard. The system prompts you for the password during initial configuration. While in FIPS mode, command line access via the serial console is protected with the admin user password. If you subsequently downgrade to a release earlier than 2.2.x, that protection is lost.

NOTE
TLS 1.0 is not supported in FIPS mode in Management Center 2.2.x and later.

CAUTION
Entering or exiting FIPS mode is a destructive operation where all user defined configuration and data is destroyed. When you enter FIPS mode, the appliance is restored to factory defaults and all previous data and configurations are destroyed. When you exit FIPS mode, the appliance goes through same zeroization process, destroying all data and configuration.

CAUTION
Backups are not compatible or transferable between FIPS and Non-FIPS mode. See Back Up the Management Center Configuration for more information.

What Happens When FIPS Mode is Enabled in Management Center 2.1.1.2

FIPS mode on Management Center 2.1 enforces the requirements of Federal Information Processing Standard 140-2 on the Management Center appliance and ensures the use of FIPS 140-2 approved algorithms and behavior. The term FIPS mode refers to secure configuration that meets FIPS requirements.

NOTE
Management Center 2.1.1.2 is the only FIPS certified release. If you enable FIPS mode on Management Center images released later than 2.1.1.2, system operation is compliant with the FIPS requirements specified at the time that 2.1 was validated; however, those releases are not certified. This is because later releases may contain new features, such as new ciphers, that will make system operation non-compliant with the FIPS requirements.

When FIPS mode is enabled, it enforces the following changes on the appliance:

- The web management console is secured with a TLS v1.2 connection. TLS v1.1 is available but not recommended.
- The remote-access command line interface is secured with SSHv2.
- The SNMPv3 agent is available for configuration. SNMPv1 and SNMPv2 are disabled.
- Only secure NTP is available.
- FIPS-relevant services must use a set of approved cryptographic algorithms. For more information about approved algorithms, see FIPS Cryptographic Algorithms for Management Center 2.1.1.2.
Additionally, management communication channels for Symantec products are restricted to the cryptographic parameters stated in FIPS Cryptographic Algorithms for Management Center 2.1.1.2.

- Only HTTPS, SCP, and Secure FTP are allowed for transferring device backups from managed devices to Management Center.
- RADIUS is not permitted as an authentication protocol.
- Managed device backups are not compatible or transferable between FIPS and non-FIPS mode for the following reasons:
  - Encryption differences between FIPS/non-FIPS mode
  - Non-FIPS backup cannot be restored to FIPS appliances without omitting certain backup portions

**NOTE**
See Back Up the Management Center Configuration in the Symantec Management Center Configuration & Management Guide for more information.

- SSL-context features are affected in the following ways:
  - HTTP connections to devices are not allowed.
  - The CA certificate list, keyring, and CCL associated with the SSL context need to be FIPS compliant.
  - Only FIPS-compliant objects—CA certificate lists, keyrings, and CCLs—are available as configuration choices. All non-FIPS-compliant objects are unavailable.
  - If an SSL context is not specified in FIPS mode, Management Center uses the default SSL context.
- Additional testing is performed when the appliance is powered on or reset. See "Section 2.8: Self-Tests" on page 31 of the FIPS 140-2 Non-Proprietary Security Policy for Management Center S400 Appliances (Management Center Security Policy Guide) for more information.

### FIPS Cryptographic Algorithms for Management Center 2.1.1.2

FIPS-relevant services include local and remote administration of Management Center:

- Web console (HTTPS over TLS).
- Remote login utility (SSHv2).
- SNMP (v3 only).
- Connections to managed Symantec products and connections to Symantec for services, such as licensing entitlements.
- FIPS-relevant services also include creation, storage, management, and deletion of Critical Security Parameters (CSPs) as defined in the Security Policy.

These services must abide by the algorithms specified in the following tables on pages 21–30 of the Management Center Security Policy Guide.

In FIPS mode, FIPS-relevant services must use only the cryptographic algorithms and functions listed in the tables below, available in the Management Center Security Policy Guide.

- **Table 10:** FIPS-Approved Algorithm Implementations for the MC Java Cryptographic Library v1.0
- **Table 11:** FIPS-Approved Algorithm Implementations for the MC OS Cryptographic Library v1.0
- **Table 12:** FIPS-Approved Algorithm Implementations for the MC SSH Library v1.0
- **Table 13:** FIPS-Approved Algorithm Implementations for UEFI OS Loader Library v4.14
- **Table 14:** FIPS-Allowed Algorithms
- **Table 15:** List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Approved algorithms can change over time. The tables listed above include the algorithms that were approved for the latest Management Center FIPS 140-2 validation for Management Center 2.1.1.2.
Cryptographic Restrictions for Products Managed by Management Center

Symantec products that are managed by Management Center have specific cryptographic protocol restrictions enforced by enabling FIPS mode. Additionally, enabling FIPS mode on the following devices imposes restrictions on the individual products (see the FIPS guides for each product for more information):

- Symantec ProxySG/Advanced Secure Gateway (ASG) (management communications occur over SSH):
  - Key Exchanges: DHGexSHA256, DHGexSHA1, DHG14, DHG1
  - Ciphers: AES256CTR, AES192CTR, AES128CTR
- Symantec devices on which management communications occur over HTTPS:
  - Cipher suites: AES256-SHA256, AES256-SHA, ECDHE-RSA-AES128-SHA256, AES128-SHA256, AES128-SHA

Enable FIPS Mode on Management Center

To determine how to enable FIPS mode on Management Center, refer to the Management Center Security Policy Guide for the model and operating system you are using.

NOTE
Currently, only 2.1.1.2 is FIPS certified.

To determine if a model or version is FIPS 140-2 validated, refer to the Cryptographic Module Validation Program (CMVP) validated module listing: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

To determine if a model or version is Common Criteria certified, refer to the Common Criteria Certified Products listing: https://www.commoncriteriaportal.org/products/

FIPS 140-2 Non-Proprietary Security Policy Documents

The following documents describe how Management Center meets the security requirements of FIPS 140-2, and how to run the appliance in FIPS mode:

FIPS 140-2 Non-Proprietary Security Policy for Management Center S400 Appliances
FIPS 140-2 Non-Proprietary Security Policy for Management Center 2.1 Virtual Appliances

Enable FIPS Mode

The CLI command fips-mode enables or disables FIPS mode.

When you enter FIPS mode, the appliance is restored to factory defaults and all previous configurations are destroyed. When you exit FIPS mode, all FIPS configurations are destroyed.

See fips-mode for the CLI command syntax.

What Happens When FIPS Mode is Disabled in Management Center 2.1.1.2

Entering or exiting FIPS mode destroys all user-defined configurations and data. When you enter FIPS mode, the appliance is restored to factory defaults, which destroys all previous data and configurations. When you exit FIPS mode, the appliance goes through same zeroization process, and destroys all data and configurations.

Backups are not compatible or transferable between FIPS and Non-FIPS mode for the following reasons:- Encryption differences between FIPS/Non-FIPS mode- Non-FIPS backup cannot be restored to FIPS appliances without omitting certain backup portions

See Back Up the Management Center Configuration for more information.
Management Center Solutions

What do you want to do in Management Center? See the following topics for assistance.

Update the Management Center License
Create and Distribute Policy
Apply a Single Policy to Both On-Premises and Cloud Users
Set HTTPS Server Certificate Hostname for Secure Device Communication
Use WAF Policy To Protect Servers From Attacks
Add and Monitor Devices
Create and Manage Jobs
Add Users and Grant Permissions
Monitor Device Health
Manage Dashboards
Integrate Reporter into
View Consolidated Reports
Modify Display of Table Data
Migrate Device Metadata from Director as Management Center Scripts
View Audit Log
Define Management Center Settings
Authenticate Users with SSL Mutual Authentication
Upload Files to Management Center
Regularly Back Up a Group of Devices
Back Up the Configuration
Configure Users, Roles, and Attributes

As the Management Center administrator, you can specify the following global settings after you set up Management Center for the first time or when needed.

Manage Users
Define Roles
Filter Devices or Device Groups in a Permission
Manage Attributes
Preview or Download Logs
Customize the Audit Log

Manage Management Center Users

The Users tab allows you to manage access Management Center. Before adding users, make sure you have defined roles.

See the following topics for details:

• Add Local Users
• View, Edit, or Delete User Accounts
• Reset a User's Web Console Password
• Expire a User's Web Console Password

Add Users and Grant Permissions

Management Center employs a role-based security model for access control, which consists of defining roles and then adding users to roles rather than granting explicit rights to features and functions.

You should create a role structure that ensures:

• Users have enough access—and no more—to perform their day-to-day jobs.
• Only authorized users can access sensitive features and data.
• The permissions that a defined role requires.
• Enforcement of your organization's access control policies.

To configure access control in Management Center, create a role structure that meets your technical and business requirements. As your organization changes, you may need to change role definitions and assignments to be certain that users continue to have appropriate access.
• Users (based on their role) should only manage specific devices, including reports on those devices.
• User roles control the actions that individuals within an organization should perform on devices for which they have access.
• Users roles should be organized into a hierarchical control model to conform to an organization's IT structure.

**Define Roles and Users**

To control access to Management Center, you should first create each role to allow access to specific areas and the operations that users can perform there; then, you can assign these roles in accordance with users' functions and responsibilities.

1. Define roles to provide access to different areas and functions in the Management Center.
   – To create a new role, see Define Roles.
   – To duplicate an existing role, see Duplicate an Existing Role.
   – (Optional) Edit an Existing Role.

2. Add Users after you have created a role structure and defined roles.
   (Optional) Add User Groups. If multiple users require the same type of access to Management Center, user groups make it easy to apply roles and permissions to a large number of users at one time. User groups contain users that control access to Management Center; you should first create each role to allow access to specific areas and the operations that users can perform there; then, you can assign roles in accordance with users' functions and responsibilities.

**Grant Permissions**

To grant permissions to Management Center that a role requires, you should understand how permissions work with roles. Grant permissions to users based on the actions you need them to perform on specific objects. See Reference: Permissions Interdependencies.

• Grant Permissions to users. See Reference: Permissions Filters Object and Attributes.
• (Optional) Grant job permissions to users. See Reference: Understanding Job Permissions

(Optional) Filter Devices in Permissions

(Optional) Filter devices or device groups in permissions. Some permissions allow access at the device and device group levels.
• To specify devices or device groups in specific permissions, see Filter Devices or Device Groups in a Permission.
• To specify object filters, see Reference: Permissions Filters Object and Attributes.

(Optional) Add Users from External Directory Services

To authenticate users using RADIUS, LDAP or Active Directory services, see Add Users from an Existing Directory Service. Available directory services to which you can authenticate users include:

• Authenticate Users Against Active Directory
• Authenticate Users Against LDAP
• Authenticate Users against RADIUS

Use Specific Attribute Values to Control Access to Policy

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Attributes are custom metadata used to refine and edit devices, device groups policy, and scripts. These attributes can be used to control access to policy, as described below.

Procedure

1. Create the Policy attribute.
2. Associate the attribute with a policy object.
   a. Select Configuration > Policy.
   b. Select the policy name and click Edit.
      The system displays the policy editor.
   c. Select the Attributes tab.
   d. Select the attribute and click Save.
3. Add the permission rule to a new or existing role.
   a. Select Administration > Roles.
   b. Select an existing role and click Edit or click Add Role.
   c. If this is a new role, provide a name and description, and click Next.
   d. **TIP**
      Symantec recommends that you enter a list of the permissions for the defined role in the Description field. This helps you and other users understand the permissions of a user's role including the intent of their job function.
   e. In the Add Role: Permissions dialog, click Add Permission.
   f. In the Object list, specify Policy.
   g. In the Action list, select All operations or a specific operation.
   h. In the Filter section, click the Add Filter icon
   i. In the Filter Type section, select Attribute has specific value.
   j. Select the attribute and assign a value to it.
   k. Click Save, then Finish.

Add Local Users

Use these setting to provide Management Center access to local users.

Security Considerations

The following items are supported:
Management Center logs all access attempts to the audit log and syslog.

- Users with the administrator role can manually expire a user’s password and force them to enter a new one.
- Management Center tracks the last access attempt in the user record and displays the record when viewing the user’s details (Administration > Users).
- Management Center tracks the number of login failures a user has had in a row.

The following items are not supported:

- Management Center does not enforce password strengths.
- Passwords do not expire automatically. You can manually expire them.
- Management Center does not automatically disable accounts if the user does not enter their password correctly after $n$ attempts.
- Management Center does not track password history.

If the unsupported features are important to you, use an external authentication service like LDAP, Active Directory LDAP, or RADIUS) instead.

**Add Roles First**

You can add local users to Management Center at any time, but it is good practice to set up the role structure before you start adding users. After roles have been added, you can assign users the specific roles that they require to perform their jobs. It is best practice to assign the most restrictive permissions possible so that users do not have more access than they need. To import users from Active Directory, LDAP or RADIUS, see Authenticate Users and User Groups using Existing Directory Service.

**NOTE**

When you select an existing user record, user details open in the right pane. In the title bar, under the user name, the local user account indicates a user that you manually added and the imported user account indicates a user that you imported using an existing directory service.

To understand more about how permissions and filters work with users and roles in Management Center, see Reference: Permissions Filters Object and Attributes and Reference: Permissions Interdependencies.

**Add Users**

**NOTE**

Management Center includes a default administrator account named admin. You cannot delete this account, but you can change the password from the web management console from Administration > Users > Management Center.

**TIP**

Before you start adding users, devise the naming convention for usernames. Once a username is saved, it cannot be changed. This does not apply to imported users—their usernames are set in LDAP, Active Directory, or RADIUS and are thus read-only.

1. Select Administration > Users.
2. Click **Add User**. The Add User: Basic Info dialog displays. **Note:** Management Center 2.0 introduces a default password policy. All new user accounts you define must have at least 6 characters by default, and common words are prohibited. See this topic for more information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username *</td>
<td>Usernames are case-sensitive and cannot be changed. <strong>Note:</strong> Although the username/password combination successfully authenticates if the username has a mixture of cases, Management Center recognizes the users as different users. For example: A user signs in as “joe” and access is setup using that specific case for username. Then later the user signs in as “Joe”. The login using “Joe” will have no access because the account created is for the user “joe”.</td>
</tr>
<tr>
<td>Password *</td>
<td>Example: admin1234</td>
</tr>
<tr>
<td>Verify Password *</td>
<td>Example: admin1234</td>
</tr>
<tr>
<td>Password expired on:</td>
<td>Does not expire</td>
</tr>
<tr>
<td>First Name</td>
<td>The actual first name that the person uses.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The actual last name that the person uses.</td>
</tr>
<tr>
<td>Email</td>
<td>The Email associated with this user and organization. Example <a href="mailto:joe@heremail.com">joe@heremail.com</a></td>
</tr>
<tr>
<td>Phone</td>
<td>The Phone number associated with this user and organization (including extension, if any)</td>
</tr>
<tr>
<td>Mobile</td>
<td>The personal mobile or cell number associate with this person.</td>
</tr>
<tr>
<td>Description</td>
<td>1024 character description can include anything from what town she resides to average commute time to security certifications in this user’s possession.</td>
</tr>
</tbody>
</table>

3. In the **Add User: Basic Info** screen, enter the user's information.

4. Click **Next**. From the Add User: Assign Roles dialog, select a role from **Available Roles** and add it **Assigned Roles**. The **default** roles are Administrator (with administrator rights) and viewOnly (with only viewing rights). You must assign a role or the user will be unable to login to Management Center. See **Define Roles** or **Edit an Existing Role**.

5. Click **Finish**. The new user displays in the Users list and has access to Management Center based on their defined role.

### View All Users and Associated Roles and Permissions

The **Summary Report** includes a section for user accounts, which includes a summary of all Management Center user accounts and their roles and permissions. To receive this report, select **User Accounts** when creating the Summary Report.

The **Management Center Users** section of the Summary Report includes two reports: **User Permissions Overview** and **User Permissions** (detail).

**NOTE**

See **Run a Summary Report** for more information about creating a Summary Report.
About the User Permissions Overview Report

The User Permissions Overview report lists the users, the number of assigned roles, and the associated number of permissions in each permission category. The permission categories are shown in the following table.

<table>
<thead>
<tr>
<th>Network(Device Mgmt.)</th>
<th>Configuration(Policy &amp; Config.)</th>
<th>Jobs</th>
<th>Reports</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Objects</td>
<td>All Objects</td>
<td>All Objects</td>
<td>All Objects</td>
<td>All Objects</td>
</tr>
<tr>
<td>Management Center</td>
<td>Management Center</td>
<td>Management Center</td>
<td>Management Center</td>
<td>Management Center</td>
</tr>
<tr>
<td>Device</td>
<td>Device Script</td>
<td>Backup Image</td>
<td>Statistics</td>
<td>Alert</td>
</tr>
<tr>
<td>Device Group</td>
<td>File</td>
<td>Scheduled Job</td>
<td></td>
<td>Attribution Definition</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
<td></td>
<td></td>
<td>Audit</td>
</tr>
<tr>
<td></td>
<td>Tenant</td>
<td></td>
<td></td>
<td>Hierarchy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Role</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device Script</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Session</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PKI (Data protection)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>User</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>User Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REST API</td>
</tr>
</tbody>
</table>

User Permission Overview Example

In this example, the user nance56 has 1 **Config** permission, 1 **Jobs** permission, and 2 **Admin** permissions:
This is because user nance56 has the following permissions:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Script - All Operations</td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>Administration</td>
</tr>
<tr>
<td>Attribute Definition - All Operations</td>
<td>Administration</td>
</tr>
<tr>
<td>Scheduled Job - Add</td>
<td>Jobs</td>
</tr>
</tbody>
</table>

About the User Permissions Report
The Summary Report also includes a detailed breakdown by user. This is called the User Permissions report.

Add Users from an Existing Directory or Service
As the Management Center administrator, you can add users from an existing directory or service.

- Authenticate Users Against LDAP
- Authenticate Users Against Active Directory LDAP
- Authenticate Users Against RADIUS
Authenticate Users Against LDAP

These options configure LDAP or LDAPS (LDAP over SSL) authentication in Management Center.

A secondary failover LDAP server can be configured in case the primary LDAP server cannot authenticate. If the secondary LDAP server cannot authenticate, authentication can only occur through Active Directory LDAP or RADIUS (if configured).

Prerequisites

Observe the following prerequisites:

- The LDAPS server must support TLSv1.1 or higher for Management Center to successfully establish the connection for authentication.
- If you are configuring LDAPS and the LDAP server SSL key uses a self-signed certificate or a certificate signed by a non-trusted root certificate authority, you must import that certificate into Management Center. To import the certificate, consider a name you'll use to define it and log in to the Management Center command line interface to enter the following sequence of commands:

# configure(config)# ssl(config-ssl)# inline ca-certificate <CA Certificate name>***

command will prompt for CA contents(config-ssl)#(config-ssl)# edit ccl browser-trusted(config-ccl-browser-trusted)# add <CA Certificate name>

Configure General Settings

1. Select Administration > Settings.
2. Click LDAP on the left. The web console displays fields on the right.
3. Specify general LDAP settings as described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must have permission</td>
<td>A user must have a role with permissions or be a member of a group with a role that has permissions in order to log in.</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true</td>
</tr>
<tr>
<td>Role attribute</td>
<td>Specify the roles to assign to imported users. Use the same name that exists in LDAP, ensuring that the spelling and case are identical.</td>
<td>businessCategory</td>
</tr>
<tr>
<td>Display name attribute</td>
<td>Specify the format of user names.</td>
<td>displayName</td>
</tr>
</tbody>
</table>

Configure Primary Server Settings

1. Select Administration > Settings.
2. Select LDAP. The web console displays fields on the right.
Enter the Primary Server Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable LDAP authentication.</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true</td>
</tr>
<tr>
<td>LDAP URL*</td>
<td>The URL used to connect to the LDAP directory server.</td>
<td>Specify the LDAP host, port, and root. Example: ldap://localhost:10389/dc=example,dc=com LDAPS example ldaps://ldapserver1:3269/dc=example,dc=com</td>
</tr>
<tr>
<td>Login user</td>
<td>If required, enter the username used for browsing.</td>
<td>Specify the username.</td>
</tr>
<tr>
<td>Login password</td>
<td>If required, enter the password used for browsing.</td>
<td>Specify the password.</td>
</tr>
</tbody>
</table>

Configure Secondary Server Settings

You can also configure a Secondary LDAP Server to take over in case the Primary Server fails. The settings under Secondary Server are specific to the Secondary LDAP Server only. The settings under Secondary RADIUS Server are specific to the secondary server only.

1. Select Administration > Settings.
2. Select LDAP. The web console displays fields on the right.
   – Enter the Secondary Server Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable LDAP authentication.</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true</td>
</tr>
<tr>
<td>LDAP URL*</td>
<td>The URL used to connect to the LDAP directory server.</td>
<td>Specify the LDAP host, port, and root. Example: ldap://localhost:10389/dc=example,dc=com</td>
</tr>
<tr>
<td>Login user</td>
<td>If required, enter the username used for browsing.</td>
<td>Specify the username.</td>
</tr>
<tr>
<td>Login password</td>
<td>If required, enter the password used for browsing.</td>
<td>Specify the password.</td>
</tr>
</tbody>
</table>

Configure Search Settings

1. Select Administration > Settings.
2. Select LDAP. The web console displays fields on the right.
Configure the LDAP Search Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore partial results on search</td>
<td>When set to <strong>true</strong>, ignores any partial results from LDAP searches. The default is <strong>false</strong>. When using this authenticator to connect to Active Directory, set this option to <strong>true</strong>.</td>
<td>false</td>
</tr>
<tr>
<td>Base DN for user search*</td>
<td>Specify where in the LDAP directory tree to initiate the username search.</td>
<td>Example: ou=users, o=organization</td>
</tr>
<tr>
<td>User search*</td>
<td>Specify the user search filter.</td>
<td>Example: (uid={0})</td>
</tr>
<tr>
<td>Base DN for group search*</td>
<td>Specify where in the LDAP directory tree to initiate the username search.</td>
<td>Example: ou=groups</td>
</tr>
<tr>
<td>Attribute to read group name*</td>
<td>Specify the group name attribute. Use the same name that exists in LDAP, ensuring that the spelling and case are identical.</td>
<td>Example: cn</td>
</tr>
<tr>
<td>Search sub-tree*</td>
<td>Specify whether to search sub-tree.</td>
<td>false</td>
</tr>
</tbody>
</table>

**Finalize Your Changes**

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

After setting your configuration options, click **Save** and then **Activate**. Then, instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.

**Supported LDAP Servers**

<table>
<thead>
<tr>
<th>Server Types</th>
<th>Configuration Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache DS</td>
<td>Apache Directory Studio™ user interface</td>
</tr>
<tr>
<td>Novell eDirectory</td>
<td>Novell ConsoleOne user interface</td>
</tr>
</tbody>
</table>

**Add LDAP Users**

After LDAP is configured, have users log in with their LDAP credentials. The first time the user logs in, Management Center adds them to the system. You cannot add external users at this time.

**Authenticate Users Against Active Directory LDAP**

Set up Active Directory LDAP authentication in Management Center. A secondary failover Active Directory LDAP server can be configured in case the primary Active Directory LDAP server cannot authenticate. If the secondary Active Directory LDAP server cannot authenticate, authentication can only occur through LDAP or RADIUS (if configured).

Prerequisites for enabling **Sync the role membership** and **Sync the group membership**:

- To sync role membership, you must define the role in Management Center before users assigned to the role in Active Directory authenticate.
- To sync group membership, you must define the group in both Management Center and Active Directory. The group names must match in order to map correctly.

After you define the roles and groups, and when a user authenticates in Management Center, the appropriate roles and/or group memberships are set up in Management Center.
Specify General Active Directory LDAP settings.

1. Select Administration > Settings.
2. Select Active Directory LDAP. The web console displays fields on the right.
3. Enter the General Active Directory LDAP Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync the role membership</td>
<td>Specify whether to assign users to roles that match the Role Attribute setting. No roles are synchronized if the Role Attribute is not set.</td>
<td>false</td>
</tr>
<tr>
<td>Sync the group membership</td>
<td>Specify whether to assign users to a user group that matches a group in Active Directory. The spelling and case must be identical to match.</td>
<td>false</td>
</tr>
<tr>
<td>User must have permission</td>
<td>A user must have a role with permissions or be a member of a group with a role that has permissions in order to log in.</td>
<td>false</td>
</tr>
<tr>
<td>Role attribute</td>
<td>Specify the roles to assign to imported users. Use the same name that exists in Active Directory, ensuring that the spelling and case are identical.</td>
<td>Specify the department to which the role is assigned.</td>
</tr>
<tr>
<td>Display name attribute</td>
<td>Specify the format of user names.</td>
<td>displayName</td>
</tr>
<tr>
<td>Base DN for user search*</td>
<td>Specify where to initiate the username search in the Active Directory tree.</td>
<td>Example: qa-auth-win2k8.organization.com</td>
</tr>
</tbody>
</table>

Specify Primary Server Settings

1. Select Administration > Settings.
2. Select Active Directory LDAP. The web console displays fields on the right.
   - Enter the Primary Server Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable AD authentication.</td>
<td>false</td>
</tr>
<tr>
<td>LDAP URL*</td>
<td>The host URL for LDAP authentication.</td>
<td>Example: ldap://localhost:389</td>
</tr>
<tr>
<td>Login Domain*</td>
<td>Specify where to initiate the username search in the Active Directory tree.</td>
<td>Example: qa-auth-win2k8.organization.com</td>
</tr>
</tbody>
</table>

Specify Secondary Server Settings

You can also configure a Secondary Active Directory Server to take over in case the Primary Server fails. The settings under Secondary Server are specific to the Secondary Server only. The settings under Secondary RADIUS Server are specific to the secondary server only.

1. Select Administration > Settings.
2. Select Active Directory LDAP. The web console displays fields on the right.
Enter the Secondary Server Settings described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable AD authentication.</td>
<td>false</td>
</tr>
<tr>
<td>LDAP URL*</td>
<td>The host URL for LDAP authentication.</td>
<td>Example: ldap://localhost:389</td>
</tr>
<tr>
<td>Login Domain*</td>
<td>Specify where to initiate the username search in the Active Directory tree.</td>
<td>Example: qa-auth-win2k8.organization.com</td>
</tr>
</tbody>
</table>

Finalize Your Changes

If you have unsaved changes, the edited settings are marked with a red triangle. See the “Pending changes” text at the top left of the dialog as an example.

After setting your configuration options, click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration. Then, instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.

### Authenticate Users Against RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. Authentication using a RADIUS server acts much like authenticating against LDAP and runs in the application layer.

Refer to [How to Set Up Cisco ACS for Management Center](#) for an example RADIUS implementation.

### Prerequisites

Prerequisites for enabling **Sync the role membership** and **Sync the group membership**:

- To sync role membership, you must define the role in Management Center before users assigned to the role authenticate.
- To sync group membership, you must define the group in both Management Center. The group names must match in order to map correctly.
- For role and group attributes to map appropriately to RADIUS attributes, you can either use the Blue Coat VSA custom dictionary file, or manually define attribute strings for attributes that are already configured in your RADIUS server.
  - **Blue Coat VSA** Install Symantec's latest dictionary of VSAs for Symantec on the RADIUS server. The latest version of the dictionary file is available with the Management Center image on the [Symantec Support site](#).
  - **Manual attribute definition** If the RADIUS server in your organization has defined attributes that you would prefer to use, you can choose to define them instead of installing the Blue Coat VSA. Define the attributes for role membership and group membership in Administration > Settings > RADIUS. If these fields are not populated with a custom attribute name, Management Center will assume that the Blue Coat VSA is in use.

With the group and role attributes defined, Management Center will apply the appropriate roles and/or group membership permissions as users authenticate in Management Center.

### Set up RADIUS authentication in Management Center.

1. Select **Administration > Settings**.
2. Select **RADIUS**. The web console displays fields on the right.
3. Configure general **RADIUS** settings.

<table>
<thead>
<tr>
<th><strong>RADIUS Settings</strong></th>
<th><strong>Description</strong></th>
<th><strong>Input Value/Format</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the authenticator enabled*</td>
<td>Enable RADIUS authentication.</td>
<td>false</td>
</tr>
<tr>
<td>Sync the role membership</td>
<td>Specify whether to assign users to roles that match the Blue-Coat-Role VSA or custom attribute.</td>
<td>false</td>
</tr>
<tr>
<td>Role Membership Attribute</td>
<td>Define a custom attribute from your RADIUS configuration to use for role membership. <strong>Note</strong>: if left blank, Management Center assumes the Blue Coat VSA Dictionary is in use.</td>
<td>string</td>
</tr>
<tr>
<td>Sync the group membership</td>
<td>Specify whether to assign users to roles that match the Blue-Coat-Group VSA or custom attribute.</td>
<td>false</td>
</tr>
<tr>
<td>Group Membership Attribute</td>
<td>Define a custom attribute from your RADIUS configuration to use for group membership. <strong>Note</strong>: if left blank, Management Center assumes the Blue Coat VSA Dictionary is in use.</td>
<td>string</td>
</tr>
<tr>
<td>User must have permission</td>
<td>A user must have a role with permissions or be a member of a group with a role that has permissions in order to log in.</td>
<td>false</td>
</tr>
</tbody>
</table>

**Configure Secondary RADIUS Server**

You can also configure a **Secondary RADIUS Server** to take over in case the Primary RADIUS Server fails. The settings under **Secondary RADIUS Server** are specific to the secondary server only.

<table>
<thead>
<tr>
<th><strong>Secondary RADIUS Server Settings</strong></th>
<th><strong>Description</strong></th>
<th><strong>Input Value/Format</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS IP Address*</td>
<td>The IP Address of the RADIUS server.</td>
<td>default: localhost</td>
</tr>
<tr>
<td>Authentication Port*</td>
<td>Port number</td>
<td></td>
</tr>
<tr>
<td>Accounting Port*</td>
<td>Port number <strong>Note</strong>: Even though the Accounting Port is a required setting, Management Center does not supply accounting (or other) data to RADIUS.</td>
<td></td>
</tr>
</tbody>
</table>
**Management Center - 3.0**

**Secondary RADIUS Server Settings**

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Input Value/Format</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connect Timeout (seconds)</strong>*</td>
<td>Connect retries is the number of times we attempt to connect to the given server before deciding to fail over to the next authentication server. For example, if RADIUS server 1 is set to a Connect Timeout of 10 seconds and 2 Connect Retries, we will try once to connect for 10 seconds and, when/if that attempt fails, we will try one more time (for 10 seconds) to connect. If both attempts fail, we will move on to the next authentication server (e.g., RADIUS 2, LDAP 1, LDAP 2...). But they are not locked out from any of those servers. Upon their next login, we will go through the exact same sequence of authentication servers until one succeeds.</td>
</tr>
<tr>
<td><strong>Connect Retries:</strong>*</td>
<td>The number of attempts the RADIUS server allows before locking you out.</td>
</tr>
<tr>
<td><strong>Shared Secret:</strong>*</td>
<td>Specific RADIUS key or password Example: RADIUS PASSWORD</td>
</tr>
</tbody>
</table>

**Supported RADIUS Servers**

<table>
<thead>
<tr>
<th><strong>Server Types</strong></th>
<th><strong>Configuration Interface</strong></th>
<th><strong>Example User Credentials and Attributes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Steelbelted</td>
<td>Windows XP VM</td>
<td>user1/1resu mcuser1/1resu (FirstName=MC1, LastName=User1) mcuser2/2resu (Role=Role_administrator) mcuser3/3resu (Group=MCAdministrator) mcuser4/4resu (No vendor-specific attributes defined) <strong>Important:</strong> The group and role attribute values should match the Blue-Coat-Group and Blue-Coat-Role VSAs, respectively.</td>
</tr>
<tr>
<td>Note: You must create a RADIUS client for every device that accesses the RADIUS server.</td>
<td>Note: Restart Windows services after making any modifications.</td>
<td></td>
</tr>
<tr>
<td>Safeword</td>
<td>Windows XP VM</td>
<td>user1/password shown on token user2/2resu (fixed password)</td>
</tr>
<tr>
<td>RSA</td>
<td>Web - Use Internet Explorer 11 Linux VM</td>
<td>Configure users with a hardware or software token.</td>
</tr>
</tbody>
</table>

**Finalize Your Changes**

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

After setting your configuration options, click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration. Then, instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.
**Authenticate Users with SSL Mutual Authentication**

In mutual SSL authentication, an SSL connection between a client and a server is established only if the client and server validate each other’s identity during the SSL handshake. The server and the client must each have their own valid X.509 certificate and the associated private key in order to perform SSL mutual authentication.

Certificates and private keys can be stored in multiple locations. On the client, one such location is a Common Access Card (CAC). However, a CAC card or reader is not required for SSL mutual authentication, you can install the certificates on your browser and into Management Center's truststore.

The following example describes an SSL mutual authentication transaction.

1. The user requests access to the Management Console.
2. Management Center presents its certificate to the browser.
3. The browser validates Management Center's certificate. This validation includes the following checks:
   - The certificate subject must match the hostname of the appliance.
   - The certificate must be issued by a CA listed in the browser’s Trusted Root Certificate store.
4. The browser confirms that the appliance has the certificate's private key by challenging the appliance to sign random data. The browser validates the signature using the appliance's certificate.
5. If appliance authentication succeeds, the browser accesses the client certificate and private key using the installed certificate or CAC. The browser then presents the certificate to the appliance.
6. The appliance validates the certificate that the browser presents. This validation includes the following checks:
   - The certificate must be issued by a CA included in Management Center's truststore.
   - The appliance confirms that the browser has the certificate's private key by challenging the browser to sign random data. The appliance validates the signature using the browser’s certificate.
   - The certificate must have a valid signature and not be expired.
7. If authentication succeeds, the appliance grants access to Management Center.
8. (If applicable) The appliance presents a Notice and Consent banner. The user provides consent.

**Prerequisites**

You must meet the following prerequisites before using SSL mutual authentication:
• The browser must have an X.509 certificate installed that will pass Management Center's trust validation. That is, if the client is using its own Root Certificate Authority (CA) or a different CA, that CA must first be installed into Management Center's truststore.
• The appliance certificate must be from a CA listed in the browser’s Trusted Root Certificate store. Install any missing client certificates or custom root CA certificate into the browser. For browser installing instructions, refer to http://wiki.cacert.org/FAQ/BrowserClients and select your browser of choice.

**Set up SSL Mutual Authentication**

1. Import one or more root CA certificates and any intermediate certificates that are required to validate the client certificates into Management Center’s truststore.
   
   \# configure(config)# ssl(config-ssl)# inline ca-certificate <CA Certificate name>***
   command will prompt for CA contents
   
   \#(config-ssl)#(config-ssl)# edit ccl client-authentication(config-ccl-client-authentication)# add <CA Certificate name>
   
   If the device is in FIPS mode, run the following commands instead:
   
   \# configure(config)# ssl(config-ssl)# inline fips ca-certificate <CA Certificate name>*** command will prompt for CA contents
   
   \#(config-ssl)#(config-ssl)# edit ccl client-authentication(config-ccl-client-authentication)# add <CA Certificate name>

2. Verify that the certificate was installed in the CA Certificate List (CCL) with the appropriate command:
   
   \# configure(config)# ssl view ccl client-authentication
   
   See # ssl for more information on the certificate viewing commands.

3. Determine the client authentication method, mandatory or optional; client authentication is off by default.

4. Issue one of the following commands:
   
   \# configure(config)# security client-authentication set-mandatory
   \# configure(config)# security client-authentication set-optional
   
   See # security for more information on the client-authentication commands.

5. Import the client-authentication certificate with its CA chain into the browser. This chain is the same CA chain that you installed in Step 1.

The flowchart below depicts the prerequisites, setup, and authentication process for mandatory and optional SSL mutual authentication.
• When SSL mutual authentication is enabled, all devices using Management Center as the host require X.509 certificates. For example, to access file services and APIs in a mandatory setting, a certificate is required.
• Browsers retain the certificate that is used. If you have installed more than one X.509 certificate and you want to use a different certificate, you must close and reopen your browser to change certificates.
Allow Users to Bypass Password if Certificate is Valid

Updated for Management Center 2.0.1.1, you can use the following CLI commands to configure Management Center to trust X.509 certificates so users do not have to enter their passwords after successful authentication:

```
(config)# security client-authentication password-requirement disable
(config)# security client-authentication set-regex
```

When the password requirement is disabled, a user does not have to enter a password to access Management Center if the system determines the certificate is valid, and finds the user in the local user database or LDAP system, if configured. The user is then automatically logged in with the permissions defined for that user in Management Center.

To validate certificates, you must create a regular expression to evaluate the information in the certificate's `subjectAltName` field. The `subjectAltName` data is compared to a regex set by the `security ssl client-authentication set-regex` command, which is used to extract the portion of the value to use as the user's identity. That value is then used to find the user in the local or LDAP authentication service. Refer to Use LDAP Subject Alternative Name Data for Certificate Validation and # ssl for more information.

**NOTE**
This method only supports the local or LDAP authentication schemes. You can use active directory but only if you set it up using the LDAP settings (Administration > Settings > LDAP). This is because a service account is needed to look up users because the system no longer has the user password.

HTTP Strict Transport Security (HSTS)

HSTS protocol support is included to allow web browsers interact with servers using HTTPS connections. To enable HSTS:

1. Have a DNS name (domain) for your Management Center appliance.
2. Purchase an HTTPS certificate from a trusted CA (using the DNS above) and have it installed.
3. Be able to access Management Center using HTTPS without any warnings or errors. In Chrome, you must have a green lock icon, showing the certificate is valid.
4. To enable the HSTS, use the CLI Command `# security ssl hsts enable`, or to disable, use `# security ssl hsts disable`

**NOTE**
With the HSTS activated, any attempted access using HTTP port 8080 gets an error instead of being rerouted to HTTPS port 8082. If you deactivate it, the domain must be removed from the HSTS in each browser. See How to Clear HSTS Settings in Major Browsers for more information.

**WARNING**
If you change the SSL certificate, statistics monitoring fails unless you install the certificate on your monitored appliances. See Statistics Monitoring Over HTTPS for more information.

Use Certificate Revocation List with SSL Mutual Authentication

Refer to Use Certificate Revocation Lists (CRL) with SSL Mutual Authentication.

Use Certificate Revocation Lists (CRL) with SSL Mutual Authentication

This feature is used in conjunction with Authenticate Users with SSL Mutual Authentication. You must configure SSL Mutual Authentication for Management Center users before performing this procedure. Also, you must ensure that client authentication is set to mandatory:

```
(config)# security client-authentication set mandatory
```

Add a CRL to Management Center.
1. Copy your CRL.

2. Enter the following command to import the CRL into Management Center:

   (config-ssl)# inline crl crl_name
   Press Ctrl-D when finished.

   Alternatively, you can specify a URL that contains your CRL data. When you enter a URL, the system periodically checks the URL to update the contents of the CRL. The refresh interval is set using the refresh-interval command.

   (config-ssl)# create crl crl_name
   (config-ssl)# edit crl crl_name
   (config-ssl-crl_name)# path http_or_https_url_of_crl
   (config-ssl-crl_name)# refresh-interval 2.5h

   Use the CRL for SSL Mutual Authentication.

3. Enter the following command:

   (config)# security client-authentication crls crl_name

   Users with certificates on the specified Certificate Revocation List are denied access to Management Center.

**Authenticate Users and User Groups using Existing Directory Service**

You can use your existing directory service to authenticate users that you have previously added to Management Center. Management Center supports integration with Active Directory and LDAP. Authenticating users against LDAP and Active Directory LDAP simplifies user and user group management because both of those directory services have the concept of group and role membership and can display existing usernames in the Audit Log and metadata.

Management Center supports authenticating users from LDAP, Active Directory LDAP and RADIUS directory services.

- Authenticate Users Against LDAP
- Authenticate Users Against Active Directory
- Authenticate Users against RADIUS

**Use Certificate Subject Alternative Name Data for Certificate Validation**

Management Center can search the certificate Subject Alternative Name (SAN) data so that it can be matched against a regular expression to validate the certificate and user. SAN is a X.509 extension that allows data to be associated with a security certificate using a subjectAltName field. SAN data can include:

- Email addresses
- IP addresses
- URLs
- DNS names
- Directory names
- Object identifier (OID) followed by a value

Management Center scans the subjectAltName field for OID data. The format of the subjectAltName field data is as follows:

   {oid}, [[ASN.1 value type code]]{value}

For example:
The subjectAltName data is compared to a regex set by the security client-authentication set-regex command, which is used to extract the portion of the value to use as the user's identity. That value is then used to find the user in the local or LDAP authentication service.

This enables Management Center to validate the certificate and allow users to bypass the password requirement, if the system determines the certificate is valid and finds the user in the local user database or LDAP system. Refer to Authenticate Users with SSL Mutual Authentication for more information.

For example:

```
# security client-authentication set-regex "'1\\.3\\.6\\.1\\.4\\.1\\.311\\.20\\.2\\.3,\\s[0]\\(.*?)@'"
```

**NOTE**
Refer to # security for more information about the client-authentication set-regex command.

### Use Public Key Authentication for CLI Access

1. In Management Center, create a user or select an existing user. See Add Users and Grant Permissions.
2. Ensure that the user has the administrator role, or a role that includes the Management Center CLI permission. See Define Roles for more information.
3. Using a client, generate the SSH public and private key that will be used to access Management Center. Linux example:

```
# ssh-keygen -t rsa
```
4. In Management Center, enable public key authentication:

```
(config)# ssh-console public-key-authentication enable
```
5. Enter the following command to add the public key you created in step 3 to Management Center:

```
(config-ssh-console)# inline client-key username client_key_name
```

In the preceding command, `username` is the user who is allowed to authenticate to Management Center using the specified client key—`client_key_name`.

Paste the key in. Press Ctrl-D when finished.

**NOTE**
View existing client keys: `(config-ssh-console)#view client-keys`
6. Users should now be able to use SSH to log into the CLI using their private key path. For example:

```
ssh alice@10.131.38.40 -o IdentityFile=/home/alice/ssh_key/key
```

In the preceding example, the username, in this case `alice`, must be the same username that you entered when you inlined the client key in step 5.

**View, Edit, or Delete User Accounts**

This topic describes how to manage users using options in the Administration User page:

- View User Information
- View User Permissions
- Edit User
- Delete a User

**View User Information**

To view user information, expand the Overview section.

**View User Permissions**

The Permissions section lists the user's permissions. Click Expand All to view the permissions and roles associated with the selected user.

- To view duplicate assignments, click Expand All and select **Highlight all duplicated permissions and roles**.
- To modify the assigned roles, click the Actions icon.
  ![Actions Icon]
- To view group inheritance information, click the hyperlink associated with the group. (Direct assignment has no group link.)
**Edit User**

To modify the user details (first name, last name, email address, phone numbers, description) or change the user's role (both local and imported), use the Edit User wizard.

1. Select **Administration > Users**.
2. In the list of users on the left, select the username to edit.
3. Click **Edit**. The web console displays the Edit User wizard.
4. Change desired information on the **Basic Info** tab. Note that you cannot change the username.
5. Click the **Assign Roles** tab to modify the user's role.
6. Click **Save**.

**Delete a User**

Organizations typically implement processes to deactivate and remove access to internal accounts—such as mailboxes, intranet, and applications—when users leave the organization. As a best practice, include deleting the user account in Management Center to the exit procedures that your organization uses to reduce the risk of a security breach.

**WARNING**

Deleting an imported user does not remove that user from Active Directory, LDAP or RADIUS.

1. Select **Administration > Users**.
2. In the list of users on the left, select the user you want to delete.
3. Click **Delete**. A Delete User dialog displays, prompting you to confirm the deletion.
4. Verify that it is the correct user, and then click **Delete User**. The user no longer displays in the Users list and is not a registered user of Management Center.

**Update Your User Profile**

You can update your profile or your password in Management Center if you have already been added as an authorized user of Management Center. If you are attempting to access a restricted network, you may have to accept the requirements in a consent banner before you login to the web console. See **Configure Consent Banner** and **Log into the Web Console**.

**Update your Profile**

Web console logins are associated with profiles (a set of personal data including name and e-mail address). Names and email addresses are required to successfully reset passwords and configure a security question.

**NOTE**

Your profile is visible to other users in Management Center who have at least a View permission for the **Users** object. For information on permissions, see **Grant Permissions** and **Reference: Permissions Interdependencies**.

1. In the web console banner, click **Show screen.** and select your username.

2. Enter or change profile information. See **Change Your Password** for specifics on changing your own user password.

3. Click **Save**. Your profile information has been updated.

**Change Security Question**

1. In the web console banner, click **Show screen.** and select your username.

2. Click the **Change Security Question**.

3. From the **Question** drop-down list, choose your security question.

4. In the **Your Answer** text field, enter your answer.

   **TIP**
   Remember that when you reset your password, you will be prompted to answer your security questions. You must enter the answer exactly as you typed it here. For example, if you choose the **Security Question: What was the name of your first boss?** If you enter **Ted**, you must enter the word **Ted** with initial caps when you are prompted for your answer at login. If you answer **ted**, you will fail the Security Question prompt.

1. Click **Save**.
Change and Reset Passwords

Select the topic for the applicable situation.

<table>
<thead>
<tr>
<th>Situation</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>User knows his/her password and wants to change it</td>
<td>Change Your Password</td>
</tr>
<tr>
<td>User forgot his/her password</td>
<td>Reset Password</td>
</tr>
<tr>
<td>Admin wants to automate the password resetting process</td>
<td>Automate Password Reset Process</td>
</tr>
<tr>
<td>Admin needs to manually change a user's password because user forgot an</td>
<td>Manually Reset a User's Web Console Password</td>
</tr>
<tr>
<td>security question or password reset process isn't automated</td>
<td></td>
</tr>
<tr>
<td>Admin wants to expire a user's web console password</td>
<td>Expire a User's Web Console Password</td>
</tr>
<tr>
<td>Admin forgot admin account password</td>
<td>Reset or Restore Admin Account Passwords</td>
</tr>
<tr>
<td>Admin wants to change a device password</td>
<td>Reset or Restore Admin Account Passwords</td>
</tr>
</tbody>
</table>

**Change Your Password**

You can change the password that you use to log into the web console.

**NOTE**
If you log in to the web console using your LDAP or Active Directory credentials, you cannot change your password.

1. In the web console banner, click

   and select your username.

   **Show screen.**

   ![Show screen](image)

   **NOTE**
   The username for the default admin login is "Management Center."

   The web console displays the **Profile** dialog. Fields marked with an asterisk (*) are required settings.

2. Click **Change Password**.
3. In the **Current Password** field, enter your current password.
4. In the first **New Password** field, enter a new password. As you type your password, the Password Strength meter indicates the strength of the password. Because the system assesses the strength of the password with each character, the meter might fluctuate while you are typing.

   **TIP**
   Symantec recommends that you use a password with at least Secure strength. You can try a number of different passwords until the Password Strength meter indicates Secure or higher.

5. In the **Retype New Password** field, enter your new password again.
6. Click **Save**. The next time you log into the web console, use your new password.

**Reset Password**

If you have forgotten your password to log in to the Management Center web console, you can request a password reset. The password reset process has the following restrictions:
- It is only good for the web console; it cannot be used for the CLI console.
- It only works for local users; it cannot be used by LDAP or RADIUS users.

**Prerequisites**

This capability requires that the administrator has enabled the Management Center password reset feature and that users have created a security password. For more information, see [Automate Password Reset Process](#).

**How to Reset Password**

**TIP**

The password resetting process requires that you answer a security question, using the exact upper/lowercase you entered when you initially defined it in your user profile. You also must have the correct email address in your profile. If you forget the answer to your security question, or failed to define an email address, you will not be able to use the automated password reset process.

1. If you have forgotten your password when logging in, click **Reset Password**.

2. Enter your **Username** and click **Next**.

   ![Password Reset Form](#)

   You then receive a notification that your password reset request was received.

3. Check your email to find the password reset message.

4. Click the password reset link included in the email. The system displays the **Reset Password** dialog.
5. Enter the answer to the Security Question, using the exact spelling and upper/lowercase you entered when defining it.
6. Enter a new password, then retype the new password.
7. Click **Change Password**.

**Manually Reset a User's Web Console Password**

If users forget their web console password, you can manually reset the password for them. (Alternatively, if you have automated the process, the user can request a password reset when logging in. See Automate Password Reset Process.) Even if you have automated the process, you may still need to manually change someone's password if the user has forgotten the answer to his/her security question.

1. Select **Administration > Users**.
2. In the list of users on the left, select the username whose password you want to change.
3. Click **Edit**. The web console displays the Edit User wizard.
   - **NOTE**
     You cannot change the password for users authenticated against LDAP, Active Directory, or RADIUS (authenticated users have the following icon:).
4. From the **Basic Info** tab, click the **Change password** link. The system displays two new fields: **New Password** and **Verify New Password**.
5. Enter a new password. If you do not enter identical text in both fields, you receive an error message.
6. Click **Save**. The dialog closes and the web console banner displays an alert indicating that the user's password was saved.
7. Communicate the new password to the user and recommend a password change as soon as possible.
Expire a User’s Web Console Password

For security reasons, you should regularly prompt users to change their passwords. You can expire a user’s password, as described below. You must have administrative privileges to expire passwords.

1. Select **Administration > Users**.
2. In the list of users on the left, select the username whose password you want to change.
3. Click **Edit**. The web console displays the Edit User dialog.

   **NOTE**
   You cannot expire the password for users authenticated against LDAP, Active Directory, or RADIUS (authenticated users have the following icon: ![Icon](https://example.com/icon.png)).

4. From the **Basic Info** tab, click **Expire password**. The system displays the expiration time and date.

   ![Edit User: John Smith](https://example.com/edit_user.png)

   Username: Test2
   Password: Change password  Expire password
   Password expired on: 11/29/16 3:56 PM UTC

After the password is expired, the user is prompted to change their password the next time they log in. If the user does not log in within the next 24 hours, they are locked out of their account and instructed to contact their administrator. You can then change the password for the user and allow them to log in again.

Reset or Restore Admin Account Passwords

**Management Center 2.1.x**

In Management Center 2.1.x or later, the UI and CLI password for the "admin" account are shared. You can change the admin password using the following methods:

- Using the **authentication-password** command.
- Using the user interface options:
  - In the web console banner, click ![Icon](https://example.com/icon.png) and select your username.

- With the reset admin account password using the Initial Configuration Wizard via the serial console.
Manage User Groups

To reduce the time and effort involved in assigning roles to users, you can create a user group, add users to it, and then assign roles to the group. Creating user groups also helps ensure consistency among users who require the same access. Before adding user groups, make sure you have defined roles.

Use the Groups tab to add, edit, and delete user groups. See the following topics for details:

- Add User Groups
- Edit a User Group
- Configure Hierarchy for Devices and Device Groups

Add User Groups

Although you can add users and assign roles to them individually, doing so can be labor-intensive if there are many users in the system who require the same permissions. To reduce the time and effort involved in assigning roles to users, you can create a group, add users to it, and then assign roles to the group. Creating user groups also helps ensure consistency among users who require the same access.

Users inherit the roles and permissions assigned to them individually and to the groups in which they are members. If users inherit permissions that seem to conflict, keep in mind that they can access an object as long as they have a role with the required permission. For example, if one of a user's groups has a role with the View permission for policy objects but another group has no policy permissions, the user can view policy objects.

NOTE

Groups cannot be members of other groups.

1. Select Administration > Groups.
2. From the Groups section, click Add Group. The web console displays the Add Group wizard.
3. In the Add Group: Basic Info page, enter the group's information. Enter a Name for your group. This group name displays on the dashboard and other areas in the web console.
   TIP
   Before you start naming user groups, devise a naming convention. For example, a user group name can be based on an organization, job function or geographical location.
4. In the Add Groups: Basic Info page, add a description (even though it is not required).
   TIP
   Although entering a description is optional, the description helps you and other users understand the purpose or function of the group. This helps to understand the correct roles and permissions to apply within the group. Symantec recommends that you always enter a clear, helpful description.
5. Click Next.
6. In the Add Group: Members dialog, select users from the Available Users and add them to the Members list using the arrow buttons. Click Next.
7. In the Add Group: Assign Roles dialog, select a group role from the Available Roles it to the Assigned Roles list. See Define Roles.
8. Click Finish. The system displays the the group that you just created in the left pane.

Edit a User Group

To modify the user group details (name or description), add or remove group members, or change the role(s) assigned to the group, you can use the Edit Group wizard.

1. Select Administration > Groups.
2. In the list of groups on the left, select the group to edit.
3. Click **Edit** or click the edit icon in the **Action** column. The web console displays the Edit Group wizard.

4. Change desired information on the **Basic Info** tab.

5. To add a user to the group:
   a. Click the **Members** tab.
   b. Select the username in the **Available Users** list.
   c. Click the right arrow button to add the user to the **Members** list.
   d. Repeat for other users you want to add to the group.

6. To remove a user from the group:
   a. Click the **Members** tab.
   b. Select the username in the **Members** list on the right.
   c. Click the left arrow button to remove the user. The user moves over to the **Available Users** list.
   d. Repeat for other users you want to remove.

7. Click the **Assign Roles** tab to modify the role(s) associated with the group.

8. Click **Save**.

**View Group Permissions and Roles**

To view the permissions and roles associated with a group click the + icon. Expand or collapse the roles and associated permissions using the expand buttons.

Modify a role by selecting the role and clicking the edit role icon

in the **Action** column.

**View Group Members**

To view the members in a group, you can edit the group or hover over the profile icon in the **Actions** column.

If a group has more than 4 members, click the profile to view the complete list.

**Delete a User Group**

Deleting a group does not remove the members in the group.

1. Select **Administration > Groups**.
2. In the list of groups on the left, select the group you want to delete.
3. Click **Delete**. A Delete Group dialog displays, prompting you to confirm the deletion.
4. Verify that it is the correct group, and then click **Delete Group**. The group no longer displays in the Groups list.

You can also select multiple groups and click **Delete**.

**NOTE**

Deleting a group does not delete any associated members or permissions. They are only disassociated from that group.

**Manage User Sessions**

Management Center tracks and logs each user session. Administrators can view and manage current user sessions from **Administration > User Sessions**. As a super admin, the ability to log in will not be affected by what you do in this dialog. You can delete (kill) any user session which will immediately log the user out of the Management Center web console.
As a best practice, Symantec recommends that all users log out of the web console after completing their tasks. As a Management Center administrator, you may need to enforce this practice. If a user has changed roles or has accepted a new job that may change their access rights, you can manage all active or stored user sessions.

1. From the web console banner, select **Administration > User Sessions**.
2. To prevent users from logging in to the web console, select the **Disable user login to Management Center** check box.
3. (Optional) To delete a user session:
   a. Select a user session. Green denotes your session (you), not an active session.
   b. Click **Kill Session**.
   c. Confirm that you want to kill the session.

### View Audit Log

You can view the history of all transactions in Management Center in the Audit Log (**Administration > Auditing**). The log is a chronological record of changes made by users of the system.

Audit Log records are:

- **Comprehensive.** Records are created automatically and cannot be deleted.
- **Centralized.** Multiple levels of transactions are logged and displayed on one screen.
- **Security-oriented.** The operating user for each transaction is logged.

Audit Log records can give you insight into daily activities at a high level as well as help you diagnose and troubleshoot issues. For example, if a number of devices experience policy-related issues, you could check the log for policy-related transactions within a selected date range. You can also examine records in the Audit Log to ensure process integrity.

**NOTE**

The audit log displays system, web-access and web logs, if configured. To access remote system logs, from the CLI enter `# rsyslog-output`.

Audit Log records can be printed in a user-friendly format. Before printing, check the bottom of the page of the Audit Log Viewer to see how many pages of records will print.

1. Learn about the types of transactions recorded in the Audit Log. See **Understanding Transaction Types** below.
2. Inspect the data recorded for transactions. See **Audit Transactions**.
3. (Optional) **Customize the Audit Log** to focus on specific transaction data.

**NOTE**

You can export the information in the audit log. From the **Network > Export Data**. You will be prompted to name the .csv file that you are exporting. Click **OK**.

### Understanding Transaction Types

The Audit Log records two levels of transactions:

- **EVENT:** High-level transactions that occur as a result of a user action, such as adding or deleting a device
- **AUDIT:** Low-level internal system actions, such as deleting connection information

Each record contains the target of the operation, the operation detected, the user who executed the operation, and additional data depending on transaction type.
In the previous example, the Object Type is Role and the AUDIT transactions are changes at the system and admin levels. Filters were applied to the record type. You might find that in most cases, EVENT records provide enough detail about transactions and their effects on the system.

### CLI Shell Audit Log Notes

When users log into the CLI shell of a device or of Management Center, the following is logged:

- Session open, close, and failure
- User, host, port, browser IP address, and close reason (if applicable)
- **Info 3**, in the Audit Log, is an internal identifier used to correlate open/closed events. The identifier is unique until Management Center reboots.

### Audit Transactions

To access the Audit Log Viewer, click Administration > Auditing.

By default, recent transactions are displayed on the first page of records. If they are not on the first page, or if you are looking for historical data, you can navigate to different pages or limit the number of records to locate the correct ones. For instructions, see Customize the Audit Log.

**NOTE**

Records do not display in the Audit Log Viewer immediately after transactions occur; refresh the web console to see most recent records. You can click the Refresh icon at the bottom of the screen to update the most recent entries.
To understand and analyze the data recorded for each transaction, refer to the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Time</td>
<td>The date (in YYYY-MM-DD format) and time (in 24-hour notation) the transaction was completed.</td>
</tr>
<tr>
<td>Operating User</td>
<td>The user who performed the operation. If no user is associated with the operation, SYSTEM is displayed.</td>
</tr>
<tr>
<td>Record Type</td>
<td>The transaction level: AUDIT or EVENT. An audit record is a system-level transaction; an event record is a user-level transaction. For more information, see Understand Transaction Types. This column is hidden by default.</td>
</tr>
<tr>
<td>Object Type</td>
<td>The type of object on which the operating user performed the action.</td>
</tr>
<tr>
<td>Operation Type</td>
<td>The operation that was completed.</td>
</tr>
<tr>
<td>Info 1 - Info 5</td>
<td>Additional reference fields for the record. Not all transaction types have additional information. Columns Info 3 through Info 5 are hidden by default.</td>
</tr>
</tbody>
</table>

**Understand Transaction Types**

The Audit Log records two levels of transactions:

- **Event**—High-level transactions that occur as a result of a user action, such as adding or deleting a device
- **Audit**—Low-level internal system actions, such as deleting connection information

Each record contains the target of the operation, the operation detected, the user who executed the operation, and additional data depending upon transaction type.
In the previous example, the Object Type is Role and the AUDIT transactions are changes at the system and admin levels. You might find that in most cases, EVENT records provide enough detail about transactions and their effects on the system. Filters were applied to the record type.

Customize the Audit Log

Because the Audit Log records all transactions on multiple levels, the log can grow very quickly—especially if you many devices are managed in Management Center and there is a high level of user activity. Although the Audit Log is designed to make it easy for you to locate the records you want, you can customize the display further to help you locate specific records, isolate records from a certain date or time, filter records pertaining to specific users or objects, and more.

Use the following methods in conjunction to customize the Audit Log display to suit your purposes.

**NOTE**

When you make the following changes in the Audit Log Viewer, the changes do not persist beyond the current browser session; the next time you log in to the web console, you must go through the same steps to change the viewer again.

Show or hide columns

You can show columns that you hid, or columns that are not visible by default, such as Record Type and Info 3 through Info 5. You can hide some columns if you want a more general look at the log or if your screen size is limited.

To see all information available in the Audit Log and ensure that you can see an appropriate level of detail, you can show all columns first and then choose which ones, if any, you want to hide.

1. On any column header, click the arrow. The web console displays a list of options.
2. Select an option to show the column. Clear an option to hide the column.
3. Click anywhere outside of the list to close it. The Audit Log shows/hides the columns you specified.
Sort columns
Because the Audit Log displays records in descending chronological order by default, you can re-arrange them to analyze the data more effectively. By default, the records are sorted in descending order of Operation Time (latest to earliest).

1. Click the header of the column you want to sort.
   – If the header displays an up arrow, the data is arranged in ascending order (A-Z, earliest to latest).
   – If the header displays a down arrow, the data is arranged in descending order (Z-A, latest to earliest).
2. Click the header again to reverse the sort order.

In the following example the columns are sorted by Operation Type, so all Authentications are displayed first.

Filter records
To limit the amount the data that the log displays and focus only on specific records, apply filters using the drop-down lists on the right. Depending on the transaction level, you may need to filter pages of records. The filters limit the record type. To narrow the search, apply one or more filters.

If applying a filter results in too few records or not the right records, remove or change some filters. To reset the filters to default, click Clear.

Configure Housekeeping Settings
Configure general housekeeping settings. When these settings are activated, they affect what is displayed in the Audit Log Viewer and how big audit logs can grow.

If you have unsaved changes, the edited settings are marked with a red triangle. See the “Pending changes” text at the top left of the dialog as an example.

1. Select Administration > Settings.
2. Click Housekeeping on the left.
3. Select the default housekeeping settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run every n hours.* Default is 12.</td>
<td>The value represents (in hours) how often to run a full audit.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Number of days of audit records to keep.*</td>
<td>The value represents the number of days that audit records are kept.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>Default is 120.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of days of job execution records to</td>
<td>The value represents the number of days that job execution records are kept.</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>keep.* Default is 120.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of days of closed alert records to</td>
<td>The value represents the number of days that alerts are kept after being</td>
<td>numeric using up and down arrows</td>
</tr>
<tr>
<td>keep.* Default is 120.</td>
<td>closed.</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

**Define Roles**

Roles are not necessarily associated with jobs or job titles; rather, each role should contain the permissions required to perform a specific task or set of tasks. Managing roles based on tasks is easier than managing permissions attached to features or functions. Because multiple users in organizations often perform the same task (for example, two teams of 20 support engineers require a Device Admin role), and tasks are shared even across different teams (five product engineers also require 'Device Admin'), the number of roles you need to define is in principle much lower than the number of users in the system. See [Edit an Existing Role](#) and [Duplicate an Existing Role](#).

**About Roles**

The role structure in Management Center has two predefined levels:

- **administrator**, which has all permissions for all objects. The default `admin` account has the administrator role.
- **viewOnly**, which has the view permission for all objects.

You can create other roles that allow view access to some objects, add or update access to some objects, or a mix of different permissions as shown in the example below.

---

![ACCESS CONTROL MODEL](image-url)
Symantec recommends that you create roles—with all necessary permissions and filters—before adding users.

**About Roles**

The role structure in Management Center has two predefined levels:

- **administrator**, which has all permissions for all objects. The default *admin* account has the administrator role.
- **viewOnly**, which has the view permission for all objects.

You can create other roles that allow view access to some objects, add or update access to some objects, or a mix of different permissions as shown in the example below.

**Procedure**

1. Select **Administration > Roles** and click **Add Role**.
2. In the **Add Role: Basic Info** dialog, enter a name for the role. If you authenticate users against LDAP, Active Directory or RADIUS, create a role in sync with the directory service.
3. (Optional) Enter a description.
   
   **TIP**
   Symantec recommends that you enter a list of the permissions for the defined role in the Description field. This helps you and other users understand the permissions of a user's role including the intent of their job function.
4. Click **Next**.
5. In the **Add Role: Permissions** dialog, click **Add Permission**.
6. From the **Object** drop-down list, select **All objects** or a specific object.
7. From the **Action** drop-down list, select **All operations** or one or more individual actions.
8. (Optional) In the **Filter** drop-down list, select a filter to apply to both the action and the object. See [Grant Permissions for information on objects, actions, and filters](#).
9. To add more permissions, repeat steps 6 through 8.
10. Optional: **Add Reporter permissions**.
11. Click **Finish**.

For information about managing roles, see **Edit an Existing Role** and **Duplicate an Existing Role**.

**Duplicate an Existing Role**

To avoid spending an excessive amount of time on defining roles with similar permissions, you can define a role based on a role that already exists in the system. For example, if you have already created a role that allows access to device groups, you can base other roles on it with different attributes.

1. Click the **Administration** tab and select **Roles**.
2. Select the role on which you want to base the new role.
3. Click **Duplicate**. Use the **Duplicate** button or the icon in the **Action** column, as shown below.

   The Roles tab displays the new role, with the name of the original role followed by (1). For example, if you duplicated the viewOnly role, the new role's name is viewOnly (1).
4. Select the role you just created and click **Edit**. The web console displays the Edit Role dialog containing two tabs:
   - **Basic Info**
   - **Permissions**
5. Update the name and description to reflect the purpose of the new role.
6. Click **Permissions**.
7. Edit the permissions for the new role; see [Grant Permissions](#) for instructions.
8. Click **Save**. The role is saved and the Roles tab displays it with the new name and description.

**Edit an Existing Role**

Use the settings on the **Administration > Roles** page to edit an existing role. From the **Roles** page you can perform the following actions:

- **Edit role**
- **Delete role**
- **Refresh view**
- **Add role**
- **Duplicate role**

**NOTE**

You cannot directly assign permissions to users; thus, you must always edit a role to change a permission. You can edit a role's basic information or the permissions that the role comprises.

To view the permissions associated with a role click the + icon. Expand or collapse the roles and associated permissions using the icons.

**Edit: Update basic information**

1. Select **Administration > Roles**.
2. Select the role whose information you want to update and click **Edit**. The web console displays the Edit Role dialog.
3. On the **Basic Info** tab, edit the name of the role or the description as required. Click **Save**.
Edit: Update permissions

1. Select Administration > Roles.
2. Select the role whose permissions you want to update and click Edit (or click the edit icon in the Action column). The web console displays the Edit Role dialog containing two tabs:
   – Basic Info
   – Permissions
3. Click the Permissions tab. The web console displays the list of permissions.
4. To change only part of a permission, select the value in the Object or Action column. See Reference: Permissions Interdependencies. Do one or more of the following as needed:
   – In the Object drop-down list, double-click and specify All objects or a specific object.
   – In the Action drop-down list, double-click and select All operations or a specific operation.
   – (If applicable) In the Filter drop-down list, click the plus sign (+) and select a filter. See Filter Devices or Device Groups in a Permission.
5. Add or remove an existing permission:
   – To add a permission, click Add Permission. See steps 7 through 10 in Define Roles for instructions.
   – To remove a permission, select it and click Remove Permission. The permission is removed from the list.
6. Click Save.

   **NOTE**
   Control Roles and Permissions through user sessions. If you edit a role's permissions while users are logged in to the web console, users must log out and log in again to see the effects of the change. See Manage User Sessions.

Delete Role

Select Administration > Roles. Select the role and click Delete or use the trash icon in the Action column.

Refresh View

Select Administration > Roles. Click

to refresh the role.

Grant Permissions

You can add, remove, and edit permissions for any role. A role must have at least one permission for the role to take effect.

1. Select Administration > Roles.
2. Select a role and click View. The web console displays the View Role dialog.
3. Click Permissions. You can add, remove, and edit permissions on this tab.

A permission consists of:

- The object, which describes the area, feature, or function that the user can access, such as devices and global settings.
- The action, which is the scope of access to an object. It details what actions a user can do with the object, such as the ability to add and edit devices, or view global settings. The actions that are available depend on the selected object. Starting in Management Center, 1.6.x, you can add multiple actions per object.
- A filter, which dictates permissions to a sub-set or specific area of the object, such as certain attributes about a device or policy. Filters are available for devices and device groups; for instructions on specifying filters, see Filter Devices or Device Groups in Permissions.
The available filters correspond to the specified actions. That is, if multiple actions are defined, the filters list includes all possible filters for those actions. If an action is subsequently deleted, the corresponding filter will also be deleted if it does not apply to any remaining actions.

**NOTE**

If the View permission for an object is not included in a role, users with the role are unable to see the object when they log in to the web console. For example, if a role does not include a permission for the Device object, users added to the role do not see the Network tab.

See Define Roles for more information about setting roles and permissions.

**Update Access When a User's Job Changes**

When a user's job changes, you can adjust their information to reflect their new job or responsibilities.

1. Select **Administration > Roles**.
2. (If applicable) Update a user's roles to reflect changes in position or responsibilities.
3. (If applicable) Update the user's basic details.
4. (If applicable) Update a role to apply changes to all users who have the role. See Edit an Existing Role.

**Update a User's Roles**

When a user has a new job or responsibilities within the organization, you might have to update their roles to ensure that they can perform their new tasks.

1. Select **Administration > Users**.
2. In the Users left pane, select the user whose roles you want to change. The user's details display.
   
   Imported users have the following icon:

3. Click **Edit**. The web console displays the Edit User dialog.
4. Click **Assign Roles**. The dialog displays a list of all the roles in the system. Roles to which the user is not assigned are listed under **Available Roles**. Roles to which the user is currently assigned are listed under **Assigned Roles**.

5. Update roles:
– To add a role, select it from Available Roles and using the arrow, add it to the Assigned Roles list.
– To remove a role, select it from Assigned Roles and using the arrow, add it to Available Roles list.

6. Click **Save**. The web console banner displays an alert indicating that the user was saved.

**NOTE**
Roles are linked to user sessions. If you edit users' roles while they are logged in to the web console, instruct them to log out and log in again to see the effects of the change.

### Restrict Access to Reporter Reports and Data

When creating or editing roles, you can set permissions to limit the Reporter report fields the role has access to. The choices you make limit the reports that users in that role are able to view and also preclude them from adding corresponding widgets to a dashboard. You can also restrict access at the dashboard level, allowing access to reports but filtering out data the role should not have access to.

1. Select **Administration > Roles**.
2. Select a role and click **Edit**.
3. Click the **Reporter Permissions** tab.
4. Click **Add Permission**.

**Show screen.**

5. Select the Reporter database to apply permissions to. **Show screen.**
If you select a database that includes All Databases in the title, the permissions you set will apply to all databases (present and future) on that device. If you select All Reporters - All Databases, the permissions you set will globally apply to all databases on all devices.

**NOTE**
If you've already applied permissions to a database, it will not display in the Reporter-Database list.

6. Click **Next**. The system displays the Add Report Permissions - Restricted Fields, Reports dialog.
7. Restrict report fields. This action excludes reports that match the fields. (You can also allow access to reports while filtering out desired data. See step 9). Select a report field to prevent this role from viewing the selected report information.

8. To view the reports affected by your choices, select **Show Restricted Reports**.
When you are satisfied with your choices, click **Close**.

9. Restrict report data using a **database filter**. This action allows access to reports you have not restricted but removes data according to the fields specified in the filter. To begin, specify a database and then add one or more filter criteria.

   **NOTE**
   If you select **All Selected Databases**, the system does not provide a filter search and you must manually enter the filter criteria. Ensure that you are entering the criteria as it is worded in the report.

10. Click **Finish**, then **Save**.

**Users Associated With Multiple Roles**

If a user is associated with more than one role (or by group association), all applicable roles are displayed. For example, when viewing reports, the user can choose a role and a corresponding database from the menu on the **Reports > Reporter** page. If a role has no access to a database, that role does not display in the **Role** drop-down menu.

**About Reporter Obfuscation**

Explains Reporter obfuscation and its properties.

When creating or editing roles, you can set permissions to obfuscate the Reporter report fields the role has access to. When you obfuscate a report field, the user can still view reports containing that field but cannot view the data in the obfuscated fields. Note the following:
• You cannot obfuscate a field that has already been restricted.
• Obfuscation persists through sorting and paging. It will also persist through filtering with the exception of Full Log Detail reports, where any deobfuscation is lost when filtering.
• Users cannot filter on any obfuscated field. Only canned filters are permitted.
• To allow a user to view the data in obfuscated fields, you must assign the deobfuscation permission to one of the user's roles.
• Reporter Report jobs run with a role specified in the configuration:
  – If a user runs a job ad-hoc or triggers a job via an event, that user must have the specified role or the Job will fail.
  – If a Reporter report job runs as a scheduled Job, it will run using the specified role. If this role includes obfuscation relevant to the report specified in the Job configuration, then the report will be obfuscated.

Obfuscate Reporter Report Fields

This topic describes how to obfuscate Reporter report fields. You cannot obfuscate fields that you have already restricted. In those cases, the Obfuscate option is grayed out.

1. Select Administration Roles.
2. Select a role and click Edit.
3. Click the Reporter Permissions tab.
4. Select All Reporters - All Database: and click Edit.

5. Select the Reporter database to apply permissions to and click Next. If you select a database that includes All Databases in the title, the permissions you set will apply to all databases (present and future) on that device. If you select All Reporters - All Databases, the permissions you set will globally apply to all databases on all devices.

Assign Reporter Database

![Reporter Database Assignment](image)

**NOTE**
If you've already applied permissions to a database, it will not display in the Reporter-Database list.

6. Select the Obfuscate checkbox to hide report fields this role should not view.
7. To view the reports affected by your choices, click **Show Restricted Reports**.

8. When you are satisfied with your choices, click **Close**.

9. Optional: Restrict report data using a **database filter**.

10. Click **Finish**, then **Save**.

**About Report Deobfuscation**

The deobfuscation permission allows users to remove obfuscation from report data.

When creating or editing roles, you can set permissions to **obfuscate** the Reporter report fields the role has access to. To allow a user to view data that has been obfuscated, you must assign the deobfuscation permission to one of the user's roles or create a new role specifically for deobfuscation. For security reasons, Symantec recommends that you create a dedicated deobfuscation user and role instead of adding the deobfuscation permission to an existing admin user.

The deobfuscation permission does not automatically remove the obfuscation in a report to reveal the data. To view obfuscated fields, users must click the obfuscated report field and enter their credentials. After successful authentication, the data for that field will be visible.

When a user deobfuscates one or more fields in a report, the deobfuscation applies only to that report. In all other reports, the same field is obfuscated.

After you deobfuscate a field, you cannot click it to view additional detail (as can be done with fields that are not obfuscated).
Add a New Deobfuscation Role

To allow a user to view data that has been obfuscated, you must assign the deobfuscation permission to one of the user's roles or create a new role specifically for deobfuscation.

1. Select Administration Roles and click Add Role.
2. In the Add Role: Basic Info dialog, enter a name for the role. If you authenticate users against LDAP, Active Directory or RADIUS, create a role in sync with the directory service.
3. (Optional) Enter a description.

   **NOTE**
   Symantec recommends that you enter a list of the permissions for the defined role in the Description field. This helps you and other users understand the permissions of a user's role including the intent of their job function.
4. Click Next.
5. In the Add Role: Permissions dialog, click Add Permission.
6. From the Object drop-down list, select Deobfuscation.
   
   **NOTE**
   The deobfuscation permission is not included in the All objects object. You must specifically assign the Deobfuscation object to the role.
7. From the Action drop-down list, select All operations.
8. (Optional) In the Filter drop-down list, select a filter to apply to both the action and the object.
9. Click Finish.

Add Deobfuscation Permission to Existing Role

1. Select Administration Roles.
2. Select a role and click Edit.
3. Select Permissions Add Permission.
4. From the Object drop-down list, select All objects and then Deobfuscate from the drop-down list.
5. Click Save.

Filter Devices or Device Groups in a Permission

You can control access to devices and device groups (folders) on a more granular level than with other objects in Management Center using permission filters. These filters are based on the attributes that you specify in device and device group properties. See Set User-Defined Device Attributes for Access Control for information.

1. Perform one of the following:
   – Add a permission. See Grant Permissions.
   – Edit a permission. See Edit an Existing Role.
2. In the Add/Edit Role dialog, select the permission and click the plus sign (+) in the Filter field. The Add/Edit Filter dialog displays.
3. Select a filter from the Filter Type drop-down list and specify filter values. See Reference: Permissions Filters Object and Attributes.
4. Click Save. The filter displays in the Filter field.
Reference: Permissions Filters Object and Attributes

Although you are not restricted to the user-defined system attributes of **Location** and **Rack**, the following helps to determine which filters to use for the Device and Device Group permissions.

**Set Filters for Device Object**

Specify Rack and Location attributes. See [Set User-Defined Device Attributes for Access Control](#) for information.

<table>
<thead>
<tr>
<th>Select the Attributes type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute has specific value</td>
<td>Attribute: Select <strong>Rack</strong>. Value: Specify the rack. Click <strong>Save</strong>. The Filter field displays &quot;Rack is '&lt;value&gt;'&quot;.</td>
<td>Devices specified with this rack in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td></td>
<td>Attribute: Select <strong>Location</strong>. Value: Specify the location. Click <strong>Save</strong>. The Filter field displays &quot;Location is '&lt;value&gt;'&quot;.</td>
<td>Devices specified with this location in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Attribute has any value</td>
<td>Attribute: Select <strong>Rack</strong>. Click <strong>Save</strong>. The Filter field displays &quot;Rack is not empty&quot;.</td>
<td>Devices specified with any rack specified in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td></td>
<td>Attribute: Select <strong>Location</strong>. Click <strong>Save</strong>. The Filter field displays &quot;Location is not empty&quot;.</td>
<td>Devices specified with any location in device properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Specific Device</td>
<td>Device: Select a device from the drop-down list. Click <strong>Save</strong>. The Filter field displays &quot;Specified Device&quot;.</td>
<td>This selected device.</td>
</tr>
<tr>
<td>Members of specific group</td>
<td>Hierarchy: Select a hierarchy. Your selection determines the values for device group. Device Group: Select the device group. Click <strong>Save</strong>. The Filter field displays &quot;Members of specified group&quot;.</td>
<td>All devices in the specified group or its sub-groups.</td>
</tr>
</tbody>
</table>

**Set Filters for Device Group Object**

Specify Primary Contact and Location attributes. See [Set User-Defined Device Attributes for Access Control](#) for information.

<table>
<thead>
<tr>
<th>Select the Filter type</th>
<th>Specify the Attributes</th>
<th>What a user can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute has specific value</td>
<td>Attribute: Select <strong>Primary Contact</strong> Value: Specify the contact. Click <strong>Save</strong>. The Filter field displays &quot;Primary is '&lt;value&gt;'&quot;.</td>
<td>Groups specified with this primary contact in group properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td></td>
<td>Attribute: Select <strong>Location</strong> Value: Specify the location. Click <strong>Save</strong>. The Filter field displays &quot;Location is '&lt;value&gt;'&quot;.</td>
<td>Groups specified with this location in group properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
<tr>
<td>Attribute has any value</td>
<td>Attribute: Select <strong>Primary Contact</strong> Click <strong>Save</strong>. The Filter field displays &quot;Primary Contact is not empty&quot;.</td>
<td>Groups specified with any primary contact in group properties under <strong>Attributes &gt; User-Defined</strong>.</td>
</tr>
</tbody>
</table>
Management Center - 3.0

Select the Filter type | Specify the Attributes | What a user can access
---|---|---
Specific Device Group | Attribute: **Select Location**
Click **Save**. The Filter field displays "**Location** is not empty".
Groups specified with any location in group properties under **Attributes > User-Defined**.

Members of specific group | Hierarchy: Select a hierarchy. Your selection determines the values for device group.
Device Group: Select the device group.
Click **Save**. The Filter field displays "Specified Device Group".
The sub-groups of the specified group (but not the group itself).

Set Filters for Policy Object

Filter permissions for specific policies. See **Edit Attributes**.

Select the Filter type | Specify the Attributes | What a user can access
---|---|---
Specific Policy | Policy: Select a policy. All policy objects that exist in Management Center are displayed here.
Click **Save**. The Filter field displays Policy Attributes.
The specified policy.

Attribute has specific value | Select an attribute. You must create an attribute and associate it with policy before using this option.
Click **Save**. The Filter field displays Policy Attributes.
The policy matching the attribute details.

Set Filters for Scheduled Job

Filter permissions for scheduled jobs. Limits the user to working with specific jobs or all jobs created by a user.

Select the Filter type | Specify the Attributes | What a user can access
---|---|---
Owner (Created by) | Select **Current User** or **Specific User**.
Click **Save**.
All jobs from created by the specified user.

Specific Scheduled Job | Select a specific, scheduled job.
Click **Save**.
The specified job.

For more information about user-defined attributes, see **Manage Attributes**.

**Preview or Download Logs**

You can sort and preview a log by file name or log type. You can preview one log or download multiple logs.

1. Select **Administration > Logs**.
2. Select a log to view. Click **Preview**. For example, to view the localhost_access.log in a text viewer, click **Preview**.
3. To download multiple logs, select the check boxes of logs that you want to download and then click **Download**. Management Center downloads a .zip archive file to the default download location.

**Available Logs**

The following table list the available logs.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost_access.log</td>
<td>WEB-ACCESS</td>
<td>Tracks users requests to the Management Center UI. These logs roll over weekly for a maximum of 4 weeks.</td>
</tr>
<tr>
<td>log.log</td>
<td>WEB</td>
<td>Primary Management Center log. The primary Management Center log rolls over when it reaches 10 MB and maintains a maximum of 9 history logs for a total of 1 GB.</td>
</tr>
<tr>
<td>debug.log</td>
<td>DEBUG</td>
<td>This log provides diagnostics information to help with debugging. The log only displays if a user enables debug diagnostics (<strong>Administration &gt; Settings &gt; Diagnostics</strong>). The DEBUG logs roll over when it reaches 10 MB and maintains a maximum of 9 history logs for a total of 1 GB.</td>
</tr>
<tr>
<td>journal.txt</td>
<td>PDM</td>
<td>Primary log for the performance data collector of Management Center. This log is useful for determining why performance data is not showing up in Management Center or is being delayed. These logs roll over weekly for a maximum of 4 weeks.</td>
</tr>
<tr>
<td>device.log</td>
<td>SYSTEM</td>
<td>Internal CLP OS log. These logs are very small and roll over every day for a maximum of 30 days.</td>
</tr>
<tr>
<td>clp_services.log</td>
<td>SYSTEM</td>
<td>Internal CLP OS log. These logs are very small and roll over every day for a maximum of 30 days.</td>
</tr>
</tbody>
</table>

**Other Logs**

Other logs include the following:

- Debug logs for each type of device. For example, `cas.log`.
- Rollover logs. Their formats are similar to the following:
Log Types

The following table describes the log types.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEB</td>
<td>Logs related to Management Center and its operation.</td>
</tr>
<tr>
<td>WEB-ACCESS</td>
<td>Logs that track user requests to Management Center web UI.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>As the name implies, these are debugging logs.</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>Internal core OS logs.</td>
</tr>
<tr>
<td>PDM</td>
<td>Performance Data processing logs. These correspond to anything related to the <code>appstat</code> processing of PDM logs from the ProxySG or other systems.</td>
</tr>
</tbody>
</table>
Manage Devices

Refer to the following topics for assistance.

Add a Device
Add a Device Group
Add Multiple Devices at Once
Customize the Network View
Edit a Device
Edit a Device Group
Launch a Device Console
Back Up Device Configurations
Change Device Password
Use Device Information for Backup Job Image Metadata
View Device Backups
Restore Device Backups
Export Device Backups
Import Device Backups
Set the Number of Backup Slots
Monitor Device Health and Statistics
Stop Managing a Device
About Pre-Deployed and Deactivated Devices
Restart a Device
Synchronize Devices
Configure Hierarchy for Devices and Device Groups
Search for Managed Devices
Perform an Operation on a Managed Device
Ensure Devices Belong to Device Groups
Monitor Device Health
Verify Device Details
View System Metrics
RMA a Device
Put Device in Read-Only Mode
Add Device Group Attributes
Add and Monitor Devices

The Network dashboard (left pane > Network) presents data about managed devices and enables you to perform operations on them. Before you can view appliance data, you must add the device to Management Center. To import multiple devices, see Add Multiple Devices at Once or Migrate Device Hierarchy from Director to Management Center.

Other actions and considerations:

• To enable secure communication with devices, see Set HTTPS Server Certificate Hostname for Secure Device Communication.
• To run operations on managed devices, see Perform an Operation on a Managed Device.
• You can manage up to 500 devices in Management Center.

Key

A — Switch views to view health or licensing device data.
B — Add new device or group. See Add a Device and Add a Device Group.
C — View device warnings and errors at a glance. See Monitor Device Health, Resolve Device Errors, and Web Console Overview for more information.
D — See Perform an Operation on a Managed Device.
E — Filter by group. See Add a Device Group and Configure Hierarchy for Devices and Device Groups.
F — Edit or delete devices. See Edit a Device.

About Hierarchy and Group Views

You require a way to administer and monitor devices in your network, which might comprise a complex organizational or geographical scheme. In Management Center, you can manage the devices in your network within a hierarchical structure.

Management Center comes with a predefined structure for device management, as follows:

• Location (Hierarchy)
  – World (Group)
    • France, Canada, Germany, and others (Subgroups)
• Organization (Hierarchy)
  – Company (Group)
    • Finance, Sales, Legal, and others (Subgroups)

You can use these predefined hierarchies and groups, but if you must organize the devices in your network using different criteria, you can create your own hierarchies and groups. Then, create device groups and subgroups to logically represent the structure of your network. Click the gear icon to view and manage hierarchies. See Configure Hierarchy for Devices and Device Groups.

Customize the Network View

You can customize the Network tab to make it easier to keep track of specific devices or device groups. When you make display changes, change column widths or order, etc., the changes are preserved even if you refresh the grid or log out.

The Network view shows information of the network, with the group folders in a section to the left and detailed information of the folders and devices displayed in a list. Each list item shows status, device type (including folders), OS version, IP address, user-defined description, and more. Click groups to drill down in the hierarchy.
Switch Between Health and Licensing Status Views

Click **Health** or **Licensing** to view corresponding device information.

Toggle Group Association

When the **Groups** toggle is off, Management Center displays a flat list of devices. When the **Group** toggle is on, Management Center displays the group hierarchy in the left panel and a list of devices associated with the group in the right panel. Select a device group to show the device members.

Click the gear icon to view and manage hierarchies. See **Configure Hierarchy for Devices and Device Groups**.

Change the Representation of Displayed Data

Click the Grid, Tile, or Icon view to change how the system represents the displayed data. Hover over a box in the tile or icon views to view device details. Right click a device box to perform device operations. For example, to launch the console. See **Perform an Operation on a Managed Device**.

Grid

Displays data in line-by-line, vertical order. This is the default view.

Tile

Displays the data as device boxes labeled with the device icon and name (and warning or error state if present).

Icon
Displays small device boxes labeled with the device icon and color coded to the current health status. This view can be useful if you have a lot of devices.

Filter devices by status

1. Select Network.
2. Go to the Filters panel on the right-side of the page. Enter filter criteria or select or clear the check boxes for statuses that you do not want to display. Click Apply.

For more information about colors and status indicators, see About Status Indicators. In the following example, the Inactive status is not checked; thus, only devices with Error, Warning, and OK status (that is, devices that are activated) are displayed.
Change Displayed Columns

1. Select **Network**.
2. Select any column heading drop-down arrow.
3. Select **Columns** and select or deselect the available columns.

The system displays the added columns. See also **Modify Display of Table Data**.
Add a Device

Before you can manage and monitor your devices, you must add them to Management Center. Devices that can be added to, and managed by, Management Center include the following appliances.

<table>
<thead>
<tr>
<th>Device</th>
<th>Go To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Secure Gateway</td>
<td>About Public Key or Credential Authentication for ProxySG or Advanced Secure Gateway</td>
</tr>
<tr>
<td>ProxySG appliance</td>
<td>About Host Key Validation</td>
</tr>
<tr>
<td></td>
<td>Add a ProxySG or Advanced Secure Gateway using Credential Authentication</td>
</tr>
<tr>
<td></td>
<td>Add a ProxySG or Advanced Secure Gateway using Public Key Authentication</td>
</tr>
<tr>
<td>Content Analysis</td>
<td>Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility</td>
</tr>
<tr>
<td>Integrated Secure Gateway</td>
<td>Add an Integrated Secure Gateway (ISG)</td>
</tr>
<tr>
<td>Malware Analysis</td>
<td>Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility</td>
</tr>
<tr>
<td>PacketShaper</td>
<td>Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility</td>
</tr>
<tr>
<td>Reporter</td>
<td>Add a Reporter</td>
</tr>
<tr>
<td>Security Analytics</td>
<td>Add a Security Analytics</td>
</tr>
<tr>
<td>SSL Visibility</td>
<td>Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility</td>
</tr>
<tr>
<td>Web Security Service</td>
<td>Add Web Security Service (WSS)</td>
</tr>
</tbody>
</table>

**TIP**

Configure how often devices are polled. See Set the Device Polling Interval.

**About Public Key or Credential Authentication for ProxySG or Advanced Secure Gateway**

When adding a device, you must specify how Management Center connects to it. Management Center can connect to a device using the following methods:

- **Credential authentication**: Management Center uses the device's credentials to connect. Credential authentication is considered less secure because the device's credentials are stored in Management Center. Therefore, use public key authentication whenever possible.

  **NOTE**

  Management Center always uses credential authentication when importing devices from Director.

- **Public key authentication**: Management Center inserts a copy of its public key onto the device. The device then "trusts" Management Center connections. This authentication method is considered more secure because device credentials are not stored on Management Center.

  **NOTE**

  You can regenerate Management Center's RSA device key. See device-communication.

  **NOTE**

  Management Center does not remove its public key from devices that are deleted and no longer managed. You can manually delete the key using the following CLI command on the ProxySG or Advanced Secure Gateway:

  ```bash
  # (config ssh-console) delete director-client-key key-id
  ```
About Host Key Validation

Host key validation is a feature of the SSH protocol. Host key validation is designed to prevent devices from impersonating legitimate servers in an attempt to steal credentials and data (man-in-the-middle attack). To prevent such attacks, each device has a unique host key that can be used to establish the identity of the host. If a device supports it, Symantec recommends that you enable host key validation because the method can warn you of a man-in-the-middle attack. In that case, Management Center notes that host verification failed and prompts you to verify the SSH host fingerprint.

You can verify the host fingerprint using one of the following methods:

- Complete the following tasks from a terminal that has a trusted network path to the device:
  
  ```bash
  # ssh keygen-lf <(ssh-keyscan device_ip 2>/dev/null)
  ```
  
  The system displays the host key.

- Enter the following commands from the device's serial connection:
  
  a. Enter the following command:
     ```bash
     # (config ssh-console) view host-public-key sshv2
     ```
  
  b. Copy the output to a file, for example, /tmp/hostkey.
  
  c. Enter the following command from a system running OpenSSH 7.2:
     ```bash
     # ssh-keygen -l -e sha256 -f /tmp/hostkey
     ```
  
  The system displays the host key.

Add a ProxySG or Advanced Secure Gateway using Credential Authentication

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select the device type.
5. Specify the **Modes**:
   - Select **Existing device** if the device is already installed. Select **Unavailable** (pre-deployment) if the device is not available yet. See About Pre-deployed and Deactivated Devices for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See Put Device in Read-Only Mode for more information.
   - Specify whether to collect statistics for the device. See Statistics Monitoring Reports.
6. In **Connection Details**, go to **Authentication Type** and click the **Credentials** tab. Set the following properties:
   - The IP address or hostname of the device
   - The SSH port
   - The username and password you use to authenticate to the device.
   - Your enable password for administrator actions
   - Confirm whether to Enable host key validation (recommended).
   - Select the SSL context to use for TLS communication. Operation:
     - The default setting is Global Default. When Global Default is selected, the system uses the SSL context that is configured in the Device Communications settings.
     - If you select a different SSL context (not Global Default), that context overrides the SSL context that is defined in the Device Communication setting.
     - If no SSL context is set in the Device Communication setting, the system uses the system-defined: default SSL context when in FIPS mode, and none otherwise.
7. Click **Connect**. Management Center attempts to connect to the device using the information you entered.
8. If you enabled host key validation, verify the SSH Host Fingerprint and click **Accept**.
9. Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.
If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

10. Verify or change the Device Name.
11. Optional—Input any applicable attributes. See Add Attributes.
12. Click Save.

The Network tab displays the device. The web console displays an alert indicating that the device was added and activated.

**Add a ProxySG or Advanced Secure Gateway using Public Key Authentication**

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click Add Device. The system displays the Add Device wizard.
4. Select the device type.
5. Specify the Modes:
   - Select Existing device if the device is already installed. Select Unavailable (pre-deployment) if the device is not available yet. See About Pre-deployed and Deactivated Devices for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See Put Device in Monitor-Only Mode for more information.
   - Specify whether to collect statistics for the device. See Statistics Monitoring Reports.
6. In Connection Details, go to Authentication Type and click the Public Key tab.
7. Set the following properties:
   - The IP address or hostname of the device.
   - The SSH port.
   - Your enable password for administrator actions.
   - Confirm whether to Enable host key validation (recommended).
   - Select the SSL context to use for TLS communication. Operation:
     - The default setting is Global Default. When Global Default is selected, the system uses the SSL context that is configured in the Device Communications settings.
     - If you select a different SSL context (not Global Default), that context overrides the SSL context that is defined in the Device Communication setting.
     - If no SSL context is set in the Device Communication setting, the system uses the system-defined: default SSL context when in FIPS mode, and none otherwise.
8. Click Connect. Management Center attempts to connect to the device using the information you entered.
9. If you enabled host key validation, verify the SSH Host Fingerprint and click Accept.
10. Enter the username and password you use to authenticate to the device. You must do this so that Management Center can install its public key onto the ProxySG appliance. The credentials are not saved.
    Management Center attempts to connect to the appliance. If the connection is established, the system displays Successful.
    If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.
11. Verify or change the Device Name
12. Optional—Input any applicable attributes. See Add Attributes.
13. Click Save.

The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.
Add an Integrated Secure Gateway (ISG)

NOTE
- To learn more about ISG support, see Integrated Secure Gateway Support.
- Public key authentication is not supported for authenticating to ISG appliances.
- Any applications running on the ISG can also be added to Management Center as individual devices. Those devices might not support certain features, for example, software upgrade. Refer to the appliance’s Device Details Settings page for more information.

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click Add Device. The system displays the Add Device wizard.
4. Select the device type.
5. Specify the Modes:
   - Select Existing device if the device is already installed, or Unavailable (pre-deployment) if the device is not available yet. See About Pre-deployed and Deactivated Devices for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See Put Device in Monitor-Only Mode for more information.
6. In Connection Details, specify the following:
   - The IP address or hostname of the device.
   - The SSH port.
   - The username and password you use to authenticate to the device.
   - Your enable password for administrator actions.
   - Confirm whether to Enable host key validation (recommended).
7. Click Connect. Management Center attempts to connect to the device using the information you entered.
8. If you enabled host key validation, verify the SSH Host Fingerprint and click Accept.
9. Management Center attempts to connect to the appliance. If the connection is established, the system displays Successful.
   - If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.
10. Optional—Verify or change the Device Name.
11. Optional—Input any applicable attributes. See Add Attributes.
12. Click Save.

Add a Reporter

NOTE
Symantec recommends that you create a new non-administrator Reporter role before adding Reporter to Management Center. If you choose to add a Reporter using the default Admin role, you must specify the role as "_admin."

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click Add Device. The system displays the Add Device wizard.
4. Select the device type.
5. Specify the Modes:
   - Select Existing device if the device is already installed, or Unavailable (pre-deployment) if the device is not available yet. See About Pre-deployed and Deactivated Devices for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See Put Device in Monitor-Only Mode for more information.
6. In **Connection**, specify the following:
   - The IP address or hostname of the device.
   - The protocol and port (HTTP or HTTPS).
   - The username and password you use to authenticate to the device.
   - The Reporter role. Specify the role assigned to this user in Reporter. If this is an admin account, input `_admin`.
   - Select the SSL context to use for TLS communication. Operation:
     - The default setting is Global Default. When Global Default is selected, the system uses the SSL context that is configured in the Device Communications settings.
     - If you select a different SSL context (not Global Default), that context overrides the SSL context that is defined in the Device Communication setting.
     - If no SSL context is set in the Device Communication setting, the system uses the system-defined: default SSL context when in FIPS mode, and none otherwise.

7. Click **Connect**. Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.
   - If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

8. Optional—Verify or change the **Device Name**.

9. Optional—Input any applicable attributes. See **Add Attributes**.

10. Click **Save**.
    The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

### Add a Content Analysis, Malware Analysis, PacketShaper, or SSL Visibility

**NOTE**
If you upgrade an SSL Visibility appliance from 3.x to 4.x, you must delete the 3.x device from Management Center and then add it back as a 4.x device.

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select the device type.
5. For SSL Visibility only, select the version **3.8.3+ or 4+**.
6. Specify the **Modes**:
   - Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See **About Pre-deployed and Deactivated Devices** for information on pre-deployment devices.
   - Select **Read/Write** or **Read Only**.
   - Specify whether to monitor the health of the device. See **Put Device in Read-Only Mode** for more information.
7. In **Connection**, specify the following:
   - The IP address or hostname of the device.
   - The protocol and port (HTTP or HTTPS).
   - The username and password you use to authenticate to the device.
   - Optional, for CA and SSLV only: The enable password. You must include the enable password only if you want to run scripts on the device.
   - Select the SSL context to use for TLS communication. Operation:
• The default setting is Global Default. When Global Default is selected, the system uses the SSL context that is configured in the Device Communications settings.

• If you select a different SSL context (not Global Default), that context overrides the SSL context that is defined in the Device Communication setting.

• If no SSL context is set in the Device Communication setting, the system uses the system-defined: default SSL context when in FIPS mode, and none otherwise.

8. Click **Connect**. Management Center attempts to connect to the device using the information you entered.
   Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.
   If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.

9. Verify or change the **Device Name**
10. Optional—Input any applicable attributes. See **Add Attributes**.
11. Click **Save**.

   The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

**Add a Security Analytics**

1. Select the **Network** tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Click **Add Device**. The system displays the **Add Device** wizard.
4. Select **Security Analytics**.
5. Specify the **Device Management Modes**:
   – Select **Existing device** if the device is already installed, or **Unavailable** (pre-deployment) if the device is not available yet. See **About Pre-deployed and Deactivated Devices** for information on pre-deployment devices.
   – Select **Read/Write** or **Read Only**.
   – Specify whether to monitor the health of the device. See **Put Device in Read-Only Mode** for more information.
6. In **Connection Details**, specify the following:
   – The IP address or hostname of the device.
   – The port (the default is HTTPS 443).
   – The username you use to authenticate to the device.
   – Enter the **Security Analytics device API key**.
   – Select the SSL context to use for TLS communication. Operation:
     • The default setting is Global Default. When Global Default is selected, the system uses the SSL context that is configured in the Device Communications settings.
     • If you select a different SSL context (not Global Default), that context overrides the SSL context that is defined in the Device Communication setting.
     • If no SSL context is set in the Device Communication setting, the system uses the system-defined: default SSL context when in FIPS mode, and none otherwise.
7. Click **Connect**. Management Center attempts to connect to the device using the information you entered.
   Management Center attempts to connect to the appliance. If the connection is established, the system displays **Successful**.
   If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.
8. Verify or change the **Device Name**
9. Optional—Input any applicable attributes. See **Add Attributes**.
10. Click **Save**.
The Network tab displays the device and the web console displays an alert indicating that the device was added and activated.

**Add Web Security Service (WSS)**

To add a WSS, you must first create an integration token on the WSS portal. Then use that token to add the WSS to Management Center.

You use WSS with Management Center to create Universal Policy Enforcement (UPE) rules.

**NOTE**
The following steps require that you have not yet set up and configured your WSS portal account. If you have already set up your portal account, contact Symantec support for assistance.

**Step 1: Create WSS Integration Token**

To create the token, do the following:

1. To create the token, log into your WSS portal and enter Service mode. Select Account Maintenance > Integrations.
2. Click New Integration. The portal displays the New Integration dialog.
3. Select the Integration Type, depending on your solution. The portal displays the integration page per the device type. The exception is CASB Integration; selecting this type adds the drop-down to the Integrations page. From you here, you tenant the CloudSOC.

Refer to the WSS documentation for more information.

**Step 2: Add WSS in Management Center.**

1. Select the Network tab.
2. (Optional) Browse to the hierarchy and folders/subfolders where you want to add the device.
3. Select Add > Add Device. The system displays the Add Device wizard.
5. Specify the Modes:
   - Select Existing device if your WSS account is configured, or Unavailable (pre-deployment) if the service is not configured or is unreachable. See About Pre-deployed and Deactivated Devices for information on pre-deployment devices.
   - Select Read/Write or Read Only.
   - Specify whether to monitor the health of the device. See Put Device in Monitor-Only Mode for more information.
6. In Connection, do the following:
   a. Select the Cloud Network to connect to, Production or Pre-Production.
      **NOTE**
      If you are participating in a beta program, click Analyze in Pre-Production.
   b. Click Connect.
7. In the Registration Required field, enter the Integration Token that you created in Step 1: Create WSS Integration Token and click Register.
   If the connection test fails, you receive an error. Make sure that the information you entered is correct and try again. If the connection test succeeds, you receive a success message.
8. Verify or change the Device Name.
9. Optional—Input any applicable attributes. See Add Attributes.
10. Click Save.

**NOTE**
If you use the Management Center failover feature and the primary fails, you must reconnect to the WSS on the secondary. Though WSS devices are propagated to the secondary, it is viewed by the WSS instance...
as a different appliance requiring registration. To reconnect to the WSS, go to Network > device > Edit > Connection Parameters.

The Network tab displays the device. The web console displays an alert indicating that the device was added and activated.

Next Steps

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>Ensure Devices Belong to Device Groups</td>
</tr>
<tr>
<td>Check information specific to the selected device.</td>
<td>Monitor Device Health</td>
</tr>
<tr>
<td>Check device metrics.</td>
<td>View System Metrics</td>
</tr>
<tr>
<td>Troubleshoot device connection.</td>
<td>Can't Connect to Device After Upgrading to 2.x</td>
</tr>
</tbody>
</table>

View and Edit Device Information

When you select a device and click Edit, you can view a variety of device information.

Edit a Device

1. Select the Network tab. (Optional) Browse to the hierarchy and folders/subfolders where the device you want to edit belongs.
2. Edit a device in one of the following ways:
   - Select the device and click Edit.
   - Click the device hyperlink in the Name column of the grid view.
   - Click the edit device icon in the Actions column.

Review and Edit Device Information

When you edit a device, the system displays the following tabs:

- Status
- Statistics
- Settings
- Connection Parameters
- Backup
- Policies
- Certificates
- License

Management Center displays the Backup, Policies, Certificates, and License tabs only when those features are supported by the device. For example, Management Center does not display the Policies tab for Reporter devices.

Status
View errors and warnings, system metrics, and health check information.

**Statistics**

Displays a dashboard of important device statistics. See Monitor Device Health.

**Settings**

- **Basic Info:** Edit the device name and description and view the deployment status, model number, serial number, and OS version. See About Pre-Deployed and Deactivated Devices.
- **Membership:** View and edit membership.
- **Attributes:** View or change the value on mandatory attributes. You cannot delete mandatory attributes.

**Connection Parameters**

- The authentication type, public key or credential.
- The IP address or hostname of the device
- The username and password you use to authenticate to the device
- The enable password for administrator actions.
- Reporter only—the role (_admin).
- SSL context setting.
  - Hostname verification and certificate trust validation for device connections is performed when the CCL for the working SSL context is defined.
  - The device-specific SSL context overrides the global context defined in the device-communication CLI command.
- Host key validation setting.

**Backup**

View system backup information; restore or delete a backup.

**Policies**

Displays the effective policy for each slot. The policy name mapped to each slot is displayed and the following assignments are displayed:

- Direct assignment - The policy was installed directly to the slot.
- Inherited from [Device Group Name] - The policy was inherited from device group that the device membership is from.

**TIP**

The Local, Central, and Forward slots display CPL policy only. See Create a CPL Policy Object or see Create a Policy fragment.

After you have completed editing the tabs for each device, click Save.

**TIP**

You can also Perform an Operation on a Managed Device.

**Certificates**

Displays a list of the certificates installed on the device. Click a certificate to review more details.

**License**

Provides a list of all installed licenses and their current status.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>Ensure Devices Belong to Device Groups</td>
</tr>
<tr>
<td>View information about the device.</td>
<td>Verify Device Details</td>
</tr>
</tbody>
</table>
**What do you want to do next?**

| Choose Operations for a Device or Device Group. | Perform an Operation on a Managed Device |
| Edit device or policy attributes.               | Edit Attributes                          |

---

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>Ensure Devices Belong to Device Groups</td>
</tr>
<tr>
<td>View information about the device.</td>
<td>Verify Device Details</td>
</tr>
<tr>
<td>Choose Operations for a Device or Device Group.</td>
<td>Perform an Operation on a Managed Device</td>
</tr>
<tr>
<td>Edit device or policy attributes.</td>
<td>Edit Attributes</td>
</tr>
</tbody>
</table>

---

**Restart a Device**

If you need to reboot a managed device, you can restart it from Management Center's web console.

*NOTE*

You can also schedule a restart by creating a job. See Schedule Device Restart.

1. Select the **Network** tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. From the **Operations** drop-down list, click **Restart**.
4. Click **OK** to confirm the reboot.

**Synchronize Devices**

Management Center supports synchronization of the following device types: SSL Visibility, Content Analysis, and Malware Analysis.

When devices have similar or exact configurations, you can copy the configuration of one device (the source) to one or more similar devices running the same or later OS versions. As an example, you can't synch from a non-FIPS image to a FIPS image.

**Prerequisites**

- Determine which device has the configuration settings you want to synchronize to other devices. This device will be your source device.
- Under **Devices** on the **Network** tab, identify the target devices and verify that their OS version is the same or later than the source device. The OS version is displayed in the device's Overview tab. See View System Metrics.

**Device Sync Details**

Different settings are synched for each device.

**Support for SSL Visibility Appliance**

**Important Notes**

- Management Center does not allow synchronization from a newer version of an operating system to an older version. For example, you cannot synchronize a 3.8.3 operating system version to a 3.8.2 operating system.
- SSL Visibility 4.x (and later) appliances synchronize Policy and PKI only.
- SSL Visibility appliances do not report platform information in the device overview. Platform is displayed as N/A as shown in the example.
What to Synchronize

- Alerts - alerting and notifications used on the device
- Users - names and passwords on the device
- PKI - certificate (or the database store)
- Policy - rules for decrypting traffic
- Remote authentication - controls the way the device authenticates, as for TACACS

Advanced Synchronization Options

SSLV 3.x now supports the following synchronization options for certificate resigning. These options are not supported in SSL Visibility 4.x:

- **Retain default resigning keys**
  When you enable this option, the resigning certificate (EC or RSA) identified as default on a ruleset option for EC or RSA will not be changed on the target device. Selecting this option allows you to use different default resigning certificates on different target devices. When using this option, Symantec recommends that you set individual rules to use “default” such that the certificate used by the rule will be the same as that specified in the ruleset options.

- **Retain rule resigning keys**
  When you enable this option, the resigning certificate (EC or RSA) specified on a rule will not be changed on the target device. Selecting this option allows you to use different resigning certificates on different target devices.

- **Retain segment definitions**
  When you enable this option, the segment definitions of the target device will not be changed. This option should only be used in rare circumstances when you want to synchronize policy but want different segment definitions. This option is only supported in SSLV 3.12.3.1 and later.

  **CAUTION**
  When Retain segment definitions is used, all segments must have a ruleset assigned to them. If a disabled segment does not have a ruleset assigned, the transfer will fail. This is by design and enforced by the SSLV device.

Support for Content Analysis (CA)

  **TIP**
  Management Center does not allow synchronization from a newer version of an operating system to an older version.

Synchronization areas:

  **NOTE**
  Refer to the Content Analysis 2.3.x Administration and Reference Guide for more information about these settings.

- **Configuration**: Not all elements of your Content Analysis appliance configuration can be saved/restored. Administration details and network information defined in the initial deployment of your appliance must be manually assigned. The following components are included:
- Alert Settings
- Alert Templates
- SMTP Settings
- Consent Banner
- Custom Logo
- NTP Settings
- Timezone Configuration
- HTTP Settings
- SNMP Settings
- Predictive Analysis Settings
- Global Anti-Virus Policy
- Kaspersky Policy
- Sophos Policy

• Sandbox Settings: Includes sandbox service and file-scanning settings.
• Firewall: Includes firewall task settings for the IntelliVM analysis environment.
• Patterns: Includes pattern groups created by users.
• Yara Rules: Includes Yara rules defined on the appliance.
• File Hashes: Synchronizes the allow list or block list file hashes with those on the source device. This operation is not a merge; any existing allow list or block list file hashes on the target devices are destroyed during synchronization.
• Scanning Profiles: Synchronizes base images and scanning profiles for on-box sandboxing. Synchronizing these eliminates the need to create individual scanning profiles on every CA device.

**NOTE**
If the base OS image is not on the target, it is transferred before synchronizing the profile.

**NOTE**
The Sandbox Settings, Firewall, Patterns, Yara Rules, File Hashes, and Scanning Profiles options apply only to CA 2.x appliances. If you select one of these options, the system does not display any 1.x CA device targets.

Support for Malware Analysis Appliance (MA)

**TIP**
Management Center does not allow synchronization from a newer version of an operating system to an older version.

What to Synchronize:

• **Settings**: All settings within these groups are synced:
  - File reputation (enabled/disabled)
  - Cleanup daemon
  - Proxy Server
  - YARA state (enabled/disabled)
  - Virus Total key
  - Task Defaults
  - Updates (enabled/disabled)
  - WebPulse

• Pattern groups created by users

**Synchronize Devices**

Follow this basic procedure.

1. Select Jobs > Add > New Job.
2. On the Add New Job page, select Synchronize Devices

3. Configuration:
   – Select a Source Device(*) from the list of available devices. After selecting a source device, click OK.
   – Select the check boxes to define What to synchronize(*). Available choices are specific to the device and are not platform specific.

4. Targets:
   – Select the Devices or Groups tab.
   – Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   – Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   – If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   – All selected targets appear in Selected Targets.

5. Job Results:
   – (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).

6. Schedule:
   Choose to trigger job execution using a Schedule or an Event.

   **Schedule**
   Use Schedule when you want to run the job now or to execute the job at a specific time.
   – Immediate—automatically runs the job after it is created.
   – No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
   – Run Once Only—specify the date and time to run the job.
   – Periodic—runs the job every x number of minutes, hours, or days, starting at the specified time and date.
   – Daily—runs the job every day at the specified time.
   – Monthly—runs the job once a month on the specified day of the month and specified time of day.
   See also Job Scheduling Options.

   **Event**
   Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   – Device added to Management Center
   – Device added to Group
   – Device removed from Group
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

7. Name:
   – Verify or change the name and add an optional description.

8. Click Save.

**Verify Device Details**

To verify a device's information after you have added it, or to help identify a device, do the following:

1. Click the Network tab, select a device to view, and click Edit.
2. Click Dashboard. The web console displays information about errors, system metrics, health checks, and resources. To refresh the values, use your browser’s refresh function.
3. If you want to launch the device console, select the Operations pull-down list (upper-right) and click Launch Console.
View Device Certificate Data

To view the certificate data for a device, you must first run the Collect Device Certificates job. After you run the job, the results can be viewed in the following ways:

- The Certificates tab at the top of the Network page.
- The Certificates tab on the device details page.

**NOTE**

At this time, you can view certificate data only for ProxySG and DEFINE IN KEYMAP 4.x appliances.

### Important Notes

- Management Center only provides data about certificates. It does not manage the certificates.
- Management Center does not do full certificate validation. That is the responsibility of the device.
- Management Center will parse user-supplied Certificate Revocation Lists (CRLs), but these are only applied to the certificates on that target device, not on all certificates in the device inventory.
- Management Center does not do full certificate path validation. Do not rely on Management Center for 100% accurate path validation.
- The full PEM of a certificate is not stored. Management Center only stores specific pieces of metadata.
- In some cases, the PEM from an DEFINE IN KEYMAP appliance cannot be extracted, and Management Center is only able to get attributes. In those cases, the certificate details may not be as complete as that provided for other certificates and the proper path might not be known.
- Upgrading and importing certificates, and then downgrading, can lead to orphan data if a device is removed after downgrade.

### View Certificate Data

1. Run the Collect Device Certificates job.
2. Select the Network page and click the Certificates tab.
3. Hover over a device to review a brief summary.

The summary indicates the number of expired and revoked certificates and also reminds you of the number expiring within the next three months.

### View Individual Device Certificate Data

1. Run the Collect Device Certificates job.
2. Select Network > devicename > Edit.
3. In the device details page, select the Certificates tab to view the certificate data.
4. Navigate through the list of certificates using the page arrows beneath the certificate list.
5. Sort through the information using the table headers.
6. Select an individual certificate to drill down into its details.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Issuer</th>
<th>Intended Purpose</th>
<th>Expiration Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Signature Trust Co.</td>
<td>Digital Signature Trust Co.</td>
<td>Certificate Signing, CRL Signing</td>
<td>Sun, 09 Dec 2018 19:47:36 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>TDC Internet</td>
<td>TDC Internet</td>
<td>Certificate Signing, CRL Signing</td>
<td>Mon, 05 Apr 2021 17:03:17 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>Trustis Limited</td>
<td>Trustis Limited</td>
<td>Certificate Signing, CRL Signing</td>
<td>Sun, 21 Jan 2021 11:38:56 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>SECOM Trust Systems CO., LTD.</td>
<td>SECOM Trust Systems CO., LTD.</td>
<td>Certificate Signing, CRL Signing</td>
<td>Tue, 29 May 2029 05:00:39 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>Chunghwa Telecom Co., Ltd.</td>
<td>Chunghwa Telecom Co., Ltd.</td>
<td></td>
<td>Wed, 29 Dec 2034 02:31:27 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>POSTA</td>
<td>POSTA</td>
<td>Certificate Signing, CRL Signing</td>
<td>Tue, 07 Feb 2023 11:06:58 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>Certsign Certificadores Digital Ltd.</td>
<td>Certsign Certificadores Digital Ltd.</td>
<td>Certificate Signing, CRL Signing</td>
<td>Wed, 27 Jun 2018 00:00:00 GMT</td>
<td>Expired</td>
</tr>
<tr>
<td>Government Root Certification Authority</td>
<td>Government Root Certification Authority</td>
<td>Certificate Signing, CRL Signing</td>
<td>Thu, 31 Dec 2037 15:59:59 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>CFCA GT CA</td>
<td>CFCA GT CA</td>
<td>Digital Signature, Non-Repudiation, Certification</td>
<td>Tue, 06 Jun 2020 08:15:00 GMT</td>
<td>OK</td>
</tr>
<tr>
<td>VeriSign, Inc.</td>
<td>VeriSign, Inc.</td>
<td></td>
<td>Tue, 01 Aug 2028 23:59:55 GMT</td>
<td>OK</td>
</tr>
</tbody>
</table>
Configure Device Connection Security Level (SSL Context)

An SSL context is a collection of ciphers, protocol versions, trusted certificates and other TLS options. Since it is very common to have multiple connections with the same settings, they are put together in a context and the relevant SSL connections are then created using this context.

This feature enables you to use a global SSL context that applies to all devices, or to assign a context on a per-device basis. For example, you might want some devices to use a more secure SSL context setting than that used by other devices.

Once an SSL context has been configured, all HTTP-based connections use that SSL context to negotiate HTTPS connections, with the following exceptions:

- ProxySG appliance: The SSL context is used only for uploading system images to the ProxySG appliance.
- Web Security Service: Permanently configured with the “cloud-services” SSL context.

**NOTE**
The SSL context feature is available in both FIPS and Non-FIPS modes.
Pre-Configured SSL Contexts

The appliance is pre-configured with the SSL contexts shown in the following table, each with a specific purpose.

<table>
<thead>
<tr>
<th>SSL Context</th>
<th>Keyring</th>
<th>CCL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bluecoat-licensing</td>
<td>bluecoat-appliance</td>
<td>bluecoat-licensing</td>
<td>Used for connections to the Symantec licensing servers.</td>
</tr>
<tr>
<td>bluecoat-remote-access</td>
<td>bluecoat-appliance</td>
<td>bluecoat-appliance</td>
<td>Used for remote diagnostics services.</td>
</tr>
<tr>
<td>bluecoat-services</td>
<td>bluecoat-appliance</td>
<td>bluecoat-services</td>
<td>Used for connections to the Symantec subscription and heartbeat servers.</td>
</tr>
<tr>
<td>cloud-services</td>
<td>bluecoat-appliance</td>
<td>bluecoat-appliance</td>
<td>Used for Web Security Service connections. This context uses the existing bluecoat-appliance keyring and CCL. You cannot remove it but you can edit it.</td>
</tr>
<tr>
<td>default</td>
<td>None</td>
<td>browser-trusted</td>
<td>Used for ingress connection configuration (ports 8082 and 9010), secure authentication services (CCL only applies), and for device connections in FIPS mode (when no other is specified). You cannot remove the default SSL context but you can edit it.</td>
</tr>
</tbody>
</table>

You can create other profiles for your own purposes or edit the profile to suit the environment.

**NOTE**

If you are using one of the pre-defined SSL contexts other than default, Management Center performs strict certificate and hostname verification. This means that the device's signing certificate must be included in the CCL specified in the SSL Context.

Specify an SSL Context

Using this feature, you can specify an SSL context in the following ways:

- Globally, using the `device-communication` CLI command.
- Per-device, using the SSL context option in the device's Connection Parameters when adding or editing a device (Network > `devicename` > Edit > Connection Parameters). If a global SSL context is set, the device-specific SSL context overrides the global setting.

If a global and individual device SSL context is not set, Management Center:

- FIPS mode: Uses the default SSL context.
- Non-FIPS mode: Trusts all certificates and does not perform hostname verification.

Create an SSL Context

Use the `create ssl-context` CLI command to create an SSL context:
(config-ssl)# create ssl-context <context_id> [keyring <keyring_id>] [ccl <ccl_name>] [protocol [ <protocol> ... ]] [cipher-suite [ <cipher-suite> ... ]]

See ssl for more information.

**Verify Certificate Trust**

To verify certificate trust in the SSL connections, you must specify a CA certificate list (CCL) when creating or editing the SSL context. If no CCL is specified, certificate trust is not validated.

**Example**

(config-ssl)# edit ssl-context mysslcontext ccl beTRUSTED_RSA

**Edit an SSL Context**

Use the `edit ssl-context` CLI command to edit an SSL context.

(config-ssl)# edit ssl-context <context_id>

**Delete an SSL Context**

Use the `delete ssl-context` CLI command to delete an SSL context.

(config-ssl)# delete ssl-context <context_id>

**FIPS Mode Considerations for SSL Context**

If Management Center is in FIPS mode, the following considerations apply to the SSL context feature:

- When the Management Center is in FIPS mode, HTTP connections to devices are not allowed.
- The FIPS-compliant SSL context accepts only FIPS-compliant configuration. The associated CA certificate list, keyring, and CCL need to be FIPS compliant.
- When FIPS mode is enabled, only FIPS-compliant objects—CA certificate lists, keyrings, and CCLs are available as configuration choices. All non-FIPS-compliant objects are unavailable.
- If you do not specify an SSL context in FIPS mode, Management Center uses the default SSL context.

Refer to the Management Center documentation for more information about running Management Center in FIPS mode.

**Add Multiple Devices at Once**

To add multiple devices using a CSV file, you can use Management Center’s template CSV file, or you can create your own. You can import multiple devices of various types, including:

- ProxySG appliances
- Advanced Secure Gateway (ASG) appliances
- Content Analysis appliances
- Malware Analysis appliances
- PacketShaper appliances
- SSL Visibility appliances
- Reporter
**Import Devices Using a CSV File**

Before importing devices, ensure that the device groups that you want to assign the devices to have been created on Management Center. See Add a Device Group for more information.

1. From the web console, click **Network**.
2. Select **Operations > Import from File**.

   ![Import from File](import_from_file.png)

   - Select **Import devices from manually created CSV file**.
   - Click **Launch Import Wizard**.

   - The web console displays the Import Devices wizard.

3. From the Select Device Type dialog, select the device type that you want to import. Click **Next**.

4. You can either Download CSV Template or **Select File** and browse to the location of the import file containing all of the devices. Click **Next**.

   **TIP**
   
   If you download the CSV template, open it and add your devices to it. Refer to the following table for descriptions of the CSV file columns.

<table>
<thead>
<tr>
<th>name</th>
<th>deploymentStatus</th>
<th>host</th>
<th>port</th>
<th>userName</th>
<th>password</th>
<th>enablePassword</th>
<th>collectPdmStats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the device name. Each device name must be unique.</td>
<td>Specify the deployment status: DEPLOYED</td>
<td>Enter the IP address.</td>
<td>Enter the port number.</td>
<td>Enter the administrator account for the device.</td>
<td>Enter the administrator password for the device.</td>
<td>Enter the enable password to enter privileged mode on the device.</td>
<td>Specify whether to collect statistics from the device for reporting: TRUE</td>
</tr>
</tbody>
</table>

5. After the devices are uploaded, they are displayed in the **Import Devices: Assign Groups** dialog.

6. Select the **Import devices from manually created CSV file**.

7. Click **Launch Import Wizard**. The web console displays the Import Devices wizard.

8. From the Select Device Type dialog, select the device type that you want to import. Click **Next**.

9. You can either Download CSV Template or **Select File** and browse to the location of the import file containing all of the devices. Click **Next**.

   **TIP**
   
   If you download the CSV template, open it and add your devices to it. Refer to the following table for descriptions of the CSV file columns.

7. After the devices are uploaded, they are displayed in the **Import Devices: Assign Groups** dialog.

8. Select the devices to assign to a device group.

   **NOTE**
   
   To add an imported device to a group using a CSV file, the group must already exist in Management Center. Therefore, ensure that you have created the desired groups before importing. You cannot create them using the CSV file.

9. After the devices have been selected, from **Device Group**, select the object selector. From the available device groups or hierarchies, select a device group. The selected device group is displayed when you select it. Click **OK**. To apply the imported devices to the device group, click **Apply**.

10. (Optional) Repeat Step 9 until all imported devices belong to a device group or hierarchy.

11. When you are finished assigning the imported devices to device groups, click **Finish**.
**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td>Ensure Devices Belong to Device Groups</td>
</tr>
<tr>
<td>View information about an imported device.</td>
<td>Verify Device Details</td>
</tr>
<tr>
<td>Edit device information.</td>
<td>Edit a Device</td>
</tr>
<tr>
<td>Check device metrics.</td>
<td>View System Metrics</td>
</tr>
</tbody>
</table>

**Set the Device Polling Interval**

You can specify the frequency with which Management Center looks for updates on managed devices. Specify an appropriate interval to ensure that device health statuses display accurately. The default interval is 10 seconds.

1. In the web console banner, select the Administration tab and select Settings.
2. Select General on the left. General fields display on the right.
3. Select Device Polling Interval (sec).
4. Enter a value in seconds.
5. Click Save and then Activate to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

**Resolve Device Errors**

One of the main benefits of using Management Center is to monitor all of your devices from a central location. Without having to log in to each device on your network, you can see if any of your devices have errors, and if so, quickly drill down to pinpoint the problem (unresponsive device, expired license, DNS server cannot be reached, CPU utilization at a critical threshold, and so forth).

**Are Any Devices in an Error State?**

An error (red) status indicates a component on the device is failing, or is far outside normal parameters, and requires immediate attention. Look at the Device Status Totals in the banner; the number inside the red circle indicates how many devices are in an error state.

![Error State Count](Count.png)

**Which Devices are in an Error State?**

Just click inside the red circle to see a list of all devices in an error state. The devices are listed in the Network tab.

![Device List](DeviceList.png)

**NOTE**

When you click a status circle, Management Center is actually setting filters. (Notice the check mark next to Error in the Filter by area.) To return the list to displaying all devices, select the check box next to each state.
What Exactly is the Error on the Device?

1. Click inside the red circle in the Device Status Totals in the banner. The Network tab displays all devices with an error (red) status.

   **NOTE**
   Make note of the Device Type; Management Center is able to display more details about some devices (such as ProxySG appliances) than others.

2. In the device list, select a device and click Edit or select the device hyperlink.

3. The Dashboard tab lists the errors and warnings found on the device. For example, *McAfee, Inc. expired 6/30/15* or *Unable to reach device*.

4. Depending on the type of error or warning, you can explore details by clicking the System Metrics and Health Checks sections. Scroll through the items, looking for red and yellow highlighted rows.

   **Show screen.**

   ![Health Checks](image)

5. In the Operations pulldown, click Launch Console to investigate the device directly and fix the problem.

**Changes in Management Center 1.9.x and Later (Device Serial Number Errors)**

If a monitored device in MC 1.9.x (or later) reports a different serial number, the device will show a health warning. Prior to 1.9.x, the system would ignore the serial number change. A serial number change might occur for various reasons, including:

- A device was returned (RMA) and replaced.
- A different device was deployed to an IP address that Management Center was monitoring, but the credentials stayed the same.
- You re-imaged a VA and gave it a different serial number when setting it up again.

To resolve the warning without losing your configuration, go to the Network page and follow steps 6 to 10 in the RMA the device topic (you don’t actually need to return the device to Symantec).

**Reactivate Statistics Monitoring**

This operation reactivates statistics data collection on monitored devices. Data collection will be reactivated on all devices that have statistics monitoring enabled, but are not currently sending data to Management Center.
This job configures devices with a URL to send required configuration and upload statistics to Management Center. The hostname and IP address in this URL is determined by Management Center based on available configuration in the order below:

1. The hostname/IP address defined in Administration > Settings > Device Communication.
2. The virtual IP address configured using the virtual-ip CLI command.
3. The configured IP address on the first available appliance interface.

If you change any of the preceding configurations, you must restart both the management-center and statics-monitoring services (see system-services restart). After the services have been restarted, this job will use the correct hostname and IP address when configuring the URL on a device for statistics export.

1. Select Jobs > Add > New Job.
3. Job Results:
    – (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).
4. Schedule:
    Choose to trigger job execution using a Schedule or an Event.
    Schedule
    Use Schedule when you want to run the job now or to execute the job at a specific time.
    – Immediate—automatically runs the job after it is created.
    – No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
    – Run Once Only—specify the date and time to run the job.
    – Periodic—runs the job every \(x\) number of minutes, hours, or days, starting at the specified time and date.
    – Daily—runs the job every day at the specified time.
    – Monthly—runs the job once a month on the specified day of the month and specified time of day.
    See also Job Scheduling Options.
    Event
    Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
    – Device added to Management Center
    – Device added to Group
    – Device removed from Group
    If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See the following note.
5. Name:
    – Verify or change the name and add an optional description.
6. Click Save.

**Purge Statistics**

To delete the backlog of statistics stored from monitoring a ProxySG, you can purge the data from Management Center storage.

**NOTE**

Management Center keeps up to 12 months of per hour data and 7 days of per minute data for all devices that have statistics monitoring enabled. To perform more advanced disk maintenance, see # service.

1. Select the Network tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. From the Operations menu, select Purge Stats Monitoring.
Change Device Password

Use these instructions to change the device password for the admin account, or other account, that was used to register the device with Management Center.

Device Notes

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProxySG and Advanced Secure Gateway (ASG)</td>
<td>• Only the password for the predefined admin account can be changed.</td>
</tr>
<tr>
<td></td>
<td>• You can change the Enable password.</td>
</tr>
<tr>
<td></td>
<td>• When challenged for the existing password, use the password for the admin account, not the Enable password.</td>
</tr>
<tr>
<td>Content Analysis (CA) 2.x and later</td>
<td>• You cannot change the password for CA appliances running releases prior to 2.x</td>
</tr>
<tr>
<td></td>
<td>• You can change the password for other accounts, besides admin.</td>
</tr>
<tr>
<td></td>
<td>• You cannot change the Enable password.</td>
</tr>
<tr>
<td>SSL Visibility (SSLV)</td>
<td>• Only the password can be changed.</td>
</tr>
<tr>
<td></td>
<td>• You can change the password for other accounts, besides admin.</td>
</tr>
<tr>
<td></td>
<td>• You cannot change the Enable password.</td>
</tr>
</tbody>
</table>

**TIP**

You can also use the REST API to change a device password. See Management Center REST API for more information.

Change Password

1. Select **Network** and the device you want to change the password for. Then select the **Operations** drop-down list and click **Change Password**.
2. Configure the job options:
   - **Current Password**
• ProxySG/ASG: Enter the current account password. For SG/ASG, use the password for the admin account, not the Enable password.
  
  • CA/SSLV: Enter the current password for the account you are changing.
  - **Password Type** - Select **Device** or **Enable**. You cannot change the Enable password on SSLV and CA devices.
  - **New Password** - Enter the new password for the account.
  - **Retype New Password** - Confirm the new password for the account.

3. Click **Save**.

### Perform an Operation on a Managed Device

The status of a managed device can control which operations are allowed on a device. See **Monitor Device Health**.

**NOTE**

Operations that are not available for the selected device or device group are grayed out in the **Operations** drop-down list.

1. Select the **Network** tab.

2. Select the device group in the left pane, and the device in the right pane.

3. Click **Operations** to display the drop-down list of options.

4. Select the desired option:
  - **View Licenses**
  - **Launch Console**
  - **Open CLI Shell**
  - **Restart**
  - **Change Device Password**
  - **Delete**
  - **Change Monitoring Status**
  - **Backup Devices**
  - **Export Backups**
  - **Import Backups**
  - **Import from File** (Add Multiple Devices)
  - **RMA Device**
  - **Purge Stats Monitoring**
  - **Remove Unused Tenant Policy**

### Remove Unused Tenant Policy

You can delete unused policy from a tenant slot. Management Center considers policy in a tenant slot to be unused if policy is installed on the appliance but does not exist in the tenant slot in Management Center, regardless of whether or not the policy was created or deployed through Management Center. Consider the following examples:

- If you create tenant policy in Management Center, deploy it to an appliance, and then remove it from Management Center, it is considered to be unused.
- If you create tenant policy on the appliance without importing it to Management Center, it is considered to be unused.

**TIP**

See also **Schedule Removal of Unused Tenant Policy**.

1. On the **Network** tab, select a ProxySG appliance.

2. From the **Operations** drop-down list, select **Remove Unused Policies**.

3. On the Remove Unused Policy: Devices dialog, select additional ProxySG appliances if required. Otherwise, click **Next**.
4. On the Policies to Remove dialog, all unused tenant policies are selected by default. Clear the policies you do not want to remove. Leave selected the policies you want to remove.

If there are no unused policies, any tenant policy on the appliance also exists in the same tenant slots in Management Center.

5. Click Next.

6. The Schedule tab shows job options. For details on running or scheduling jobs, see Job Scheduling Options.

7. Click Finish when the job is complete.

**Collect Device Certificates**

The **Collect Certificates** job collects all certificate lists and associated certificates from the target device and extracts the metadata from them. After running the job, refer to View Device Certificate Data to view the results.

**NOTE**
The **Certificates** tab does not display unless the **Collect Certificates** job has been run for that device.

**Supported Devices**

The **Collect Certificates** job supports the following devices:

- ProxySG appliance
- SSL Visibility 4.x appliance

**NOTE**
The **Collect Certificates** job takes six minutes or more on DEFINE IN KEYMAP appliances.

**Collect Certificates**

1. Select Jobs > Add > New Job.
2. On the Add New Job page, select Collect Certificates.
3. **Targets:**
   - Select the Devices or Groups tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   - All selected targets appear in Selected Targets.
4. **Job Results:**
   - (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).
5. **Schedule:**
   - Choose to trigger job execution using a Schedule or an Event.
   - **Schedule**
     - Use Schedule when you want to run the job now or to execute the job at a specific time.
     - Immediate—automatically runs the job after it is created.
     - No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
     - Run Once Only—specify the date and time to run the job.
     - Periodic—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
     - Daily—runs the job every day at the specified time.
     - Monthly—runs the job once a month on the specified day of the month and specified time of day.
   - See also Job Scheduling Options.
Event
Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

– Device added to Management Center
– Device added to Group
– Device removed from Group

If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

6. Name:
   – Verify or change the name and add an optional description.

7. Click Save.

8. Navigate to the device’s detail page to view the job results. See View Device Certificate Data.

Configure Hierarchy for Devices and Device Groups

In Management Center, a hierarchy (Administration > Manage Hierarchies) is a logical organization that helps you manage your devices. The hierarchy is the highest level in the device structure in Management Center and each device group must reside within one or more of these hierarchies. Management Center organizes its many managed devices into hierarchies with parent and child configurations.

Because you can manage up to 500 devices, creating hierarchies is critical in managing device health, status, deploying policy and handling large jobs. The key to understanding Management Center hierarchical configurations is to remember the basic rules of managing device groups, devices, and managing policies that can be deployed to all the devices in your organization.

Create hierarchies to represent geographical regions, organizational or departmental structure, deployment type, or anything else appropriate for your network. For example, a company that has to manage many ProxySG appliances might create the following hierarchies:

Lab A ProxySGs: SG-LabA All ProxySGs on campus: SG-HQ All ProxySGs in the state: SG-Cal

Hierarchy Properties

Hierarchies have the following properties:

• Any hierarchies that you create are at the same level as the predefined Location and Organization hierarchies. Once a device group has been created within a hierarchy, it cannot be moved to another hierarchy.

• A device may be associated with only one device group within a hierarchy. A device may be assigned to groups in different hierarchies.

Hierarchies—Inheritance When Used in Policy and Scripts

The hierarchical structure of Management Center enables you to more easily manage policy across a large number of devices. When used with policy or scripts, hierarchies allow you to establish a precedence for device variable substitution. The precedence determines which inherited device attributes are used when assigning policy. When a device is a member of several hierarchies, the ranked order of the hierarchy dictates the attribute values that are assigned. Using this hierarchical structure, multiple devices can merge their policy attributes, devices can inherit policy attributes from a parent device group, or child devices can be directly assigned policy.

Only hierarchies that have been specifically marked for use in policy are evaluated when resolving device substitution variables. To enable policy use, edit the hierarchy and select Use this hierarchy for policy assignment, script execution, and substitution variable inheritance. When a device is a member of several hierarchies, the attribute that is used during policy evaluation depends on the precedence of the hierarchies. See the following sections for additional information.
NOTE
The concept of attribute inheritance applies to group membership, and does not alter attribute settings configured on individual appliances. Attributes assigned at the device level are not changed when resolving device substitution variables. Devices only inherit device attributes if a specific value has not yet been assigned to the attribute on the device.

Add a Hierarchy

Select Administration > Manage Hierarchies > Add Hierarchy. Or click the gear icon in the left pane of the Network page, then Add Hierarchy.

In the dialog, configure the hierarchy properties.

- **Hierarchy Name**: Enter a unique name.
- **Comments**: Enter useful comments to differentiate this hierarchy from others.
- **Root Folder Name**: The hierarchy name you entered automatically populates the field. Accept the name if you do not want to create a root folder within the hierarchy. To create a new root folder, enter a name for it in the Root Folder Name field. Click Save.
- **Policy, scripts**: Select this option when you want to use the hierarchy for policy assignment, script execution, and substitution variable inheritance. When this option is selected, inheritable values or variables are evaluated based on the hierarchy precedence specified in the Manage Hierarchies page. If this option is not selected, any specified values are used only for organizational purposes.

**TIP**
The root folder is the parent folder for all subfolders. For example, in the hypothetical Beach Names hierarchy, Beach Names is the parent folder for the subfolders (West Coast Beaches, East Coast Beaches and Gulf Coast Beaches).

After creating a hierarchy, add a device group to the hierarchy. See Add a Device Group.

Manage Hierarchies

Select Administration > Manage Hierarchies > Add Hierarchy. Or click the gear icon in the left pane of the Network page.
Manage Hierarchies

- To edit a hierarchy, select the hierarchy and click **Edit**.
- To duplicate a hierarchy, select the hierarchy and click **Duplicate**.
- To delete a hierarchy, select the hierarchy and click **Delete**.
- To change the order of precedence, select the hierarchy and click **Move Up** or **Move Down**. The upper-most hierarchy attribute settings are those that will be used for policy evaluation. In the preceding graphic, if a device is a member of a group in both the **Location** and **Device Group** hierarchies, and the two groups have differing values for the same attribute, the attribute value specified in the **Device Group** hierarchy is applied in policy. See **Hierarchy Device Attribute Example** for more information.

**NOTE**
You can delete any hierarchy except for the **Device Groups** hierarchy.

**TIP**
If you delete a hierarchy that contains devices, the devices are still members of any other hierarchies to which they belong. If you delete the last hierarchy to which a device belongs, click **Unassigned Devices** to see the device.

Hierarchy Device Attribute Example
Example Corporation has the following device groups: **Main1** and **DC1**.

<table>
<thead>
<tr>
<th>Device Group</th>
<th>Hierarchy</th>
<th>Attribute Name/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main1</td>
<td>Main</td>
<td>Campus/California</td>
</tr>
<tr>
<td>DC1</td>
<td>DC</td>
<td>Campus/Northridge</td>
</tr>
</tbody>
</table>

As you can see, Example’s administrator has created an inheritable attribute called **Campus** and set the value differently for the two groups. The two groups each contain many devices, but they both include the ProxySG appliance, 198.51.100.14, albeit in different hierarchies.

Example’s administrator has created CPL that includes the following substitution variable:

```
${device.attributes.campus}
```

This CPL sets the value of the campus attribute. The value set during policy evaluation is determined by the order of the hierarchies at the time of policy evaluation. In this example, **Main** has precedence over **DC** because it is higher in the list.
Practically, this means that if **Main1** is assigned as a target and the policy is installed, the device 198.51.100.14 will inherit the **Campus** attribute value **California** (the value set in the **Main** hierarchy). However, if the admin subsequently moves **DC** above **Main** and installs policy again, 198.51.100.14 would inherit the **Campus** attribute value **Northridge**.

### Put Device in Read-Only Mode

You might want to monitor some devices while also preventing configuration changes on them. Management Center displays a lock next to devices in read-only mode, as shown below.

#### Allowed Operations for Read-Only Mode

<table>
<thead>
<tr>
<th>Operation</th>
<th>Allowed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Metadata</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit Attributes</td>
<td>Yes</td>
</tr>
<tr>
<td>RMA</td>
<td>Yes</td>
</tr>
<tr>
<td>Purge Stats Monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td>Import from file</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Management Center - 3.0

<table>
<thead>
<tr>
<th>Operation</th>
<th>Allowed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign Group Membership</td>
<td>Yes</td>
</tr>
<tr>
<td>Use as a policy target</td>
<td>Yes</td>
</tr>
<tr>
<td>Install Policy</td>
<td>No</td>
</tr>
<tr>
<td>Remove unused policy</td>
<td>No</td>
</tr>
<tr>
<td>Execute script</td>
<td>No</td>
</tr>
<tr>
<td>Backup Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Export Backup</td>
<td>Yes</td>
</tr>
<tr>
<td>Restore Backup</td>
<td>No</td>
</tr>
<tr>
<td>Launch Console</td>
<td>Yes</td>
</tr>
<tr>
<td>Activate Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Deactivate Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Restart Device</td>
<td>Yes</td>
</tr>
<tr>
<td>Device sync as a source</td>
<td>Yes</td>
</tr>
<tr>
<td>Device sync as a Target</td>
<td>No</td>
</tr>
</tbody>
</table>

### Add a Device in Read-Only Mode

1. Select the **Network** tab.
2. Select **Add Device**.
3. Select the type of device.
4. Select **Existing device** from the **Deployment status** menu.

#### NOTE

Devices added with the **Deployment Status** set to **Unavailable (pre-deployment)** cannot be set to **Read Only**.

5. Set the **Edit mode** as **Read Only**.
6. Enter the connection details and follow the rest of the **Add a Device** process.

### Put an Existing Device in Read-Only Mode

1. Select the **Network** tab.
2. Locate the device, select it, and click **Edit**.
3. In the **Settings** tab, select **Read Only**.
4. Click **Save**.

### Search for Managed Devices

You can search for devices in your network using several methods.

**Search by Name or IP Address**

In most cases, searching by the name or IP address is the most efficient way to locate a device.

1. Click the **Network** tab.
2. In the search field at the top of the tab, enter one of the following:
   - Device name
   - String in the device name
   - IP address of the device
   - Octet or part of an octet in the device IP address
3. Press Enter or click the search icon (magnifying glass).

   The system returns a list of all devices that match the search criteria in a **Search** window. Select a device to view it, or click the **X** in the top right corner of the window to close it.

**Browse the Hierarchy**

Select the **Network** tab and browse the hierarchy and folders for the device. This method is convenient if you know where the device is located in the folder structure, or if the folder structure is not too deep or complex.

### Stop Managing a Device

To stop managing a device in Management Center, you **delete** it. You should only delete a device from your network if you are certain that you will not need to manage and it in the future.

**NOTE**

When you delete a device, you remove it permanently from Management Center, and the only way to restore it is to add it again. If you want to stop monitoring a device temporarily, deactivate it instead of deleting it.

1. Click the **Network** tab.
2. Locate the device you want to delete. See Search for Managed Devices.
3. (Recommended) Verify that the device is the one you want to delete. See Verify Device Details.
4. Select the device, and then click **Delete**. The device and all related information, including reports is permanently removed from the system.

**CAUTION**

Deletion cannot be undone. Once removed from the network, the device needs to be registered again.

5. Confirm that the device was deleted. Deleting a device configuration can take up to 60 seconds to complete.

### Set User-Defined Device Attributes for Access Control

User-Defined attributes can either be custom attributes that you create from the Administration tab (or if you edit the attributes system attributes of Location and Rack). System attributes contain values that Management Center collects for reporting purposes.
Management Center - 3.0

- **Connection Parameters** - IP or hostname, Username, Password, Enable Password and SSH Port number.
- **Name** - Device Name
- **Membership** - The hierarchy and device group that the device belongs. See Configure Hierarchy for Devices and Device Groups.
- **Attributes** - Customized Location and Rack attributes or new custom attributes (or metadata) that administrators can create. See Add Attributes.

1. Collect statistics for the device by clicking the check box. See Statistics Monitoring Reports.
2. Use the up/down arrows to specify a Bandwidth Cost. Set Bandwidth Cost for Reports.
   
   **NOTE**
   The bandwidth cost is a multiplier and is thus not expressed in a specific currency unit. For example, you can specify a value to represent on average how you pay per gigabit for data usage on your network.

3. If the User-Defined attribute has a red asterisk * it is required. You must specify a value before continuing.
   
   **TIP**
   Administrators can create attributes in addition to the user-defined attributes of Location and Rack. To define your own device and device group attributes, see Add Attributes and Edit Attributes.

For more fine-grained control of a device or device group, you can add permissions for the specified attributes. See Reference: Permissions Filters.
Upgrade System Images on Managed Devices

Restrictions

- Downgrading a Content Analysis 2.x appliance, and retaining your configuration is not supported.
- Upgrading SSL Visibility appliances from 3.x to 4.x requires other tasks not documented here. If you upgrade an SSL Visibility appliance from 3.x to 4.x, you must delete the 3.x device from Management Center and then add it back as a 4.x device.
- Downgrading SSL Visibility appliances from 4.x to 3.x is not supported.

Refer to the CA and SSL Visibility product documentation and release notes for information about these restrictions.

Install System Image

To install system images on managed devices, complete the following steps.

1. Ensure that the system image has been uploaded to Management Center and that it has been associated with the correct device type. See Upload Files to Management Center for more information.
2. Select Jobs > Add > New Job.
3. On the Add New Job page, select Install System Image.
4. Configuration:
   - System Image: Select the system image. Select Restart device(s) after installation to restart the target device after installation, which is required to load the installed image on some device types.
   - Image device type: This field auto populates depending on your choice above.
   - Delivery method:
     - Upload image to targets: Choose this option to push the image to the target devices. If the target devices are connected to Management Center using SSH public key connections, Management Center will not be able to push the system image because the system does not store the device credentials. If you must push the image to the target device, you must use the Device Credentials authentication method. If device credentials cannot be used, enable the Download Image from Management Center for targets with Public Key authentication check box to allow the target device to pull the image from Management Center. Upload is supported for the Malware Analysis, SSL Visibility, Content Analysis, ProxySG, and Advanced Secure Gateway appliances.
       **NOTE**
       Do not alter the file names for Malware Analysis images when uploading them to the Management Center file server. This is required for successful installation of the image to the Malware Analysis when the appliance has downloaded the image but installation was scheduled for another time.
     - Download image from Management Center: Choose this option so that the target devices download the image from the Management Center file server. This method is supported only by Content Analysis, ProxySG, and Advanced Secure Gateway.
       Select download over secure connection to have the device retrieve the image from the Management Center file server. This operation requires that Management Center knows the device credentials. During the download operation, Management Center, if necessary, installs its certificate chain on the target device.
       **NOTE**
       ASG does not support image installation using the download over secure connection option. Install ASG images using HTTP (described below) or Upload Image to Targets delivery methods. For more information, refer to the ASG product limitations.
       If you choose the non-secure option, HTTP must be enabled on Management Center. To enable HTTP, enter the following CLI commands:
# security http enable

If you enable HTTP after using HTTPS, you must delete the HTTPS cookie from your browser to be able to use the HTTP connection for the UI.

5. **Targets:**
   - Select the **Devices** or **Groups** tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   - All selected targets appear in **Selected Targets**.

6. **Job Results:**
   - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

7. **Schedule:**
   - Choose to trigger job execution using a **Schedule** or an **Event**.
     - **Schedule**
       - Use **Schedule** when you want to run the job now or to execute the job at a specific time.
       - **Immediate**—automatically runs the job after it is created.
       - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
       - **Run Once Only**—specify the date and time to run the job.
       - **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
       - **Daily**—runs the job every day at the specified time.
       - **Monthly**—runs the job once a month on the specified day of the month and specified time of day.
     - See also **Job Scheduling Options**.
     - **Event**
       - Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
       - **Device added to Management Center**
       - **Device added to Group**
       - **Device removed from Group**
     - If you select more than one event type, the job runs if **any** of the conditions are met and the device is an appropriate target. See the following note.

8. **Name:**
   - Verify or change the name and add an optional description.

9. Click **Save**.

**Troubleshooting**

If the upgrade operation is not successful, check the following:

- Verify HTTP/HTTPS connectivity between Management Center and the target device(s).
- If Management Center is configured with a server certificate issued by a Certificate Authority, ensure that the certificate chain is added to the "management-center" CA Certificate List.
- Verify that the image being installed is associated with the correct device type.
- Check Management Center and target device logs for errors.
View Effective Policy for each Slot on a Device

Effective Policy is the policy that will be applied to the device in situations where more than one policy could be applied. For example, administrators sometimes inadvertently assign a policy to a specific device and a different policy to the group that device resides in. The Effective Policy shows the policy that takes precedence—in this case, the device-specific policy.

1. From the Network tab, select a device to view the effective policy.
2. Click Edit.
3. From the Edit Device dialog, select the Policies tab.

Five slots are displayed under Effective Policy. The fields are not editable and are grayed out. However, the Tenant Policies slot can have many more than one tenant policy per tenant slot. The slots are organized as follows:

- **VPM** - The VPM slot is a unique policy created by Visual Policy Manager.
- **Local**
- **Central**
- **Forward**
- **Tenant Policies** - The Tenant Policies slot included policy for every tenant that will be passing traffic through the ProxySG appliance.

**How the effective policies are assigned**

- Direct assignment - The policy was installed directly to the slot.
- Inherited from [Device Group Name] - The policy was inherited from device group that the device membership is from.
- CPL Policy is displayed in the following slots:
  - **Merged** - Because there can be thousands of tenants passing traffic through the device, no specific mapping of the tenant policies to the slot is possible. As a result, if there are 2 or more tenant policies mapped to the slot, the policies display as Merged.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group.</td>
<td></td>
</tr>
<tr>
<td>View information about the device.</td>
<td></td>
</tr>
<tr>
<td>Choose Operations for a Device or Device Group.</td>
<td></td>
</tr>
<tr>
<td>Edit device attributes.</td>
<td></td>
</tr>
<tr>
<td>Edit policy attributes.</td>
<td></td>
</tr>
</tbody>
</table>

**Compare the Device Policy Version with Current Policy Version**

You can compare the policy version installed on the device with the current policy version that is stored in Management Center. This can help you determine if you the desired policy version is installed on the device.

1. Select **Configuration > Policy** and click the policy to open the editor.
2. Click the **Targets** tab.
3. Select the target device and click **Compare**.
Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>View all of the details about an existing policy, including policy object information, the policy version, and the associated attributes.</td>
<td>View Existing Policy Information</td>
</tr>
<tr>
<td>Compare different versions of the same policy.</td>
<td>Compare Different Versions of the Same Policy</td>
</tr>
</tbody>
</table>

Launch a Device Console

Management Center offers a central location from which you can open the console of any managed Symantec device so that you can make immediate configuration changes on the device. This topic applies to all managed devices.

Launch Device Console

1. Select the **Network** tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. Do one of the following:
   - From the **Operations** drop-down list, click **Launch Console**.
   - Click the device link to edit the device and select **Operations** > **Launch Console**.
4. Log in to the device.

Launch ProxySG/ASG Admin Console

Management Center 2.4x and later support the new Admin Console available on ProxySG or Advanced Secure Gateway (ASG) appliances running SGOS 6.7.4 or later. To use the Admin Console, you must first install the package. For more information, see [Install the ProxySG Appliance Admin Console](#).

1. Select the **Network** tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. Do one of the following:
   - From the **Operations** drop-down list, click **Launch Console**.
   - Click the device link to edit the device and select **Operations** > **Launch Console**.
4. Select an Admin Console package in the **Console** field. If you have more than one Admin Console version installed, the system displays the compatible versions so you can select the desired version to use.

5. Log into the device. Choose the authentication method—**Automatic** or Manual (**Specify Credentials**).
NOTE
To log into the ProxySG Admin Console automatically, provide users with the **Device Console (auto login)** permission.

6. Click **Configure** to display the Admin Console.

**Install the ProxySG Admin Console**

Management Center 2.4.x and later include support for the new ProxySG Admin Console. The improved Admin console does not require Java and has been redesigned to help you complete tasks more efficiently. It is supported on both the ProxySG and Advanced Secure Gateway (ASG) appliances.

To use the new Admin Console, you must first download the installation package from the Management Center or ProxySG/ASG appliance Software Download site on the Broadcom Support site. The packages are signed to ensure their integrity. Management Center validates the package signature when you install the package.

**NOTE**
If this is your first time using the Admin Console, refer to the SGOS Release Notes and Administration Guide for your version to learn about features, known issues, and bug fixes.

**Admin Console Requirements**

- Available only on ProxySG and ASG appliances running 6.7.4 and later.
- To login automatically to the Admin Console, users must have the **Device - Console (auto-login)** permission.
- To provide users with read-only or read-write privileges, assign the **Device - View** or **Device - Manage** permissions. See **Grant Permissions** for more information.

**Admin Console Notes**

If Public Key authentication is enabled, you will be prompted to enter the device's admin credentials when accessing advanced URLs with the Admin Console.

**Step 1—Download the Admin Console Installation Package**

1. Go to [https://support.broadcom.com/security](https://support.broadcom.com/security) and log in with your Broadcom credentials.

   **NOTE**
   Refer to the following content for more information:
   - Symantec Getting Started

2. Follow the instructions in **Download Symantec Software and Tools**.

3. If you intend to install the installation package from a URL, copy the URL of the installation package. Otherwise, download the installation package.

**Step 2—Install the Installation Package on Management Center**

1. Select **Administration > Packages**.
2. Add the file using one of the following methods:
   - **Browsing**:
     a. Click **Add Package**.
     b. Click **Select File** and browse to the file(s).
     c. Select the file.
     d. Click **Open**.
Step 3—Launch the Admin Console

To launch the Admin Console, see Launch a Device Console.

Access the CLI of a Managed Device

Management Center offers a central location from which you can open a CLI shell of a managed Symantec device so that you can make immediate configuration changes on the device.

NOTE
You can also Access the Management Center CLI.

Supported Devices

The following devices are supported:

NOTE
The CLI shell is not supported for use with Web Security Service, SSL Visibility 3.x, and PacketShaper.

- ProxySG and Advanced Secure Gateway (ASG)
  Automatic authentication is supported for both credentials and public-key authentication. When using public-key authentication, the user account is "director" or "management-center," depending on the SGOS version.
- DEFINE IN KEYMAP 4.x and later
- Malware Analysis
  Automatic authentication uses the "g2" username and will succeed only if the password is in sync with the user interface credentials.
- Content Analysis
- Reporter
- Security Analytics
  Automatic login is not supported because Management Center does not store the credentials.

Authentication Methods and Requirements
You can authenticate to a device’s CLI shell using the following methods:

- **Automatic authentication**
  If Management Center stores the authentication credentials, you can click **Login Automatically**. The user must have the following permissions for the device to use this option: `<Device, CLI Access (auto-login)>`
  If a user is granted permissions for automatic authentication, they can also do manual authentication.

- **Manual authentication**: Manually enter your login credentials. The user must have the following permissions for the device to use this option: `<Device, CLI Access>`

**Access a Device’s CLI**

1. Select the **Network** tab.
2. In the left pane, select the device group, and then select the device in the right pane.
3. Select one of the following:
   - From the **Operations** drop-down list, click **Open CLI Shell**.
   - Highlight the device, right-click and select **Open CLI Shell**.
   - Click the device. In the device details page, Click the **Operations** drop-down list and select **Open CLI Shell**.
     A new browser window opens.
4. Examine the device's host key to ensure the connection has not been compromised.

   If Management Center has stored the host key information and can verify it, the system displays a green check mark and this text: **Management Center has confirmed the authenticity of the device connection.**

   **NOTE**
   Currently, Management Center only stores the host key information for the ProxySG and ASG appliances.
   If Management Center does not store the host key information, it displays the information, along with this message: **Management Center has no recorded host key for this device and so cannot verify the secure connection to the device. Before continuing, confirm that the device fingerprint matches the expected fingerprint.**
5. Log in to the device.

   Device authentication requires specific user permissions. See **Requirements**.

**Compare Device Configurations**

The **Jobs > Compare Config** job compares the configuration settings of managed devices to those on a "golden" device. The report displays the configuration options that are not identical. The job results are saved to **Jobs > Archived Files**.

**Supported Devices**

The **Compare Config** job supports the following devices:

- ProxySG appliance
- Advanced Secure Gateway
- Content Analysis
- SSL Visibility 4.x
- Malware Analysis

**Compare Device Configurations**

1. Select **Jobs > Add > New Job** and click **Compare Config**.
2. **Configuration**:
   - Select the source device or source file to be used as the "golden device" for comparison.
Source File: Use the Save Config job to save device configurations as a JSON file to be used as the source file for the comparison. See Save Device Configurations for more information.

NOTE
If you have saved a configuration file and the system does not show it in the file list, download the file from the file archive and upload it to Management Center (see Upload Files to Management Center).

– Determine whether to compare devices with different software versions.

NOTE
When selecting this option, you must carefully review the job results because they will likely include false positives. This is because the configuration structure can differ between device versions.

– Enter the JSON paths to include or exclude, or select individual configuration sections. Use hard returns to enter multiple JSON paths.

If you are not familiar with the JSON paths available in your device configuration, select all of the sections. Then, run the job and view the saved configuration file to determine if additional filtering is required. JSON paths are entered using standard JSON path expressions. For example, enter $.Policy to specify the Policy node at the root level.

The JSON paths you enter override in the Paths to Include section overwrite any of the selected categories. For example, if you enter $.Auth and have selected Tenants, Policy Slots, and PKI in the Sections to Compare, only the Auth configuration will be saved. All categories are ignored.

If you enter one or more JSON paths in the Paths to Exclude section, the checkboxes in Sections to Compare are used, with the exception of any specified in the Paths to Exclude.

3. Targets:
Select the devices or groups to compare to the source device. The selected devices must be running the same system image as the source device.

– Select the Devices or Groups tab.
– Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
– Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
– If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
– All selected targets appear in Selected Targets.

4. Job Results:
– (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).

5. Schedule:
Choose to trigger job execution using a Schedule or an Event.

Schedule
Use Schedule when you want to run the job now or to execute the job at a specific time.

– Immediate—automatically runs the job after it is created.
– No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
– Run Once Only—specify the date and time to run the job.
– Periodic—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
– Daily—runs the job every day at the specified time.
– Monthly—runs the job once a month on the specified day of the month and specified time of day.

See also Job Scheduling Options.

Event
Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
– Device added to Management Center
– Device added to Group
– Device removed from Group

If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

6. **Name:**
   – Verify or change the name and add an optional description.

7. Click **Save**.

**View Job Results**

When you run the job, the Job Progress window displays the status of the job. If there are configuration differences, the **Status** shows **Completed with warnings**. To view details about the differences:

1. Select **Jobs > Archived Files**.
2. Select the job and click **Download**.
3. Open the zip file downloaded by your browser.
4. Open the HTML file and review the configuration differences—highlighted in the file.

**Viewing Notes**

- Identical sections are omitted for the sake of brevity.
- Additions, omissions, and changes are highlighted in green, yellow, and red.
- Arrays only include items that differ.

**Set Boot Image**

Create a job to specify the default system image. The job installs the system image and waits for the device to reboot so that it can verify the correct image is installed before reporting success or failure.

**NOTE**

If the specified image is already set as the default image or is running, the device will not reboot.

**Supported Devices**

This job is supported only for the following devices:

- Advanced Secure Gateway
- Content Analysis 2.x and later
- ProxySG
- SSL Visibility 4.x and later

**Create Boot Image Job**

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Set Boot Image**.
3. **Configuration**:
   – Select the device type for which you are going to set the boot image. The system displays compatible devices in the **Targets** section.
4. **Targets:**
   – Select the Devices or Groups tab.
   – Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   – Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   – If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   – All selected targets appear in Selected Targets.
You can select a device group of mixed devices; the system extracts the devices that match your selection (supported device type and version).

5. **Image:**
   – Select the system image to boot.
   – The system displays all images stored on the selected target devices.
   – If a device does not have the selected image, a warning is displayed; the job will still run successfully, skipping those devices.
   – If a device already has the selected image installed, installation is skipped.

6. **Job Results:**
   – (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).

7. **Schedule:**
   Choose to trigger job execution using a Schedule or an Event.
   **Schedule**
   Use Schedule when you want to run the job now or to execute the job at a specific time.
   – Immediate—automatically runs the job after it is created.
   – No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
   – Run Once Only—specify the date and time to run the job.
   – Periodic—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
   – Daily—runs the job every day at the specified time.
   – Monthly—runs the job once a month on the specified day of the month and specified time of day.
   See also Job Scheduling Options.
   **Event**
   Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   – Device added to Management Center
   – Device added to Group
   – Device removed from Group
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

8. **Name:**
   – Verify or change the name and add an optional description.

9. Click **Save**.

**Integrated Secure Gateway Support**

Management Center includes the following support for ISG appliances:
• Basic metrics, for example, CPU and memory.
• Image management: Download of images from Management Center; setting boot image.
• Restart
• Restore factory defaults.
  
  **CAUTION**
  Network settings are not preserved.

• Web CLI shell.
• CLI scripting.

**RMA a Device**

If you need to return a device to Symantec using Return Merchandise Authorization (RMA), follow the procedure below to replace the defective device with the replacement device in Management Center. This procedure assumes you have initiated the RMA process with Symantec.

1. Record the serial number of the defective device. You will need this number when performing the **RMA Device** operation below.
2. (Optional) Deactivate the defective device. See **Activate or Deactivate a Device**.
   
   **NOTE**
   Deactivated devices show on the Network tab with a gray status. If you don't deactivate the device, it will show on the Network tab with a red status.
3. Return the defective device to Symantec.
4. Install the replacement device in the network. If you assign it the same IP address and credentials, you do not need to add the device into Management Center; otherwise, you will need to **Add a Device**.
5. Go to the **Network** tab and select the replacement device.
6. From the **Operations** drop-down list, select **RMA Device**.
   
   **NOTE**
   Management Center will attempt to connect to the device and retrieve its serial number. If it succeeds, it will display it next to **Serial Number detected on device**.
7. In the **Provide previous Serial Number** field, enter the serial number of the defective device.
8. (ProxySGs only) Decide whether you want to apply existing Statistics Monitoring data from the defective device and migrate it to the replacement device. Select the desired option:
   – migrate Statistics Monitoring data
   – ignore Statistics Monitoring data

9. Click Update Device.
10. From the Operations drop-down list, click Restart.

**View Security Analytics API Key**

The Security Analytics API key is used for web services APIs. It is not visible on the web UI by default.

For more information about this procedure, refer to the Security Analytics documentation.

**Retrieve the API key**

- Navigate to the Security Analytics appliance.
- Log in to the Security Analytics appliance with the account that you wish to use for Management Center authentication.
- Select Account Name > Account Settings and click Reset API Key to view and copy the API key.
- In the Account Settings dialog, click Reset API Key to view and copy the API key.
- After you close the Account Settings dialog, the API key will not be available again. You must click Reset API Key to generate a new key.
- When you click Reset API Key, the previous API key is deleted.
- A new user account does not have an API key until the user logs in to the web UI, opens Account Settings, and clicks Reset API Key.

**Reference: Device Communication**

This topic describes Management Center to device communication.
ProxySG Appliance SSH Ciphers
Management Center uses the following ciphers for SSH communication with the ProxySG appliance:
- aes256-ctr
- aes192-ctr
- aes128-ctr
If you cannot add a ProxySG appliance because it is in FIPS mode and the ciphers used are not on Management Center, use one of preceding ciphers on the ProxySG appliance.

All Other Appliances
Management Center uses HTTPS to communicate with all devices except the ProxySG. Management Center restricts communication to the TLSv1.1 and TLSv1.2 protocols and a variety of ciphers that use:
- ECDHE/DHE key exchange
- RSA/DSA certificate authentication
- 128 – 256 bit AES stream cipher with optional CBC/GCM modes
- SHA – SHA384 message authentication

Supported Key Exchange in Management Center Operations that use SSH/SCP
Management Center supports the following key exchange algorithms for SSH/SCP connections:
- DHGex
- DHG
- Curve25519
If a user attempts to export a backup to a server using SCP and the target server does not support the at least one of the preceding key exchange algorithms, the export may fail with the message A connection could not be established or The secure handshake failed during key exchange. This applies to any operation using SSH/SCP, for example, importing backups.

Back Up Device Configuration Now
Management Center allows you to initiate and automate the configuration backup of supported devices. You can select one or more devices or device groups to back up immediately or schedule a job for the backup.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

**NOTE**
To schedule device backup, see Schedule Device Back Up.

1. From the **Network** tab, select the supported devices or device groups to back up.
2. From the **Operations** drop-down list, select **Backup Devices**. The devices that you selected appear in the **Selected** list.
3. Click Next. The system displays the **Backup Devices: Image Settings** screen.

4. Enter the **Backup Name** and **Backup Description**. Optionally, you can use variables, as shown in the following graphic. (See Use Device Information for Backup Job Image Metadata.)

5. To include private key data in the backup, select **Include Private Data**. Currently, only the ProxySG and SSL Visibility appliances support this feature; the option is ignored for other device backups. For the ProxySG appliance, key rings can only be backed up if they were configured to show **Show key**
pair option) when created. Keys that were not configured to show are not included in backups, even if Include Private Data is selected.

Note: Completed backups that include private key data include pki in the content details. ProxySG example:

<table>
<thead>
<tr>
<th>Content Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>full-pki</td>
</tr>
<tr>
<td>full</td>
</tr>
</tbody>
</table>

6. To secure the backup with the data protection key, select Encrypt Backup. Encrypted backups are only decrypted when the information is sent to the device. When you view the encrypted backup using the preview tab, only the encrypted data shows.

CAUTION
Changing the Encryption Key may make any backups unrecoverable. See Encrypt Sensitive System Data for more information.

7. Do one of the following:

- To immediately begin the backup of the selected devices, select Run Now.
- To execute the backup of the selected devices at a later time, select Create Job... See Schedule Device Back Up, for more information.

Next Steps

<table>
<thead>
<tr>
<th>Task</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the configuration backups for a device and view the content of a backup file</td>
<td>View Device Backups</td>
</tr>
<tr>
<td>Restore a device configuration</td>
<td>Restore Device Backups</td>
</tr>
<tr>
<td>Export a device backup</td>
<td>Export Device Backups</td>
</tr>
<tr>
<td>Import a device backup</td>
<td>Import Device Backups</td>
</tr>
</tbody>
</table>

Regularly Back Up a Group of Devices

To be able to restore or roll back a configuration in case it gets corrupted, you need to back up your configurations on a regular basis. In this example, we will back up a device group on a weekly basis, during a time when the network is less busy (such as a weekend).

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Create a device group for the devices you want to back up on a schedule. See Add a Device Group.
2. Create a Backup Device job. Select the device group you created in step 1, and schedule the job to run on a Periodic basis, every 7 days starting on a weekend day. See Schedule Device Back Up.
3. Verify the backups are being created for each device in the group. See View Device Backups.
4. Restore a backup when necessary. See Restore Device Backups.
Use Device Information for Backup Job Image Metadata

Administrators can control the name and description of the backup created by a job (based on the specific device that is backed up). To use the device information in a backup job, administrators need to start a backup job from the **Network** tab rather than the **Jobs** tab.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Select a device from the **Network** tab.
2. From the **Operations** drop-down list, select **Backup Devices**. Select the device(s) to back up.
3. Click **Next**. The web console displays Backup Devices: Image Settings dialog 'Manual Backup (04/04/15)' in the Backup Name field.

   ![Backup Devices: Image Settings](image)

   Although the backup name is shown as mandatory, use **Variable Substitution** to replace the words 'Manual Backup'. In the example shown, the device name variable will be replaced when the job is run.

   **TIP**

   Use `${today}` in the **Description** field of the backup to display the date that the backup is run. If you run the backup now, today's date displays in the backup description.

4. Click **Run Now**. The Job Progress dialog displays the backup while it runs.
5. Select **Continue in Background** or click **Close** when the backup **Status** is Complete.

**View Backups**

View backups from the **Backup** tab of the device.
View Device Backups

For any device whose configuration you have backed up, you can view a list of backup files as well as view the content of the backup files. Once the list is displayed, you can delete or restore the backups.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

1. Click the Network tab.
2. Select a device group in the left pane, then select the device and click the device name hyperlink or click Edit. 
   
   **NOTE**
   
   To configure the maximum number of backups stored per device, see Set the Number of Backup Slots.

3. In the device editor, select the Backup tab. The web console displays all of the successful backups, including each backup's name, description, date/time of the backup, device type, OS version, date/time it was last exported, and date/time it was last restored.
4. Select a backup from the list.
5. Click View. The Manual Backup Viewer displays the backup in a text editor.
6. If the backup exceeds the text editor limit, a warning displays:

   ![Warning Image]
   
   Click Download. The file will download to your local Downloads folder. When the file is finished downloading, you can open it in Notepad or other text editor.
7. To pin or unpin a backup, click in the Pinned column. A checked box appears on pinned backups. A pinned backup cannot be manually deleted or automatically pruned (replaced with another backup).
8. To delete an unpinned backup, select it and click Delete.
9. To apply a particular backup configuration to the device, select it and click Restore. See Restore Device Backups for more information.

Restore Device Backups

When you restore a device backup, Management Center replaces the device's current configuration with the backed up configuration. You can restore a configuration immediately, or schedule the restore for a late date.
Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

**Restore Backup Immediately**

1. Select the **Network** tab.
2. Select a device group in the left pane, and then select the device in the right pane.
3. Select **Edit**, then the **Backup** tab in the editor.
4. In the list of backups, choose the backup version you want to restore.
   
   **NOTE**
   
   If the backup you want to restore isn't listed, it's possible that it was exported and pruned from the appliance. In this case, you would need to import the backup before you can restore. See Import Device Backups.
5. Click **Restore**. The web console displays the Restore Configuration dialog that displays the following information:
   
   - **Device** - The device name
   - **Backup Image** - The name of the backup
   - **Description** - The description given at the time that the backup was made
   - **Created** - The date and time of the backup
   - **Last Restored** - The date and time that the backup was last restored
6. To restore the configuration immediately, click **Restore**. The system displays the running/completed job and more details about the job.
7. (Optional) To view the contents of the backup (configuration), click **View Contents**.
8. (Optional) To view the device output from the restored backup:
   
   a. Select **more details**. The Device Output dialog displays the number and type of warnings.
   
   b. You can navigate in between the errors and warnings.
   
   c. Select **Download as Text** or **Close**.

**Schedule Device Backup Restore**

1. Select the **Network** tab.
2. Select a device group in the left pane, and then select the device in the right pane.
3. Select **Edit**, then the **Backup** tab in the editor.
4. In the list of backups, choose the backup version you want to restore.
5. Click **Restore**, then **Create Job**.
6. **Backup**:
   
   - Verify the details of the backup. To view the contents of the backup (configuration), click **View Contents**.
7. **Job Results**:
   
   - Optional—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).
8. **Schedule**:
   
   Define a schedule for the job. See Job Scheduling Options for more information.
   
   - **Immediate**—automatically runs the job after it is created
   - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to manually execute the job
   - **Run Once Only**—specify the date and time to run the job
   - **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date
   - **Daily**—runs the job every day at the specified time
   - **Monthly**—runs the job once a month on the specified day of the month and specified time of day
9. **Name**:
   
   - Verify or change the name and add an optional description.
10. Click **Save**
Schedule Device Back Up

Management Center allows you to initiate and automate the configuration backup of supported devices. This job backs up the configuration of the selected device(s) on a defined schedule; any supported type of device can be backed up.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

**TIP**
See also Back Up Device Configurations.

1. Select Jobs > Add > New Job.
2. On the Add New Job page, select Backup Device.
3. Configuration:
   - Enter the **Backup Name** and **Backup Description**. Optionally, you can use variables, as shown in the following graphic. (See Use Device Information for Backup Job Image Metadata.)

   ![Backup Device Configuration](image)

   **Note:** Completed backups that include private key data include `pki` in the content details. ProxySG example:

   ```
   Content Details
   full-pki
   full
   ```
• **Encrypt Backup**: Secures the backup with the data protection key. Encrypted backups are only decrypted when the information is sent to the device. When you view the encrypted backup using the preview tab, only the encrypted data shows.

**CAUTION**
Changing the Encryption Key may make any backups unrecoverable. See [Encrypt Sensitive System Data](#) for more information.

4. **Targets**:
   - Select the **Devices** or **Groups** tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   - All selected targets appear in **Selected Targets**.

5. **Job Results**:
   - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. **Schedule**:
   Choose to trigger job execution using a **Schedule** or an **Event**.

   **Schedule**
   - **Use Schedule** when you want to run the job now or to execute the job at a specific time.
     - **Immediate**—automatically runs the job after it is created.
     - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
     - **Run Once Only**—specify the date and time to run the job.
     - **Periodic**—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
     - **Daily**—runs the job every day at the specified time.
     - **Monthly**—runs the job once a month on the specified day of the month and specified time of day.
   See also [Job Scheduling Options](#).

   **Event**
   - **Use Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
     - **Device added to Management Center**
     - **Device added to Group**
     - **Device removed from Group**
   If you select more than one event type, the job runs if **any** of the conditions are met and the device is an appropriate target. See the following note.

7. **Name**:
   - Verify or change the name and add an optional description.

8. Click **Save**.

**Next Steps**

<table>
<thead>
<tr>
<th>Task</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the configuration backups for a device and view the content of a backup file</td>
<td>View Device Backups</td>
</tr>
<tr>
<td>Restore a device configuration</td>
<td>Restore Device Backups</td>
</tr>
<tr>
<td>Export a device backup</td>
<td>Export Device Backups</td>
</tr>
</tbody>
</table>
Export Device Backups

The Export Backup operation allows you to copy or move configuration backups to an external server. Copying backups to another server provides extra insurance by essentially creating a backup of a backup. Or, if you move the backups off Management Center and put them on an external server, you can make room for more backups on the Management Center appliance.

Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored.

NOTE
Management Center supports the following key exchange algorithms for SSH/SCP connections: DHGex, DHG, and Curve25519. If a user attempts to export a backup to a server via SCP and the target server does not support at least one of those key exchange algorithms, the export may fail with the message A connection could not be established or The secure handshake failed during key exchange. This also applies to other Management Center operations that use SSH/SCP.

Enter a unique name and a description for the Export. Click Next.

1. Navigate to the New Job: Export Backup page using one of the following methods:
   – Select Network and a device or a device group whose configuration backup you want to export. Then select the Operations drop-down list and click Export backups. If you have configured a location for the backup already, Management Center immediately exports the backup to the configured location. However, if you have not configured a location for the backup, the New Job wizard begins, displaying the New Job: Basic Info dialog.

2. Configure the job options:
   – Export to Server(*) - Enter the server location using FTP, HTTP, HTTPS, or SCP.
   – Username - Enter the server username.
   – Password - Enter the password for this user.
   – Backups to Include:
     • Not Yet Exported: Include backups that have never been exported.
     • Previously Exported: Include backups that were previously exported.
     • Prune Backups: Remove the backups from the backup slots after exporting the backups. You are essentially moving the backups if you select this option. If you leave this option cleared, you are copying the backups to an external server.
   – Retention Count(*) - Enter the number of backups to keep for each device. This overrides the default number of backup slots configured per device. (See Set the Number of Backup Slots.)
   – Prune Pinned - Select this option to remove backups, even if they have been pinned (locked).

3. Targets:
   – Select the Devices or Groups tab.
   – Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   – Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   – If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   – All selected targets appear in Selected Targets.

4. Job Results:
   – (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).
5. **Schedule:**
   Choose to trigger job execution using a **Schedule** or an **Event**.
   
   **Schedule**
   Use **Schedule** when you want to run the job now or to execute the job at a specific time.
   - **Immediate**—automatically runs the job after it is created.
   - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
   - **Run Once Only**—specify the date and time to run the job.
   - **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
   - **Daily**—runs the job every day at the specified time.
   - **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

   **Event**
   Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   - **Device added to Management Center**
   - **Device added to Group**
   - **Device removed from Group**
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

6. Define when you want to schedule the export to occur or select **Run Now** to export the configurations immediately. See **Job Scheduling Options**.

7. **Name:**
   - Verify or change the name and add an optional description.

8. Click **Save**.

### Import Device Backups

From the Management Center **Network** tab, you can import device backups that you have previously exported. You may want to do this so you can restore an exported backup that has been pruned from Management Center.

**NOTE**
Backups created while a device is in FIPS mode cannot be imported to a device that is not in FIPS mode. Conversely, standard backups (non-FIPS mode) cannot be imported to a device in FIPS mode.

**NOTE**
SNMP trap settings are not backed up or restored.

### Supported Devices

Management Center supports configuration backup/restore/import/export of the following device types:

- ProxySG
- Content Analysis
- Malware Analysis
- SSL Visibility
- Content Analysis 2.1

1. Click the **Network** tab. Select a device from a device group.
2. From the **Operations** drop-down list, click **Import Backups**. The web console displays the Import Backups dialog.
3. From the Import dialog, select one of following:
– **Import from local file**: If the file is stored on a local system, browse to the backup file.
– **Import from server**: If the file is stored on a web, FTP, or SCP server, define the URL path to the file and server credentials.
  - **Download URL**(*) - Enter the URL using HTTP, HTTPS, FTP, or SCP.
  - **Username** - Enter the server username.
  - **Password** - Enter the password for this user.

4. **Replacement Strategy**(*): Select **All** or **As Required**.
   – **All**: Replaces all of the existing backups with the backups that you are importing.
   – **As Required**: Takes into account how many slots that you have provisioned for device backups in **Administration > Settings > General**. If the maximum number of device backup slots is 10, and you have eight backups that are pinned (locked) and you are importing three backups, then Management Center will attempt to satisfy the requirement to replace three backups. As a result, only two backups will be imported because only two backup slots are available.

5. You can prune (delete) backups when exporting to a server, and you can do the reverse when importing backups by overwriting pinned backups. Select the **Replace Pinned Backups** check box. (You can pin backups from the Backup tab. See [View Device Backups](#).

6. Click **Import**.

**SSL Visibility Appliance - What is Backed up and Synchronized?**

This page describes the SSL Visibility appliance configuration items that are backed up or synchronized.

**Policy**
- FIPS configuration and version
- Policy versions
- System options
- Rulesets
- Lists (IP address, cipher suites, certificates, etc.)

**PKI**
- FIPS configuration and version
- RSA and ECDH data
- Certificate authority data
- Trusted and known certificate data
- HSM data

**Users**
- Usernames
- Passwords
- Roles
- User IDs
- FIPS configuration and version
Platform

- Version information
- FIPS configuration and version
- Network settings
- NTP settings
- Remote logging settings
- SNMP settings
- Login banner settings

Alerts

- Mail configuration and roles
- FIPS configuration and version

Remote authentication

- TACACS settings

Add a Device Group

A device group is a folder in the device organizational structure that exists below the hierarchy level and contains devices or sub-folders.

**NOTE**
You can also add a cluster, which represents a group of services bundled in a chassis or in AWS or Kubernetes auto-scaling groups.

1. Select the **Network** tab. In the left pane, select the hierarchy in which you want to create the device group.

2. (If applicable) Browse to the folder in which you want to create the device group. Select **Add Group**.
3. On the **Add Group: Basic Info** dialog, enter a name and a description.
4. Select a parent group from the **Parent Group** drop-down list. Click **Next**.
5. On the **Add Group: Attributes** dialog, use the up/down arrows to specify Bandwidth Cost. Bandwidth Cost is a multiplier and is thus not expressed in a specific currency unit. For example, you can enter a value to represent on average how you pay per gigabit for data usage on your network. See Bandwidth Cost for Reports.
6. (Optional) Specify your Primary Contact for the device group, as well as the Location device group and the sub-group.
7. Click **Next**. The Add Group wizard displays the **Add Group: Membership** window.
8. Select devices from the **Available Devices** list and add them to the **Associated Devices** list.
9. Click **Finish**. The new device group is displayed under the network tab. If you cannot see the new device group, select **Unassigned Devices**. See also **Ensure Devices Belong to Device Groups** or **Configure Hierarchy for Devices and Device Groups**.

**TIP**
You can define attributes for a particular a device, device groups policy and script objects. See **Manage Attributes**.

### Edit a Device Group

You can edit any device group, including the system's predefined parent groups (the top-level folders in the Location and Organization hierarchies).

1. Select the **Network** tab.
2. In either Tiles view or Details view, browse to the parent folder of the group you want to modify.
3. Select the group and click **Edit**. The web console displays the Edit Group wizard.
4. Edit the information on each tab as required:
   - **Basic Info** - Change the device group name and description.
   - **Attributes** - Under System, change the statistics collection option and bandwidth cost. For information on the User-defined attributes, see **Filter Devices or Device Groups in a Permission**.
   - **Membership** - Add or remove devices.
5. Click **Save**.

### Ensure Devices Belong to Device Groups

Symantec recommends that you periodically verify that all devices are assigned to groups. A device might become unassigned if no groups were selected when the device was added to Management Center, or if the groups to which the device was assigned were deleted. See **Edit a Device Group**.

Because unassigned devices do not display in any groups, users might not manage them or even be aware of them if they work only in device groups or only have access to specific device groups in their role filters.
NOTE
A device group can be inside another device group, but a device group cannot be in multiple hierarchies.

1. Click the Network tab. From the left pane, click Unassigned Devices. Unassigned devices display in the right pane.
2. Select a device you want to assign to groups and click Edit. The web console displays a wizard with the following tabs:
   – Basic Info
   – Connection Parameters
   – Membership
   – Attributes
   – Policies
   
   NOTE
   An error message displays at the bottom, citing the reason why the device is not assigned to a device group.

3. Click Membership. Enter a location for the device.
4. Click Save. A message stating: [device name] was saved successfully.
5. (Optional) To assign by dragging and dropping the device to a device group, select the device and drag it into the device group into the tree on the left. Drop the device. Confirm the move. Click OK.

Drag and Drop Device Groups
A device group is a folder in the device organizational structure that exists below the hierarchy level and contains devices or sub-folders.

1. Click the Network tab. Select a device group. While holding the mouse, drag the device group into another device group or hierarchy.
   
   NOTE
   Device groups cannot be unassigned and will be ignored if you drop them outside of the Device Group.

2. When you drop the group, confirm the move by clicking OK.
   
   NOTE
   While you are dragging the selected device group, the message that hovers over the pointer changes according to where Management Center perceives that you are dropping the device group. See Move Items.

Add a Group to Represent Chassis or Cloud Services (Device Cluster)
A device cluster is a special type of group that represents a group of services bundled in a chassis or in some virtualization auto-scaling environment such as AWS. In addition to organizing devices, a cluster can store meta data about how a device operates within that group. When AWS autoscaling or other software is managing the devices in the
cluster, that software will communicate cluster membership information directly to Management Center—users will not be able to change cluster membership.

All operations that can be performed on a group also apply to clusters, with the following restrictions:

- A device can only be assigned to one cluster.
- A cluster must stand alone. It cannot be inside another cluster. One or more groups can be put inside a cluster, however.

**Procedure—Add Device Cluster**

1. Select the **Network** tab. In the left pane, select the **hierarchy** in which you want to create the device cluster.

2. (If applicable) Browse to the folder in which you want to create the device cluster. Select **Add Cluster**.

   **NOTE**
   This system does not display the **Add Cluster** option unless the **Folders** option is enabled.

3. In the **Add Cluster: Basic Info** dialog, enter a name and a description.

4. Select a parent group from the **Parent Group** drop-down list. Click **Next**.

5. In the **Add Cluster: Attributes** dialog, use the up/down arrows to specify Bandwidth Cost. Bandwidth Cost is a multiplier and is thus not expressed in a specific currency unit. For example, you can enter a value to represent on average how you pay per gigabit for data usage on your network. Set **Bandwidth Cost for Reports**.

6. (Optional) Specify your **Primary Contact** for the device group, as well as the Location device group and the sub-group.

7. Click **Next**. The Add Cluster wizard displays the **Add Cluster: Membership** window.

8. Select devices from the **Available Devices** list and add them to the **Associated Devices** list.

9. Click **Finish**. The new device cluster is displayed under the network tab. See also **Ensure Devices Belong to Device Groups** or **Configure Hierarchy for Devices and Device Groups**.

   **TIP**
   You can define attributes for a particular a device, device groups, clusters, and policy and script objects. See **Manage Attributes**.

**Add Device Group Attributes**

Device Group attributes are **Primary Contact** or **Location** or are custom attributes that you create.

1. Select the **Administration > Attributes** section.

2. From the **Manage Attributes** list, you can select the following:
   - **Device**
   - **Device Group**
   - **Policy**
   - **Device Script**

3. Click **Device Group**.
4. Click **Add Attribute**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description or Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name (*)</td>
<td>Name that displays throughout Management Center.</td>
</tr>
<tr>
<td>Name (*)</td>
<td>This name contains underscores if spaces are used in the Display Name.</td>
</tr>
<tr>
<td>Type (*)</td>
<td>Boolean, String, Decimal, Date, Pick List</td>
</tr>
<tr>
<td>Note:</td>
<td>Depending the <strong>Type</strong> that you choose the remaining properties will differ.</td>
</tr>
<tr>
<td>Format (*)</td>
<td>Alpha, alphanumeric, Email, Phone, Text, URL, World Phone</td>
</tr>
<tr>
<td>Min Length (*)</td>
<td>Set a numeric value as the Minimum Length of this attribute (starting with 0). It must be a smaller numeric value than the Maximum Length.</td>
</tr>
<tr>
<td>Max Length (*)</td>
<td>Set a numeric value as the Maximum Length of this attribute (1024 character limit). It must be a larger numeric value than the Minimum Length.</td>
</tr>
<tr>
<td>Default Value</td>
<td>The Default Value is required when you create or edit a device group.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Restricts the device attribute to the specified device type. The default is <strong>All Device Types</strong>.</td>
</tr>
<tr>
<td>Note:</td>
<td>The Device Type property applies only to device attributes. If you add a value to an attribute on a device and subsequently change the device type, the value will be deleted from unsupported devices. The system warns you of this before you apply your changes.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>All attributes that are checked as mandatory will be mandatory when you add or edit a device. For example, if you define the Location attribute as mandatory, you will be required to enter a location.</td>
</tr>
<tr>
<td>Inheritable</td>
<td>Checking this box denotes that the device can inherit the attributes assigned the Device Group.</td>
</tr>
<tr>
<td>Description</td>
<td>Give a useful description of this attribute to distinguish it from the others when viewing all of the attributes in a list.</td>
</tr>
</tbody>
</table>

5. When you are done editing the attribute properties, click **Finish**. Your new device group attribute is saved in the Device Group Attributes list.

To use attributes that can be inherited from a group, see **Enable Attribute Group Inheritance**.

**Enable Attribute Group Inheritance**

To use attributes that can be inherited from a group, do the following:

1. Define the attribute as a **device** attribute. Mark the attribute as inheritable.
2. Edit the group that you want to assign the value to. Locate the attribute from step 1.
3. Set the desired value. Inherited variables are only supported on the default hierarchy (Device Groups). User-defined hierarchies are not supported.
4. Create a script with variable substitution.
5. Reference the substitution variable in the script as **${device.attributes.myattr}** where **myattr** is the name of the attribute you defined.
6. When the script runs, the system looks for **myattr** on the device.
If the value is not set, it looks up the group the device is associated with in the default hierarchy. It then walks the group structure looking for that value. If it finds the value, it will be replaced; otherwise, it is ignored. Group inheritance within hierarchies is described in Configure Hierarchy for Devices and Device Groups.

**Receive Alert Error Notifications**

This page describes the options on the Administration > Settings > Alerts page. Management Center generates two different types of alerts:

- Alerts for Management Center itself.
- Alerts for errors detected by Management Center on devices it is monitoring.

These alerts cause SNMP events to be raised if SNMP alerting is enabled on Management Center.

**Management Center Alerts**

The following alerts are generated for events that occur on Management Center itself (not to be confused with alerts that occur on managed devices):

<table>
<thead>
<tr>
<th>Description</th>
<th>Message Example or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal critical errors.</td>
<td>Subscription URLs are not installed. Unable to complete the subscription download process on Management Center. Currently, only the Web Application Firewall (WAF) component uses subscriptions.</td>
</tr>
<tr>
<td>Database disk quota warning.</td>
<td>Statistics Monitoring DB exceeded allowed disk quota. Collector to reject upload requests.</td>
</tr>
<tr>
<td>Errors with auditing user actions.</td>
<td>Unable to write audit record, user: &lt;username&gt;, event: &lt;action&gt;.</td>
</tr>
<tr>
<td>License errors due to duplicate serial or server avoidance.</td>
<td>License error &lt;message_string&gt;. If the system detects that a VA is being used in a way that precludes Management Center from validating the license. This is case is called “server avoidance” and results in an alert. Note: Server avoidance alerts only occur with VAs that are required to have connectivity to the Symantec license service. Hardware and special offline VA licenses are not affected.</td>
</tr>
<tr>
<td>Description</td>
<td>Message Example or Description</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>License expiration warnings.</td>
<td>Management Center health goes into a Warning state when the license is 30 days from expiring. For example, if the license will expire on January 30th, the Messages option in the web console banner displays Warning-level alerts, such as the following, starting on January 1st.</td>
</tr>
</tbody>
</table>

![License](image.png)

Component 'Device Inventory' will expire on 2018-01-30

The web console banner displays an alert for each licensed component.

Once a license expires, Management Center goes into an Error state and remains in that state for another 15 days or until the license is updated (whichever occurs first). For example, starting on January 30th, the Messages option in the web console banner displays Warning-level alerts for each licensed component until the license is renewed. Once the license is renewed, the warning is marked as complete and removed from the Alerts page. See Manage Alerts for more information.

If you do not renew the license within 15 days after the expiration date, you will be unable to load the web console. You must renew the license through the CLI using `licensing load` or see #licensing in the Configuration Management Guide for more. |
| Migration errors during an upgrade. | Migration step: `<step_name>` failed. Changes made by the step have been rolled back, but migration steps that have completed successfully have been retained. Subsequent steps have been canceled. A migration step is when the system has to update data as part of the upgrade. |
| Version repository errors. | If there is an internal error or problem starting Management Center version repository. Management Center uses this service to store:

- Device backups taken by Management Center for devices
- Device scripts
- Policy objects
- Unable to initialize the `<repository_name>` repository. |

**Alerts for Managed Devices**

These are errors that Management Center detects on a managed device. These alerts are triggered from events such as the loss of connectivity or a device taking too long to respond. The associated settings are on the Administration > Settings > Alerts page.

To enable the alerts, you must select the global option called Raise alerts on device errors. After enabling that option, you can enable or disable individual alerts or change the alert thresholds and severity.

To configure the alert, set a threshold that must be exceeded to trigger the alert and then set the severity. The severity level is what triggers alert notification. The severity can be set to INFO, WARNING or ERROR.

- If the value is set to INFO, the alert will only be recorded on the Alerts page in Management Center. *No external notification is sent.* To configure external notification, you must set the severity to WARNING or ERROR.
- If the value is WARNING or ERROR, an alert notification is sent.
**TIP**
See [Configure Alerts for Device Errors](#) for more information.

## Device Alert Events

The following events can result in alerts for managed devices (if configured):

<table>
<thead>
<tr>
<th>Description</th>
<th>Message Example or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware monitor warnings or critical errors.</td>
<td>(&lt;\text{monitor_name}) has exceeded (&lt;\text{level_name}) level of (&lt;#)%, current usage is (&lt;#)%). If one of the Hardware Monitor Setting (<a href="#">Administration &gt; Settings &gt; Hardware Monitor Settings</a>) values is exceeded, an alert is generated. You can disable these using the <strong>Monitor Enabled</strong> setting. Also:</td>
</tr>
<tr>
<td></td>
<td>• Memory Usage — When the memory utilization of the device exceeds the configured threshold. A distribution metric is used to prevent a short term spike from causing an alert.</td>
</tr>
<tr>
<td></td>
<td>• CPU Usage — When the CPU utilization of the device exceeds the configured threshold. A distribution metric is used to prevent a short term spike from causing an alert.</td>
</tr>
<tr>
<td>Device errors.</td>
<td>(\text{Device Health Response Time} — \text{On average, the time it takes for a device to reply with its health status exceeds the configured time.})</td>
</tr>
<tr>
<td></td>
<td>(\text{Device Details Response Time} — \text{On average, the time it takes for a device to reply with its details (OS, name, etc.) exceeds the configured time.})</td>
</tr>
<tr>
<td></td>
<td>(\text{Device Connection Failure} — \text{The number of consecutive times a device has a connection failure, meaning we could not establish a connection or it failed to respond at all.})</td>
</tr>
<tr>
<td></td>
<td>(\text{Error Health Check} — \text{The number of consecutive times a device reports a health check error. For example, a ProxySG appliance's DNS lookup is failing.})</td>
</tr>
<tr>
<td></td>
<td>(\text{Warning Health Check} — \text{The number of consecutive times a device reports a health check warning.})</td>
</tr>
<tr>
<td>Device license errors.</td>
<td>(\text{Raise alert whenever a device's license (or any of its sub-components) are about to expire. The warning shows within 30 days of the expiration.})</td>
</tr>
<tr>
<td></td>
<td>(\text{License component} &lt;\text{component_name}, for device} &lt;\text{device_name}, has, or will, expire on} &lt;\text{date}&gt;.)</td>
</tr>
<tr>
<td></td>
<td>(\text{If a device license expires, the warning alert closes to open an error alert.})</td>
</tr>
<tr>
<td></td>
<td>(\text{State changed from NEW to CLOSED. System closed alert because license expired.})</td>
</tr>
<tr>
<td></td>
<td>(\text{If a device license, in the warning state, is renewed, the warning alert closes because of subscription renewal.})</td>
</tr>
<tr>
<td></td>
<td>(\text{State changed from NEW to CLOSED. System closed alert because license was renewed.})</td>
</tr>
<tr>
<td></td>
<td>(\text{If a device license, in the error state, is renewed, the error alert closes because of subscription renewal.})</td>
</tr>
<tr>
<td></td>
<td>(\text{State changed from NEW to CLOSED. System closed alert because license was renewed.})</td>
</tr>
</tbody>
</table>
NOTE
You can disable all of the Hardware Monitor Settings by deselecting the Monitor Enabled setting. (Administration > Settings > Hardware Monitor Settings)

Next Steps — Configure SNMP and SMTP Notification
After configuring your alerts, you will not receive alert notification unless you configure the SNMP (System Settings > SNMP Alerts) and SMTP (System Settings > SMTP Alerts) communication settings. You must provide information for the SNMP destination and the SMTP mail server. You must also set the What to Send option to ERROR to receive alert notifications for alerts not controlled by the Administration > Settings > Alerts page. These include internal alerts within Management Center (HW failure, memory issues, and so on). See Configure SNMP Alerts and Configure SMPT Alerts for more information.

Configure SMTP Alerts
Configure the mail server for sending device health monitoring notifications from Management Center and specify which administrators receive the alerts. These settings are for sending the alerts received from managed devices, not from Management Center itself.

NOTE
These settings are different from those in the SMTP CLI command. The CLI SMTP settings are for configuring SMTP settings for Management Center core health monitoring notification.

NOTE
The message supports basic HTML formatting, which might not be supported by all email clients.

1. Select Administration > Settings.
2. Click SMTP Alerts on the left. SMTP fields display on the right.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>What to send*</td>
<td>Specify OFF to turn off e-mail notification or ERROR when errors occur with mail delivery. Note: If you select OFF, device alerts are still sent if SMTP alerting is enabled on the Administration &gt; Settings &gt; Alerts page.</td>
<td>OFF</td>
</tr>
<tr>
<td>Mail Server*</td>
<td>The SMTP mail server to use for outgoing mail.</td>
<td>Example: smtp.organization.com</td>
</tr>
<tr>
<td>Send to address*</td>
<td>E-mail addresses to which alerts are sent. For example, enter administrators' e-mail addresses or a distribution list.</td>
<td>A comma-separated list of valid e-mail addresses.</td>
</tr>
<tr>
<td>From address*</td>
<td>The e-mail address from which e-mails are sent.</td>
<td>Example: <a href="mailto:bccm@organization.com">bccm@organization.com</a></td>
</tr>
</tbody>
</table>

4. Enter the username and passphrase, if applicable.
5. Specify the variables to use in the subject line and message body. You can use the following:
   - ${severity}
   - ${priority}
   - ${category}
   - ${state}
   - ${message}
   - ${sourceType}
Shows the source of the alert, typically DEVICE but can be other sources. If the source is DEVICE, the following are available:

- ${device.name}
- ${device.model}
- ${device.host}
- ${device.name}
- ${device.type}
- ${device.osVersion}
- ${device.serialNumber}

6. Click Save to store the settings on the server. If you are unable to save your changes, make sure that all required settings are specified.

   **NOTE**
   Click Cancel to remove your current changes and revert to the default or last saved settings.

7. Click Activate to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

### Configure SNMP Alerts

If configured, an SNMP trap is sent each time an alert is generated by Management Center. These traps are sent in the Management Information Protocol (MIB) format. By default, no SNMP traps are sent.

**TIP**
For information on SNMP best practices, see Management Center: SNMP Monitoring Best Practices.

To enable SNMP traps, see Configure Alerts for Device Errors.

The Simple Network Management Protocol (SNMP) itself does not define which variables a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs).

**TIP**
The MIBs are available on the Downloads page. Refer to the Management Center Release Notes for information on MIBs.

### Restrictions

- SNMPv1 traps are not supported in Management Center 1.10.1.1 and later.

### Configure SNMP settings for Management Center

This section describes how to configure SNMP settings for Management Center. Management Center 3.0 and later support two SNMP trap notification targets. The same **Engine ID** should be used for both in SNMPv3 traps. For best practice information, refer to the Management Center 2.1 SNMP Monitoring Best Practices.

**NOTE**
If you want to enter a password for the SNMP traps, see SNMP Settings.

1. Select Administration > Settings.
2. Select SNMP Alerts.
3. Specify SNMP settings for **Trap notification target #1**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong></td>
<td>Enable/disable SNMP Alert target.</td>
<td>True/False</td>
</tr>
<tr>
<td><strong>SNMP Destination IP</strong></td>
<td>Specify an IP address for the listener.</td>
<td>Example: 192.0.2.0</td>
</tr>
<tr>
<td><strong>SNMP Destination port</strong></td>
<td>Specify the port for the listener.</td>
<td>Example: 155</td>
</tr>
<tr>
<td><strong>SNMP Version</strong></td>
<td>Specify the protocol version for the SNMP listener.</td>
<td>2</td>
</tr>
<tr>
<td><strong>Community</strong></td>
<td>A password that allows access to a device's statistics (transmitted in plaintext).</td>
<td>Enter the password. See <a href="#">SNMP Settings</a>.</td>
</tr>
<tr>
<td><strong>Engine ID</strong></td>
<td>The unique SNMP engine ID based on the device IP. This engine ID is associated with the specific Management Center installation and displays in each SNMP packet to identify the source of the packet. Applies to SNMPv3 only.</td>
<td>Click <strong>generate</strong> to generate the engine ID.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Use name used to access the management module.</td>
<td>Enter the username.</td>
</tr>
<tr>
<td><strong>Auth Protocol</strong></td>
<td>The authentication protocol algorithm to use. SHA is the default.</td>
<td>SHA</td>
</tr>
<tr>
<td><strong>Auth Passphrase</strong></td>
<td>Passphrase to use for authentication.</td>
<td>Enter the passphrase.</td>
</tr>
<tr>
<td><strong>Priv Protocol</strong></td>
<td>The protocol to use for SNMP message privacy. AES is the default.</td>
<td>AES</td>
</tr>
<tr>
<td><strong>Priv Passphrase</strong></td>
<td>Passphrase to use when encrypting messages.</td>
<td>Enter the passphrase.</td>
</tr>
</tbody>
</table>

4. Optional: Go to **Trap notification target #2** and repeat step 3 to configure a second SNMP trap notification target.
5. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

### Configure Alerts for Device Errors

Use the settings on the **Administration > Settings > Alerts** page to enable alerts, configure alerting thresholds, and specify alert severity.

#### About Alerting

- An alert is raised according to the severity you configure (INFO to ERROR).
- An alert is only generated if the device stays above the specified alert threshold for longer than 60 seconds (about 100 seconds on average).
- The alert clears when the device returns to normal.
- The alert count will increment for each detection of the same alert. Multiple alerts are not sent.
- SNMP or SMTP messaging can be enabled for each alert.
Enable Alerting

1. Go to Administration > Settings > Alerts.
2. Select Raise Alerts on Device Errors. This is a global switch. If it is not enabled, no alerts are generated.
3. To enable or disable a specific alert, select Enable alert.

4. Examine the threshold settings for the alert and change them if desired.
5. Specify the severity to trigger the alert: INFO, WARNING, or ERROR.
6. Optional—Indicate whether to send email notification for the alert.
7. Optional—Enable SNMP trap notification.
8. Click Save.
9. Click Activate to restart the service.

View Alerts

To view and manage your alerts, see Manage Alerts.

Manage Alerts

Management Center provides an area for administrators to store and manage various alerts. The settings on the Administration > Alerts page enable you to change the state of an alert, change the owner, provide feedback, or find a specific alert.

NOTE
This is different from the message viewer. To view messages in the Recent Messages pane, see Read Alerts.

Related Tasks
• Create Alerts
• Edit Alerts
• Configure Alerts for Device Errors
• Receive Alert Error Notifications

Go to the Alerts management page using one of the following methods:
• Select Administration > Alerts.
• Click the Alert Notification
  icon. This shows the number of open (or unresolved) alerts.

Overview

The landing page shows the current alerts and the options available for management.
• Sorting options allow you to view the alerts based on various criteria.
**Details and Filters Tabs** give quick information about the alert(s).

**Navigation** options at the bottom allow you to go to specific pages.

**Management options** allow you to take action on specific alert(s).

Select message(s) to access the available quick **Operations**. These allow you to edit information on an alert without having to open the edit screen.

### Sort Alerts

The primary element on the landing page is the list of available alerts. These can be sorted by different columns.

*Indicates columns that are NOT shown by default

<table>
<thead>
<tr>
<th>Sort By...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Impact level of an alert on the affected category.</td>
</tr>
<tr>
<td>Priority</td>
<td>Importance level of resolving an alert.</td>
</tr>
<tr>
<td>Message</td>
<td>Current status of an alert. Alerts are either considered open or closed.</td>
</tr>
<tr>
<td>Count*</td>
<td>Number of times an issue is reported.</td>
</tr>
<tr>
<td>Source*</td>
<td>System reporting an alert. <strong>Note:</strong> This field is populated only if an external network is reporting an issue.</td>
</tr>
<tr>
<td>Category</td>
<td>Element affected by an alert.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of an alert.</td>
</tr>
<tr>
<td>Received</td>
<td>Date and time an issue is reported as an alert</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Received status of an alert.</td>
</tr>
<tr>
<td>Owner</td>
<td>Person currently responsible for an alert.</td>
</tr>
</tbody>
</table>
Sort and view the alerts with these options:

- Adjust the length of columns by hovering between two columns to get the adjustment cursor.
- To sort the list, you have two options:
  - Click on a column header. The first click sorts the list by that column in ascending order. A second click sorts it in descending order.
  - Hover over a column header, then select **Menu Arrow > Sort Ascending** or **Sort Descending**.
- To customize which columns show, hover over any column header, then select **Menu Arrow > Columns**.
- To reset the columns back to the default columns and width, hover over any column header, then select **Menu Arrow > Reset Columns**.

Details and Filters Tabs

Get an overview of a specific alert or use filter options in order to find specific alerts.

**TIP**
If you need more space to view the alerts list, collapse this pane by clicking the arrow tab on the left of it. See **Filters Panel** for an example image.

**Preview Details Panel**

Gives a brief summary of the selected alert. If you need to view more details, such as the history of the alert, see **Editing Alerts**.

**NOTE**
Select only one alert to preview the details.

**Filters Panel**

Find specific alerts with various filters. Once applied, the **Filters** tab shows how many active filters there are.
Apply/Clear
Save or delete any filter changes selected.

Customize
Select the filters that show in the Filter Panel.
**Time Range**
Select the time range you want to search in.

<table>
<thead>
<tr>
<th>Hour Options</th>
<th>Day Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 1 Hr</td>
<td>Last 24 Hrs</td>
</tr>
<tr>
<td>Last 12 Hrs</td>
<td>Last 3 Days</td>
</tr>
<tr>
<td>Last 24 Hrs</td>
<td>Last 7 Days</td>
</tr>
</tbody>
</table>

**State**
Select the alert current status(es).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>New or unworked issues.</td>
</tr>
<tr>
<td>Pending</td>
<td>Already known issue, but resolution hasn't started.</td>
</tr>
<tr>
<td>Assigned</td>
<td>Assigned to a specific user.</td>
</tr>
<tr>
<td>In Progress</td>
<td>A resolution has been started.</td>
</tr>
<tr>
<td>Resolved</td>
<td>The issue has been resolved.</td>
</tr>
<tr>
<td>Closed</td>
<td>The issue has been closed. This can be used whether or not the issue has been resolved.</td>
</tr>
</tbody>
</table>

**Acknowledge**
Select the receipt status(es).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledge</td>
<td>Alert received by owner.</td>
</tr>
<tr>
<td>Unacknowledge</td>
<td>Alert not received by owner.</td>
</tr>
</tbody>
</table>

**Category**
Select the element(s) affected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy specific.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Scripts, Shared Objects, Tenants, and Files.</td>
</tr>
<tr>
<td>License</td>
<td>Device license status.</td>
</tr>
<tr>
<td>Operational</td>
<td>Alerts related to the function of a device or Management Center.</td>
</tr>
<tr>
<td>System</td>
<td>Networks linked to Management Center, including files, software, hardware, and firmware.</td>
</tr>
<tr>
<td>Security</td>
<td>Security related alerts.</td>
</tr>
<tr>
<td>Other</td>
<td>For an issue not listed in any other category.</td>
</tr>
</tbody>
</table>

**Priority**

Select the importance level of resolution.

<table>
<thead>
<tr>
<th>Priority Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Urgent</td>
</tr>
</tbody>
</table>

**Owner**

Select the current owner.

**NOTE**

Alerts that are not assigned (in the Owner sorting column) will not show up if an owner is selected.

**Keyword Search**

Next to the Preview/Filter pane is the keyword searching option. If you know keywords in the alerts you are looking for, enter them into the search box and click the magnifying glass or press Enter. To clear the search terms, click the (×) within the search box.

**Navigation**

Navigate between pages and set navigation options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginning</td>
<td>&lt;&lt;</td>
<td>Go to the first page.</td>
</tr>
<tr>
<td>Back</td>
<td>&lt;&lt;</td>
<td>Go back a page.</td>
</tr>
<tr>
<td>Page Number</td>
<td>Page 1 of 1</td>
<td>Current page number and total page count. Type a number to go to a specific page.</td>
</tr>
<tr>
<td>Option</td>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Forward</td>
<td><img src="image" alt="Forward Icon" /></td>
<td>Go forward a page.</td>
</tr>
<tr>
<td>End</td>
<td><img src="image" alt="End Icon" /></td>
<td>Go to the last page.</td>
</tr>
<tr>
<td>Refresh</td>
<td><img src="image" alt="Refresh Icon" /></td>
<td>Refresh the list.</td>
</tr>
<tr>
<td>Page Size</td>
<td><img src="image" alt="Page Size Icon" /></td>
<td>Number of alerts displayed per page.</td>
</tr>
</tbody>
</table>

**Create Alerts**

To create an alert, go to the **Alerts** page using one of the following methods:

- Select **Administration > Alerts**.
- Click the **Alert Notification** icon. This shows the number of open (or unresolved) alerts.

**Create an Alert**

1. Click **Raise Alert** to create a new alert.
2. Enter the message you want to associate with the alert.
3. Assign a severity.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Severity Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info*</td>
<td><img src="icon_info.png" alt="Info" /></td>
<td>Low</td>
<td>Little or no impact.</td>
</tr>
<tr>
<td>Warning</td>
<td><img src="icon_warning.png" alt="Warning" /></td>
<td>Medium</td>
<td>Potential to cause errors.</td>
</tr>
<tr>
<td>Error</td>
<td><img src="icon_error.png" alt="Error" /></td>
<td>High</td>
<td>Errors found.</td>
</tr>
<tr>
<td>Fatal</td>
<td><img src="icon_fatal.png" alt="Fatal" /></td>
<td>Critical</td>
<td>System failure.</td>
</tr>
</tbody>
</table>

4. Assign a priority.
5. Assign a state.
6. Set the owner. The administrator currently logged in is set as the default owner. You may assign it to a different owner as long as the person has previously been added as a user. See Add Local Users.

**NOTE**
Alerts created by the system will show as **not assigned** in the **Owner** sorting column.

7. Assign a category, which describes the element affected by the alert.

<table>
<thead>
<tr>
<th>Option</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Policy specific.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Scripts, Shared Objects, Tenants, and Files.</td>
</tr>
<tr>
<td>Option</td>
<td>Element(s)</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operational</td>
<td>Alerts related to the operation of a device or Management Center.</td>
</tr>
<tr>
<td>System</td>
<td>Networks linked to Management Center, including files, software, hardware, and firmware.</td>
</tr>
<tr>
<td>Security</td>
<td>Security related alerts.</td>
</tr>
<tr>
<td>Other*</td>
<td>For an issue not listed in any other category.</td>
</tr>
</tbody>
</table>

8. (Optional) Enter a more detailed description of the alert and/or the reasons for it.
   
   **TIP**
   
   If you forget any information for the detailed description, you can always [Edit](#) it or add note to the [Journal](#) tab at a later time.

9. Specify alert notification settings. The alert can trigger an email or SNMP trap. The notifications use the information specified in the SMTP and SNMP configuration settings.

10. Click **Save**.

**Edit Alerts**

To edit an alert, go to the [Alerts](#) page using one of the following methods:

- Select **Administration > Alerts**.
- Click the **Alert Notification** icon. This shows the number of open (or unresolved) alerts.

**Edit Alerts**

1. To edit all the information for an alert, select a message and then click **Edit**. Alternately, right-click a message to get the **Edit** option.
   
   **NOTE**
   
   Only one message can be selected for editing at a time.

   Edit alert information in the **Details** tab. The system displays a summary of the current saved status of the alert. The action buttons include:

   - **Save Alert** for any changes you make.
   - **Acknowledge** or **Unacknowledge** the receipt of the message.
   - **Discard** any changes.
   - **Take Ownership** to instantly assign it to yourself.

2. Edit any of the desired information in the **Alert Message**, **Response**, or **Source** panels. To change information with fixed values, click the down arrow to view the list of available states. For example, clicking the down arrow for **Severity** enables you to choose from **Info**, **Warning**, **Error**, **Fatal**.
   
   **NOTE**
   
   Alerts created by the system will show as **not assigned** in the **Owner** sorting column.

3. When finished with your changes, click **Save Alert**.

**Other Alert Management Actions**

- Select message(s) to **Delete** them. Alternately, right-click the message(s) to get the **Delete** option.
- Messages are automatically removed by the system after a set time. The default is 120 days. See Configure Housekeeping Settings for more information.
To change the amount of days alerts are retained:

a. Select **Administration > Settings > Housekeeping**.

b. Change the value in **Number of days of closed alert records to keep**.

c. Click **Save**.

d. (Optional) Click **Activate** to push your changes to the server immediately.

**NOTE**
Select message(s) to **Acknowledge** or **Unacknowledge** the receipt of them. Alternately, right-click the message(s) to get the acknowledgment options.

**NOTE**
Only messages of the same receipt status can be selected at the same time for the button to work. Example: Under the **Acknowledged** column, all messages marked **not yet**.

- **Refresh** the list of available alerts.

**Alert Change Log**

A history of the changes made to the alert are logged in the **Journal** tab beneath the **Notes** field. All notes are collapsed for easy viewing. Click the down arrow to open a note. Actions you can take include:

- Add more information in the **Notes** field.
- **Add Note** to the alert.
- **Clear** any information typed.
Distribute Configurations to Devices

The Symantec Management Center enables you to distribute common configurations and policies that you created and want enacted across other managed devices. Your enterprise might have dispersed data centers that contain hundreds of hierarchies, device groups and devices. Groups of devices might have different functions, thus requiring different sets of configurations or policies.

Two methods provide this ability.

- **Script Method**—Create scripts that contain common device configurations for specific managed devices. Give various users (with the correct permissions) the ability to create and modify script objects.
  - **Execute a ProxySG Configuration Script on Multiple Devices**
- **Policy Method**—Use Symantec Content Policy Language (CPL) or the Visual Policy Manager (VPM) to define policy and validate it before distributing to other managed devices.
  - **Distribute ProxySG Policy to Multiple Devices**

Create and Distribute Configurations Using Scripts

Create commonly used device configurations in a script. After you create the script, you choose to execute the script on a device immediately, or you can create a job. Scripts are collection of CLI commands that are executed in the order shown within the script itself. Scripts are NOT in any type of scripting language. Scripts can be executed on the following devices:

- Blue Coat ProxySG appliance
- Advanced Secure Gateway
- Content Analysis appliance
- SSL Visibility 4.x appliance
- Reporter 10.3 and later

**NOTE**
To successfully execute a script on a Content Analysis, Reporter 10.3, or SSLV 4.x appliance, you must specify the device's enable password in the device’s connection settings (Network > devicename > Edit > Connection Parameters). See Add a Device for more information.

Add a Script

1. Select **Configuration > Scripts**. Click **Add Script**.
   - **Name**—The name displays in the **Script Object** list.
   - **Type**—Scripts can be imported from devices and then executed on supported, managed devices.
   - **Description**—Although entering a description is optional, the description helps differentiate versions of the same script. For more information about the script, see View Script Information.
2. Ensure **Replace substitution variables** is selected. See Use Substitution Variables in Policies and Scripts.
3. Click **Save**. The new script displays in the **Script Objects** list.
4. Select the script and click **Edit**. The Management Center displays the script **Editor**.
5. Create the script. Optional tasks:
   - Optimize a Script for Use on Other Devices
   - Apply Logical Expressions to Scripts and Policy
   - Optimize a Script for Use on Other Devices
6. Click **Save**.
Next Steps

After you create script object, you can refine it or leave it as an empty object while you perform other tasks (for example, edit script details) or you execute the script now. Refer to the following table to determine the next step to take.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a job to execute a script on a schedule</td>
<td>Schedule the Execution of a Configuration Script</td>
</tr>
<tr>
<td>Execute the script now</td>
<td>Execute Scripts</td>
</tr>
<tr>
<td>Compare script versions</td>
<td>Compare Versions of the Script</td>
</tr>
<tr>
<td>Import a script from a managed device</td>
<td>Import Script from a Device</td>
</tr>
<tr>
<td>Restore previous version of a script</td>
<td>Restore a Version of Script</td>
</tr>
<tr>
<td>Customize object filters</td>
<td>Customize Object Filters</td>
</tr>
<tr>
<td>View script information</td>
<td>View Script Information</td>
</tr>
<tr>
<td>Manage attributes</td>
<td>Manage Attributes</td>
</tr>
<tr>
<td>Filter by attributes and keyword search</td>
<td>Filter by Attributes and Keyword Search</td>
</tr>
</tbody>
</table>

Customize Object Filters

Filters control the specific objects that are searchable.

1. Select Configuration > Policy or Scripts.
2. The Filter panel contains the following fields.
   - Name—Filters by the Object Name.
   - Reference Id—Filters by the Operation type.
   - Type—Filters by the Object Type.
   - Description—Filters by the Object Description.
   - Author—Filters by the user who last changed the Object.

   **TIP**
   To substitute variables in policies, policy fragments or scripts, see Variable Substitution.

3. The Filter panel also includes mandatory attributes. See Manage Attributes.
4. To customize filters, click Customize.

<table>
<thead>
<tr>
<th>Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select filters displayed in the filter panel</td>
</tr>
</tbody>
</table>

   a. Select the filters to be visible on the Filter panel.
   b. Click Save.
**View Script Information**

Whenever you create a script, Management Center automatically saves information about it. This information is called *metadata*.

1. Select **Configuration > Scripts**.
2. From the **Script Objects** list, select a script and click **Edit**.

**View Script Object Information**

1. Click the **Info** tab.
2. Under **General Information**, the **Overview** displays the information you entered when creating the script object:
   - **Name**(*)—The name of the script that you gave it when you created it
   - **Type**(*)—The device type that the script applies to
   - **Description**—This describes the script, but is not a required field
   - **Replace substitution variables**
3. Metadata displays under **Latest Revision**. Click **Save**.
   
   **NOTE**
   If you edited any of the fields in **Overview**, fields marked with a red asterisk (*) are required and cannot be left blank.

**View Script Versions**

1. Click the **Versions** tab. The Version Control page lists all versions of the selected script. When a script object is created it is assigned the version number 1.0. Every time that the script attributes change or the script is edited, the version increases by increments of 0.1.
2. Select an early version of script to compare.
3. Press and hold the Ctrl key while selecting the newer version of the script.

- **Version Number**—When a script object is first created, its version is 1.0. Each subsequent time the object is modified—for example, if the object properties are edited the version number increments by 0.1. For example, when you add script text to the object and save it, the version becomes 1.1.
- **Date**—The time and date stamp indicates when the script was last updated.
- **Author**—The author is the user who saved the current version of the script displayed.
- **Comments**—If the author entered comments or a description about the script, they are displayed here. Metadata displays automatically-generated comments as follows:
  - **"Script Object created"**—When the script container is initially created and script has not been added yet.
  - **"Name changed"**—When the script name is edited.
  - **"Description changed - former script has been overridden"**—When the script description is edited.
  - **"Name and description changed - former script has been overridden"**—When both the name and description are edited.

   **TIP**
   Of these metadata, the comments are usually the most important in helping you and other users understand the purpose and intent of creating the specific script version. Symantec recommends that you always enter clear, helpful comments when creating scripts.

**View Script Attributes**

Click the **Attributes** tab. The Attributes page displays all attributes currently assigned to selected script. The attributes are custom attributes that you created. See **Manage Attributes**.

**View Device Script Output**

When you execute a script on a device, the Job Progress dialog displays the status of the executing script. You can view the device output of currently executing scripts and scripts that have already executed on a device by clicking **More**.
Details. Any output line that starts with "%" is considered a warning (and is standard for ProxySG appliances). Navigation buttons enable you to jump between warnings and are useful when viewing the device output for long scripts. You can view the raw output in a text editor by selecting Download as Text.

Set the Maximum Number of Script Revisions to Store in Management Center

After you create or import a script, you can edit the script to execute on devices of the same type. You can specify the number of revisions of scripts to store before Management Center begins to prune. You can specify up to 999 script revisions.

1. Select the Administration > Settings. Click General. General fields display on the right.
2. Select Maximum number of script revisions to store.
3. Enter a number (limit) from 0 to 999.
4. Click Save and then Activate to cause the server to load and apply the currently saved configuration.

Execute Scripts

You can execute any script that is saved in Management Center in the Script Object list. Before executing a script, you can Preview a Script With Variables Replaced. This shows the script variables without committing them to a device and inadvertently causing a device configuration to change.

Scripts are automatically assumed to execute in configure mode on the ProxySG appliance. For scripts that use commands not in configure mode, exit configure mode before executing the script. Licensing commands are the exception, and cannot execute in configure mode. Example:

```
;;exit configure mode
exit
user-license queue
;;re-enter configure mode
configure terminal
```

TIP
See also Schedule the Execution of a ProxySG Configuration Script.

Execute a Single Script

Direct from a Script

1. Select Configuration > Scripts.
2. Select a script object and then click Edit.
3. To execute the script, click Execute on Device.
4. Select a target device or device group. Click Execute.
5. OR
6. Select Edit and click the Editor tab. At times, administrators with the correct privileges want to execute a script immediately after updating a script. While in the rich text editor ensures that all edits have been saved and click Execute on Device. Select the device Target and click Execute.

NOTE
Each time you start a job manually, the Management Center displays a Job Progress dialog. To run the script in the background (no window) while you perform other tasks, click Continue in Background.

From a Job Operation

See Schedule the Execution of a Configuration Script.
(Optional for all script executions) While the Job Progress dialog displays the script executing, click more details to view the Output, Download as Text, or Close the dialog.

Add Error Handling for Scripts

You can specify the behavior Management Center should take when encountering errors or warnings while running a script. Any response line starting with a "%" is an error, and any response line starting with "Warning" is a warning. Management Center provides two levels of script error handling: one at the job level and another within the script itself.

- When multiple scripts are specified in a job, you can specify the error handling if a warning or error in a script is encountered.
- You can add comments within a script to specify the behavior when a warning or error is encountered.

The following table describes these error-handling comments.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Text Comment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop on Error</td>
<td>stop-on-error</td>
<td>When this directive is encountered, Management Center runs script line-by-line and will abort script execution if an error occurs. Inline commands are treated as one command to the EOF instruction.</td>
</tr>
<tr>
<td>Continue on Error</td>
<td>continue-on-error</td>
<td>When this directive is encountered, Management Center ignores all subsequent errors until another directive is reached (if there is one).</td>
</tr>
<tr>
<td>Stop on Warning</td>
<td>stop-on-warning</td>
<td>When this directive is encountered, Management Center runs line-by-line and reports a failure if warnings are encountered.</td>
</tr>
<tr>
<td>Continue on Warning</td>
<td>continue-on-warning</td>
<td>When this directive is encountered, Management Center ignores all subsequent warnings.</td>
</tr>
<tr>
<td>Execute as Batch</td>
<td>begin-batch end-batch</td>
<td>Instructs Management Center to submit everything between these comments as a single &quot;command.&quot; You must have a begin-batch and an end-batch. An end-batch without a begin-batch results in an error before script execution.</td>
</tr>
<tr>
<td>Operation</td>
<td>Text Comment</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Refresh Session</td>
<td>refresh-session</td>
<td>Instructs Management Center to return the device CLI to its default starting position. This is useful for situations in which the script operation encounters an error, such as a missing policy object, that would cause a script error when the next command is run. Using Refresh Session, you can reset the CLI to its starting position and execute a new set of commands. For ProxySG and ASG, the starting position is <code>#(config)</code>, while DEFINE IN KEYMAP and Content Analysis use the enable mode. Any directives encountered before Refresh Session are enforced. For example, if Continue on Error is encountered before Refresh Session, it will still be enforced after Refresh Session is executed.</td>
</tr>
</tbody>
</table>

**Insert Script Error Handling**

You can add script error handling in the following ways:

- Using the Operations menu.
- Inserting them manually in the script.

Manually insert the directives using standard comment format. For example:

```
! - MC stop-on-error Script section ! - MC stop-on-warning
```

You can insert multiple error-handling directives in your script. For example:

```plaintext
ssl
!- MC: continue-on-error
!- Creating will fail if it already exists, but we're OK with it already existing
create keyring show-director newkeyring
delete keylist newkeylist
create keylist newkeylist
delete certificate newkeyring

ssl edit keylist "notfound" clear exit
!- MC: refresh-session ssl edit keylist "found" clear exit

!- MC: stop-on-error

!- MC: begin-batch
create certificate newkeyring
US
CA
Los Angeles
Company Inc
Development
example.com
admin@example.com
```
In the preceding example, the administrator has inserted a "Continue on Error" directive before creating a keyring. This is because it is OK if the keyring already exists. The admin has inserted "Refresh Session" to make sure the device goes back to its starting place to ensure the following script commands execute successfully. The admin has then inserted a "Stop on Error" directive so script execution will fail if an error occurs after this point. The final directive is to execute commands as a batch (a single command).

Job and Script-Level Error Handling Interaction

The error handling inserted into scripts works in conjunction with the error handling specified for the entire script in the job settings. For example, if a script contains a directive for "Continue on Error", Management Center ignores all errors encountered after that directive and the script continues to run—even if the job setting specifies "Stop on Error." The same is true for warnings.

Import Script from a Device

Scripts are sequentially-running CLI commands for a device configuration. It makes sense to import device configurations that are currently on a device because you know that the configuration is correct. Importing an entire device configuration is essentially backing up a device into Management Center and may not exist as a whole such as in the following situations:

- You want to restore a previous version of script that exists only on a device. For example, you started editing script in Management Center, but realize that the script on the device is correct and complete.
- A device has a full configuration that you want to use as a script (template) to execute on another like device.

1. Select Configuration > Scripts.
2. Scripts can only be imported into an existing script object. Select a script name. Click Edit.
3. Click Import.
4. Select a device to import the script. Click OK. The web console displays the Import Script dialog.
5. From What to Import, select Entire Configuration or Only selected sub-sections.
6. Click **Import**. The comment you enter is saved as script metadata.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>View existing script information.</td>
<td>View Script Information</td>
</tr>
<tr>
<td>Restore a version of the script.</td>
<td>Restore a Version of Script</td>
</tr>
<tr>
<td>Execute the script, as is, to devices.</td>
<td>Execute a Script</td>
</tr>
</tbody>
</table>

**Restore a Version of Script**

After time, you might find that the script executed on devices needs improvement or must change because of changes in business requirements or practices. In such situations, you can modify scripts as needed, or revert to an earlier version of a script that is appropriate. When you have determined which version of script to restore, you can restore it using the version history.

1. Click the **Configuration** tab and select **Scripts**. From the **Script Objects** list, select the script name. If required, search for the object; see **Filter by Attributes and Keyword Search**.
2. Click **Edit**. Click the **Versions** tab. Versions of the script are listed in descending numerical order.
3. From the **Version Control** page, verify that the version you want to restore is the correct one. Perform one or both of the following as required.
   − Check the version metadata. See **View Script Information**.
   − Preview a script with the variables replaced.
4. After you have identify the version to restore, select it and click **Restore**. The web console displays the Restore dialog.
5. In the **Comment** field, specify the reason for the restore.
6. Click **Restore**. The restored version of the script is incremented to the latest version in the **Script Objects** list, and the comment you entered in step 6 is displayed in the **Comments** column.

**Optimize a Script for Use on Other Devices**

Running scripts that contain machine-specific variables on multiple devices often fail. To fix that issue, you can add local variables or can optimize the script.

- **Local variables**: You can add local variables to any device scripts.
- **Script optimization**: The optimization tools are only supported for use with ProxySG or Advanced Secure Gateway (ASG) devices. Access the optimization tools by selecting Configuration > Scripts > **ScriptName** > Tools

**Add Local Variables to a Script**

Management Center allows you to insert local variables into your script. You can use these local variables to create script templates, for example.

**NOTE**
You can also [Insert Local Variables in Scripts for Use with Management Center API](#).

**Step 1 - Define the Local Variable**

To create a local variable, define the variable:

- Set a local variable to some value:
  
  ```
  ${@set-local localVariableName = value}
  ```

- Set a local variable based on the value of another variable. Note that the nested variable is not nested in `{}`:

  ```
  ${@set-local localVariableName = $variable}
  ```

For example:

```
${@set-local deviceLocation = $rack}
```

**Step 2 - Reference the Variable**

Reference the local variable in the following ways:

```
${@get-local localVariableName}
```

Or

```
${locals.localVariableName}
```

**Clean Up and Remove Problematic Script Entries**

**NOTE**
Currently, these tools can only be used with ProxySG and Advanced Secure Gateway (ASG) appliances.

Management Center provides the following script optimization tools:

- **Make scripts portable**.
  Troubleshoot and optimize the script so that it runs without errors. This process has the following options:
– **Replace appliance-name with parameters.**
  
  This tool replaces appliance-name `XXXX` with appliance-name `${locals.applianceName}` and adds a `${@set-local applianceName}` to the top of the script.

– **Replace username and passwords in Active Directory (AD) authentication.**
  
  This process finds any security windows-domains and replaces the hard-coded username and password with variables. The process also adds the following:
  
  - A conditional `${if locals.adUseExistingAccount}` to surround the inline domain-details
  - An `${else} join .... ${end}` statement
  
  These statements are added so you can decide whether to use the existing account or a different account (based on the local variable `adUseExistingAccount`).

  If there is a defined Kerberos-user, the process also replaces `<password>` with `${locals.kerberosPassword}`.

– **Remove any inline policy.**
  
  This process removes all inline policy; policy should be contained in policy objects, not as inline policy.

– **Remove "create" operations for default settings.**
  
  This process removes any lines starting with the following attributes:
  
  - "adn-compress disable"
  - "attribute adn-byte-cache disable"
  - "attribute use-adn disable"
  - "enforce-signed disable"
  - "create format "dns""
  - "create format "clientagent_v1""
  - "create log "dns"
  - "create log "client-agent"

  The process also removes:
  
  - All commands from `create https-console "HTTPS-Console"` to the exit
  - The default interface 0:0 and ip-default-gateways statements
  - All default CCLs See Insert Local Variables in Scripts for Use with Management Center API.

  • **Remove inline policy.**
    
    This process removes all inline policy; policy should be contained in policy objects, not as inline policy.

  • **Correct PEM encoded certificates**
    
    This process corrects any PEM certificates that have incorrect formatting due to line breaks or other issues.

  • **Remove Default CCLs**
    
    When you import a script, the system inserts default CA Certificate Lists (CCLs) into the script. These default certificate lists cause errors when you try to run the script again. This operation removes the following default CCLs:
    
    - bluecoat-appliance
    - bluecoat-image-validation
    - bluecoat-license
    - bluecoat-services

  When you run one or more of these processes, the system does not automatically save the changes. Because the changes are not saved, you can compare the new script version with the original version to ensure that the changes are acceptable. Select **Compare** to view the changes. For more information, see **Compare Versions of the Script.**

**Insert Local Variables in Scripts for Use with Management Center API**

In Management Center 3.0 and later, you can use the REST API to pass local variable values into device scripts. This action is helpful when you want to change values in device scripts without editing them.
The `parameters` variable can be inserted into scripts and then modified using the Management Center API. The syntax of the `parameters` variable is:

```
parameters.property
```

The variable can be placed anywhere in the script.

**Simple Example**

```
logout ${parameters.username}
```

**Recommended Example Using a Default and Local Variable**

In this example, the user enters a local variable within the script and sets it to a parameter value that is specified in the API script execute function. If the script is run without the parameter or through the user interface, the user also specifies a default that is used.

```
${@set-local username = $parameters.username(MY_DEFAULT)}
...
users;
logout ${@get-local username}
```

**Pass in a Parameter Value**

The REST API function `api/script/{uuid}/execute` is used to define the local value. For example:

```
curl -k -u admin:admin -H "Content-Type: application/json" -X POST https://myhost:8082/api/scripts/1b923b85-e71b-43d3-bfc5-e4ace3e34fda/execute -d '{"deviceUuids": ["091644CB-D7EE-403D-BB27-2914279B3546"], "parameters": {"username": "emma"}}'
```

1. Insert the `parameters` variable in the script.
2. Save the script.
3. Use the REST API `api/script/{uuid}/execute` function to modify the parameter variable as desired.

**Add a Script Operation (Includes, If Statements, and Error Handling)**

You can add the following script insertions:

- Insert Include
- Insert If
- Insert Error Handling

**Add a Script Operation**

1. Select Configuration > Scripts, highlight the row the script is on and click Edit.
2. Place your cursor where you want to insert the operation.
3. Click Operations and select the desired operation.
4. Modify the inserted operation as needed. See sections below for more information.
5. Click Save.

**Insert Include**

This feature allows you to:

- Include one script inside another. For example:
  ```
  ${include:IncludeKeys}
  ```
- Specify a specific version of the included script. For example:
  ```
  ${include:IncludeKeys[1.2]}
  ```
The script type is considered when including scripts. ProxySG scripts can run only on ProxySG appliances, but ASG scripts can be run on both appliances. Therefore, you cannot include an ASG script in an SG script, though the converse is allowed.

**NOTE**
Cyclical script references are not allowed. If detected, the system generates errors.

**Insert If**
See *Apply Logical Expressions to Scripts and Policy*.

**Insert Error Handling**
See *Add Script Error Handling*.

**Apply Logical Expressions to Scripts and Policy**
Logical expressions allow you to build intelligence into scripts and policy, so they to make decisions when executing. As the system processes a script or pushes policy to devices, it can process `${if ...}` and `${else}` expressions to determine whether to apply elements of the configuration to all, or only some, of the selected devices or policies.

For example, logical expressions could be applied to a configuration change where some members of a group of ProxySG appliances have a user group called "clerks" while another group of appliances does not. If the "clerks" policy is found in appliances in locations where those users exist, update policy. If it does not, skip that update.

When used in conjunction with the `${if ...}` and `${else expressions, ${foreach ...}` can be used to iterate over a set of values, in order to to apply unique `${if ...}` and `${else logic to loop script processing to test for a specific value.

**Add an If Expression to an Existing Script**
1. Select the script and click *Edit*.
2. Click *Operations* and select *Insert If*.
3. Modify the inserted `${if condition} as needed.
4. Click *Save*.

**Supported Expressions**

`${if variable}`
Test for the existence of a variable. If the variable has a value, the scripted condition evaluates as true.

**TIP**
You can use two hyphens to comment out an if condition. When `${--if ...}` is encountered, the script will skip the associated action.

`${if variable=value}`
Test for the value of a variable. If the variable has a matching value, the scripted condition evaluates as true. If the value entry includes spaces, enclose in quotation marks.

**CAUTION**
You cannot have spaces around the =.

`${else ..}`
Used in conjunction with an `${if ...` expression. During script processing, when an `${if ...` expression is not matched, an `${else expression determines an alternate course of action.

`${foreach ..}`
Used in configuration scripts and policy to iterate over the values in a collection of attributes. Though not required in scripts where ${if ...} and ${else} are used, ${foreach ...} triggers a loop of processing, while testing each target device to match trigger attributes.

**Examples**

The examples below use custom variables. For more information on defining variables and using them in scripts, see Use Substitution Variables in Policies and Scripts.

**Define simple if else logic flow**

This example defines one DNS server address on ProxySG devices running in a network named "Guest Wireless", and set another DNS address on appliances in other, unspecified networks.

${if device.attributes.Network="Guest_Wireless"}

dns-forwarding edit primary add server 8.8.8.8

${else}

dns-forwarding edit primary add server 203.0.113.5

${end}

**Define advanced if else logic flow with foreach**

In this example, the script uses foreach to identify only the specific device members Management Center will apply configuration changes to. Unlike the previous example, defining the script in this manner takes action only on those devices that are explicitly identified in the script.

${foreach device.memberOf group}

${if group='Data Center 2'}

dns-forwarding edit primary add server 203.0.113.5${end}

${if group='Data Center 3'}

dns-forwarding edit primary add server 203.0.113.6 ${end}

${end}

**Compare Versions of the Script**

As a troubleshooting step or as part of performance evaluation, you might want to identify the changes between an earlier version and a later version of a script. Management Center shows the changes made.

1. Select Configuration > Scripts. From the Script Objects list, select the script name. If needed, search for the object; see Filter by Attributes and Keyword Search.
2. After you select the script, click Edit. Click the Versions tab.
3. Select an earlier version of the script to compare with the current version.
4. Press and hold the CTRL key while selecting the later version of the script to compare.
5. Click Compare. The web console displays the Compare Scripts dialog.
   The two scripts are displayed side-by-side; the web console displays the version you selected first (earlier version) on
   the left and your second selection (later version) on the right.
   – A script highlighted in red exists in the former version and was removed in the later version.
   – A script highlighted in yellow indicates that a line exists in both versions of script, but there are differences in the
     line.
   – A script marked in green does not exist in the former version and was added in the later version.

TIP
See Restore a Version of Script.

Use Substitution Variables in Policies and Scripts
Substitution variables are generic terms (like attributes or shared objects) that you can include in policies and scripts.
These terms are attributes you might have setup on your devices, groups, etc. When Management Center installs policy
or executes a script that includes substitution variables, it attempts to replace them with values specific to the current
transaction—that is, the current device, policy, or script. For example, if you install policy that includes the substitution
variable ${device.name}, the variable is replaced with the device name set in Management Center.

CAUTION
Substitution variables are case-sensitive. To ensure that you have entered them with correct spelling and case,
use the Preview option before installing policies or executing scripts. The preview warns you if a substitution
variable is invalid.

Use in Shared Policy
When you include shared policy objects in your policy, you must enable variable substitution or the shared object's CPL
will not be substituted for the include variable. For example, if you create a URL list called allowlist and include it
in a policy object, the system creates the CPL entry ${include:allowlist}. The allowlist URL list will only be
included if Replace substitution variables is selected when the policy is installed.

NOTE
While you may use substitution variables in CPL layers, Management Center performs the substitution when
installing the CPL to the device. The UI markup (XML) remains unchanged. Therefore, if you open the installed
VPM policy locally from the ProxySG appliance and try to install it, the substitution variables will not be replaced
in the resulting CPL (because this workflow bypasses Management Center). This could result in malformed or
unexpected policy, depending on how the variables are being used.

To include and process substitution variables:
1. Verify that Replace substitution variables is enabled in the policy object (see Create a CPL Policy Object) or script
   (see Create and Distribute Configurations Using Scripts).
2. Include substitution variables in the CPL or script. See Supported Variables below.
3. Install the policy or execute the script. As the target device processes the policy or script, it attempts to replace the
   variables with the appropriate values.
   If the policy or script is associated with a device group, Management Center inspects every device in the group
   structure for the variable and attempts to replace all instances with specific values.

Syntax
Substitutions have the following form:

${name}
where name is an expression that expands to a string or block of text at runtime.

For example, the substitution `${device.description}` expands to the description entered in the current device's properties in Management Center.

If the device does not have a description (because Description is an optional field), the substitution expands to an empty string unless you also specify a default value. See Specify a Default Substitution Value below for details.

**Examples**

Substitute the device's serial number.

```java
${device.serialNumber}
```

Substitute the value of the device’s Rack attribute.

```java
${device.attributes.Rack}
```

**Supported Variables**

**Device - `${device.field}`**

The following variables are available for policies and scripts.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${device.memberOf}</code></td>
<td>List of the groups to which a device is assigned</td>
</tr>
<tr>
<td><code>${device.uuid}</code></td>
<td>Internal ID of device</td>
</tr>
<tr>
<td><code>${device.modelNumber}</code></td>
<td>Device model number</td>
</tr>
<tr>
<td><code>${device.description}</code></td>
<td>Text in the Description field in device properties in Management Center</td>
</tr>
<tr>
<td><code>${device.name}</code></td>
<td>Text in the Device Name field in device properties in Management Center</td>
</tr>
<tr>
<td><code>${device.serialNumber}</code></td>
<td>Device's serial number</td>
</tr>
<tr>
<td><code>${device.osVersion}</code></td>
<td>Operating system version running on the device</td>
</tr>
<tr>
<td><code>${device.type}</code></td>
<td>The device type, for example, ProxySG.</td>
</tr>
<tr>
<td><code>${device.attributes.name}</code></td>
<td>System or user-defined device attribute value, including any values inherited from the device group</td>
</tr>
</tbody>
</table>

**Device Connection - `${device.connection.field}`**

The following variables are available for policies and scripts. A variable might not be applicable to every device.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${device.connection.host}</code></td>
<td>Host IP address</td>
</tr>
<tr>
<td><code>${device.connection.port}</code></td>
<td>Port number</td>
</tr>
<tr>
<td><code>${device.connection.connectionType}</code></td>
<td>Designates the way the connection is established and optionally how authentication is performed. For example, <code>SSH_PUBLIC_KEY</code></td>
</tr>
<tr>
<td><code>${device.connection.network}</code></td>
<td><code>PRODUCTION</code> or <code>PREPRODUCTION</code></td>
</tr>
<tr>
<td><code>${device.connection.username}</code></td>
<td>User name for authentication. Only relevant for ProxySG/ASG when credentials are used.</td>
</tr>
</tbody>
</table>

**Policy - `${policy.field}`**
The following variables are available for policies only (not scripts).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${policy.author}</td>
<td>Last user who edited and saved the policy</td>
</tr>
<tr>
<td>${policy.description}</td>
<td>Text in the Description field in policy properties</td>
</tr>
<tr>
<td>${policy.name}</td>
<td>Text in the Name field in policy properties</td>
</tr>
<tr>
<td>${policy.referenceId}</td>
<td>Text in the Reference Id field in policy properties</td>
</tr>
<tr>
<td>${policy.revision}</td>
<td>Policy's current Version number</td>
</tr>
<tr>
<td>${policy.revisionDescription}</td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td>${policy.attributes.name}</td>
<td>User-defined policy attribute value</td>
</tr>
</tbody>
</table>

**Policy Fragment- ${fragment.field}**

The following variables are available for policy fragments.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${fragment.author}</td>
<td>Last user who edited and saved the policy fragment</td>
</tr>
<tr>
<td>${fragment.description}</td>
<td>Text in the Description field in policy fragment properties</td>
</tr>
<tr>
<td>${fragment.name}</td>
<td>Text in the Name field in policy fragment properties</td>
</tr>
<tr>
<td>${fragment.referenceId}</td>
<td>Text in the Reference Id field in policy fragment properties</td>
</tr>
<tr>
<td>${fragment.revision}</td>
<td>Policy fragment's current Version number</td>
</tr>
<tr>
<td>${fragment.revisionDescription}</td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td>${fragment.attributes.name}</td>
<td>User-defined policy fragment attribute value</td>
</tr>
</tbody>
</table>

**Script - ${script.field}**

The following variables are available for scripts only (not policies).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${script.author}</td>
<td>Last user who edited and saved the script</td>
</tr>
<tr>
<td>${script.description}</td>
<td>Text in the Description field in script properties</td>
</tr>
<tr>
<td>${script.versionDate}</td>
<td>Date of last update</td>
</tr>
<tr>
<td>${script.name}</td>
<td>Text in the Name field in script properties</td>
</tr>
<tr>
<td>${script.type}</td>
<td>Selected Type in script properties</td>
</tr>
<tr>
<td>${script.revision}</td>
<td>Script's current Version number</td>
</tr>
<tr>
<td>${script.revisionDescription}</td>
<td>Comments entered for the last revision</td>
</tr>
<tr>
<td>${script.attributes.name}</td>
<td>User-defined script attribute value</td>
</tr>
</tbody>
</table>

**Specify a Default Substitution Value**

Unless you specify a default value, some transactions can produce unsubstituted variables, resulting in empty strings. The following are examples of such transactions:

- An optional field such as Description is empty
- An attribute that is not marked as mandatory has no value
- A field is not applicable, such as when a script or policy has not been revised
Syntax

A default substitution has the following form:

\${name(default_name)}

where:

- name is an expression that expands to a string or block of text at runtime
- default_name is the value that will be used instead of an unsubstituted variable

Example

If a policy fragment was edited, use the comments entered for the last revision. If the fragment was never edited, use the specified text "No revision".

\${fragment.revisionDescription(No revision)}

Use Regular Expressions

Policy and script processing can make use of Regular Expressions (RegEx).

Syntax

regex

Example

RegEx can be used in variables to produce generic results as follows:

\${device.osVersion;regex(SGOS (.*) )} will return just the number portion of SGOS version for SG devices

And RegEx can be used as part of a condition with specific strings:

\${device.osVersion;regex(SGOS (.*) )="6.7.3.100"} will test for the specific version of SGOS.

Preview a Script With Variables Replaced

Management Center enables you to check the variable replacement in a script before you execute it. Previewing a script avoids inadvertently changing a device configuration.

NOTE

Devices that are in your network deployment should not be used to test configurations.

For scripts that use commands not in configure mode, you must exit configure mode before executing the script. Most commands are executed in configure mode. Licensing commands are the exception, and cannot execute in configure mode.

1. Select Configuration > Scripts.
2. Open a script object.
3. From the Editor tab, click **Preview**.
4. Select a device to preview the script and click **OK**.

5. The Preview Script window displays the entire script.

6. Click **Close**.
Organize Scripts by Attribute

This use case describes how to use attributes to logically organize your scripts. This technique can be useful when you have a large number of scripts and want to better organize them. Think of the attributes as folders for your scripts. By adding different attributes, you can organize your scripts in different ways.

In this example, we want to organize scripts by their purpose, but you can organize them in other ways as well.

1. Select `Administration > Attributes > Device Scripts`.
2. Click `Add Attribute` to create a new attribute definition.

   The new attribute's name is **Purpose** because we want to logically arrange the scripts by their purpose.

   **NOTE**
   Ensure that `Displayed as a default column` is checked so this attribute will automatically display on the script list grid.

3. Click `Save`.
4. Select `Configuration > Scripts`. You will see the **Purpose** header on the grid.

   If you want to move the **Purpose** column, you can drag it to a different position.

5. Hover the mouse cursor over the **Purpose** header to display the down arrow and click it.

6. Select `Group by this field`.
7. Select a script and click `Edit`.
8. Select the **Attributes** tab and enter a value in the **Purpose** field.

9. In this example, we have used **Test**, **Iteration 1**, and **Iteration 2**. You can see how the grid now organizes the scripts around their attribute values.

You can also setup the attribute to be a picklist if you want to have predefined values.

Schedule the Execution of a Configuration Script

A script is a set of configuration commands, stored in a single text file. When you want to execute the same script on multiple devices, you can create the script once in Management Center and then execute it on all devices on which you want to put that configuration. To accomplish this goal, you create and test the script on a single device, and then create a job to execute the script on selected targets.

Before You Begin

1. (Optional) Create a device group for the devices the configuration script will be executed on. See Add a Device Group.
2. Create a script object. See Create and Distribute Configurations Using Scripts.
3. (Optional) Import all or part of a configuration from one of your devices. See Import Script from a Device.
4. Test the script by executing it on one device. See Create and Distribute Configurations Using Scripts.

Schedule Script Execution

When you have completed the tasks in Before You Begin, you are ready to create a job to execute the script on multiple devices.

1. Select `Jobs > Add > New Job`.
2. On the `Add New Job` page, select `Execute Script`.
3. **Configuration:**
   - Click **Add** to select one or more scripts to execute.
   - **Runs on** displays the compatible devices the script can run on.

   **NOTE**
   ProxySG scripts can run on Advanced Secure Gateway (ASG) appliances, but ASG scripts will not run on ProxySG appliances. Therefore, if you include one ASG script and one ProxySG script, the system displays only ASG targets.
   - If you select **Continue on Fail**, the job will continue to run even if that script execution fails.
   - **Continue on Warning** is selected by default.

4. **Targets:**
   - Select the **Devices** or **Groups** tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   - All selected targets appear in **Selected Targets**.

5. **Job Results:**
   - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. **Schedule:**
   Choose to trigger job execution using a **Schedule** or an **Event**.

   **Schedule**
   Use **Schedule** when you want to run the job now or to execute the job at a specific time.
   - **Immediate**—automatically runs the job after it is created.
   - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
   - **Run Once Only**—specify the date and time to run the job.
   - **Periodic**—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
   - **Daily**—runs the job every day at the specified time.
   - **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

   See also **Job Scheduling Options**.

   **Event**
   Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   - **Device added to Management Center**
   - **Device added to Group**
   - **Device removed from Group**

   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

7. **Name:**
   - Verify or change the name and add an optional description.

8. Click **Save**

   After Management Center runs the script execution job, confirm that the script was executed on the target devices.

---

**Create and Distribute Policy**

When you first configure Management Center, you can create new policies or import existing policies from managed devices. When you have been managing devices from Management Center for a longer period of time, you might also
want to edit policies to change current device configurations. One of Management Center's most powerful features is the ability to create and modify policy objects before deploying multiple policies across data centers containing hundreds of hierarchies, device groups, and devices.

**Policy Editing Conflict Management (Policy File Locking)**

Starting with Management Center 1.6, a policy file is automatically "locked" as soon as a user starts editing policy. If another user tries to edit the same policy, that user will receive the following message.

The policy lock is released after the user saves or cancels the changes. When a policy lock is active, another user may force that policy to unlock by clicking **Unlock** on the policy grid.

Policy locking affects the content of policy only. Other attributes (Targets, Info, etc.) can be changed even while the policy is being edited by another user.

**Create and Edit CPL Policies**

Content Policy Language is a language for specifying the policy rules for the ProxySG appliance.

**NOTE**

For complete information about the Content Policy Language, refer to the *Content Policy Language Reference*. Another way to create CPL policy is to create CPL fragments (or building blocks). See Create a CPL Policy Fragment.

Management Center gives you great flexibility for creating and modifying CPL policies, as well as the power to deploy multiple policies to a range of devices or device groups. Use CPL to accomplish the following:

- Create and modify the CPL directly from the policy editor (**Configuration > Policy > PolicyName > Edit**). See Use Content Policy Language (CPL) to Create Policy.
- Create policy without assigning it to devices immediately. See Create a CPL Policy Object.
- Find and edit sections of the policy. See Find a Policy Section and Edit a Policy Section.
- Modify and test policy and group related rules together. See Refine Existing CPL Policy.
- Correct and modify the behavior of existing policy by re-ordering policy sections. See Change the Order in which Policy Rules are Evaluated.
- Create versions of policy, and restore previous versions when needed. See Restore a Version of Policy.
- **View** or compare policy versions.
- Enable substitution variables to be used, for any variable, so that you don't have to modify each attribute in each policy if a configuration has changed. See Use Substitution Variables in Policies and Scripts.
- Create policy attributes and apply them to policy objects. See Add Policy Attributes.
- Add target devices and install policy to them.
- Deploy multiple policies to a group of devices by using Management Center’s job feature. See Install Multiple Policies.
- Import existing policy from a managed device. See Import Policy from a Device.
- Check the consistency of installed policy.
- **View** the deployed policy on a device.
- View existing policy information. See View Existing Policy Information.
- **Deploy** universal CPL policy.

**Create VPM Policies**

The Visual Policy Manager enables you to specify the policy rules using a GUI editor for the ProxySG appliance and install the policy to the VPM slot. For complete information about the Visual Policy Manager, refer to the Visual Policy Manager Reference and Advanced Policy Tasks.

You can:
Create and modify policy in the legacy or web-based VPM. See Add a VPM Policy Object.
Select a reference device to edit VPM policy. See Select Reference Device for VPM Policy.
Create versions of policy, backup and restore previous versions when needed. See Restore a Version of Policy.
View the CPL or XML source.
View or compare policy versions.
Create or edit Attributes and apply them to policy objects.
Add target devices and install policy to them.
Deploy multiple policies to a group of devices by using Management Center’s job feature. See Install Multiple Policies.
Import existing policy from a managed device. See Import Policy from a Device.
Check the consistency of installed policy.
View the deployed policy on a device.
View existing policy information. See View Existing Policy Information.
Clone to universal VPM policy.

Create Universal VPM Policies

Deploy universal policy.
Create a universal policy object.
Import existing policy from a managed device. See Import Policy from a Device.
Transform existing VPM policy into universal policy.
Use the Visual Policy Manager to apply policy to on-premises and remote users.
Select a reference device to edit VPM policy. See Select Reference Device for VPM Policy.
Create versions of policy, backup and restore previous versions when needed. See Restore a Version of Policy.
View the CPL or XML source.
View or compare policy versions.
Create or edit Attributes and apply them to policy objects.
Add target devices and install policy to them.
Deploy multiple policies to a group of devices by using Management Center’s job feature. See Install Multiple Policies.
Check the consistency of installed policy.
View the deployed policy on a device.
View existing policy information. See View Existing Policy Information.

Create Tenant Determination Policies

A Tenant Determination File contains rules for routing request traffic to the proper tenant. This determination criteria controls which set of tenant policy will be evaluated for a given request. If a tenant determination cannot be made, the “default” tenant policy is used. You can:

Create and edit tenant determination policies directly from the policy editor (Configuration > Policy > PolicyName > Edit) (without assigning the policy to devices immediately).
Use tenant determination rules to properly route traffic to the correct web application (or group of web applications). See Specify Tenant Determination Rules (Tenant Determination File) and Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.
Create versions of policy, backup and restore previous versions when needed. See Restore a Version of Policy.
Create policy attributes and apply them to policy objects. See Add Policy Attributes.
Add target devices and install policy to them.
Deploy multiple policies to a group of devices by using Management Center’s job feature. See Install Multiple Policies.
Check the consistency of installed policy.
View the deployed policy on a device.
View existing policy information. See View Existing Policy Information.

Create WAF Application Policies
A WAF Application Object represents a web application (or group of applications) and the associated WAF security settings. The WAF application object is associated with a specific tenant and WAF Security Profile. You can:

- Use WAF Application policies to associate a Security Profile to a tenant, manage optional CPL fragments, and control WAF Application settings. See Configure WAF Security Rules (WAF Security Profile) and Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.
- Create versions of policy, backup and restore previous versions when needed. See Restore a Version of Policy.
- Create policy attributes and apply them to policy objects. See Add Policy Attributes.
- Deploy multiple policies to a group of devices by using Management Center’s job feature. See Install Multiple Policies.
- View existing policy information. See View Existing Policy Information.

Create SSL Visibility URL List Policies

You can create policy in Management Center that manages URL lists for SSL Visibility appliances, and then deploy the policy to a group of SSL Visibility appliances. See Create SSL Visibility URL List Policy.

Create SSL Visibility IP Address List Policies

You can create policy in Management Center that manages IP address lists for SSL Visibility appliances, and then deploy the policy to a group of SSL Visibility appliances. See Create SSL Visibility IP Address List.

Create Local Content Filter Databases

You can create a local content filter database in Management Center that all of your ProxySG or Advanced Secure Gateway appliances can use in policy. This database is hosted on Management Center. See Create a Local Content Filter Database for details.

Organize Policy in Folders

To make it easier to find your policy, you can logically organize your policy objects, scripts, shared objects, and files using folders. This feature is supported on all pages in the Configuration section, except for Tenants.

1. Go to the policy page you'd like to add a folder to.
2. Click Add > Add Folder.
   
   NOTE
   
   This system does not display the Add Folder option unless the Folders option is enabled.

3. Provide a name and optional description and click Save.
   The system displays the folder in the left pane. If you don't see the folder list, toggle the Folders option.

4. Drag and drop the job(s) you'd like to move to the folder.
5. Optional—If you want to make the folder a sub-folder of another folder, drag and drop it to the top-level folder.

Use Content Policy Language (CPL) to Create Policy

You can compose CPL directly in the web console editor.
CAUTION
Before writing policies in CPL, Symantec strongly recommends that you understand the fundamental concepts underlying policy enforcement in ProxySG appliances, as well as how to write correct CPL. For comprehensive information on CPL, refer to the Content Policy Language Reference.

1. Select Configuration > Policy. From the Policy Objects list, select the policy object to edit. Ensure that the policy's object type is CPL. Select the policy. If you have a lot of policies narrow your search using Filter and Keyword Search.
2. Select Edit and the Editor tab. The other tabs available for viewing and editing purposes are the following:
   – Targets
   – Versions
   – Attributes
   – Info
3. The middle pane displays the sections in the policy, and the Quick Navigation pane on the right displays a summary of the sections in the object.
4. In either the middle pane or in Quick Navigation, select the section you want to edit. If needed, expand the sub-section (default, override, or mandatory) to edit.

   TIP
   A policy object is organized into sections. Each section has a name and a purpose, and can contain up to three sub-sections of CPL that you can use to organize policy: Default, Override, and Mandatory. See Edit a Policy Section. If the modular sections perform slowly, you can select the Single Pane Layout icon.

   This is useful if the CPL is particularly long or if you prefer working with a single pane of code. Note that switching to a single pane and saving the policy erases all metadata about your sections. You cannot recover the sections by switching back. However, you can either discard the changes without a save, or you can restore a previous version.
5. Enter the CPL in the appropriate sub-section(s).
6. Repeat steps 3 and 4 as needed.
7. Click Save. Management Center prompts you to enter a comment for the save operation.

   ![Save Changes](image)

   Save changes to policy object: Acceptable Use.

   Enter a comment for the commit operation:

   Added override section

   2026 of 2048 characters left

   ![Save, Compare, Cancel]

8. (Optional) Click Compare to see the differences between the previous version and the version you are about to commit. For information on comparing versions, see Compare Different Versions of the Same Policy and Compare the Device Policy Version with Current Policy Version.
9. Enter a description of your changes and click **Save**. The comment you enter is saved as policy metadata. For information on metadata, see **View Existing Policy Information**.

**Working with CPL Policy Fragments**

A fragment is piece of CPL that you can include in a CPL policy. Fragments are meant to be reusable. For example, you can create a library of policy fragments, and then include them into larger CPL policies later. For instance, you can define a host block list using just a fragment, and then include that host block list fragment into a larger policy file later. See **Create a Policy fragment** and **Edit a Policy Fragment**.

**CAUTION**

If you do NOT enable variable substitution in the CPL, variable substitution is not enabled for CPL Fragments as well.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable variable substitution for CPL Policy and CPL Policy Fragments.</td>
<td><strong>Use Substitution Variables in Policies and Scripts</strong></td>
</tr>
<tr>
<td>Add new attributes that can be made available to the CPL Policy.</td>
<td><strong>Add Policy Attributes</strong></td>
</tr>
<tr>
<td>Add or edit sections of a CPL Policy.</td>
<td><strong>Install Policy</strong></td>
</tr>
<tr>
<td>Import a policy from a device to Management Center.</td>
<td><strong>Import Policy from a Device</strong></td>
</tr>
<tr>
<td>Modify/test policy and group related rules together.</td>
<td><strong>Refine Existing CPL Policy</strong></td>
</tr>
</tbody>
</table>

**Manage CPL Policies**

When you are first setting up Management Center, you can create new policies or import existing policies from managed devices; however, when you have been managing devices from Management Center for a longer period of time, you might also want to edit policies to change current device configurations.

Management Center gives you great flexibility in both creating and modifying your policies. You can:

- Create and modify the CPL directly in the Policy Editor
- Correct and modify the behavior of existing policy by re-ordering policy sections
- Create versions of policy, and restore previous versions when needed
- Create policy without deploying it to devices immediately

Ensuring that devices are configured and behave as required could involve creating, modifying, and testing policy. For example, you might create policy in your evaluation environment, install it to a small group of devices, observe the devices in a test phase, and then edit the policy as needed based on your observations.

Learn about creating and maintaining policy in Management Center:

1. Create policy and deploy it to devices. You could do some or all of the following:
   - Use Content Policy Language (CPL) to Create Policy in the Policy Editor.
   - Import Policy from a Device.
   - Add Policy Attributes
   - Install Policy to devices or device groups.
   - Install Multiple Policies to devices or device groups.
   - Add or Remove Devices Associated with Policy.
2. To add custom metadata to policies, see **Add Attributes**.
3. Compare the Device Policy Version with Current Policy Version to see the revisions and policy information.
4. **Compare Different Versions of the Same Policy** to find the edited version of a policy that you want to use.

**Create a CPL Policy Object**

You can create policy in CPL to specify the behaviors that you want for devices. The first step to create policy in Management Center is to create the container for the CPL, or the policy object.

**NOTE**

Before writing policies in CPL, Symantec strongly recommends that you understand the fundamental concepts underlying policy enforcement in ProxySG appliances, as well as how to write correct CPL. For comprehensive information on CPL, refer to the [Content Policy Language Reference](#).

1. Select **Configuration > Policy**.
2. Click **Add Policy**. From the Create New Policy: Basic Information dialog, fill in the following fields:
3. Enter the **Policy name(*)** - The name that displays in the Policy Object list.
4. Select **CPL** from the drop-down list.
5. Enter the **Reference Id** - Enter a Reference Id that you can filter on when building policy.

**NOTE**

The Reference Id must begin with a letter, and must contain only letters, numbers and "_".

6. Select the **Tenant** to which this policy object will be applied.
7. Enter a **Description**. Although entering a description is optional, the description helps differentiate versions of the same policy. For more information, see View Existing Policy Information.
8. To enable variable substitution, select the check box **Replace substitution variables**. See Use Substitution Variables in Policies and Scripts Click **Next**.

**CAUTION**

If you do NOT enable variable substitution in the CPL, variable substitution is not enabled for CPL Fragments as well. See Create a CPL Policy Fragment.

9. From the Attributes page, select the attributes to apply to the CPL Policy. All attributes that are marked as mandatory with a red asterisk are required. You can change the value of the required attribute before continuing. Click **Next**.
10. Select the devices to install the CPL. You can associate devices with the policy at any time. See Add or Remove Devices Associated with Policy.
11. Choose the slot where your Policy will be installed. With CPL as the Policy type, the following slots are available:
   - **Local** - Use this file to store policy specific to your organization, such as departmental policies and company-wide policies. This option is selected by default.
   - **Forward** - This file contains forwarding rules.
   - **Central** - This slot contains policy common to your entire organization.
12. Click **Finish**. The newly created policy object displays in the Policy Objects list.

**Determine Your Next Step**

After you create a policy object, you can refine it or leave it as an empty object while you perform other tasks (for example, associate devices with it or edit policy details). Refer to the following table to determine the next step to take.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine an existing CPL policy.</td>
<td><a href="#">Refine Existing CPL Policy</a></td>
</tr>
<tr>
<td>Enable variable substitution for CPL Policy and CPL Policy Fragments.</td>
<td><a href="#">Use Substitution Variables in Policies and Scripts</a></td>
</tr>
<tr>
<td>Validate existing policy.</td>
<td><a href="#">Preview Policy Before Installing It</a></td>
</tr>
<tr>
<td>Import an external CPL policy.</td>
<td><a href="#">Import External Policy</a></td>
</tr>
</tbody>
</table>
Add or Edit CPL Policy Sections

You can add a policy section using one of two methods: you can use part of existing policy to create the section, or add a new section and then add policy to it.

**NOTE**
These features are only available if the Modular Layout is selected.

### Add a Section Based on an Existing Policy Section

While composing the CPL or after importing policy from a device, you might find some policy rules that should be extracted from their respective sections and put into a new section. You can select some or all of the text in a section and convert the selection to a new section. When you convert a selection, the Policy Editor preserves the order of the CPL already written.

1. Select **Configuration > Policy**.
2. In the **Policy Objects** list, select the CPL policy to which you want to add a section. Click **Edit**.
3. From the **Editor** tab, locate the policy section that contains the text you want to convert to a new section.
4. Select the text and click **Operations > Convert Selection to New Section**. The Policy Editor displays the new section.
5. Enter or modify the CPL as needed. Click **OK**.
6. Click **Save**.

### Add a New Section

You can add more sections to a new or existing policy object. A new policy object has an empty section by default.

1. Select **Configuration > Policy**.
2. In the **Policy Objects** list, select the CPL policy that you want to add a section. Select the policy name. Click **Edit**.
3. Click the **Editor** tab. Locate the area that you want to add a new policy section. Click the **Operations > New Section**.
4. In the **Section name** field, enter a name for the section.
5. From the **Purpose** drop-down list, select from the list of defined policy purposes or you can create your own **Custom Solution**.

6. Click **OK**. The new section is added at the top of the Editor. Continue to edit the CPL as needed.

   **NOTE**
   
   If you do not name the section, and only give it a purpose, the section appears as Untitled.

7. To commit your changes, click **Save**.

### Edit a Policy Section

While creating a CPL policy or after importing a policy from a device, you might it useful to edit the policy rules within a section. Because policy is applied to devices and can contain many types of rules, you can edit those rules within a section making policy easier to navigate, organize and deploy.

1. Select **Configuration > Policy**.

2. In the **Policy Objects** list, select the CPL policy that you want to edit and click **Edit**.

3. Click the **Editor** tab. Locate the policy section that you want to edit. You can search for a section in the Quick Navigation pane. Click **Edit**. The Policy Editor displays the Edit Section dialog. Although you can name the section what best suits your needs, from the Purpose drop-down list, select from a defined list of rules that can be applied to your policy section:
   - Connection - Access Control
   - Connection - Termination
   - Authorization
   - Threat protection - Outbound Policy - Forward Proxy
   - Threat protection - Outbound Policy - Reverse Proxy
   - Threat protection - Inbound Policy
   - DLP Policy
   - Privacy
   - Content Filtering
   - Quality of Service
   - Caching
   - Bandwidth Management
   - Custom Solution

4. Click **OK**. The edited section is added at the top of the Editor.

   **NOTE**
   
   If you do not name the section, and only give it a purpose, the section appears as Untitled.

5. To commit your changes, enter a comment for the commit operation and click **Save**. The comment you enter is saved as policy metadata.

6. (Optional) To exit without saving your edits, click **Cancel**.

7. (Optional) Click **Compare** to see the differences between the existing policy version and the version you are about to commit.

### Find a Policy Section

You can search for an existing policy section using keywords. When you perform the keyword search, the system searches policy sections and matches partial and full strings. The search does not include previous versions of policy.

1. Select **Configuration > Policy**. From Policy Objects, find the CPL Policy you want under **Type**. Or from the **Filters** dialog on the right, go to the **Type** drop-down list and select **CPL**. Click **Apply Filters**. From the displayed CPL policies, select the policy you want. Click **Edit**.

2. Click the **Editor** tab. Above the **Quick Navigation** pane, in the search field, enter your search term. You can perform this search with all sections collapsed; any matches will cause sections to expand.
3. Press Enter or click the magnifying glass icon.

If the search finds no match
If the search does not find a match, the display does not change. You can search again using a different keyword.

If the search finds matches
If the search finds matches:
• To the right of the search field, the navigation arrows

  and the number of results display, as in the following example:

• In the main Policy Editor pane, the first match is highlighted.
• In the Quick Navigation pane, the section that contains the first match is highlighted.

To go to the next search result, click the right navigation arrow.

The result number shows the next match (for example, "2 of 13") and the selections in the main pane and Quick Navigation update to reflect the match.

Clear the search results
To clear search results, click the X in the search field.

Work with CPL Policy Sections

Layout Modes

Single Pane Layout
If the modular sections perform slowly, you can select the Single Pane Layout icon.

This is useful if the CPL is particularly long or if you prefer working with a single pane of code.

NOTE
Switching to a single pane and saving the policy erases all metadata about your sections. You cannot recover the sections by switching back. However, you can either discard the changes without a save, or you can restore a previous version.
Modular Layout

When you open a policy for editing, it defaults to the Modular Layout.

If your policy contains numerous sections or sub-sections, you can use features here to make writing and reviewing policy more manageable.
**Navigate sections**

**NOTE**
These sections only appear in the Modular Layout

The [Quick Navigation](#) pane displays an overview of all the sections in the policy object you are viewing. Each section is represented thus:

<table>
<thead>
<tr>
<th>Name</th>
<th>(Purpose)</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>override</td>
</tr>
</tbody>
</table>

where **Name** is the section name and **Purpose** is the purpose you selected when you created or edited the section.

When you change the order of policy sections or change a section name or purpose, the Quick Navigation pane displays the update immediately.

**Collapse a section**

Policy sections are expanded by default.

- To collapse a policy section, click the up arrow

  ![Untitled (Custom Solution)](image)

  in the section title bar.

- To expand a collapsed section, click the down arrow

  ![Untitled (Custom Solution)](image)

  in the title bar.

**Collapse all sections**

- To collapse all policy sections, click the **Collapse all sections** icon

- To expand all sections, click the **Expand all sections** icon

**Move sections**

You can move policy sections:
• Click the order up icon

in a section title bar to move the section up.

• Click the order down icon

in a section title bar to move the section down.

• Hover over the title bar of the section you want to move until the pointer changes to a

Drag the section to its new location.

Moving policy sections affects how policy is evaluated. See Change the Order in which Policy Rules are Evaluated for information.

Change the Order in which Policy Rules are Evaluated

You can change the order of the sections in policy, which in turn changes policy behavior. The CPL is evaluated from top to bottom—lower layers override higher layers; thus, the order of sections affects the order in which policy rules in each section are evaluated. Changing the order of policy sections can alter the effectiveness of policy, result in a rule overriding other rules, or cause unintended behaviors. See the following examples.

1. Select Configuration > Policy.
2. In the Policy Objects list, select the policy. If needed, search for the object; see Filter by Attributes and Keyword Search.
3. (Recommended) To collapse a section, click the

at the left of the title bar. You can click the

on the title bar of a collapsed section to expand it.
4. Hover over the title bar of the section you want to move. The pointer changes to a

Drag the section to its new location.
Alternatively, you can use the selection arrows

in the title bar to move the section up or down, respectively.
5. Move sections around in the policy object until you are satisfied that the policy will evaluate as you intend. If the policy has many sections, you can use the Quick Navigation pane on the right to quickly go to the section you want. See Navigate Policy Sections for instructions. A red asterisk (*) beside the policy object name denotes pending changes.
6. Click Save.

Example

The following is a basic example of how changing the order of sections can change the behavior of policy.
Consider a policy section with the purpose Threat protection - Inbound Policy. It contains the following CPL:

; Deny EXE downloads

;
Another policy section has the purpose **Access Control**. It contains the following CPL:

```plaintext
; Users in specified subnet are allowed transactions
client.address=192.0.2.0/24 ALLOW
```

Refer to the following table to see how the order of policy sections can affect the behavior of policy.

<table>
<thead>
<tr>
<th>Order of policy sections</th>
<th>How policy is evaluated</th>
<th>Resulting behavior</th>
</tr>
</thead>
</table>
| 1. Threat protection - Inbound Policy
  2. Access Control        | The Access Control section overrides the Threat protection section.                    | Everyone in the network is denied EXE downloads except for users in the specified subnet. |
| 1. Access Control
  2. Threat protection - Inbound Policy | The Threat protection section overrides the Access Control section.            | Users in the specified subnet are allowed transactions with the exception of EXE downloads; everyone in the network is also denied EXE downloads. |

### Refine Existing CPL Policy

**CAUTION**

The policy that you write is deployed to devices as it displays in the Policy Editor; Management Center does not attempt to compile or otherwise validate the CPL. If the policy does not compile, the Policy Editor displays a "Policy Install Failed" error message after you attempt to install it.

Much of the flexibility of managing policy in Management Center derives from the ability to organize policy rules in one or more **policy sections**, which you can use to group similar or related rules together.

### CPL Policy objects and sections

Policy in Management Center is structured thus:

- **Policy object**—The container for all policy that can be installed to a specific slot on a device. It has metadata and can be versioned. Device association is done at this level.
  - **Policy section**—A container for a high-level category of policy.
    - **Sub-section**—A container for the CPL; it specifies the default, override, and mandatory behavior affected by the policy.

If the modular sections perform slowly, you can select the **Single Pane Layout** icon.

This is useful if the CPL is particularly long or if you prefer working with a single pane of code.

**NOTE**

Switching to a single pane and saving the policy erases all metadata about your sections. You cannot recover the sections by switching back. However, you can either discard the changes without a save, or you can restore a previous version.

See [Work with CPL Policy Sections](#) for more information.

After you have written CPL directly in the Policy Editor or imported policy from a device, you should attempt to refine it as much as possible using these sections. Writing policy in sections, or breaking down an imported policy into sections, makes policy easier to read and edit.
Configuring policy for specific devices or multiple devices at once involves several methods of creating, testing, and updating policy.

1. Search for policy objects that contain the CPL you want to edit; see Filter by Attributes and Keyword Search. Once you have found the policy object, you can determine the policy section to edit; see Find a Policy Section.
2. (Optional) Make sure that the policy you are editing is the one you want. See View Existing Policy Information.
3. (If applicable) Edit the CPL directly in the Policy Editor. See Create the Content Policy Language. Refer to the Content Policy Language Reference for information on CPL syntax.
4. (If applicable) If policy does not behave as intended or must be improved, modify it by moving sections within policy. See Change the Order in which Policy Rules are Evaluated.
5. If the policy isn't working properly, you may want to compare the OS version on the associated device with the policy version. See Check Consistency between Policy and Devices.
6. (If applicable) Add sections to contain policy for other purposes. See Add a New CPL Policy Section.
7. (If applicable) Edit a section's name or purpose. See Edit a Policy Section.
8. Click **Delete Policy**, if you want to Delete a selected policy. A message displays "Are you sure you want to delete the policy?" Click **Yes** or **No**.

Launch Legacy or Web-Based VPM

Select one of the following topics:

- Launch Legacy Visual Policy Manager (Java)
- Launch Web-Based VPM

Legacy VPM—Set Up and Enable Java in Your Browser

When using the legacy VPM editor, Symantec recommends that you use the recommended Java version listed here.

Releases prior to Java 1.8 use a vulnerable cryptographic hash (SHA1) function that Management Center no longer supports. If you are using Java 1.8.131 or later, and would like to launch the VPM editor from within Management Center, you will need to upgrade your ProxySG(s) to an appropriate SGOS version:

- For SGOS 6.5.x, use 6.5.9.10 or later
- For SGOS 6.6.x, use 6.6.4 or later
- For SGOS 6.7.x, use 6.7.2 or later

Versions prior to these SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.

If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command.

1. From your browser, install the recommended Java version. Enable Java in your browser. Because every browser behaves differently, confirm that the correct Java version is installed and enabled by using your browser to go to: https://www.java.com/verify

   **NOTE**
   You may need to restart your browser after updating Java.

   **NOTE**
   Note: Some browsers no longer support Java.

1. After you have verified that your Java version is correct and a reference device is available, the **Launch VPM Editor** button is enabled.
2. Click **Launch VPM Editor** to open the Visual Policy Manager Editor. However, the following error can occur:
If you see this error after relaunching the VPM Editor it means that you need to allow java to run in your browser and accept the certificates that Java requires.

Launch Legacy Visual Policy Manager (Java)

This topic describes the requirements for running the legacy Visual Policy Manager (VPM). Refer to the ProxySG appliance Visual Policy Manager Reference for information on constructing policy using the VPM. This topic assumes that you are familiar with those steps.

Legacy VPM Requirements

- When using the legacy VPM editor, Symantec recommends that you use the recommended Java version listed here. Releases prior to Java 1.8 use a vulnerable cryptographic hash (SHA1) function that Management Center no longer supports. If you are using Java 1.8.131 or later and wish to use the Java-based VPM editor from within Management Center, you will need to upgrade the ProxySG to an SGOS version where this issue is addressed. Depending on the branch of SGOS running on your ProxySG appliances, load the appropriate version to support Management Center:
  - SGOS 6.5.x: 6.5.9.10 or later
  - SGOS 6.6.x: 6.6.4.1 or later
  - SGOS 6.7.x: 6.7.2.1 or later

  Versions prior to these SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.

  NOTE
  If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command. See # security for more information.

- Before using the VPM editor in Management Center, Symantec strongly recommends that you understand how the VPM Editor works and underlying policy enforcement in ProxySG appliances. For comprehensive information on creating policy, as well as assigning and changing enforcement domains for policy rules in the VPM, refer to the ProxySG Appliance Visual Policy Manager Reference and Advanced Policy Tasks.

- Ensure that you have the latest VPM resource XML file installed on your ProxySG. You can download the XML file from the Symantec Support site: https://support.symantec.com/content/dam/bluecoat/download/modules/security/SGv6/policyclassifier.xml

Launch the Legacy VPM

1. Select Configuration > Policy. From the Policy Objects list, locate the VPM policy object you want to edit. To narrow your search, you can do a Filter by Attributes and Keyword Search.

  NOTE
  To add a new VPM policy object, refer to Add a VPM Policy Object.

2. Click the policy name hyperlink or highlight the row and click Edit. Verify that you are in the Editor tab.
3. If necessary, import policy from the reference device. Click Import. See Select Reference Device for VPM Policy.
4. Click Launch VPM Editor. When the system displays the following message, click Run.
5. If you see a Security Warning, check the IP address and click **Continue**.

6. The web console displays the Visual Policy Manager.
   1. Add layers and rules, as required by your policy.
   2. Click **Save policy** when finished. The edited policy displays in the Policy Objects list with an updated revision number.

   **NOTE**
   If Java is not enabled on your browser, the VPM Editor cannot launch. See Setup and Enable Java in Your Browser.

### Select Reference Device for VPM Policy

The reference device is the device you designate as the source device for VPM policy configurations. You must select a reference device to launch the VPM editor.

1. Select **Configuration > Policy**. From the Policy Objects list, select a VPM policy. Click **Edit**.

   **TIP**
   A default reference device is not automatically populated. Associate at least one deployed device with the policy or manually configure a reference device to enable editing.

2. While the **Editor** tab is selected, select a Reference Device, using the object selector.

   **WARNING**
   Resolve displayed warnings before launching the VPM editor. The Launch VPM Editor button is grayed out if warnings are present.
3. To associate a reference device, from the Select Device dialog, select the check box by the device that you want to use as a reference. The selected device automatically displays in the Selected view. Click OK.

4. (Optional) You can create and edit a VPM policy as soon as you have selected a reference device and no warnings are displayed. Click Launch VPM Editor.

Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove devices associated with the policy.</td>
<td>Add or Remove Devices Associated with Policy</td>
</tr>
<tr>
<td>Restore a version of the policy.</td>
<td>Restore a Version of Policy</td>
</tr>
<tr>
<td>Create and edit a VPM policy using the VPM Editor.</td>
<td>Launch Visual Policy Manager</td>
</tr>
<tr>
<td>Import a policy configuration from a device.</td>
<td>Import Policy from a Device</td>
</tr>
</tbody>
</table>
View VPM Policy Source
Management Center enables you to view the CPL or XML policy source of a VPM policy.

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the VPM policy name.
   If needed, search for the policy object; see **Filter by Attributes and Keyword Search**.
3. With the policy selected, click **Editor**. The system displays the editor.
4. View the policy:
   - Click **Last Generated CPL** to view the CPL source.
   - Click **XML (UI Markup)** to view the XML source.

5. (Optional) **Edit** the policy.

Add a VPM Policy Object
To add a VPM policy object, complete the following steps.

1. Select **Configuration > Policy**.
2. Click **Add Policy**. The system displays the Create New Policy: Basic Information dialog.
3. Enter a name for the policy object.
4. Select **VPM** for the **Policy Type**.
5. Enter a **Reference ID**. Although entering a reference ID is not required, it is useful for filtering objects when building policy. If you do not enter a reference ID, the system assigns a default ID based on the policy name you enter. Imported policy objects are assigned a default ID.
6. Enter a description in the **Description** field. Although entering a description is not required, the description helps differentiate versions of the same policy.

7. If you are to include shared objects, verify that **Replace Substitution Variables** is enabled. See [Use Substitution Variables in Policies and Scripts](#) for more information.

8. Click **Next**.

9. Enter or select values for the defined attributes.

10. Click **Finish**.

### Launch Web-Based VPM

When editing a VPM policy object, you can choose to use the web-based VPM introduced in SGOS 6.7.4.x (if the device supports it).

**NOTE**

Before using the VPM editor in Management Center, Symantec strongly recommends that you understand how the VPM Editor works and underlying policy enforcement in ProxySG appliances. For comprehensive information on creating policy, as well as assigning and changing enforcement domains for policy rules in the VPM, refer to the [Web Visual Policy Manager WebGuide](#) and the ProxySG Appliance [Visual Policy Manager Reference](#).

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the desired VPM policy.
3. Click **Launch Web-Based VPM**.

![Launch Web-Based VPM](#)

The status indicates the VPM is launching.

![Preparing VPM Launcher](#)

4. Wait for the resources to download.

![Preparing VPM Launcher](#)

5. When the resources have finished downloading, the system displays the web-based VPM.
Web-Based VPM Shared Include Example

The following procedure describes how to include a shared policy object using the web-based VPM.

1. Select Configuration > Policy.
2. From the Policy Objects list, select the desired VPM policy.
3. Click Launch Web-Based VPM. The VPM opens in your browser.

4. Select or create the desired policy layer.
5. On the desired line number, click the field under Destination and select Set from the menu.
6. Select the desired list:
7. (Optional) Set the desired action condition by clicking the **Action** field.
8. When finished setting the destination and conditions, click **Save policy**.
   To exit the VPM Editor without saving changes, click the back arrow in the upper-left corner.

9. Enter a brief description of the policy changes in the **Save Changes** field, click **Save**.
10. Use the back arrow to exit the VPM Editor.

**Create Shared Objects**

**NOTE**
Users are warned if they attempt to delete a shared object currently assigned to a policy object. The error message lists all policies to which the shared object is assigned. When presented with the message, the user
must confirm the deletion by selecting **I understand that once I choose to delete the Object above, this action cannot be undone.**

**Create CPL Fragments**

CPL policy fragments are reusable building blocks of CPL policy. Because fragments are not complete CPL policy, you do not deploy them to devices but include them within policy that you deploy to devices.

- Create a CPL Policy Fragment
- Include a Policy Fragment

**Create a Category List**

A **category list** is a named set of URL categories that can be easily referenced in policy, allowing you to assign an allow or deny condition to all the categories in one simple rule, or reuse the list in multiple policy rules.

- Create Category Lists
- Category List Example

**Create a Category List Template**

A **category list template** provides a starting point for defining which categories to include in a category list. The template contains a subset of the complete list of WebPulse categories, typically used to restrict the categories a less-privileged user can select when creating a category list.

- Use Category List Templates

**Create a URL List**

URL lists allow you to easily create URL exceptions to your policy. The URL list can be easily included in your existing policy.

- Create URL List (URL Policy Exceptions)
- URL List Example

**Create an IP Address List**

Easily create IP address lists for use on the SSL Visibility appliance.

- Create SSL Visibility IP Address List

**Manage List Triggers**

When you create a URL or category list, Management Center includes subconditions and associated triggers optimized for the type of URL or category entered. These triggers are enabled by default but you have the option to disable some of them.

- Manage URL and Category List Triggers

**Create WAF Security Profile**

A **WAF Security Profile** is a shared object that defines the Web Application Firewall settings for the associated WAF application object. The WAF Security Profile is assigned to one or more WAF applications that can be installed on ProxySG appliances to set WAF policy.

- Configure WAF Security Rules (WAF Security Profile)

Creating a WAF Security Profile is step 3 in **Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.**
Create a CPL Policy Fragment

CPL fragments are shared objects. Like other shared objects, Policy fragments are reusable building blocks of CPL policy. Because fragments are not complete CPL policy, you include them within policy that you deploy to devices. Individual CPL policy fragments cannot be deployed by themselves.

Create a CPL Policy Fragment in the same way that you create CPL Policy.

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard. Fill in required fields.
   - Object name (*) - Required name
   - Object type (*) - From the drop-down list, choose CPL Fragment.
   - Reference ID (*) - Enter a Reference ID that you can filter on when building policy.

   **NOTE**
   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".

   - Description - Enter a meaningful description to help you when reusing this fragment.
   - Replace substitution variables - select this option if you want to replace specific values within the policy fragment. See Use Substitution Variables in Policies and Scripts.

   **NOTE**
   If Replace substitution variables is NOT selected when creating a CPL Policy, the CPL Policy Fragments will not be included in the CPL.

3. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the value of the attribute for this policy fragment. See Add Attributes.
5. Include shared objects in your CPL fragment. See Include a Shared Policy Object in CPL or VPM Policy.
Create URL List (URL Policy Exceptions)

URL lists allow you to easily create URL lists for use in policy. These lists can then be included in your existing policy for ProxySG or SSL Visibility appliances. An example implementation is described [here](#).

URL lists are shared objects. Because URL lists are not complete policy, you do not deploy them to devices but include them within policy that you deploy to devices.

**NOTE**
If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit ${include} and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

URL lists include **policy triggers that you may want to disable** to improve performance.

**Step 1 - Create the URL List Object**

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Fill in required fields.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose **URL List**.
   c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.  
      **NOTE**
      The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
   d. **Description** - Enter a meaningful description to help you when reusing this fragment.
4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See **Add Attributes**.
5. Click **Finish**. The URL list displays in the editor.

**Step 2 - Add URLs**

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired URL list. The system displays the URL list editor.
3. Enter the URL in the **URL** field and click **Add**.
The system displays the text entered into the **Description** field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:
   a. Create a URL list and copy the URLs.
   b. Click **Paste URLs**. The system opens the Paste URLs: Enter URLs dialog.
   c. Copy the URLs into the Paste URLs: Enter URLs dialog. Press **CTRL+V** or right-click and click **Paste**. The URLs are added to the list.
   d. Click **Next**. The system opens the Paste URLs: Validate dialog.
   e. Click **Finish**.

5. Click **Save**.

**Enabling and Disabling URLs**

You can disable an individual URL by selecting it and clicking **Disable**.

You can enable a URL by selecting it and clicking **Enable**.
Step 3 - Include the URL List in Policy

When you have completed your changes, you can include the URL list in CPL, as described in Include a Policy Fragment. The URL list will be included in the CPL as a named condition that can then be referenced using condition=referenceId. See the example below for details.

You can then install your policy as described in Install Policy.

**Whitelist Scenario Example**

**Enabling and Disabling URLs**
You can disable an individual URL by selecting it and clicking **Disable**.

You can enable a URL by selecting it and clicking **Enable**.

**URL List Example**

In this example, the administrator has created a simple acceptable use policy and would like to allow some URLs that would otherwise be blocked.

This CPL is stored in a policy object called **ASUP**. The **ASUP** policy object has **Replace substitution variables** enabled. Though the URL filtering blocks all news sites, she would like to allow cnn.com, yahoo.com, and nytimes.com. To allow these sites, the administrator does the following.

**Step One - Create the URL List Object**
1. Selects **Configuration > Shared Objects**.
2. Clicks **Add Object**. The web console displays the Create New Shared Object wizard.
3. Enters the following data:
   a. Object name: **whitelist**
   b. Object type: **URL List**
   c. Reference ID: autofill
   d. Description: **List of allowed URLs**
4. Clicks **Next**.
5. Clicks **Finish**.

**Step Two - Add Allowed URLs**
1. In the **whitelist** policy editor, the administrator enters **cnn.com** in the **URL** field and clicks **Add**.
2. Adds `yahoo.com` and `nytimes.com`, as described in the preceding step.
3. Clicks **Save** and enters a brief description of the change. The **whitelist** object now looks like this.

### Step Three - Add the URL List to the ASUP Policy

1. Selects **Configuration > Policy > ASUP**. The ASUP policy opens in the editor. Remember that the administrator has previously enabled **Replace substitution variables**.
2. Clicks **Operations > Insert > Insert Include**.
3. In the Insert Policy Include window, selects **whitelist** and clicks **OK**.
   
   The **ASUP** CPL now looks like this:

   ```plaintext
   NOTE
   The name of the condition corresponds to the shared object's reference ID, not its name. You can preview the policy by going to the **Targets** tab, adding a target, selecting the target, and clicking **Preview**.
   
   Though the URLs have been defined, they have not been added as a rule.
   4. To create the rule, the administrator adds the following rule to the CPL to implement the whitelist:
      ```plaintext
      condition=whitelist ALLOW
      ```
      
      See example below.
   ```plaintext
   5. Clicks **Save**.
   The **ASUP** CPL is now ready to be pushed to target devices.
   ```

### Manage URL and Category List Triggers

The policy rules that are created when you generate CPL for a URL or category list consist of a subcondition and a trigger.

**NOTE**

A condition (or subcondition) is a boolean combination of trigger expressions. Triggers are individual tests that can be made against components of the request. With a few notable exceptions, triggers test one aspect of request, response, or associated state against a boolean expression of values. For more information about CPL conditions and triggers, refer to the Content Policy Language Reference.

When you create a URL or category list, Management Center includes subconditions and associated triggers optimized for the type of URL or category entered. These triggers are enabled by default but you have the option to disable some of them. You might want to disable a trigger to improve performance for long lists, for example.
**URL List Triggers**

The included URL list subconditions and triggers are described in the following table. By default, the url.* triggers are used. You can switch to the server_url.* triggers if needed (for example, if the URL list is used in a forwarding layer).

<table>
<thead>
<tr>
<th>Subcondition</th>
<th>Associated Trigger</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_name/ url.domains</td>
<td>url.domain</td>
<td>example.com/ useexample.com198.51.100.10</td>
</tr>
<tr>
<td>list_name/ server_url.domains</td>
<td>server_url.domain</td>
<td>example.com/useexample.com198.51.100.10</td>
</tr>
<tr>
<td>list_name/ certificate_hostnames</td>
<td>server.certificate.hostname</td>
<td>example.com</td>
</tr>
<tr>
<td>list_name/ addresses</td>
<td>url.address</td>
<td>198.51.100.10</td>
</tr>
<tr>
<td>list_name/ server addresses</td>
<td>server_url.address</td>
<td>198.51.100.10</td>
</tr>
</tbody>
</table>

**Category List Triggers**
The included category list subconditions and triggers are described in the following table.

<table>
<thead>
<tr>
<th>Subcondition</th>
<th>Associated Trigger</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_name/</td>
<td>category</td>
<td>category='Adult/Mature Content'</td>
</tr>
<tr>
<td>category</td>
<td>Matches the content categories using the requested URL.</td>
<td></td>
</tr>
<tr>
<td>list_name/</td>
<td>server.certificate.hostname.category</td>
<td>server.certificate.hostname.category='Adult/Mature Content'</td>
</tr>
<tr>
<td>cert_category</td>
<td>Matches the category using the hostname in the server certificate. This applies only to SSL connections; the associated trigger examines the SSL certificate to detect the category associated with the hostname that is being visited.</td>
<td></td>
</tr>
</tbody>
</table>

Category List Triggers

The included category list subconditions and triggers are described in the following table.

<table>
<thead>
<tr>
<th>Subcondition</th>
<th>Associated Trigger</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_name/</td>
<td>category</td>
<td>category='Adult/Mature Content'</td>
</tr>
<tr>
<td>category</td>
<td>Matches the content categories using the requested URL.</td>
<td></td>
</tr>
<tr>
<td>list_name/</td>
<td>server.certificate.hostname.category</td>
<td>server.certificate.hostname.category='Adult/Mature Content'</td>
</tr>
<tr>
<td>cert_category</td>
<td>Matches the category using the hostname in the server certificate. This applies only to SSL connections; the associated trigger examines the SSL certificate to detect the category associated with the hostname that is being visited.</td>
<td></td>
</tr>
</tbody>
</table>

Change URL or Category List Triggers

1. Select **Configuration > Policy > Shared Objects** and edit the URL or category list.
2. Click the gear icon to open the Advanced Settings dialog.
   
   ![Show screen.](image)

3. Select or deselect the desired triggers and click **Save**.

Create a Local Content Filter Database

The Local Content Filter Database is a list of URL categories that each of your ProxySG, Advanced Secure Gateway, and SSL Visibility (SSLV) appliances subscribe to, for use in policy. Unlike shared lists and policy-based categories, the local database feature creates a file that is hosted on the Management Center appliance. Configured ProxySG, Advanced Secure Gateway, and SSLV appliances query Management Center for updates to the database at regular intervals.
NOTE
Local database content filter configuration is supported on all SGOS devices and versions. SSL Visibility supports local category database configuration in the 3.x branch in 3.9.4.1 and later (except Virtual Appliance versions), and in the 4.x branch, version 4.2.x and later.

Step 1 - Create a Local Database Policy Object
1. In the Management Center web user interface, Click Configuration > Policy.
2. Click Add Policy. The web console displays the Create New Policy wizard.
3. Fill in required fields.
   a. Policy name (*) - Required name
   b. Policy type (*) - From the drop-down list, select Local Database.

   Create New Policy: Basic Information

   Basic Information

   Policy name: Example_Local_Database

   Policy type: Local Database

   Reference ID: Local_Database

   Description:

   1024 of 1024 characters left

   c. Reference ID (*) - Enter a Reference ID that you can filter for when building policy.

   NOTE
   The Reference ID is auto-generated. If you choose to define it manually, the Reference ID must begin with a letter and must contain only letters, numbers, or underscores.

   d. Description - (Optional) a meaningful description to help you when referring to this Local Database.

4. Click Next. The Create New Policy wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute values for the local database. See Add Attributes for more information on working with attributes.
5. Click Finish. The editor displays the new local database.

Step 2 - Add Categories to the Local Database

Supported Local Category Syntax

The local category editor supports the following syntax:
- **Domain**: example.com
- **Domain with path**: example.com/directory/server
- **Subdomain**: server.example.com/
- **Top Level domains**: .gov, .net, .com...
- **Single label host names**: server1
- **IPv4 address**: 203.0.113.5
- **IPv6 address**: [2001:db8:0:1:1:1:1:1]
- **IPv6 with embedded IPv4 addresses**: [0:0:0:FFFF:203.0.113.5]

### Local Category Limitations

Local category support has the following limitations:

- Each local database can contain up to 200 categories.
- The same URL cannot be included in more than four categories in a single local database.

### Define and Manage Local Categories

1. Click **Add Category**. The system displays the **Add Category** dialog.

![Add Category Dialog](image)

   - **Name**: Category 1
   - URLs:
     - www.mycompany.com
     - www.internet.com
     - www.symantec.com

2. Define URLs or IP addresses for this category. Note the syntax and limitations note at the beginning of this section. The text editor in this dialog validates the syntax of entries with red text.

3. Repeat steps one and two until you are satisfied with the categories and their entries, then click **Save**. The system displays the **Save Changes** dialog. Enter a comment to save the new local database and click **Save**.

### Optional Step - Import Categories

Management Center supports importing of local database categories included in text files with an .ldb extension. For more information, see **Create a Local Database File**. If you have previously created a local database file, you can import it into your new database by clicking **Import**.

**NOTE**

Management Center can also export category content in JSON format from the **Configuration > Policy** page. If you have previously done so, you can import that file into your new database by clicking **Import**. For more information on exporting policy objects, see **Export Policy or Shared Objects to Local Disk**.

**NOTE**

Plain text-formatted local database files (such as those exported from SGOS devices) are not compatible with the import function.

### Edit a Category

Refine the entries in your database categories.

1. Click the **memo pad** icon
at the far right of the category name for the category you want to modify. The system displays the **Add Category** dialog. You can enter, modify, or delete entries, just as when you initially created the category.

2. Click **Save** to save your changes. The Add Category dialog closes. Management Center displays an asterisk before Local Database at the top of the page, indicating that the updated category definition must be committed.

3. Click **Save**

**View Database Versions**

Management Center uses version control to track each change to a local database. Use the following steps to view, compare, or restore versions of a local database.

1. While viewing your local database, click the **Versions** tab.
2. Select an entry and click **View**. The system displays the **Preview of Version x.x** dialog.
3. Click either of the buttons at the top of this list to expand all or collapse all categories.
4. Click **Close** to close the preview dialog.

**Compare Database Versions**

1. While in the **Versions** tab, hold CTRL or ⌘ on your keyboard and simultaneously click to select two versions of the local database you want to compare.
2. Click **Compare**. The system displays a version of the policy editor with both versions of the local database. In this display, new content highlighted in green, modified content in yellow, and removed content in red.
### Step 3 - Deploy the Local Database

Management Center hosts your new local policy file, and each of your SSL Visibility, ProxySG or Advanced Secure Gateway appliances can now be configured to request it. By default, SSLV and SGOS will query the configured remote host for a local category database once an hour.

**Record the Local Database Direct URL**

Management Center automatically generates a URL from which your devices can retrieve the local database.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>define category Allowed</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>google.com</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>usa.gov</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>test.com</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>symantec.com</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>mycompany.com</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>example.com</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>test.net</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>end</td>
<td>9</td>
</tr>
</tbody>
</table>

1. While editing a local database, click the **Info** tab.
2. In the **Direct URL** field, click the **copy icon** to copy the URL to your system's clipboard.
3. Use the Direct URL to configure the local policy remote URL on your appliance. See the next section for Local URL configuration steps for your appliance.
4. (Optional) Click the **refresh icon** to regenerate the Direct URL. The previous URL becomes invalid when a new URL is generated.
Local Database URL Protocol Note

Your SSL Visibility, ProxySG or Advanced Secure Gateway appliances must have the certificate chain for Management Center in its stores before they can establish an HTTPS connection to Management Center URLs like the one used to host the local database. See your product documentation for steps to install the Management Center console certificate to initiate this trust relationship. If your appliance does not have the Management Center certificate installed, you may modify the provided URL to use HTTP in place of HTTPS, and port 8080 in place of 8082. In addition, Management Center must also have HTTP management enabled with the CLI command: `security http enable` before it can host HTTP content. Modified in this way, the URL in above image is as follows: `http://<MC_IP>:8080/direct/policy/F5kdR6lt`

**NOTE**
If you enable HTTP after using HTTPS, you must delete the HTTPS cookie from your browser to be able to use the HTTP connection for the UI.

Manual Deployment - SSL Visibility

Configure SSL Visibility appliances running version 3.9.4.1 or later, or 4.2.x or later.

1. Log into the SSL Visibility web management console.
2. Click **Policies > Host Categorization List**.
3. Under **Host Categorization Database Providers**, click **Local**. The **Host Categorization Status and Database Settings** details display.
4. Click the Pencil icon next to **Host Categorization Database Settings**. The system displays the **Edit Host Categorization Status and Database Settings** dialog.

5. Paste the URL from the **Direct URL** field in the **Info** tab in the Management Center web interface into the **URL** field.

Show screen...
6. Ensure that the **Manual Download Mode** check is clear if you want SSLV to query Management Center periodically for updates to the local database.

7. (Optional) If your SSLV configuration requires a proxy to reach Management Center on your network, enter the connection and authentication details as appropriate.

8. 3.9.4.1 only - (Optional) if your appliance has the HTTPS CA and server certificates for Management Center, select the **External CA** list containing that certificate.

**NOTE**
If your SSL Visibility appliance does not have the HTTPS certificate in its PKI stores, refer to the **Local Database URL Protocol Note** above.

**Manual Deployment - ProxySG and Advanced Secure Gateway**

*Install the URL in each appliance you want use this local database.*

1. Log in to your ProxySG or Advanced Secure Gateway management console.
2. Browse to **Configuration > Content Filtering > Local Database**.
3. Paste the URL from the previous step into the **URL** field and click **Apply**.
4. Click **Download Now** to retrieve the database for the first time.
5. Browse to **Content Filtering > General** and put a check in the **Enable** box next to **Local database**. Click **Apply**. This ensures that the appliance will retrieve database updates automatically, as they become available.

(Optional) Scripted Configuration - ProxySG and Advanced Secure Gateway

Management Center can configure each of your ProxySG and Advanced Secure Gateway appliances with the help of a script. Follow the steps below if you would prefer to have Management Center push the settings to each of your ProxySG or Advanced Secure Gateway appliances.

1. In the Management Center management console, browse to **Configuration > Scripts**.
2. Click **Add Script**.
3. Name the new script. In this example, we use **LocalDBSettings**.
4. Select the device type of **ProxySG** or **Advanced Secure Gateway**, as appropriate, and click **Save**.
5. Enter the following details for your new script, replacing the URL in the example for the unique URL generated by your Management Center:

   ```plaintext
   content-filter local download url http://MC_IP:8080/direct/policy/
   F5kdR6lt download auto download get-now exit provider local enable
   ```

6. Click **Save** and enter a comment for the commit operation.
7. Click **Execute on Device**.
8. Select one or more target appliances and click **Execute**. Management Center applies the script to the selected appliances and displays the results in the **Job Progress** dialog.

**TIP**
For more information on writing configuration scripts, see **Create a Script**.

**Define and Manage Local Categories**

1. Click **Add Category**. The system displays the **Add Category** dialog.
2. Define URLs or IP addresses for this category. Note the syntax and limitations note at the beginning of this section. The text editor in this dialog validates the syntax of entries with red text.

3. Repeat steps one and two until you are satisfied with the categories and their entries, then click **Save**. The system displays the **Save Changes** dialog. Enter a comment to save the new local database and click **Save**.

**Optional Step - Import Categories**

Management Center supports importing of local database categories included in text files with an .ldb extension. For more information, see Create a Local Database File. If you have previously created a local database file, you can import it into your new database by clicking **Import**.

**NOTE**

Management Center can also export category content in JSON format from the Configuration > Policy page. If you have previously done so, you can import that file into your new database by clicking **Import**. For more information on exporting policy objects, see Export Policy or Shared Objects to Local Disk.

**NOTE**

Plain text-formatted local database files (such as those exported from SGOS devices) are not compatible with the import function.

**Edit a Category**

Refine the entries in your database categories.

1. Click the **memo pad** icon at the far right of the category name for the category you want to modify. The system displays the **Add Category** dialog. You can enter, modify, or delete entries, just as when you initially created the category.

2. Click **Save** to save your changes. The Add Category dialog closes. Management Center displays an asterisk before Local Database at the top of the page, indicating that the updated category definition must be committed.

3. Click **Save**

**View Database Versions**

Management Center uses version control to track each change to a local database. Use the following steps to view, compare, or restore versions of a local database.
1. While viewing your local database, click the **Versions** tab.
2. Select an entry and click **View**. The system displays the **Preview of Version x.x** dialog.
3. Click either of the buttons at the top of this list to expand all or collapse all categories.
4. Click **Close** to close the preview dialog.

**Compare Database Versions**

1. While in the **Versions** tab, hold CTRL or ⌘ on your keyboard and simultaneously click to select two versions of the local database you want to compare.
2. Click **Compare**. The system displays a version of the policy editor with both versions of the local database. In this display, new content highlighted in green, modified content in yellow, and removed content in red.
Record the Local Database Direct URL

Management Center automatically generates a URL from which your devices can retrieve the local database.

1. While editing a local database, click the **Info** tab.
2. In the **Direct URL** field, click the **copy icon** to copy the URL to your system’s clipboard.
3. Use the Direct URL to configure the local policy remote URL on your appliance. See the next section for Local URL configuration steps for your appliance.
4. (Optional) Click the **refresh** icon to regenerate the Direct URL. The previous URL becomes invalid when a new URL is generated.

Local Database URL Protocol Note

Your SSL Visibility, ProxySG or Advanced Secure Gateway appliances must have the certificate chain for Management Center in its stores before they can establish an HTTPS connection to Management Center URLs like the one used to host the local database. See your product documentation for steps to install the Management Center console certificate.
to initiate this trust relationship. If your appliance does not have the Management Center certificate installed, you may modify the provided URL to use HTTP in place of HTTPS, and port 8080 in place of 8082. In addition, Management Center must also have HTTP management enabled with the CLI command: `security http enable` before it can host HTTP content. Modified in this way, the URL in above image is as follows: http://<MC_IP>:8080/direct/policy/F5kdR6lt

**NOTE**
If you enable HTTP after using HTTPS, you must delete the HTTPS cookie from your browser to be able to use the HTTP connection for the UI.

**Manual Deployment - SSL Visibility**

Configure SSL Visibility appliances running version 3.9.4.1 or later, or 4.2.x or later.

1. Log into the SSL Visibility web management console.
2. Click **Policies > Host Categorization List**.
3. Under **Host Categorization Database Providers**, click **Local**. The **Host Categorization Status and Database Settings** details display.
4. Click the Pencil icon next to **Host Categorization Database Settings**. The system displays the **Edit Host Categorization Status and Database Settings** dialog.

5. Paste the URL from the **Direct URL** field in the **Info** tab in the Management Center web interface into the **URL** field.
6. Ensure that the **Manual Download Mode** check is clear if you want SSLV to query Management Center periodically for updates to the local database.
7. (Optional) If your SSLV configuration requires a proxy to reach Management Center on your network, enter the connection and authentication details as appropriate.
8. 3.9.4.1 only - (Optional) if your appliance has the HTTPS CA and server certificates for Management Center, select the **External CA** list containing that certificate.
NOTE
If your SSL Visibility appliance does not have the HTTPS certificate in its PKI stores, refer to the Local Database URL Protocol Note above.

Manual Deployment - ProxySG and Advanced Secure Gateway

Install the URL in each appliance you want use this local database.

1. Log in to your ProxySG or Advanced Secure Gateway management console.
2. Browse to Configuration > Content Filtering > Local Database.
3. Paste the URL from the previous step into the URL field and click Apply.
4. Click Download Now to retrieve the database for the first time.
5. Browse to Content Filtering > General and put a check in the Enable box next to Local database. Click Apply. This ensures that the appliance will retrieve database updates automatically, as they become available.

(Optional) Scripted Configuration - ProxySG and Advanced Secure Gateway

Management Center can configure each of your ProxySG and Advanced Secure Gateway appliances with the help of a script. Follow the steps below if you would prefer to have Management Center push the settings to each of your ProxySG or Advanced Secure Gateway appliances.

1. In the Management Center management console, browse to Configuration > Scripts.
2. Click Add Script.
3. Name the new script. In this example, we use LocalDBSettings.
4. Select the device type of ProxySG or Advanced Secure Gateway, as appropriate, and click Save.
5. Enter the following details for your new script, replacing the URL in the example for the unique URL generated by your Management Center:
   
   define category TestLocalPolicy1
   www.facebook.com ;test facebook
   www.linkedin.com ;test linkedIn
   end
   define category TestLocalPolicy2

6. Click Save and enter a comment for the commit operation.
7. Click Execute on Device,
8. Select one or more target appliances and click Execute. Management Center applies the script to the selected appliances and displays the results in the Job Progress dialog.

TIP
For more information on writing configuration scripts, see Create a Script.

Create a Local Database File

Management Center supports importing of local database categories included in text files with an .ldb extension. To create the local database file, open a text file and save it with your preferred name and then change the extension .ldb.

Example 1

1. Open a text file and save it as example1.
2. Change the file extension to .ldb.
   The file should now be named example1.ldb.
3. Add the following:
   define category TestLocalPolicy1
   www.facebook.com ;test facebook
   www.linkedin.com ;test linkedIn
   end
   define category TestLocalPolicy2
www.stackoverflow.com ;test stackoverflow
end

4. Save the file again.

These entries create a local database policy with two categories named TestLocalPolicy1, and TestLocalPolicy2. Notice that comments need to have an empty space and ; after the URL.

Example 2

1. Open a text file and save it as testPolicy2.
2. Change the file extension to .ldb.
   The file should now be named testPolicy2.ldb.
3. Add the following:
   define category HTTP_allowlist
   symantec.com ;here's a comment
   www.linkedin.com
   end
   define category FTP_allowlist
   facebook.com ;here's another comment
   linkedin.com
   end
4. Save the file again.

After creating a local database file, you can import it into Management Center as described in Create a Local Content Filter Database.

Create SSL Visibility List Policy

You can create policy in Management Center that manages URL or IP address lists for SSL Visibility appliances, and then deploy the policy to a group of SSL Visibility appliances. The following options are available:

- Create IP address or URL lists in Management Center and add them to an SSL Visibility list policy.
- Import URL or IP address lists from an SSL Visibility appliance into a Management Center list.
- Map Management Center lists to SSL Visibility IP address or URL lists; when the SSL Visibility list policy is deployed, the lists will be synchronized (with the Management Center list being the "master").

Step 1 - Create the List Object

Regardless of whether you are creating the list entries directly in Management Center or importing them from SSL Visibility, you first need to create an IP address or URL list object.

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields.
   a. Object name (*) - Required name
   b. Object type (*) - From the drop-down list, choose the type of list: URL List or IP Address List.
c. Reference ID (*) - Enter a Reference ID that you can filter for when building policy.
   
   NOTE
   The Reference ID must begin with a letter and must contain only letters, numbers, and "_".

d. Description - Enter a meaningful description to help you when reusing this object.

4. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute’s value for this policy fragment. See Add Attributes.

5. Click Finish. The new list displays in the editor.

Step 2 - Add URLs or IP addresses to the List (Optional)

You can optionally add URLs or IP addresses to this list or if the list already exists on the SSL Visibility device, you can import the list (see Step 3).

Step 3 - Import URLs or IP addresses from an SSL Visibility Appliance

If one of your SSL Visibility appliances already has URL or IP address lists, you can save time by importing the list into a Management Center list (instead of retyping the list in Management Center).

1. Select Configuration > Shared Objects.
2. Select the URL or IP address list you created in Step 1.
3. Select **Import > From Device**. The Source Device dialog lists all the SSL Visibility devices that have been added to Management Center.

4. Enable the check box next to the SSL Visibility device containing the list you want to import into Management Center and click **Next**. The Select Policy dialog displays the lists on the SSL Visibility device.
5. Select the list name you want to import and click **Import**.

6. Click **Import and overwrite**. The entries contained in the list in the SSL Visibility appliance are now listed in the Management Center list.

7. Click **Save**.

**Step 4 - Create the SSL Visibility Policy Object**

Management Center has a policy type specific to SSL Visibility lists. You create the SSL Visibility lists policy as described in this step and then add IP address or URL lists to it as described in Step 5.

1. Select **Configuration > Policy**.
2. Click **Add Policy**. The Create New Policy wizard opens.
3. **Policy name**: Enter a descriptive name for the policy.
4. **Policy type**: Choose **SSLV Lists** from the drop-down.
5. **Reference ID**: This is supplied automatically, based on the policy name (spaces are replaced with underscores).
6. (Optional) **Description**: Enter a description up to 1024 characters.
7. Click **Next**.
8. Click **Finish**.

**Step 5 - Add Lists to the SSL Visibility List Policy**

After you have created the SSL Visibility list policy, you can add one or more IP address or URL lists to it.

1. In the SSLV Lists policy screen, click **Add List**. The system displays the URL Lists window.
2. Select the check box next to the list you want to include in the policy.
3. Click OK. The list(s) are shown in the policy.
4. Click Save.

**Step 6 - Mapping Management Center Lists to SSL Visibility Lists**

When Management Center syncs policy to the SSL Visibility device, it needs to know which Management Center lists correspond to which lists on the SSL Visibility device. This is accomplished by mapping the SSL Visibility list to the Management Center list. During the policy sync, Management Center compares the entries in the mapped lists. Any entries on the Management Center list that aren't present on the SSLV list will be added to the SSL Visibility list. Any entries on the SSL Visibility list that aren't in the Management Center list will be deleted.

1. In the SSLV policy, click **Add List**.
2. Select the list.
3. In the **Subject/List Name on SSLV** field, enter the name of the SSL Visibility list that you want to map to.
4. Click **OK**.

**NOTE**
When the list policy is synched to SSL Visibility appliances, any lists that aren’t on the SSL Visibility appliance will be created as subject/domain name lists. However, note that Management Center will not delete a subject/domain name list on the SSL Visibility appliance if it isn’t present in the Management Center policy.

You can install the SSLV list policy directly on an SSL Visibility device or create a job to schedule the policy installation.
Troubleshooting SSLV List Execution

If an SSLV List policy contains a shared object that has been deleted, policy execution will fail. To help you identify the problem before executing the policy, the system displays **Error: List not found** in the policy list.

<table>
<thead>
<tr>
<th>List Name</th>
<th>Type</th>
<th>Reference ID</th>
<th>Subject/List Name on...</th>
<th>Version Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error: List not found</td>
<td></td>
<td></td>
<td>IP_List1</td>
<td>Latest Version</td>
</tr>
<tr>
<td>URL List</td>
<td>URL List</td>
<td>URL_List</td>
<td>URL_List</td>
<td>Latest Version</td>
</tr>
</tbody>
</table>
If the SSLV list policy that contains a deleted shared object is executed, the system returns a specific error stating that one or more lists could not be found. You must remove all missing lists before successfully executing the policy.

Create SSL Visibility URL List Policy

You can create policy in Management Center that manages URL lists for SSL Visibility appliances (SSLV), and then deploy the policy to a group of SSL Visibility appliances. The following options are available:

- Create URL lists in Management Center and add them to an SSLV list policy.
- Import URL lists from SSLV into a Management Center URL list.
- Map Management Center URL lists to SSL Visibility lists; when the SSLV list policy is deployed, the lists will be synchronized (with the MC list being the "master").

Step 1 - Create the URL List Object

Regardless of whether you are creating the list entries directly in MC or importing them from SSLV, you first need to create a URL list object.

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields.
   a. Object name (*) - Required name
   b. Object type (*) - From the drop-down list, choose URL List.
   c. Reference ID (*) - Enter a Reference ID that you can filter for when building policy.
      NOTE
      The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
   d. Description - Enter a meaningful description to help you when reusing this fragment.
4. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See Add Attributes.
5. Click Finish. The URL list displays in the editor.

Step 2 - Add URLs to the List (Optional)

You can optionally add URLs to this list or if the list already exists on the SSL Visibility device, you can import the URLs from the list (see Step 3).

Step 3 - Import URLs from an SSL Visibility Appliance
If one of your SSL Visibility appliances already has URL lists, you can save time by importing the URLs into a Management Center URL list (instead of retyping the URLs in MC).

1. Select **Configuration > Shared Objects**.
2. Select the URL list you created in Step 1.

3. Select **Import > From Device**. The Source Device dialog lists all the SSL Visibility devices that have been added to Management Center.
4. Enable the check box next to the SSL Visibility device containing the URL list you want to import into Management Center and click **Next**. The Select Policy dialog displays the lists on the SSL Visibility device.
5. Select the list name you want to import and click **Import**.

6. Click **Import and overwrite**. The URLs contained in the list in the SSL Visibility appliance are now listed in the URL list.

7. Click **Save**.

**Step 4 - Create the SSL Visibility Policy Object**

Management Center has a policy type specific to SSLV lists. You create the SSLV lists policy as described in this step and then add URL lists to it as described in Step 5.

1. Select **Configuration > Policy**.
2. Click **Add Policy**. The Create New Policy wizard opens.
3. **Policy name**: Enter a descriptive name for the policy.
4. **Policy type**: Choose **SSLV Lists** from the drop-down.
5. **Reference ID**: This is supplied automatically, based on the policy name (spaces are replaced with underscores).
6. (Optional) **Description**: Enter a description up to 1024 characters.
7. Click **Next**.
8. Click **Finish**.

**Step 5 - Add URL Lists to the SSLV List Policy**

After you have created the SSLV lists policy, you can add one or more URL lists to it.

1. In the SSLV Lists policy screen, click **Add List**. The URL Lists window opens.
2. Select the check box next to each URL list you want to include in the policy.
3. Click OK. The list(s) are shown in the policy.

**Step 6 - Mapping Management Center URL Lists to SSL Visibility URL Lists**

When Management Center syncs policy to the SSL Visibility device, it needs to know which MC URL lists correspond to which URL lists on the SSLV device. This is accomplished by mapping the SSL Visibility list to the MC URL list. During the policy sync, Management Center compares the entries in the mapped lists. Any entries on the MC list that aren't present on the SSLV list will be added to the SSLV list. Any entries on the SSLV list that aren't in the MC list will be deleted.

1. In the SSLV policy, click Add List.
2. Select the URL list.
3. In the **Subject/List Name on SSLV** field, enter the name of the SSLV URL list that you want to map to.
4. Click **OK**.

**NOTE**
When SSLV list policy is synched to SSL Visibility appliances, any URL lists that aren't on the SSLV will be created as subject/domain name lists. However, note that Management Center will not delete a subject/domain name list on the SSLV if it isn’t present in the MC policy.

You can install the SSLV list policy directly on an SSL Visibility device or create a job to schedule the policy installation.
Troubleshooting SSLV List Execution

If an SSLV List policy contains a shared object that has been deleted, policy execution will fail. To help you identify the problem before executing the policy, the system displays **Error: List not found** in the policy list.

<table>
<thead>
<tr>
<th>List Name</th>
<th>Type</th>
<th>Reference ID</th>
<th>Subject/List Name on Target</th>
<th>Version Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error: List not found</td>
<td></td>
<td></td>
<td>IP_List1</td>
<td>Latest Version</td>
</tr>
<tr>
<td>URL List</td>
<td>URL List</td>
<td>URL_List</td>
<td>URL_List</td>
<td>Latest Version</td>
</tr>
</tbody>
</table>
If the SSLV list policy that contains a deleted shared object is executed, the system returns a specific error stating that one or more lists could not be found. You must remove all missing lists before successfully executing the policy.

Create IP Address List

Using this feature, you can create IP address lists for use on the SSL Visibility appliance, Blue Coat ProxySG appliance, or Advanced Secure Gateway (ASG). IP address lists are shared objects, and are similar to URL lists.

Step 1 - Create the IP Address List Object

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields.
   a. Object name (*) - Required name
   b. Object type (*) - From the drop-down list, choose IP Address List.
   c. Reference ID (*) - Enter a Reference ID that you can filter for when building policy.
      NOTE
      The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
   d. Description - Enter a meaningful description to help you when reusing this object.
4. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined a policy attribute as mandatory, you can choose the attribute’s value for this policy fragment. See Add Attributes.
5. Click Finish. The new IP address list displays in the editor.

Step 2 - ProxySG and ASG Only: Configure CPL Settings

1. Select Configuration > Shared Objects.
2. Select or edit the desired IP address list. The system displays the IP address list editor.
3. Click the gear box. Show screen.
4. In IP List - Advanced Settings, select the appropriate CPL trigger and click save.

The triggers allow you to add an IP address list object as either a source or destination object:

- **Source Object Triggers:**
  - `client.address`
  - `client.effective_address`

- **Destination Object Triggers:**
  - `url.address`
  - `url.server_address`

Refer to the [Content Policy Language Reference](#) for more information about these triggers.

**Step 3 - Add IP Addresses**

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired IP address list. The system displays the IP address list editor.
3. Enter the IP address in the **IP Address** field and click **Add**.
NOTE
The system displays the text entered into the Description field as a comment in the generated policy.

4. Alternatively, paste in multiple IP addresses:
   a. Create an IP address list and copy it in.
   b. Click Paste IP addresses. The system opens the Paste IP addresses: Paste IP addresses dialog.
   c. Copy the URLs into the Paste IP addresses: Paste IP addresses dialog. Press CTRL+V or right-click and click Paste. The URLs are added to the list.
   d. Click Next. The system opens the Paste IP addresses: Validate dialog.
   e. Click Finish.
5. Click Save.

Enabling and Disabling IP Addresses

You can disable an individual IP address by selecting it and clicking Disable.

You can enable an IP address by selecting it and clicking Enable.

Step 4 - Include the IP Address List in Policy

SSL Visibility

When you have completed your changes, you can include the IP address list in your SSLV policy object, as described in Create SSL Visibility List Policy.

You can then install your policy as described in Install Policy.

ProxySG

When you have completed your changes, you can include the IP address list in your ProxySG or ASG VPM or CPL policy object, as described in Include a Shared Policy Object in CPL or VPM Policy.

NOTE
See Add a VPM Policy Object and Create a CPL Policy Object for information.

You can then install your policy as described in Install Policy.
Enabling and Disabling IP Addresses
You can disable an individual IP address by selecting it and clicking Disable.

You can enable an IP address by selecting it and clicking Enable. ssl

SSL Visibility
When you have completed your changes, you can include the IP address list in your SSLV policy object, as described in Create SSL Visibility List Policy.

You can then install your policy as described in Install Policy.

ProxySG
When you have completed your changes, you can include the IP address list in your ProxySG or ASG VPM or CPL policy object, as described in Include a Shared Policy Object in CPL or VPM Policy.

NOTE
See Add a VPM Policy Object and Create a CPL Policy Object for information.

You can then install your policy as described in Install Policy.

Include a Shared Policy Object in CPL or VPM Policy
Use the CPL or VPM to reference policy fragments (such as URL lists, IP address lists, categories, category lists, and CPL fragments). CPL fragments are shared objects. Because fragments are not complete CPL policy, you include them within policy that you deploy to devices. Individual CPL policy fragments cannot be deployed by themselves.

To learn about creating policy fragments, see Create a CPL Policy Fragment. In Management Center 3.0 and later, CPL fragments can also include shared objects.

Add a Shared Object to a CPL Fragment
Include a CPL fragment, URL list, or category list.

1. Select Configuration > Shared Objects.
2. In the Shared Policy Objects list, click the CPL fragment to which you want to add the shared object. The policy is displayed in the Editor.
3. Place the text cursor into the policy section where you want to include the shared object and select Operations > Insert > Insert Include. You can only place a shared object into an existing policy section. The web console displays the Select Policies dialog.
4. From the available policy fragments, select the shared object to include.
5. To commit your changes, click Save and enter a comment for the commit operation. The comment that you enter is saved as policy metadata.
Add a Shared Object to CPL

Include a CPL fragment, URL list, or category list as a building block of CPL Policy.

1. Select Configuration > Policy.
2. In the Policy Objects list, select the CPL policy to which you want to add policy fragment. The policy is displayed in the Editor.
3. Click the Info tab.
4. Ensure that Replace substitution variables is selected.
   **NOTE**
   If you do NOT enable variable substitution in the CPL, the CPL Fragments will not be included.
5. Place the text cursor into the policy section where you want to include the policy fragment and select Operations > Insert > Insert Include. You can only place a fragment into an existing policy section. The web console displays the Select Policies dialog.

If you have not placed your cursor where you want to insert the policy fragment, Management Center displays the following error:

6. From the available policy fragments, select the shared object to include.
7. Click OK. The included policy fragment is displayed in the section where you placed your cursor. You can continue editing the CPL policy.

8. To commit your changes, click Save and enter a comment for the commit operation. The comment that you enter is saved as policy metadata.

9. (Optional) To exit without saving your edits, click Cancel.

10. (Optional) Click Compare to see the differences between the existing policy version and the version you are about to commit.

   NOTE
   For more information about adding or editing CPL Policy sections, see Add or Edit CPL Policy Sections.

Add a Shared Object to VPM Policy

Reference categories, category lists, and URL lists in a VPM policy. Categories that are added from Management Center are listed in under a custom Management Center provider. To view these click Configuration > Edit Categories... in the VPM. Management Center categories can be selected in any VPM object that lists categories, such as Request URL Category.

You cannot use this procedure to add CPL fragments. To add a CPL fragment, insert an include statement with the fragment's reference ID into the VPM CPL layer. For example, ${include:allowlist}.

   NOTE
   If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit ${include} and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.

1. Select Configuration > Policy.
2. From the Policy Objects list, select the desired VPM policy.
3. Review the Included Objects section.
4. Any lists already included in the policy are displayed in the **Included Objects** list. You may only reference shared objects if they are associated with the policy. To add available lists:
   a. Click **Add Object**.
   b. Select the additional lists to add to the policy, then click **OK**.

   **TIP**
   You can search for lists using the **Keyword Search**.

5. Make note of the reference ID for the object(s) you want to set.

6. (Optional) If you want to limit the lists to specific revisions in order to avoid unintentional changes, you can lock the revision version.
   a. Select an object.
   b. Click **Select Version**.
   c. Select **Use specific version**.
   d. Select the version number from the menu.
   e. Click **Save**.

7. (Optional) Select any lists to remove and click **Delete**.

   **NOTE**
   If any of the lists are in use, you need to launch the VPM Editor to remove or change the rules that reference them in the policy.

8. Once finished editing the available shared objects for the policy, click **Save**.

9. Click **Launch VPM Editor**.

   **NOTE**
   The following steps are shown using the legacy VPM editor. If you use the web-based editor, see [Web-Based VPM Shared Include Example](#) and [Launch Web-Based VPM](#).

10. Select or create the desired policy layer.

11. On the desired line number, right click the field under **Destination** and select **Set** from the menu.

12. Select the desired list:
   - By the reference ID from the objects list.
For a category, select any VPM object that lists categories.

**NOTE**

Shared objects are read-only. You cannot use the *Edit* option when setting the destination object. If you do try to edit it, it gets overwritten the next time you open the VPM editor.

13. (Optional) Set the desired action condition by right-clicking under the **Action** field.

14. When finished setting the destination and conditions, click **Save policy**. (Optional) To exit the VPM Editor without saving changes, close the VPM Editor and then click **Do not Save Policy**.

15. Enter a brief description of the policy changes in the **Save Changes** field, click **OK**, then click **Close**.

16. Close the VPM Editor.

17. Back in Management Center, on the VPM policy, click the **Info** tab.

18. Ensure that **Replace substitution variables** is selected, then click **Save**.

For more information about adding or editing VPM Shared Objects, see Create Shared Objects.

### Work with Categories

Refer to the following topics:

- Create Category Lists
- Category List Example
- Use Category List Templates
- Create Custom Categories
- Custom Category Example

### Create Category Lists

A *category list* is a named set of URL categories that can be easily referenced in policy, allowing you to assign an allow or deny condition to all the categories in one simple rule, or reuse the list in multiple policy rules. Category lists are shared objects, and are similar to URL lists.

**NOTE**

Before completing this procedure, you might want to verify that your categories are up-to-date.

Category lists include *policy triggers that you may want to disable* to improve performance.

**NOTE**

If you use shared objects in your VPM policy and install that policy onto an appliance, the policy will not function properly if you later edit the policy locally (on the appliance) and save it. Explicit ${include} and substitution variables can result in invalid syntax errors. URL lists, category lists, IP address lists, etc., result in empty objects.
Step 1 - Create the Category List Shared Object

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields.
   - **Object name** (*) - Required name
   - **Object type** (*) - From the drop-down list, choose Category List.

![Create New Shared Object: Basic Information](image)

- **Reference ID** (*) - Enter a Reference ID (or accept the default name) will be used when building policy. The ID can be specified as the condition name in CPL.

   **NOTE**
   The Reference ID must begin with a letter and must contain only letters, numbers, and "_".

- **Template** — If you (or someone else) has previously created a category list template, click and select the template. The template will restrict what categories can be defined in the list. See Use Category Templates for more information.

- **Description** - Enter a meaningful description to help you identify this category list when including in policy.

4. Click Next. The Create New Shared Object wizard displays the Attributes dialog. If you defined any policy attributes, you can choose the attribute's value for this category list. See Add Attributes.
5. Click Finish. A tree of categories displays in the Editor tab. Note that the categories are grouped into folders (Business Related, Legal Liability, Non-Productive, and so forth) for organizational purposes—these folder names are not part of the policy.

Show screen...
NOTE
If you selected a template, you may not see all folders and categories.

Step 2 - Select Categories
After you have created the category list object, you can select the categories associated with the list. The list should include all categories that you want to treat the same way in policy. For example, the categories in the list should all be ones that you would want to deny access to or allow access to; the actual policy action (deny/allow) will be defined in the policy.

1. The tree of category folders should be displayed in the Editor. If the list isn't currently displayed, select Configuration > Shared Objects and click the defined list name to bring it up in the Editor.
2. Select the categories you want to include in your list. Follow these general guidelines:
   – To see what categories are in a folder, click the + to expand.
   – Selecting a folder's checkbox selects all categories in that folder.
   – You can unselect any category within a selected folder by clicking its check box.
   – When a folder is expanded to display its categories, Management Center displays the category descriptions and examples as well.
3. To view the category names assigned to this list, look at the Selected Categories panel at the bottom of the window.
4. Click **Save** and enter a brief description of the change.

**Step 3 - Include the Category List in Policy**

When you have defined the category list, you can include the object in CPL, as described in Include a Policy Fragment. In addition, you must create an allow/deny condition using `condition=referenceId`. See the Category List Example for details.

You can then install your policy as described in Install Policy.

**TIP**

If you want to check into which category Symantec WebPulse categorizes a URL, go to sitereview.bluecoat.com and enter the URL.

**Category List Example**

In this example, the administrator has created a simple acceptable use policy and would like to deny access to a list of categories that should not be allowed on the corporate network.

This CPL is stored in a policy object called **ASUP**. The **ASUP** policy object has Replace substitution variables enabled.
Step One - Create the Category List Object

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Enter the following data:
   a. Object name: **blocked_categories**
   b. Object type: **Category List**
   c. Reference ID: **blocked_categories**
   d. Template: (leave blank)
   e. Description: **a list of categories that should be denied in policy**
4. Click **Next**.
5. Click **Finish**.

Step Two - Select Categories that Should be Denied

The administrator would like to deny access to all legal liability categories and security threats, so she will select all the categories in the Legal Liability folder and Security Threats subfolder.

1. With a tree of available categories displayed in the Editor, click the Legal Liability check box. The Adult Related and Liability Concerns folders are also checked.
2. Click the + next to the Adult Related and Liability Concerns folders to display the category names, descriptions, and examples in these folders.
3. Expand the Security Threats folder to display the category names, descriptions, and examples in this folder.
4. Click the Security Threats check box to select all of its categories.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult Related (8 of 8)</td>
<td>Sites that contain material of adult nature that does not necessarily</td>
</tr>
<tr>
<td>Adult/Mature Content</td>
<td>be inappropriate for all age groups.</td>
</tr>
<tr>
<td>Extreme</td>
<td>Sites that are extreme in nature and are not suitable for general use.</td>
</tr>
<tr>
<td>Intimate Apparel/Swimsuit</td>
<td>Sites that contain images or offer the sale of swimsuits or intimate apparel</td>
</tr>
<tr>
<td>Mixed Content/Potentially Ad...</td>
<td>Sites with generally non-offensive content but that also have</td>
</tr>
<tr>
<td>Nudity</td>
<td>Sites containing nude or seminude depictions of the human body.</td>
</tr>
<tr>
<td>Pornography</td>
<td>Sites that contain sexually explicit material for the purpose of entertainment</td>
</tr>
<tr>
<td>Sex Education</td>
<td>Sites that provide information (sometimes graphic) on reproductive health</td>
</tr>
<tr>
<td>Sexual Expression</td>
<td>Sites that provide information about, promote, or cater to sexual expression</td>
</tr>
<tr>
<td>Liability Concerns (7 of 7)</td>
<td>Sites that include a visual depiction of a minor engaging in sexual activity</td>
</tr>
<tr>
<td>Child Pornography</td>
<td>Sites that discuss, encourage, promote, offer, sell, supply or facilitate</td>
</tr>
<tr>
<td>Controlled Substances</td>
<td>controlled substances related to illegal or harmful substances.</td>
</tr>
<tr>
<td>Gambling</td>
<td>Sites where a user can place a bet or participate in a betting game.</td>
</tr>
<tr>
<td>Piracy/Copyright Concerns</td>
<td>Sites that provide information or technology for cracking or piracy.</td>
</tr>
<tr>
<td>Scam/Questionable/Ilegal</td>
<td>Sites that advocate or give advice on performing acts that are illegal.</td>
</tr>
<tr>
<td>Violence/Hate/Racism</td>
<td>Sites that depict extreme physical harm to people, animals or property.</td>
</tr>
</tbody>
</table>
5. Click **Save** and enter a brief description of the change.

**Step Three - Add the Category List to the ASUP Policy**

1. Select **Configuration > Policy > ASUP**. The ASUP policy opens in the editor. Remember that the administrator has previously enabled **Replace substitution variables**.
2. Place the text cursor into the policy section where you want to include the category list and click **Operations > Insert > Insert Include**.
3. In the Insert Policy Include window, select **blocked_categories** and click **OK**. The inserted CPL now looks like this:

   \_${include:blocked.categories}_

   Though the category list has been defined, the condition still needs to be defined to deny access.
4. To create the condition to deny access to the category list named **blocked_categories**, the administrator adds the following line to the CPL:

   condition=blocked_categories DENY
5. Click **Save**.

6. To preview the code that is generated for this policy, go to the **Targets** tab, select a device, and click **Preview**.

   ![Preview](image)

   **NOTE**
   You can see in the preview that two conditions are created. The first condition (blocked_categories/url_category) just looks up the URL in WebPulse to find the category. The second condition (blocked_categories/cert_category) is used for SSL connections—it can sometimes glean extra information by looking up the host name in the SSL certificate.

The **ASUP** CPL can be pushed to target devices at the appropriate time.

### Use Category List Templates

A **category list template** provides a starting point for defining which categories to include in a category list. The template contains a subset of the complete list of WebPulse categories, typically used to restrict the categories a less-privileged user can select when creating a category list. For example, if you have a user with restricted permissions, you may not want him to control policy for any category—just particular ones that are appropriate for his role.

#### Create a Category Template

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.

3. Fill in required fields.
   - **Object name**- Required name
   - **Object type**- From the drop-down list, choose **Category List Template**.
   - **Reference ID**- Enter a Reference ID (or accept the default name).
NOTE
The Reference ID must begin with a letter and must contain only letters, numbers, and “_”.

**Description** - Enter a meaningful description to help you when applying this category list template.

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this category list. See Add Attributes.

5. Click **Finish**. A tree of categories is displayed.

6. Select the categories you want to include in the template. Follow these general guidelines:
   - To see what categories are in a folder, click the + to expand.
   - Selecting a folder's check box selects all categories in that folder.
   - You can unselect any category within a selected folder by clicking its check box.
   - When a folder is expanded to display its categories, Management Center displays the category descriptions and examples as well.

7. To view the category names assigned to this template, look at the Selected Categories panel at the bottom of the screen.

8. Click **Save** and enter a brief description of the change.

**Use a Category List Template**

To use the category list template, select it when creating a category list. The user can only select categories from this restricted list.

1. Select **Configuration > Shared Objects**.

2. Click **Add Object**
The web console displays the Create New Shared Object wizard.

3. Fill in required fields.
   - **Object name** — Required name Object type (*) - From the drop-down list, choose Category List.
   - **Reference ID** — Enter a Reference ID (or accept the default name) that you can use when building policy. The ID can be specified as the condition name in CPL.
     
     **NOTE**
     
     The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
   - **Template** — Click and select the template. The template will restrict what categories can be defined in the list.
   - **Description** — Enter a meaningful description to help you when reusing this category list.

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute’s value for this category list. See **Add Attributes**.

5. Click **Finish**. The Editor displays just the categories in the template, and the user can create a category list by choosing from the categories in the template.

**Show screen...**

6. Select the categories you want to include in the list.
7. To view the category names assigned to this list, look at the Selected Categories panel at the bottom of the window.
8. Click **Save** and enter a brief description of the change.

This category list can now be used in policy. See **Include a Policy Fragment**.

**NOTE**

To apply a category list template to an existing category list, edit the category list, go to the Info tab, select the template, and then save the list.

**NOTE**

When the CPL for a category list is generated and the list contains categories not present in the template (most likely because the template had been changed since last saving the list), those categories are not included in the condition definition CPL. If this occurs, a warning is included as a comment above the condition CPL, indicating which categories were removed.
Update Symantec Global Intelligence Network (BCIS/BCWF) Category Lists

The category list used to select the categories associated with category list or category list template objects (Policy > Shared Objects) might not match the list provided by sitereview.bluecoat.com. To ensure that the list of categories are synchronized with the latest updates, complete the following actions.

NOTE
You must have the Settings > Update permission to perform this operation.

1. Select Policy > Shared Objects.
2. Edit an existing category list or category list template, or create a new category object. See Create Category Lists and Use Category List Templates for more information.
3. Click the Manage Category Source icon.

The system displays the Manage Category Source dialog. If an update is available, the Latest Version section displays "An update is available. Download Now."

4. To update the categories, select the Download Now link. If you are in an offline network, retrieve the categories.xml file from the Broadcom download site and drag and drop it into the dialog (2.3.2.1 and later). See Download Symantec Software and Tools for more information.

5. If any of the existing categories were out-of-date, the system notifies you of each change and prompts you to accept the changes.

NOTE
If you choose to keep an existing category, the system displays the category as Unrecognized because the metadata for that category no longer exists.
6. If managed Reporter devices update their category lists, you must examine your saved reports to identify any out-of-date categories. For example, Reporter 10.4.1.1 includes new categories and you must complete this action or your saved reports will not work after the Reporter upgrade. To do this, open the report, identify any disparities, and update the filter with the new name(s). See Customize Reporter Report Options for more information about adding report filters.

   NOTE
   For more information about content filtering by category, refer to the SGOS Administration Guide.

Create Custom Categories

The category shared object allows you to easily create custom categories for use in policy. These categories can then be included in your existing policy for ProxySG appliances. An example implementation is described here.

Although a category object appears similar to a URL list, the category object generates a define category instruction in policy instead of a condition and subcondition definition. For example, if you create a category called blocklist and add example.com to it, the generated policy will look like this:

```
; Generated by Management Center from Category: Complex Category define category blocklist http://example.com/ end
```

As shown above, all custom categories created in Management Center are preceded by a comment noting the source of the category. On the ProxySG appliance, these categories are treated as yet another category source, like WebFilter, for example.

   NOTE
   A category differs from a category list, which is a named set of URL categories that can be easily referenced in policy.

Step 1 - Create the Custom Category

1. Select Configuration > Shared Objects.
2. Click Add Object. The web console displays the Create New Shared Object wizard.
3. Fill in required fields.
   a. Object name (*) - Required name
   b. Object type (*) - From the drop-down list, choose Category.
c. **Reference ID (*)** - Enter a Reference ID that you can filter for when building policy.

   **NOTE**
   The Reference ID must begin with a letter and must contain only letters, numbers, and "_".

d. **Description** - Enter a meaningful description to help you when reusing this object.

4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See Add Attributes.

5. Click **Finish**. The new category displays in the editor.

### Step 2 - Add URLs

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired category. The system displays the category editor.
3. Enter the URL in the **URL** field and click Add.

   **NOTE**
   The system displays the text entered into the **Description** field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:
   a. Create a category and copy the URLs.
   b. Click **Paste URLs**.
c. Copy the URLs into the Paste URLs: Enter URLs dialog. Press **CTRL+V** or right-click and click **Paste**. The URLs are added to the list.

d. Click **Next**. The system opens the Paste URLs: Validate dialog.

e. Click **Finish**.

5. Click **Save**.

**Step 3 - Include the Category in Policy**

When you have completed your changes, you can include the category in CPL or in the VPM, as described in **Include a Policy Fragment**. The category will be included in the CPL as a category definition that you will then reference in a proxy layer. See the example below for details.

You can then install your policy as described in **Install Policy**.

**News Whitelist Scenario Example**

**Enabling and Disabling URLs**

You can disable an individual URL by selecting it and clicking **Disable**.
You can enable a URL by selecting it and clicking Enable.

Custom Category Example

In this example, the administrator has created a simple acceptable use policy and would like to add a new whitelist category for news.

This CPL is stored in a policy object called ASUP. The ASUP policy object has Replace substitution variables enabled. Though the URL filtering blocks all news sites, she would like to allow cnn.com, yahoo.com, and nytimes.com. To allow these sites, the administrator does the following.

Step One - Create the Category Object
1. Selects Configuration > Shared Objects.
2. Clicks Add Object. The web console displays the Create New Shared Object wizard.
3. Enters the following data:
   a. Object name: News Whitelist
   b. Object type: Category
   c. Reference ID: autofill
   d. Description: List of allowed URLs
4. Clicks Next.
5. Clicks Finish.

Step Two - Add URLs
1. In the News Whitelist policy editor, the administrator enters cnn.com in the URL field and clicks Add.
2. Adds yahoo.com and nytimes.com, as described in the preceding step.
3. Clicks Save and enters a brief description of the change. The News Whitelist object now looks like this.

Step Three - Add the Category to the ASUP Policy
1. Selects Configuration > Policy > ASUP. The ASUP policy opens in the editor. Remember that the administrator has previously enabled Replace substitution variables.
2. Clicks Operations > Insert > Insert Include.
3. In the Insert Policy Include window, selects News Whitelist and clicks OK. The ASUP CPL now looks like this:
4. To create the rule, the administrator adds the following rule to the Web Filter layer in CPL to implement the News Whitelist:

```
category=News_Whitelist ALLOW
```

See example below.

NOTE
The name of the category corresponds to the shared object's reference ID, not its name. You can preview the policy by going to the **Targets** tab, adding a target, selecting the target, and clicking **Preview**.

5. Clicks **Save**.

The ASUP CPL is now ready to be pushed to target devices.

### Use WAF Policy To Protect Servers From Attacks

As more and more organizations move to web applications, they are exposed to new and sophisticated threats. While traditional firewalls and IPS systems are effective for detecting threats in layers 3 and 4, they cannot interpret the logic inside the application layer, making them ineffective against web application threats. Web Application Firewalls (WAF) were designed for just this purpose. WAF devices protect web applications by inspecting traffic and controlling access to applications.

### About WAF Policy

As described in **Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks**, WAF policies are designed to protect backend web applications and servers in a reverse proxy deployment from external security threats.

The Management Center WAF policy feature uses the following policy elements:

**Tenants.** Management Center WAF policy is centered around the concept of tenants. Tenants are administrative entities defined on the ProxySG appliance that allow policy to be applied to a request matching specific properties or conditions. Tenants represent one or more web applications. Each WAF application object (see below) is associated with a tenant.

**Tenant Determination File.** A Tenant Determination file includes policy conditions that control which tenant policy slot is evaluated for an HTTP request. When policy matches a request, the tenant is identified and all policy associated with the tenant ID is applied to the request. For example, a tenant's rules could indicate that all traffic to port 80 must have this tenant's policy applied to it. After setting these rules on Management Center, you deploy this file to your ProxySG appliances.

**WAF Security Profile.** A WAF security profile is a shared object that defines the Web Application Firewall settings for the associated WAF application object. For its rules to be enforced, a WAF security profile must be associate with a WAF application object.

**WAF Application Object.** WAF policy is configured through the use of a WAF application object. A WAF application represents a tenant (a web application or group of web applications) and its associated WAF security profile settings. Therefore, to create a WAF application, you must associate it with a tenant (web application) and a WAF security profile (security settings).

### About the Default Tenant

For new WAF deployments, you begin by associating a WAF application with the **default tenant**. The default tenant contains the policy rules applied to all requests that do not match a specific tenant. This ensures that all requests have a base level of WAF protection, and simplifies the deployment process.
After deploying policy to the default tenant, create additional tenants as needed. For example, you can define a tenant for your Salesforce application and another tenant for your SharePoint application. Then, you can create and apply specific policy to protect and control each of those tenants.

**About Tenant Determination**

The criteria that determines the correct tenant policy to apply to a request are called *tenant determination* rules. As shown below, tenant determination is controlled through the use of a `<tenant>` layer in the Landlord CPL slot on the ProxySG appliance.

**NOTE**

On Management Center, you configure the Landlord slot by creating a Tenant Determination File. In other words, the Landlord slot on the ProxySG appliance is referred to as a Tenant Determination File on Management Center.

The `<tenant>` layer in the Landlord slot specifies conditions and `tenant()` properties. Within this layer, a small subset of CPL conditions are supported. These conditions are used like a switch statement (conditional logic flow) to specify which tenant slot CPL should be evaluated for a given request. When the conditions on a line evaluate to true, the `tenant()` property is set and evaluation of the current layer ends.

After tenant determination, the request is routed through a tenant, whose policy is evaluated for that transaction. When no specific tenant is determined for a request, the default tenant policy is used. Tenant determination criteria governs which tenant's policy applies to a given request.

**Reference: Conditions and Examples**

**Supported Conditions**

The following table shows the tenant conditions supported in Management Center.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Available Qualifiers</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Address</td>
<td>matches</td>
<td>Client Address matches 10.167.3.25</td>
</tr>
<tr>
<td>Client Effective Address</td>
<td>matches</td>
<td>Client Effective Address matches 10.167.0.87</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>matches</td>
<td>Proxy Address matches 10.140.2.104</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>=</td>
<td>Proxy Port = 80</td>
</tr>
<tr>
<td>Port</td>
<td>=</td>
<td>Port = 80</td>
</tr>
<tr>
<td>URL</td>
<td>equalscontainsmatches regex</td>
<td>URL equals <a href="http://www.example.com/test">http://www.example.com/test</a></td>
</tr>
<tr>
<td>URL Domain</td>
<td>contains</td>
<td>URL Domain contains example.com</td>
</tr>
<tr>
<td>URL Extension</td>
<td>equalsis not present</td>
<td>URL Extension equals .net</td>
</tr>
<tr>
<td>URL Host</td>
<td>equalscontainsmatches regex</td>
<td>URL Host equals <a href="http://www.example.com">http://www.example.com</a></td>
</tr>
<tr>
<td>URL Path</td>
<td>equalscontainsmatches regex</td>
<td>URL Path equals /example</td>
</tr>
<tr>
<td>URL Query</td>
<td>equalscontainsmatches regex</td>
<td>URL Query contains ?name=</td>
</tr>
</tbody>
</table>

**Tenant Determination CPL Example**

The following CPL rules provide an example of tenant determination in the Landlord slot.

```
<tenant>
url.path.substring="/Webapp/portal" tenant(webapp_portal)
```
In the preceding CPL, the condition on each line is evaluated. If the condition is a match, the tenant() property on that line is set appropriately and the evaluation of the <tenant> layer exits. If no tenant is determined, the tenant(default) is used.

**NOTE**
The tenant(default) property is implicit and does not actually need to be included in the CPL rules. Always deploy WAF policy to the default tenant to ensure that all requests are processed by the WAF. Specific applications (or groups of applications) that require different WAF security settings can then be split off into unique tenants as required.

**WAF Policy Evaluation Example**
The example below describes WAF policy evaluation:

1. The ProxySG appliance intercepts a request.
2. The appliance examines the initial connection parameters (source, destination, port, URL).
3. The appliance applies policy to the traffic.
4. The Landlord policy (Tenant Determination File) is examined.
5. The request is set to a specific tenant slot, or to the default tenant slot.
6. The appliance re-evaluates the request using a CPL stack that contains the appropriate tenant policy.
7. If allowed by policy, the ProxySG appliance sends the traffic to the appropriate server.

**Determine Your Next Step**
If you are configuring WAF policy, continue to Manage Tenants, which is step 2 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

**Specify Tenant Determination Rules**
A Tenant Determination file includes policy conditions that control which tenant policy slot is evaluated for an HTTP request. When policy matches a request, the tenant is identified and all policy associated with the tenant ID is applied to the request. On the ProxySG appliance, this file is called the "Landlord Policy." See About WAF Policy for more information about the Landlord policy.

Specifying Tenant Determination rules is step 3 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

**Step 1 — Create a Tenant Determination File**
1. Select Configuration > Policy and click Add Policy.

The web console displays the Create New Policy: Basic Information wizard.
2. Enter a name for the policy object.
3. Select Tenant Determination File for the Policy Type.
4. (Optional) In the Reference ID field, enter a Reference ID that you can filter on when building policy.
   **NOTE**
   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".
5. (Optional) Enter a description in the Description field. Although entering a description is optional, entering a description can help you understand the purpose of the policy when you later refer to it.
6. Click Next.
7. Enter or select values for the defined attributes.
8. Click Finish.
   The new tenant determination policy object appears in the Policy Objects editor. When installed on a ProxySG appliance, this tenant determination file configures the policy in the ProxySG Landlord slot. Because no other tenants have yet been defined, this policy object directs requests to the default tenant. (The default tenant contains the policy rules applied to all requests that do not match a specific tenant.) For initial setups, WAF policy should be installed to the default tenant. To proceed, deploy the tenant determination file to your ProxySG appliances and continue to Configure WAF Security Rules (WAF Security Profile) to create a Security Profile.
9. (Optional) Add Target Devices.
10. (Optional) Install Policy.

**Step 2 — Optional: Add Tenant Determination Rules for Other Tenants**

Use this optional procedure to add additional tenants after deploying WAF policy to the default tenant. Only complete these steps if you require WAF application objects with different security profiles.

Tenant determination rules specify the properties used to identify a tenant. You specify these properties using a simple, natural language interface that generates equivalent CPL rules.

1. Select Configuration > Policy.
2. Click the policy name hyperlink or highlight the row and click Edit.
The selected file displays in the **Editor** tab.

3. Click **Add Rule**.

![Editor Tab](image)

The system displays the Add Rule dialog.

4. Click the **Tenant** field and select a tenant from the Select Tenant dialog.

![Select Tenant Dialog](image)

The Select Tenants dialog displays existing tenants in Management Center. For more information, see **Manage Tenants**.

5. Click **OK** to exit the Select Tenant dialog.

6. In the **Determination Rules** field, use the natural language fields to create the tenant's determination rules:
   a. Select **All** or **Any** of the following rules.
   b. Select a rule condition, for example, **URL Extension**.
      The following conditions are available: **Client Address**, **Client Effective Address**, **Port**, **Proxy Address**, **Proxy Port**, **URL**, **URL Domain**, **URL Extension**, **URL Host**, **URL Path**, **URL Query**.
      Starting with ProxySG 6.7, the tenant rule conditions include redirect-based authentication controls within a tenant slot, `tenant.connection()`. This gives an early trigger for client gestures, such as **URL Port** and **Proxy Port**. The CPL generated includes conditional text to prevent ProxySG 6.6 or earlier from running the trigger. Also, the connection does not apply to the default tenant.
   c. Select an operator, for example, **equals**.
      The available operators may change based on the specified rule condition.
   d. Enter a value, for example, **.pdf**.
Address fields support IPv4 and IPv6 single and subnet addresses. For example:

7. Use the icons to add more rules.
   – To add another rule, click +
   – To delete a rule, click -
   – To add a nested set of rules, click □

8. When you are finished making changes, click Save.
9. (Optional) Add Target Devices.
10. (Optional) Install Policy.

Tenant determination rules are enabled by default. To disable a rule, highlight the rule and click Disable.
Tenant Determination Rule Example

Determination Rule
The selected tenant's policy will apply when the following condition is met

| All | of the following rules: |
| URL Domain | contains | .com |
| URL Domain | contains | casino |
| URL Domain | contains | finance |
| Any | of the following rules: |
| Port | = | 80 |
| Port | = | 443 |

Determine Your Next Step
If you are configuring WAF policy, deploy the tenant determination policy to your appliances, which is step 4 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

Configure WAF Security Rules
A WAF security profile is a shared object that defines the Web Application Firewall settings for the associated WAF application object. You associate the WAF security profile with a WAF application object to define the security rules for that object. You can create as many WAF security profiles as you need but a WAF application object can be associated with only one security profile.

Configuring a WAF security profile is step 5 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

Step 1 — Create a WAF Security Profile
1. Select Configuration > Shared Objects > Add Object.

The web console displays the Create New Shared Object: Basic Information wizard.
2. Enter a name for the policy object.
3. Select WAF Security Profile for the Object Type.
4. (Optional) In the Reference ID field, enter a Reference ID that you can filter on when building policy.
   
   **NOTE**
   
   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".
5. Enter a description in the Description field. Although entering a description is optional, entering a description can help you understand the purpose of the policy when you later refer to it.
6. Click Next.
7. Enter or select values for the defined attributes.
8. Click Finish.

The new WAF security profile object appears in the Policy Objects editor.

**Step 2 — Configure WAF Security Rules**
1. Select **Configuration > Shared Objects**.
2. Click the WAF security profile hyperlink or highlight the row and click **Edit**.

**Shared Policy Objects**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklisted_categories</td>
</tr>
<tr>
<td>category_whitelist</td>
</tr>
<tr>
<td>DLP - Outbound</td>
</tr>
<tr>
<td>High Secure</td>
</tr>
</tbody>
</table>
The selected file displays in the **Editor** tab.
3. Review the following settings and adjust to create the desired security settings:

| Request Validation | Controls general HTTP request properties such as size restrictions, WAF validation properties, allowed methods, and allowed file types. The default settings are adequate for most environments. To ensure Management Center is efficiently managing traffic, consider the following:

- In the **Protocol Compliance** settings, the action is triggered when the size of one or more parts of the request exceeds the specified limit. If the action is set to Ignore, the query string, headers, and body are scanned up to the specified count or size, and any excess is ignored. For example, if you set the Body: Max size to 10 KB, set the action to Ignore, and the appliance receives a request with a body size of 15 KB, then the first 10 KB of the request are scanned. The remaining 5 KB are not scanned, blocked, or monitored. If you have enabled this setting and specified the `http.request.data=condition` in policy, WAF engines use the greater of the two values for scanning. For more information, see the `http.request.body.inspection_size()` property in the [Content Policy Language Reference](#).

- In the **WAF Properties** settings:
  - The **Null Byte Detection**, if enabled, might cause false positives. If this setting does cause multiple false positives, Symantec recommends disabling this setting.
  - The **Parameter Pollution Separator** setting should not be enabled unless a protected backend, such as ASP.NET/IIS, is concatenating like-named query arguments.

- In the **Restricted File Upload Types**, enable as many file types as possible without backend functionality being degraded. As a minimum, Symantec recommends restricting uploads of EXE and HTML files. To restrict file types:
  a. Select **Block uploads based on the apparent data type**
  b. Select the file types to restrict
  c. Click **Save**.

For further information, see the following CPL gestures in the [Content Policy Language Reference](#):

- `http.request.body.inspection_size()`
- `http.request.detection.other.invalid_json()`
- `http.request.body.data_type()`
- `http.request.detection.other.null_byte()`
- `http.request.detection.invalid_form_data()`
- `http.request.detection.other.multiple_header()`
- `http.request.detection.other.parameter_pollution()`
- `http.request.detection.other.parameter_pollution_separator()`

| Request Normalization | Enables the recommended normalization settings for each request part, and what action to take when normalization issues are encountered. For advanced normalization control, refer to `http.request.normalization.default()` in the [Content Policy Language Reference](#). |
| Blocklist                                                                 | Enables/disables the Blocklist engine and sets block/monitor behavior when a request triggers one of the blocklist rules. The signature-based blocklist discovers well-known attack patterns quickly and efficiently. To ensure Management Center is efficiently managing traffic, consider the following:
- Configure the **Use effective date** setting to efficiently handle newly published rules. By configuring this setting in this way, pre-existing rules continue to block attacks, and new rules monitor traffic to verify that the new rules are not creating false positives. To configure this setting to allow existing rules to block traffic and new rules to monitor it:
  a. Select **Use effective date**.
  b. In the **Effective Date** field, select a date before the effective date of the new rules; for example, if new rules had an effective date of October 31, 2018, then you could select October 30, 2018. When selecting an effective date, consider which rules you want to have blocking traffic and which you want monitoring traffic. The further in the past you select for your effective date, the more rules that will have a Monitor verdict.
  c. In the **Verdict before** field, select **Block**.
  d. In the **Verdict after** field, select **Monitor**.
  e. Click **Save**.
- Set actions for individual rules; for example, if a single rule returns excessive false positives, set the action for that rule to Ignore. To set an action for an individual rule: Actions that are set for individual rules are exemptions to the global effective date rule; therefore, the action set for the individual rule overrides the action of the global rule.
  a. In the table of rules, locate the individual rule.
  b. Click the plus symbol to expand the rule.
  c. Select the radio button for the appropriate action.
  d. Click **Save**.
For further information, see the `define application_protection_set` gesture in the Content Policy Language Reference. |
**Analytics Filter**

Enables/disables the Analytics Filter engine and sets Analytics Filter block/monitor behavior. Analytics Filter is a scoring engine that detects attack characteristics and triggers intelligently based on the sum of the anomalies.

To ensure Management Center is efficiently managing traffic, consider the following:

- Configure the **Use effective date** setting to efficiently handle newly published rules. By configuring this setting in this way, pre-existing rules continue to block attacks, and new rules monitor traffic to verify that the new rules are not creating false positives. To configure this setting to allow existing rules to block traffic and new rules to monitor it:
  
  a. Select **Use effective date**.
  
  b. In the **Effective Date** field, select a date before the effective date of the new rules; for example, if new rules had an effective date of October 31, 2018, then you could select October 30, 2018. When selecting an effective date, consider which rules you want to have blocking traffic and which you want monitoring traffic. The further in the past you select for your effective date, the more rules that will have a Monitor verdict.
  
  c. In the **Verdict before** field, select **Block**.
  
  d. In the **Verdict after** field, select **Monitor**.
  
  e. Click **Save**.

- Set actions for individual rules; for example, if a single rule returns excessive false positives, set the action for that rule to Ignore. To set an action for an individual rule: Actions that are set for individual rules are exemptions to the global effective date rule; therefore, the action set for the individual rule overrides the action of the global rule.
  
  a. In the table of rules, locate the individual rule.
  
  b. Click the plus symbol to expand the rule.
  
  c. Select the radio button for the appropriate action.
  
  d. Click **Save**.

For further information, see the `define application_protection_set` gesture in the *Content Policy Language Reference*.

**Security Engines**

Specifies security engine settings (these are known as WAF engines in the ProxySG documentation). The content nature detection engines include **HTML Injection**, **Command Injection**, **Code Injection**, **SQL Injection**, **XSS**, and **Directory Traversal**.

To ensure Management Center is efficiently managing traffic, consider the following:

- Customize the security engines to inspect particular parts of an HTTP request. By default, the security engines inspect all parts. Disabling the settings for some parts might reduce false positives.

- For the **Command Injection** and **Code injection** settings, disable the settings for technologies that are not relevant to your installation. Disabling these settings can decrease false positives.

For further information, see the `define application_protection_set` gesture in the *Content Policy Language Reference*. 
<table>
<thead>
<tr>
<th>XML Validation</th>
<th>These options ensure the XML is valid and check for potentially malicious constructs.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To ensure Management Center is efficiently managing traffic, consider the following:</td>
</tr>
<tr>
<td></td>
<td>• The <strong>XML External Entity (XXE)</strong> setting inspects requests for XML External Entity injection attacks, which may allow external malicious content to be processed by an XML parser.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>XInclude Reference</strong> setting inspects requests for XInclude elements that might reference malicious content.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Invalid XML</strong> setting inspects requests for XML documents that are not well formed.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Expand CDATA Sections</strong> setting enables parsing of CDATA sections. As CDATA sections are not expanded nor interpreted by the XML parser, these sections can be used to evade detection of malicious content. Enable parsing of CDATA sections to detect potentially malicious content.</td>
</tr>
<tr>
<td></td>
<td>For further information, see the following CPL gestures in the <strong>Content Policy Language Reference</strong>:</td>
</tr>
<tr>
<td></td>
<td>• http.request.detection.xml.xxe()</td>
</tr>
<tr>
<td></td>
<td>• http.request.detection.xml.xinclude()</td>
</tr>
<tr>
<td></td>
<td>• http.request.detection.xml.invalid()</td>
</tr>
<tr>
<td></td>
<td>• http.request.detection.xml.cdata()</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request Security</th>
<th>These options ensure that requests are safe by checking for common attacks like HTML tag injection, buffer overflow, header injection, and request smuggling.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The <strong>Buffer Overflows</strong> settings protect your servers from buffer overflow attacks by setting a global length limit for various parts of the request. By default, the <strong>Buffer Overflows</strong> setting is disabled as it can trigger false positives in some environments.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Aggressive Header Injection Blocking</strong> setting blocks header injection attacks, in additional to the protection your ProxySG appliance already provide by default; however, this setting might produce excessive false positives in some environments.</td>
</tr>
<tr>
<td></td>
<td>For the <strong>Block Insecure SSL Ciphers</strong> setting, if one or more of these ciphers have been enabled on the ProxySG appliance, then you can disable them here. For example, if one tenant has legacy applications that still require an insecure cipher and all other tenants should not use this cipher, then disable this cipher in all other tenants. To disable ciphers, select <strong>Block Insecure SSL Ciphers</strong> and select the ciphers you want to block.</td>
</tr>
</tbody>
</table>
These options make server responses more secure by obfuscating the back-end technology and directing browsers to implement additional client-side security.

To ensure Management Center is efficiently managing traffic, consider the following:

- **The Force "secure" and "HttpOnly" Cookie Flags setting** modifies Set-Cookie response headers to include the Secure and HttpOnly flags. The secure flag prevents browsers from sending cookies using cleartext and the HttpOnly flag helps prevent Cross-Site Scripting (XSS) attacks.

- **The Rewrite the "Server" Response Header to "unknown" and Web Application Fingerprinting Protection settings** hide information about the backend from potential malicious parties.

- **The HTTP Public Key Pinning setting** instructs the browser to recognize certain public keys for a set period of time for the site. Generally, this setting is not recommended due to the complexity and risk enabling it poses. Support for this setting has been deprecated or removed in some popular browsers.

- **For the HTTP Strict Transport Security setting**, if your site fully supports HTTPS, enable this setting for enhanced security. When initially enabling this setting, validate that the setting is functioning properly by selecting a low value for the Age. When you’ve validated it, Symantec recommends that you select an Age of at least 10368000 seconds (120 days) and ideally 31536000 (one year).

- **The X-XSS-Protection setting** inserts an X-XSS-Protection header into the response. It instructs browsers to not render a page if the appliance detects certain types of XSS attacks in the response.

- **The X-Content-Type-Options setting** inserts an X-Content-Type-Options header into the response. It helps prevent attacks that leverage inconsistencies between the Content-Type response header and the actual content type of the body that the browser’s MIME sniffing determines.

- **The Clickjacking: X-Frame-Options setting** inserts an X-Frame-Options header into the response. It helps prevent clickjacking attacks by ensuring that your site’s content can only be embedded in a frame of the same origin of your site.

- **The Enable Response Error Code Cloaking setting** hides common error codes. Error codes that the server returns can contain information that might be useful to malicious parties. Enable this feature, and select error codes you want to hide and that won’t impair functionality by them being hidden.
| Optimizations | Disable WAF controls for POST requests consisting of binary data; bypass WAF scanning for cache hits. To ensure Management Center is efficiently managing traffic, consider the following:  
* The **POST Body Processing Control** settings are not required to be enabled for most environments. If these settings are disabled and you receive false positives pertaining to the POST body, then you might need to enable these settings.  
* For the **Cache Control** setting, Symantec recommends enabling the **Bypass WAF Scanning for Cache Hits** setting. In most environments, this setting significantly improves performance.  
For further information, see the **http.request.detection.bypass_cache_hit()** gesture in the **Content Policy Language Reference**. |
|---|---|
| Logging | These options control when the header and body of HTTP requests are logged to the **x-bluecoat-request-details-header** and **x-bluecoat-request-details-body** access log fields. Sensitive data, such as personally-identifiable information, might be logged unless masking is performed. For information on log details and masking, see the following CPL gestures in the **Content Policy Language Reference**:  
* **http.request.log_details[header, body]()**  
* **http.request.log.mask_by_name[regex_pattern]()**  
* **http.request.log.mask_by_value[regex_pattern]()** |
| Cross-Site Request Forgery | Detects Cross-Site Request Forgery (CSRF) attacks. Once enabled, select the WAF event (block, monitor, or ignore), the expiry of the token, and the authentication link for User IDs and the Client IP.  
By default, the **Enable CSRF Protection** setting is not enabled. Enable this setting only for applications that do not have protection, such as anti-CSRF tokens, from CSRF attacks. If the application does not have CSRF protection and you enable this setting, limit the scope of this setting. This setting modifies HTTP transactions and might disrupt user traffic, if applied too broadly. For further information, see the following CPL gestures in the **Content Policy Language Reference**:  
* **http.csrf.authentication_link()**  
* **http.csrf.detection()**  
* **http.csrf.token.insert()** |
| Exemptions | Define exemptions to your WAF policy to handle false positives. To create exemptions, see **Manage WAF Security Policy**. |
### PCI DSS Compliance

Displays the status of PCI DSS Compliance for the WAF security profile or WAF application. The possible compliance states are as follows:

- **Compliant**
  - All PCI DSS requirements are met.
- **Partial Compliance**
  - One or more PCI DSS requirements are met, but not all.
- **Non-Compliant**
  - No PCI DSS requirements are met.

See [Verify PCI DSS Compliance](#), for more information.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many of the options include a Block/Monitor/Ignore setting. This setting indicates the action taken when suspicious content is identified. For new WAF deployments, Symantec recommends setting the action to Monitor.</td>
</tr>
</tbody>
</table>

4. *(Optional)* After making one or more changes, click Compare to review a side-by-side comparison of the changes.
5. Click Save.

To create exemptions to your WAF policy, set a security control to "Ignore," or create an appropriate exemption definition, see Manage WAF Security Policy.

### Determine Your Next Step

If you are configuring WAF policy, continue to Configure WAF Application Objects, which is step 6 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

### Configure WAF Application Objects

A WAF application object represents a web application (or group of applications) and its associated WAF security settings. The WAF application object is associated with a specific tenant and WAF Security Policy. You install this policy on ProxySG appliances to configure WAF settings.

Configuring a WAF application object is step 6 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

### Create a WAF Application Object

1. Select Configuration > Policy and click Add Policy.

   ![Policy Objects](image)

   The web console displays the Create New Policy: Basic Information wizard.
2. Enter a name for the policy object.
3. Select **WAF Application Object** for the Policy Type.
4. (Optional) In the **Reference Id** field, enter a Reference ID that you can filter on when building policy.
   
   **NOTE**
   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".
5. Click the **Tenant** field, select a tenant from the Select Tenant dialog or click **Add** to create a new one, and click **OK**. If this is a new WAF deployment, select the default tenant.
   
   **NOTE**
   A WAF application should first be deployed to the default tenant slot to ensure that all requests are processed by the WAF. Additional WAF applications, security profiles, and tenants can then be created to handle specific web application requirements.

6. Enter a description in the **Description** field. Although entering a description is optional, the description helps differentiate versions of the same policy.
7. Click **Next**.
8. Enter or select values for the defined attributes.
9. Click **Finish**.

The new WAF application object appears in the Policy Objects editor.
Configure the WAF Application Object
If you are not already editing the WAF application object, select Configuration > Policy and click the policy name hyperlink or highlight the row and click Edit. The selected file displays in the Editor tab.

Step 1 - Confirm Tenant Selection
Confirm your tenant selection. To select a different tenant, select the pencil icon.

Step 2 - Specify WAF Application Settings
The WAF Application Settings panel enables you to set policy generation controls.

1. Select a WAF Security Profile:
   a. Click the WAF Security Profile text field or pencil icon.
   b. In the Select Policy dialog, select the desired WAF Security Profile or click Add to create a new one.
c. Click OK to close the Select Policy dialog.

d. Specify the WAF Security Profile version to use. Select **Always Use the Latest Version** or specify a specific version in the **Use Specific Version:** field.
   - (Optional) To override all WAF Security Profile settings, select **Disable entire Security Profile**.
   - (Optional) To globally change all Block/Monitor verdicts, select **Change all WAF controls to: Monitor** or **Block**.

   **NOTE**
   To set the behavior to **Ignore**, disable the entire WAF Security Profile.

   – Specify the user notification (exception) page to use for blocked requests.

**Step 3 - Set Compression**

Select Enable compression level (**Low**, **Medium**, **High**) to allow WAF to compress data in transit.

**Step 4 - Specify Allow Rules**

Set the criteria for allowing traffic through the ProxySG appliance. Specify these rules using rules associated with a tenant, a CPL fragment, or by manually entering them using the **Custom Rules** option. If you do not want allow rules or want to add your own in CPL, select **No Allow Rules**.

**NOTE**
Because reverse proxy deployments have a global Deny policy, you must specify rules to allow traffic. If this WAF application is associated with the default tenant, you will receive an error (because the default tenant has no allow rules) and must specify the allow rules using one of the other methods.
Step 5 - Add CPL Fragments

Adding a CPL fragment is optional. Add valid CPL layers only. Do not add individual CPL rules. Adding individual rules can lead to errors and unpredictable results.

1. Click Add CPL Fragment. The web console displays the Add CPL Fragment dialog.

   - **Add CPL Fragment**
     - **CPL Fragment Name:**
     - **Always use the latest version**
     - **Use specific version:**

   a. Click the **CPL Fragment** text field or pencil icon. The web console displays the Select Policy dialog.

   b. Select the CPL Fragment. See Create a CPL Fragment for information about creating CPL fragments.
   c. Click OK.
   d. Select **Always Use the Latest Version** or specify a specific version in the **Use Specific Version:** field.

   If **Always use the latest version** is selected, Management Center will always include the latest available version of the Security Profile when installing the WAF application to a ProxySG appliance. If you are concerned about deploying untested changes, select **Use Specific Version**.

Save Changes

To finalize your settings, you must review your policy and save your changes.

1. (Optional) After making one or more changes, click **Compare** to review a side-by-side comparison of the changes.
2. When you are finished making changes, click **Save**.
3. (Optional) **Add Target Devices**.
4. (Optional) **Install Policy**.
Determine Your Next Step

If you are configuring WAF policy, continue to Analyze and Refine WAF Policy (Deal with False Positives), which is step 9 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

Analyze and Refine WAF Policy (Mitigate False Positives)

After installing an initial version of WAF policy on one or more target devices, you can analyze the results of the traffic to determine what attacks have been detected. There is a chance that the detection engines have flagged a legitimate request as an attack. For example, if a blog post includes an example of a cross-site scripting (XSS) attack, the appliance interprets the example as an actual attack and blocks the post. This might be undesirable behavior and considered a false positive.

Address this and other kinds of false positives with the following workflow. Refer to the Web Application Firewall Solutions Guide for more information.

Analyze and Refine WAF Policy describes steps 8 and 9 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

Analyze and Refine WAF Policy Workflow

<table>
<thead>
<tr>
<th>Step</th>
<th>Overview</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check access logs to determine which rules or engines you must update to address false positives, false negatives, and other wanted behavior. A useful search criteria is the transaction ID. For example, when a user tries to visit a page and receives an exception page, you can use the associated transaction ID to run a forensics report. The Full Log Detail report then displays the log line matching that transaction ID.</td>
<td>Generate a Reporter Report Reference: Reporter Report Descriptions Searching for Specific Report Data (Search and Forensic Report). Generate a Reporter Report Reference: Reporter Report Descriptions Searching for Specific Report Data (Search and Forensic Report).</td>
</tr>
<tr>
<td>2</td>
<td>Optional-Perform a policy trace.</td>
<td>Launch a Device Console Launch a Device Console To enable policy tracing on the ProxySG appliance, select Configuration &gt; Policy &gt; Policy Options. Under Default Policy Tracing, select Trace all policy execution and click Apply.</td>
</tr>
<tr>
<td>3</td>
<td>Based on your analysis of the access logs, create policy exemptions to eliminate false positives and other unwanted behavior.</td>
<td>Manage WAF Security Policy</td>
</tr>
<tr>
<td>4</td>
<td>Run traffic through the appliance and confirm through access logs (and optionally, other troubleshooting tasks) that requests match both general rules and exceptions appropriately.</td>
<td>Repeat steps 1 through 3 in this table as often as required.</td>
</tr>
</tbody>
</table>
After confirming that false positives no longer occur, consider your next step. You can do any of the following according to your needs:

- Update policy actions from monitor to block. Then, move to a production environment when your WAF policy is stable and you observe no other issues with how the appliance handles traffic.
- Continue to test and refine policy, move to production, and then update policy actions to block.
- Continue to test and refine policy, move to production, and gradually update each engine or policy’s actions to block.

Repeat the previous steps as needed.

### Manage WAF Security Policy

As described in Analyze and Refine WAF Policy (Deal with False Positives), you will need to refine your WAF security policy to ensure it is working properly.

Refining your WAF Security Policy is step 9 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

#### Add Exemptions

After installing the WAF protection policy and reviewing the access logs, you will likely find several sites that were incorrectly characterized as threats. To troubleshoot this, add exemptions to your WAF security policy. You can add exemptions using the available security options or define your own in CPL.

1. Select **Configuration > Shared Objects**.
2. Click the hyperlink associated with the WAF security profile or highlight the row and click **Edit**.

**Shared Policy Objects**

1. Click **Exemptions** > **Add Exemption**.
The system displays the Add Exemption dialog.

4. Provide a name for the exemption in the **Description** field.

5. Add a URL Exemption from the available security options or a custom CPL exemption:
   - Standard exemption:
     a. In the **Build exemption from:**; click **Security Profile Sections**.
     b. Enter the URL for this exemption.
     c. Select the desired **Validation, Normalization, Security Engines, Blocklist, and Analytics Filter** options.
     NOTE
         You can exempt the URL from all **Blocklist** or **Analytics Filter** processing or per rule (by specifying a CSV list of rule IDs).
     d. Click **Save** to close the Add Exemption dialog.
   - Custom CPL exemption:
     a. in the **Build exemption from:**; click **Custom CPL**.
     b. Add the CPL and click **Save** to close the Add Exemption dialog.

   The system adds the exemption for the URL or CPL. If the exemption list is long, filter for specific exemptions using the search box above the table. To clear the filter, delete the text and press Enter (or click the magnifying glass).

6. In the policy editor, click **Save**.

**Set Block/Monitor/Ignore Actions**

When first implementing a WAF protection policy, it is important to observe the effects of rules before inadvertently blocking traffic. To begin, ensure that new rule actions are set to **Monitor**. Then review access logs to identify false positives, create policy exemptions (as described above) to address those issues, and repeat until false positives no longer occur. Then, update policy actions from **Monitor** to **Block**.

Options that support the Block/Monitor/Ignore action include an action drop-down menu. To set, select the appropriate action and click **Save**.
For example, to set the **Blocklist** action to **Block**:

1. Select **Configuration > Shared Objects**.
2. Select the **WAF Security Policy** and click **Edit**.
3. Click **Blocklist**.
4. Verify that **Enable Blocklist** is selected.
5. Select **Block** and click **Save**.

Some options allow you to be even more granular, allowing you to modify individual rules, as shown below.

**Use Effective Date to Manage New Rule Updates**

When Application Protection Subscription (APS) updates are published, the updated Blocklist and Analytics engine content is immediately available. Because the updated engine rules can potentially change the behavior of the existing WAF security policy, Management Center enables you to use this activation date as a decision point. The **Effective Date** option is that decision point, enabling you to control rule selection based on the date the rules were added.

For example, rules qualified in a pre-production environment can be set to block-mode, and new rules can be set to monitor mode. This functionality enables an organization to take advantage of new rules immediately, but in a manner that will not introduce new false positives that cause requests to be blocked. After the new rules are sufficiently qualified, the effective date can be migrated forward, thereby setting the new rules into block mode.

Additionally, by using multi-tenancy this can be controlled on a per-tenant basis. This facilitates different update strategies and a tenant-configurable update cadence. For example, some tenants may choose to always use the latest rules, whereas some risk-adverse tenants may employ a very deliberate APS update qualification process. Multi-tenancy provides flexibility for diverse infrastructures where a one-size-fits-all approach may not be ideal.

Only **Blocklist** and **Analytics Filter** use the **Effective Date** option.
Verify WAF Policy Compliance With PCI DSS Requirement 6.6

NOTE
This is an optional step in configuring your Web Application Firewall.

The Payment Card Industry Data Security Standard (PCI DSS) specifies a set of data security requirements for web sites, including one (Requirement 6.6) that can be satisfied by enabling specific Web Application Firewall options to comply with the standard.

Management Center provides a visual indicator of the level of PCI DSS Compliance for WAF Applications and WAF security profiles and allows you to modify the current settings, if needed.

- Compliant
  All PCI DSS requirements are met.
- Partial Compliance
  One or more PCI DSS requirements are met, but not all.
- Non-Compliant
  No PCI DSS requirements are met.

WAF Application
The example below shows the location of the PCI DSS compliance status indicator in the WAF application.
In this case, the WAF application is in partial compliance because its associated WAF security profile has one or more, but not all, options in compliance. To bring the WAF application into compliance, click the link to open the associated WAF security profile.
WAF Security Profile

As you can see in the preceding example, this WAF security profile is in partial compliance because one of its options, Vulnerability Scanners, is in compliance. To bring the WAF security profile into compliance, all non-compliant options must be modified.

To change a setting, click the + to the left of the option. The system displays the remediation required to achieve compliance and a link to the setting. In the following example, the remediation is "Linux, Windows, or OSX command injection must be on block if enabled."

PCI DSS Compliance Report

As you can see in the preceding example, this WAF security profile is in partial compliance because one of its options, Vulnerability Scanners, is in compliance. To bring the WAF security profile into compliance, all non-compliant options must be modified.

To change a setting, click the + to the left of the option. The system displays the remediation required to achieve compliance and a link to the setting. In the following example, the remediation is "Linux, Windows, or OSX command injection must be on block if enabled."
When you click the link, the system displays the command injection section in the WAF security profile so you can make the necessary change. After making a change, navigate back to the **PCI DSS Compliance Report** and click **Refresh** to update the status.

**Non-Compliance**

Normally, a WAF Application is non-compliant because the associated WAF security profile is not in compliance. However, even if the WAF security profile is fully compliant, a WAF application can be shown as non-compliant in the following cases:

- You have disabled the security profile by selecting the **Disable entire Security Profile** option.
- You have changed all WAF controls to Monitor using the **Block/Monitor Override** option.

Either of these actions cause the WAF application to be non-compliant.

**Apply a Single Policy to Both On-Premises and Cloud Users**

You can create universal policy using VPM or CPL.

**Prerequisites**

To use the universal policy feature, you must first:

- Have a valid Web Security Services (WSS) account configured to accept policy from the Management Center via the WSS on-boarding wizard. Existing WSS cloud customers may contact Customer Support for configuration assistance.
- Configure your WSS account for on-premises policy enforcement.
- Enable enforcement domains and create policy on the reference ProxySG appliance. Although you can import universal policy from a source that does not have enforcement domains enabled, you cannot deploy the policy unless you launch the VPM Editor and save a new revision of policy. This generates the CPL with enforcement domains enabled.

**SSL Requirements**

Universal policy requires proper SSL certificate validation. You must:

- Ensure that Management Center is able to connect to [https://sgapi.es.bluecoat.com](https://sgapi.es.bluecoat.com)
- Verify that no inline proxies will disrupt SSL connections to your devices.
- If Management Center uses the explicit HTTP proxy, ensure that it does not decrypt traffic

**Software Version Requirements**

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProxySG appliance</td>
<td>6.7.1.1 or later; 6.5.9.14 or later (6.6.x is not supported at this time)</td>
</tr>
<tr>
<td>Web Security Service</td>
<td>6.9.5.1 or later</td>
</tr>
<tr>
<td>Management Center</td>
<td>1.8.1.1 or later (1.10.1.1 or later for CPL universal policy)</td>
</tr>
</tbody>
</table>

**Solution Steps**

1. **Add** the WSS as a device.
2. Select the policy to be used for universal policy by doing one of the following:
   a. Create a new universal **VPM** or **CPL** policy object.
   b. **Edit** an existing CPL policy object.
c. Transform an existing VPM policy object into universal policy.
3. If you created a new universal VPM or CPL policy object, import the policy from the reference ProxySG appliance.
4. Edit the VPM or CPL universal policy:
   a. Use the classifier to analyze the policy to determine if it's valid for WSS.
   b. Using the classifier results, modify your policy. Determine if a rule should apply only to the WSS, the appliance, or both (universal).
   c. Save the policy.
   d. Repeat as necessary until you are satisfied with the classifier results.
5. Add WSS and any on-premises devices as targets.
   
   **NOTE**
   
   You cannot add WSS and other devices as targets in the same operation because they have different deployment types. You must add WSS devices in a separate operation.
6. Install the policy to the targets.

**Add a Universal VPM Policy Object**

To add a universal VPM policy object, complete the following steps.

1. Select **Configuration > Policy**.
2. Click **Add Policy**. The system displays the Create New Policy: Basic Information dialog.
3. Enter a name for the policy object.
4. Select **Universal VPM Policy** for the **Policy Type**.
5. Enter a **Reference ID**. Although entering a reference ID is not required, it is useful for filtering objects when building policy. If you do not enter a reference ID, the system assigns a default ID based on the policy name you enter.
   Imported policy objects are assigned a default ID.
   
   **NOTE**
   
   The Reference ID must begin with a letter, and must contain only letters, numbers and "_".
6. Enter a description in the **Description** field. Although entering a description is not required, the description helps differentiate versions of the same policy.
7. Indicate whether to **Replace Substitution Variables**. See Use Substitution Variables in Policies and Scripts for more information.
8. Click **Next**.
9. Enter or select values for the defined attributes.
10. Click **Finish**.

**Transform Existing VPM Policy into Universal VPM Policy**

To transform an existing VPM policy object into a universal policy object, you clone it as described below.

1. Select **Configuration > Policy**.
2. From the **Policy Objects** list, select the policy name or highlight the policy and click **Edit**.
3. Click **Clone to Universal...**
4. In the Clone and convert to Universal dialog, review the name and modify it if necessary. Then click **Clone**.
The system displays the new universal VPM policy. By default, the policy is titled with the original policy name with - Universal appended. For example, if the original policy name is VPM Sunnyvale, the new universal policy name is VPM Sunnyvale - Universal. You can now open the VPM and edit the universal policy.

**Refine and Validate Universal VPM Policy**

After creating universal VPM policy, you must refine your universal policy rules. Each policy rule can apply only to on-premises users, only to remote users (Web Security Service - WSS), or to both (universal policy). These categories are called enforcement domains. Before uploading the rules to the WSS, you must analyze the policy to ensure it will run as expected. Then, use the VPM to edit and finalize your policy.

**Legacy VPM Requirements**

- When using the legacy VPM editor, Symantec recommends that you use the recommended Java version listed here. Releases prior to Java 1.8 use a vulnerable cryptographic hash (SHA1) function that Management Center no longer supports. If you are using Java 1.8.131 or later and wish to use the Java-based VPM editor from within Management Center, you will need to upgrade the ProxySG to an SGOS version where this issue is addressed. Depending on the branch of SGOS running on your ProxySG appliances, load the appropriate version to support Management Center:
  - SGOS 6.5.x: 6.5.9.10 or later
  - SGOS 6.6.x: 6.6.4.1 or later
  - SGOS 6.7.x: 6.7.2.1 or later
Versions prior to these SGOS releases use a signing algorithm (MD5withRSA) that is disabled in Java 1.8.131 by default. If you receive an error that the signed jar uses an unsupported signature, you are running Java 1.8.131 or later with a version of SGOS not supported by that version of Java.
NOTE
If you must use Java 7 (not recommended), you will need to enable HTTP on Management Center (resulting in insecure access). Use the `security http enable` command. See # security for more information.

• Before using the VPM editor in Management Center, Symantec strongly recommends that you understand how the VPM Editor works and underlying policy enforcement in ProxySG appliances. For comprehensive information on creating policy, as well as assigning and changing enforcement domains for policy rules in the VPM, refer to the ProxySG Appliance Visual Policy Manager Reference and Advanced Policy Tasks.

• Ensure that you have the latest VPM resource XML file installed on your ProxySG. You can download the XML file from the Symantec Support site: https://support.symantec.com/content/dam/bluecoat/download/modules/security/SGv6/policyclassifier.xml

Procedure
1. Select Configuration > Policy. From the Policy Objects list, locate the universal VPM policy object you want to edit. To narrow your search, you can do a Filter by Attributes and Keyword Search.
2. Click the policy name hyperlink or highlight the row and click Edit. Verify that you are in the Editor tab.
3. If necessary, import policy from the reference device. Click Import. See Select Reference Device for VPM Policy.
4. Click Analyze Policy > Analyze in Production to open the policy classifier.

   ![Policy Classifier](image)

   NOTE
   If you are participating in a beta program, click Analyze in Pre-Production.

   The system displays the policy classifier in a new tab. The classifier breaks down the policy to illustrate whether each rule will perform as expected in the WSS.

   ![Universal Policy Enforcement to Blue Coat Cloud Overview](image)

5. Review the classifier recommendations:
   – Examine the information displayed in the Overview tab. If the policy is not 100% enforceable on the WSS, click the Recommendations tab for more information.
   – If necessary, refer to the Migration, Policy, and Dependencies tabs for additional information.
   – The WSS tab provides general information about the WSS. Use this information to inform your policy edits.
6. Open the legacy or web-based VPM:
   a. Navigate back to the policy editing page and click Launch VPM Editor.
   b. The web console displays the Visual Policy Manager.
7. Keeping both the classifier and VPM open, edit your policy rules.
   
   **NOTE**
   If you use Windows, use **ALT+Tab** to switch between the VPM editor and the analysis tab. Displaying each application in a separate monitor also works well.

   For each rule, specify whether it should apply only to appliances (Appliance), both appliances and the WSS (Universal), or the WSS only.

   **Show screen.**

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Time</th>
<th>Action</th>
<th>Track</th>
<th>Enforcement</th>
<th>Comm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Authentic...</td>
<td>Any</td>
<td>Using HTT...</td>
<td>Any</td>
<td>Allow Access...</td>
<td>None</td>
<td>Universal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Destination...</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>None</td>
<td>WSS</td>
<td></td>
</tr>
</tbody>
</table>

   **NOTE**
   For details on enforcement domains, refer to “The Visual Policy Manager” chapter in the 6.7.1.1 Visual Policy Manager Reference.

8. Save your VPM changes.
9. As you save your changes, the classifier notes that the data is stale, prompting you to refresh. Click **Refresh** to update the classifier to reflect your changes.

   **NOTE**
   You might notice blank lines in the classifier. Appliance-only rules are blanked out before sending to the WSS. The rules are replaced with blank lines.

10. Review the new results. If the policy requires modification, repeat step 6.
11. Repeat steps 7 through 9 until you are satisfied with your changes.

You are now ready to add targets and install the universal VPM policy.

**Deploy Universal CPL Policy**

Any CPL policy object can be used for universal policy, as described below.

1. Create a new CPL policy object or edit an existing CPL policy object.
2. Analyze the CPL policy.
3. Make changes to optimize the on-premise and WSS portions of the policy.
4. Repeat steps 2 and 3 until you are satisfied with the policy.

Each policy rule can apply only to on-premises users, only to remote users (Web Security Service - WSS), or to both (universal policy). These categories are called **enforcement domains**. Before uploading the rules to the WSS, you must analyze the policy to ensure it will run as expected.
Analyze the CPL Universal Policy

1. Select Configuration > Policy.
2. Click the policy name hyperlink or highlight the row and click Edit. Verify that you are in the Editor tab.
3. Click the cloud icon and select Analyze Policy > Analyze in Production to open the policy classifier.

   NOTE
   If you are participating in a beta program, click Analyze in Pre-Production.

   The system displays the policy classifier in a new tab. The classifier breaks down the policy to illustrate whether each rule will perform as expected in the WSS.

4. Review the classifier recommendations:
   - Examine the information displayed in the Overview tab. If the policy is not 100% enforceable on the WSS, click the Recommendations tab for more information.
   - If necessary, refer to the Migration, Policy, and Dependencies tabs for additional information.
   - The WSS tab provides general information about the WSS. Use this information to inform your policy edits.

5. Using what you have learned from the classifier, edit your CPL policy. For example, if you think a section should apply only to on-premise appliances, do the following:
   a. Highlight the section.

   ```xml
   <proxy Web Filter>
     url domain=playboy.com FORCE_DENY
     category=News,WhiteList
     category=Gambling, hacking, games, news) exception(content_filter_denied)
   </proxy>
   
   <proxy Resticted Access>
     group=exec, managers url domain=fantasyfootball.com ALLOW
   </proxy>
   ```
b. Select **Operations > Insert > Insert On-Premises Segment.**

The system then applies the on-premise enforcement rule to the highlighted text.

```xml
<proxy "Web Filter">
  url domain=com|playboy.com FORCE_DENY
  category=News|WhiteList ALLOW
  category=(gambling, hacking, games, news) exception(content_filter_denied)

# if enforcement=appliance
  <proxy "Internal Access">
    groups=exec, managers url domain=fantasyfootball.com ALLOW
    # TODO
  
</proxy>
</proxy>
```

6. As you save your changes, the classifier notes that the data is stale, prompting you to refresh. Click **Refresh** to update the classifier to reflect your changes.

7. Repeat steps 4 through 6 until you are satisfied with your changes.

You are now ready to **add targets** and **install** the universal CPL policy.

**Select Reference Device for Universal CPL Policy**

You must associate a reference device with your universal CPL policy before you can install it to the Web Security Service Production Network.

1. Select **Configuration > Policy.** From the Policy Objects list, select the CPL policy. Click **Edit.**

   **TIP**
   A default reference device is not automatically populated. Associate a least one deployed device with the policy or manually configure a reference device to enable editing.

2. Select the cloud button > **Add Reference Device.**
3. To associate a reference device, from the Select Device dialog, select the check box by the device that you want to use as a reference. The selected device automatically displays in the Selected view. Click OK.

Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy universal policy.</td>
<td>Apply a Single Policy to Both On-Premises and Cloud Users</td>
</tr>
<tr>
<td>Add or remove devices associated with the policy.</td>
<td>Add or Remove Devices Associated with Policy</td>
</tr>
<tr>
<td>Restore a version of the policy.</td>
<td>Restore a Version of Policy</td>
</tr>
<tr>
<td>Import a policy configuration from a device.</td>
<td>Import Policy from a Device</td>
</tr>
</tbody>
</table>

Deploy Tenant Policy

Tenant policy describes a framework that provides large organizations with high service availability, flexibility for multiple tiers of administration, and ensures that all appliances in the network are used efficiently.

- **Tenant Policy** - An infrastructure that segregates the policy elements that effect users of each user network defined within domains. Even though they use the same ProxySG appliance, two groups of users could have vastly different policy sets.

- **Role-Based Administration** - A set of Management Center controls that allows a tiered-based approach to managing ProxySG appliances and their associated policy. The top-tier administrators can view and manage all levels of policy, second-tier (or branch) administrators can manage only their own level of policy and those beneath them, and bottom-tier or tenant-level administrators can only view the policy for their own users.

All administrators control policy appropriate to their roles. Policy can be written specifically to route traffic from where users are to one of several ProxySG appliances in your network, depending on load and availability.

Refer to the following deployment steps.

**Step 1: Plan Network Configuration**

Who performs this step: ProxySG administrator

Before proceeding, it is important to plan how your organization is structured. For example, determine the following:

- How user networks are grouped or separated (for example, by geographic location)
- What interfaces receive traffic from those users
- Why types of policy can be deployed to the tenant slot

**Step 2: Configure Management Center**

Who performs this step: Management Center admin/Super Admin
After configuring the appliance(s), add them to Management Center and define roles and administrators. Then, configure default, group, and tenant policy to the appliances. User roles will dictate which users can see and manage policy for each appliance or group of appliances.

1. Add a configured appliance to Management Center. From the Management Center web console, access the online help and search for the topic entitled Add a Device for the steps to add each ProxySG appliance to Management Center. Repeat this process for each configured ProxySG in your network. To import many devices at one time, from the online help search for Add Multiple Devices at Once.

2. To keep your devices organized, see the instructions for how to create hierarchies, device groups and sub-groups. A device group is a folder in the device organizational structure that exists below the hierarchy level and contains devices or sub-folders. Arrange device groups and devices in a way that makes sense.
   - Configure Hierarchy for Devices and Device Groups
   - Add a Device Group
   - Drag and Drop Device Groups

3. Create device attributes to help manage your organization's network of appliances and groups of appliances. Device attributes can be used to identify the location of a given appliance, the region or branch office it's associated with or even which tenants are associated with each appliance. For more information, see the following topics in the online help:
   - Manage Attributes
   - Add Device Attributes
   - Add Device Group Attributes

4. Assign attributes to your configured appliances. For instructions, see Edit a Device.

5. Create administrator roles with different sets of permissions. After you Define Roles, see the types of the permissions that are most valuable per role that you have created. This guide contains a reference topic Reference: Permissions Interdependencies that is invaluable when creating the roles in your organization. The following example shows how to create a role for managing a device group that you created (Add a Device Group).

6. Create administrator groups. From the Administration tab, click Groups > Add Group.

7. Add admin users. For instructions on how to create administrator accounts, see Grant Permissions.

8. Create policy attributes. For instructions on how policy attributes can be used to organize and refine policy, see the following online help topics:
   - Manage Attributes
   - Add Policy Attributes
   - Mandatory Attributes

9. Define tenants. See Manage Tenants for instructions.

10. Create tenant policy in VPM (Create a VPM Tenant Policy Object) or CPL (see Create the Content Policy Language).

11. Confirm that the correct policies are deployed to each device slot. See View Deployed Policy for each Device Slot.

Manage Tenants

Tenants are administrative entities defined on ProxySG appliances. Each request is routed through a tenant, whose policy is evaluated for that transaction. When no specific tenant is determined for a request, the default tenant policy is used. Tenant determination criteria governs which tenant's policy applies to a given request. Add these tenants to Management Center to create and deploy tenant-specific policy.

On the ProxySG appliance, there are two options for controlling tenancy determination:

1. The `multi-tenant` criterion command specifies a substitution expression that is evaluated for tenancy determination.

2. Using the `<tenant>` layer in the Landlord CPL slot to specify conditions and `tenant()` properties.

   **NOTE**
   The Management Center WAF interface leverages option #2 to control tenancy determination via the Tenant Determination object. See About WAF Policy for more information.
When evaluating an HTTP request, if the tenant determination rules produce a match against an installed tenant, then that tenant's policy will be evaluated. If that fails to set the `tenant()` property, or the `tenant()` property setting does not correspond to an installed tenant policy, then the default tenant policy is applied to this traffic. Default tenant policy applies to all requests where tenancy couldn't be determined during the initial connection.

Obtain the tenant identifiers before you write multi-tenant policy in Management Center. For more information on multi-tenant policy, refer to the Multi-Tenant Policy Deployment Guide.

Selecting a tenant is step 2 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks. A base-level of WAF policy should be installed to the default tenant before any additional tenants are created. This ensures that all requests are processed by the WAF.

**Add a Tenant**

1. Select **Configuration > Tenants**.

2. Click **Add Tenant**.

The web console displays the **Add Tenant** dialog.
3. Enter a **Display Name**.
4. Enter the **Tenant ID**. This controls the name of the tenant slot where policy will be installed. This ID is also used in the tenant determination CPL using the `tenant()` property.
5. (Optional) Enter a **Description** (up to 1024 characters).
6. Click **Save**.

By default, the **Tenants** list is sorted in alphabetical order by **Display Name**. You can also sort by **Tenant ID** or **Description** by clicking the column headings. If the list is long, use the Keyword Search field to search for any string in the name, ID, or description. The search is case-sensitive.

**Modify a Tenant**

1. Select **Configuration > Tenants**.
2. From the Tenants list, select the tenant to modify and click **Edit**. The web console displays the **Edit Tenant** dialog.
3. Edit the **Display Name** or **Description**.
4. Click **Save**.

**Delete Tenants**

1. Select **Configuration > Tenants**.
2. From the Tenants list, select one or more tenants to remove.
3. Click **Delete**.
4. Select **Yes** to delete the selected tenants.

**CAUTION**
You cannot delete the default tenant or any tenant that is currently referenced in Management Center policy. Attempting to delete the default or a referenced tenant results in a "Delete failed" error message.

**Determine Your Next Step**
If you are configuring WAF policy, continue to Specify Tenant Determination Criteria (Tenant Determination File), which is step 2 in **Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks**.

**Create a VPM Tenant Policy Object**
A **VPM Tenant policy object** defines the policy for a VPM Tenant. When creating a VPM Tenant policy object, you select the attribute values that apply to the policy (if attributes have been defined). Then, select the devices or groups to which you deploy the policy; alternatively, you can define these device/group targets later.

**NOTE**
To write tenant policy in CPL instead of using the VPM, see **Create the Content Policy Language**.

To write tenant policy in CPL instead of using the VPM, see **Create the Content Policy Language**.

1. Select **Configuration > Policy** and click **Add Policy**.
   - The web console displays the Create New Policy: Basic Information wizard.
2. Enter a name for the policy object.
3. Select **VPM Tenant** for the Policy Type.
4. (Optional) In the **Reference Id** field, enter a Reference ID that you can filter on when building policy.
   **NOTE**
   - The Reference ID must begin with a letter, and must contain only letters, numbers and ".".
5. Select the Tenant to which this policy object will be applied.
6. Enter a description in the **Description** field. Although entering a description is optional, the description helps differentiate versions of the same policy.
7. Indicate whether to **Replace Substitution Variables**. See **Use Substitution Variables in Policies and Scripts** for more information.
8. Click **Next**.
9. Enter or select values for the defined attributes.
10. Click **Finish**.
    - The new VPM Tenant policy object displays in the Policy Objects editor.
Determine Your Next Step

After you create a tenant policy object, you can either add policy to it immediately or leave it as an empty object while you perform other tasks (for example, associate more devices with it or edit policy details). Refer to the following table to determine the next step to take.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add policy.</td>
<td>Launch Visual Policy Manager</td>
</tr>
<tr>
<td>Import policy.</td>
<td>Launch Visual Policy Manager</td>
</tr>
<tr>
<td>Learn about deploying multi-tenancy policy on ProxySG appliances.</td>
<td>Multi-Tenant Policy Deployment Guide</td>
</tr>
<tr>
<td>Create and manage tenants from Management Center.</td>
<td>Manage Tenants</td>
</tr>
<tr>
<td>View policies deployed to each slot on a device.</td>
<td>View Deployed Policy for each Device Slot</td>
</tr>
</tbody>
</table>

Import VPM Tenant Policy from Source Device

A VPM Tenant policy object can be used to define the policy used in a tenant slot. After creating the VPM Tenant (as described in Create a VPM Tenant Policy Object), you must add policy to it. You can add policy by the legacy or web-based VPM or by importing existing VPM policy from a source device.

Certain features available in normal VPM policy are not available in VPM Tenant policy. These include the Admin Access and Admin Authentication layers. Any existing Admin Access or Authentication layers will not be present in the imported contents.

**NOTE**
To write tenant policy in CPL, see Create the Content Policy Language.

1. Select Configuration > Policy.
2. Select the VPM Tenant object and click Edit.
3. Select Import > From Device.

The system displays the Import Policy: Source Device dialog.

4. Select the source device and click Next.
5. Click **Import**.

The dialog closes and the following message is displayed in the editor:

**The CPL for this VPM policy is out of date and needs to be regenerated before it can be deployed. Please launch the VPM editor and save a new revision to update the CPL.**

This is because only the VPM contents are imported, not the generated CPL.

6. To regenerate the CPL, click **Launch VPM Editor**.

The dialog closes and the following message is displayed in the editor:
7. Click **Save Policy**.
8. Enter a comment for your save and click **OK**.
9. Click **Close**.

The CPL now displays in the editor.

**Determine Your Next Step**

Refer to the following table to determine the next step to take.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about deploying multi-tenancy policy on ProxySG appliances.</td>
<td>Multi-Tenant Policy Deployment Guide</td>
</tr>
<tr>
<td>Create and manage tenants from Management Center.</td>
<td>Manage Tenants</td>
</tr>
<tr>
<td>View policies deployed to each slot on a device.</td>
<td>View Deployed Policy for each Device Slot</td>
</tr>
</tbody>
</table>

**Schedule Removal of Unused Tenant Policy**

You can delete unused policy from a tenant slot. Management Center considers policy in a tenant slot to be unused if policy is installed on the appliance but does not exist in the tenant slot in Management Center, regardless of whether or not the policy was created or deployed through Management Center. Consider the following examples:

- If you create tenant policy in Management Center, deploy it to an appliance, and then remove it from Management Center, it is considered to be unused.
- If you create tenant policy on the appliance without importing it to Management Center, it is considered to be unused.

**NOTE**

This operation is not supported in Multistep Device Jobs.

**NOTE**

See also **Remove Unused Tenant Policy**.

1. Select **Jobs > Add > New Job** .
2. On the **Add New Job** page, select **Remove Unused Policy**.
3. **Configuration**:
   - To remove all unused tenant policy, skip to step 2 **Targets**. To exclude some tenant IDs, click the + and enter those tenant IDs.
   - The tenant ID is the name of the tenant slot where policy will be installed. This ID is also used in the tenant determination CPL using the tenant() property. Go to **Configuration > Tenants** to view the existing tenant IDs.
4. **Targets**:  

---

341
– Select the **Devices** or **Groups** tab.
– Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
– Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
– If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
– All selected targets appear in **Selected Targets**.

5. **Job Results:**
– (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

6. **Schedule:**
Choose to trigger job execution using a **Schedule** or an **Event**.

   **Schedule**
   Use **Schedule** when you want to run the job now or to execute the job at a specific time.
   – **Immediate**—automatically runs the job after it is created.
   – **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
   – **Run Once Only**—specify the date and time to run the job.
   – **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
   – **Daily**—runs the job every day at the specified time.
   – **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

   See also **Job Scheduling Options**.

   **Event**
   Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   – **Device added to Management Center**
   – **Device added to Group**
   – **Device removed from Group**

   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

7. **Name:**
– Verify or change the name and add an optional description.

8. Click **Save**.

**Install or Import Policy**

To install or import policy, refer to the following.

**Preview Policy Before Installing It**

**Install Policy**

**Install Multiple Policies**

**Import Policy or Shared Objects**

**Import External Policy**
Preview Policy Before Installing It

Management Center deploys policy to devices as it appears in the Policy Editor, and does not attempt to compile or otherwise validate your CPL. To make sure that the CPL is correct and that the ProxySG appliance will process the policy as intended, you can preview the policy for specific devices before installing it.

If the policy includes substitution variables, the policy preview displays the specific values that replace the variables for each associated device.

1. Create policy (Create the Content Policy Language) or edit existing policy (Refine Existing CPL Policy).
2. (If policy includes substitution variables) On the Basic Information tab when creating policy, or on the Info tab when editing policy, select Replace substitution variables.
3. Click Targets and select the device for which you want to preview policy.
4. Click Preview.

If you have unsaved policy changes, choose Unsaved Changes or view the Latest Saved Version. The web console displays the CPL in a Preview dialog.

**TIP**

Only saved policy can be installed. Use Preview to verify your unsaved policy before saving it. Then save and install it.

Inspect the CPL for any errors and edit it if needed. If the policy includes substitution variables, all variables are replaced with appropriate values (except for cases where no value is available). For more information, see Use Substitution Variables in Policies and Scripts.

Install Policy

When you create policy, you do not have to install it to devices immediately; you can save it, continue to edit and test it, and then deploy it to devices when it is complete and working as expected.

**WARNING**

You cannot install a shared object. Shared objects are used to augment policy, not to replace policy. See Create Shared Objects.

You can only install the latest version of policy; if you want to install an earlier version, restore that version first. See Restore a Version of Policy.

Policy Installation Methods

Install policy using one of the methods described in the following table.

<table>
<thead>
<tr>
<th>Type</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Configuration &gt; Policy</td>
<td>Install policy using job wizard. You can select more than one script to install in the same job.</td>
</tr>
<tr>
<td>Install to All</td>
<td>Configuration &gt; Policy &gt; Policy_Name &gt; Edit &gt; Targets</td>
<td>Install policy using job wizard.</td>
</tr>
<tr>
<td>Install to Target</td>
<td>Configuration &gt; Policy &gt; Policy_Name &gt; Edit &gt; Targets</td>
<td>One click policy installation. Does not use the job wizard.</td>
</tr>
<tr>
<td>Install Policy</td>
<td>Jobs &gt; Add &gt; New Job &gt; Install Policy</td>
<td>Install policy using job wizard.</td>
</tr>
</tbody>
</table>
**Install Policy**

The following procedure also applies to **Install to All**.

1. Select **Configuration > Policy** and highlight one or more policy rows. Click **Install**.

2. **Policies:**
   - For each policy, click **All Predefined Targets** to install the policy to all target devices specified for the policy (**Policy > Edit > Targets**), or click **Selected Targets** to select specific target devices.
   - Select **Force installation (don't abort the job on installation warnings)** if you want the job to run even if installation warnings are encountered. When you select this option, Management Center will install the policy even if it is identical to that already installed on the device. If this option is not selected and the policy is identical, the job will execute successfully (without reporting any associated warnings) with a note that no installation was actually performed.
   - If you run a job many times a day and force installation, a large number of policy deployment records can be recorded in your database. In that case, Symantec recommends that you do not select this option if you want to limit the number of deployment entries in the database.
     - Click **Add More Policies** to add other policies to your installation.
     - If you selected multiple policies, verify the order of policy installation. Click the **Remove** button to remove a policy file or the arrows to move them up or down in the installation order.

3. **Job Results:**
   - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

4. **Schedule:**
   Choose to trigger job execution using a **Schedule** or an **Event**.
   - **Schedule**
     - **Use Schedule** when you want to run the job now or to execute the job at a specific time.
     - **Immediate**—automatically runs the job after it is created.
     - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
     - **Run Once Only**—specify the date and time to run the job.
     - **Periodic**—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
     - **Daily**—runs the job every day at the specified time.
     - **Monthly**—runs the job once a month on the specified day of the month and specified time of day.
   - **Event**
     Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
     - **Device added to Management Center**
     - **Device added to Group**
     - **Device removed from Group**
   - If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

5. **Name:**
   - Verify or change the name and add an optional description.

6. Click **Save**.

**Install to Target**

1. Select **Configuration > Policy**.
2. Select the policy name and click **Edit**.
3. Click the **Targets** tab and click **Install to Target**.
NOTE
If you attempt to install policy that is identical to that already installed on the device, the system informs you that they are identical and prompts you to confirm the installation. If you proceed with installation, the policy is installed. This can be useful if you want to view policy warnings associated with the installation.

Determine Your Next Step
If you are configuring WAF policy, continue to Configure WAF Security Rules (WAF Security Profile), which is step 5 in Use Web Application Firewall (WAF) Policy To Protect Servers From Attacks.

Install Multiple Policies
When you create policy, you do not have to install it to devices immediately; you can save it, continue to edit and test it, and then deploy it to devices when it is complete and working as expected. You can create multiple policies without having to install the policies right away. This is particularly useful for large deployments of policies to multiple devices or device groups.

You can schedule multiple policies to deploy to device groups, as long as the following are true:

- Each policy does not have unsaved changes. To ensure that the latest policy changes are installed, click Save Changes in the Editor.
- Any devices you want to associate with the policy have been added and activated in Management Center.

It is a best practice to only schedule installation of policies that are the latest version. However, you can Force Installation of Policies, by selecting the Force Installation check box. During installation of policies, Management Center ignores the following installation warnings:
  – Mismatched on-box policy object
  – Mismatched OS versions

TIP
By forcing the Installation, you are ensuring that large deployments of policies DO NOT fail when encountering devices that may have the above issues.

1. From the Jobs tab select the Scheduled Jobs section. Click Add Job. The Add Job Wizard displays the Add Job: Basic Info dialog. Fields marked with an asterisk (*) are required.
2. Enter a unique Name (*) for this large policy deployment. Enter a Description.
   TIP
   For example, the unique Name can be Install Policies on All Active ProxySG Appliances, and the Description can be Deploy policies to all activated ProxySG appliances.
3. Click Next. The Add Job wizard displays the Add Job: Operation dialog.
4. From the Operation drop-down, select Install Policy. The policy marked with a red asterisk is a mandatory policy and is installed regardless of the other policies you select.
5. From **Select Policies to Install**, select the Object Selector

To choose the policies to install, click the check box associated with each policy. This action immediately populates the **Selected** list. Click **OK**. Choose the Force installation check box. Click **Next**. The Add Job wizard displays the Add Job: Targets dialog.

Each selected policy will be installed to targeted devices (excluding devices that are not active).

**NOTE**

You cannot choose targets at this point. If you are not sure of the devices targeted by the selected policies, click **Back**. Management Center has built in intelligence, so that only properly configured policies can only be applied to appropriate targets.

6. Click **Next** to choose a **Schedule**. See **Job Scheduling Options** and **Install Policy**.

**Import Policy or Shared Objects**

You can import policy into Management Center. For example, if a knowledge base article includes sample policy, you could import it directly into Management Center. You could also share policies between Management Center instances.

You can import policy into Management Center in the following ways:

- Import Policy from a File (Policy or Shared Objects Grid)
- Import Policy from a File (Object Edit)
- Import Policy from a Device
NOTE
If you import a policy without a reference ID, the system assigns a reference ID with the format auto_generated_id_1. You can change the ID after importing the file.

Import Policy from a File (Policy or Shared Objects Grid)

You can import policy from the following file types:

- Management Center (.json)
- Content Policy Language (.cpl, .bpf, .txt)
- Visual Policy Manager (.xml)

1. Select Configuration > Policy or Configuration > Shared Objects.
2. Click Import.

The system displays the Import Policy wizard.

3. Drag and drop the file into the Select File dotted-line area. Alternatively, browse to the file.
4. Click Next.
5. If the imported file contains multiple policies, you might want to exclude some from import. To do this, clear the Import Policy check box.
In the preceding example, the VPM policy has been excluded from import.

6. Choose whether to create a new policy or to update an existing policy.
NOTE
The wizard displays only policy objects that are relevant to the file type. If the policy uuid or reference ID in the import file matches a policy already on the system, **Update existing policy** is the default (with the matching policy prepopulated in the **Policy** field under **Update Existing Policy**). Otherwise, **Create new policy** is the default.

- To update an existing policy, ensure that **Update existing policy** is selected. Clear the **Import Policy** check box for any policies you do not want to change.
- To update a different policy than the one shown, click the pencil icon, select the policy or policies to replace, and click **OK**.
7. Click **Import**. The system displays the results of the import.
8. Click **Close** to exit the wizard.

**Import Policy from a File (Object Edit)**

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.
2. Select the policy object and click **Edit**.
3. Click **Import > From File...** or **Operations > Import > From File...** (CPL or CPL Fragments).
4. Drag and drop the file into the **Select File** dotted-line area. Alternatively, browse to the file.
5. Click **Import**.

**Import Policy from a Device**

Importing policy from a device is useful in the following situations:

- You want to use a device’s currently installed policy as the starting point for a managed policy.
- A device has a policy configuration that you want to use as a policy template to deploy on other like device(s).

**Universal VPM Policy Considerations**

Although you can import universal VPM policy from a source that does not have enforcement domains enabled, you cannot deploy the policy unless you launch the VPM Editor and save a new revision of policy. This generates the CPL with enforcement domains enabled.

**Import from Device**

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.
2. Select a policy object or CPL fragment and click **Edit**.
3. Click **Import > From Device...** or **Operations > Import Policy > From Device...**. The web console displays the Import Policy wizard.
4. From the **Source Device** drop-down list, select the device from which to import the policy configuration and click **Next**.
5. Select the policy that you want to import. Depending on whether the policy is a VPM or CPL policy, the deployment type is shown next to the policy:
– **VPM** - This policy contains policy created by the Visual Policy Manager and is deployed in the V slot.

– **Central** - This policy contains policy common to your entire organization and is deployed in the C slot.

– **Local** - This policy contains policy specific to your organizational structures, such as departmental policies or local (geographic-specific) policies and is deployed in the L slot.

– **Forward** - This policy contains forwarding rules for the policy and is deployed in the "F" slot.

– **Landlord** - Policy rules for tenant determination.

– **Default tenant** - Policy rules for all requests where tenancy cannot be determined during the initial connection.

– **Tenant** - Policy specifically for tenants.

**NOTE**
For details on tenant policy, refer to the Multi-Tenant Policy Deployment Guide.

– **WSS** - Used for WSS targets (universal VPM policy) only.

6. Select **Import Policy**.
The web console prompts you to confirm the overwrite of the existing policy in Management Center.

7. Click **Import and Overwrite** to accept the import.

8. (Optional) Click **Compare** to view the differences between an earlier version of a policy and the current version. See Compare Different Versions of the Same Policy.

9. Enter a comment for the commit operations and click **Save**. The comment that you enter is saved as metadata.

Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export policy</td>
<td>Export Policy and Shared Objects to Local Disk</td>
</tr>
<tr>
<td>View existing policy information</td>
<td>View Existing Policy Information</td>
</tr>
<tr>
<td>Restore a version of the policy</td>
<td>Restore a Version of Script</td>
</tr>
<tr>
<td>Deploy the policy, as is, to devices</td>
<td>Install Policy</td>
</tr>
</tbody>
</table>

View Policy

To view policy, refer to the following.

Preview Policy Before Installing It

View Existing Policy Information

View Deployed Policy for each Device Slot

View Devices Associated with Policy

View Policy Versions

Management Center enables you to view CPL or VPM policy versions.
NOTE
A policy file can have up to 99999 versions. By default, Management Center keeps an unlimited number of versions. In practice this will become an issue as storage is limited and eventually you would run out. So we have a housekeeping script to delete old version. It was limited to 999 and we changed it to 9999

1. Select Configuration > Policy.
2. From the Policy Objects list, select the policy name.
   If needed, search for the policy object; see Filter by Attributes and Keyword Search.
3. With the policy selected, click Edit. The system displays the editor.
4. Select the Versions tab.

5. Select the policy version you want to view.
6. Click View. The Preview dialog displays.
   - CPL Example:
– VPM example:

7. (Optional) To compare policy versions, see Compare Different Versions of the Same Policy.
8. (Optional) To restore an earlier version of the policy, See Restore a Version of Policy.
9. Click Close.

View Existing Policy Information

Whenever you create a version of policy, Management Center automatically saves information about it. This information is called metadata.

1. You can view metadata by selecting Configuration > Policy.
2. Select a policy and click Edit.

View Policy Object Information

1. Click the Info tab. The Version Control page displays all versions of the selected policy.
2. Under General Information, the Overview displays the information you entered when creating the policy object:
   - Policy name(*)—The name of the Policy that you gave it when you created it
   - Policy type(*)—The Policy type can either be CPL or VPM.
   - Description—This is the Description that you entered when you created the policy. If you edit this field, make sure to click Save before leaving the Info tab.
   - Replace substitution variables
     TIP
     Variable substitution is powerful and can be applied to policies and scripts. See Use Substitution Variables in Policies and Scripts.
3. Metadata displays under Latest Revision:

View Available Policy Versions

1. Click the Versions tab. The Version Control page displays all versions of the selected policy. When a policy object is created it is assigned the Version number 1.0. Every time that add attributes or edit it in any way, the version increases by increments of 0.1.
2. Select an early version of policy to compare.
3. Press and hold the Ctrl key while selecting the later version of policy to compare.

   - Version Number—When a policy object is first created, its version is 1.0. Each subsequent time the object is modified—for example, if the object properties are edited or when policy is added to it—the version number increments by 0.1. For example, when you add policy to an object and save it, the version becomes 1.1.
   - Date—The time and date stamp indicates when the policy was last updated.
   - Author—The author is the user who saved the current version of the policy.
   - Comments—If the author entered comments about the policy, they are displayed here. Metadata displays automatically-generated comments as follows:
     • Policy Object created—When the policy container is initially created and policy has not been added yet.
     • Name changed—When the policy name is edited.
     • Description changed—When the policy description is edited.
     • Name and description changed—When both the name and description are edited.
     TIP
     Of these metadata, the comments are usually the most important in helping you and other users understand the purpose and intent of creating the specific policy version. Symantec recommends that you always enter clear, helpful comments when creating policy.
View Associated Policy Attributes

1. Select the **Attributes** tab. The Attributes page displays all attributes currently assigned to this Policy. The attributes are custom attributes that you created. See Add Policy Attributes or Edit Policy Attributes.
2. You can edit the Associated attributes. If you do, you need to save your changes. Click **Save**. Doing this actually increases the version number by an increment of 0.1.

Set the Maximum Number of Policy Versions to Store in Management Center

1. Select the **Administration > Settings**. Click **General**. General fields display on the right.
2. Select **Maximum number of policy revisions to store**.
3. Enter a number (limit) from 0 to 9999. If the you leave the value at 0, Management Center does not prune.
4. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

View Deployed Policy for each Device Slot

1. From the **Network** tab, select a device.
2. Click **Edit**.
3. From the Edit Device wizard, select the **Policies** tab.

The deployment slots are not editable.

Policies are assigned to slots in the following ways:

- Direct assignment - The policy was installed directly to the slot and not inherited from the device group to which the device belongs.
- Inherited from [Device Group Name] - The policy was inherited from the device group to which the device belongs.

Notes:

- Local, Central, and Forward are CPL policy slots.
- VPM Tenant and Landlord can be either CPL and VPM.
- Policy deployed to the Landlord slot overrides any previous policy deployed to the Landlord slot.

View Devices Associated with Policy

You can view the devices that are associated with a policy.

1. Select **Configuration > Policy**. From the **Policy Objects** list, select the policy you want to view. If needed, filter on attributes. See Filter by Attributes and Keyword Search.
2. Click **Edit**. Select the **Targets** tab.

   **NOTE**
   Only those devices that can support the policy selected are displayed. This helps to know which policies can be installed on which devices.
3. For each device listed, verify the following:
– **Enabled**—If selected, the policy that is installed on the device is enabled.
– **Name**—The name that was entered in Management Center during device registration.
– **Device Count**—The number of devices available.
– **Device Model**—The device hardware model.
– **Installed Version**—The version of policy installed on the device. If no version is listed, the device is still associated with policy, but policy has not been installed.
– **OS Type**—The operating system on the device.
– **State**—Displays historical association data for devices (whether deleted or not).

**Configure Policy**

Configuring policy for specific devices or multiple devices at once involves several methods of creating, testing, and updating policy.

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>What you can do</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write new policy; the behavior that you want is not yet expressed in policy in Management Center.</td>
<td>Create policy, which involves first creating a policy object.</td>
<td>Create a CPL Policy Object</td>
</tr>
<tr>
<td>Create a policy using the Visual Policy Manager.</td>
<td>Create a VPM Policy Object.</td>
<td>Add a VPM Policy Object and Launch Visual Policy Manager</td>
</tr>
<tr>
<td>Create rules to route traffic to the proper tenant.</td>
<td>Create tenant determination rules.</td>
<td>Specify Tenant Determination Rules (Tenant Determination File)</td>
</tr>
<tr>
<td>Specify rules to protect your WAF applications.</td>
<td>Create a WAF Application object.</td>
<td>Configure WAF Application Objects</td>
</tr>
<tr>
<td>Remove devices from policy or add devices to policy; you want to keep the policy but change the devices that use it.</td>
<td>Associate devices with, or disassociate devices from, a specific policy.</td>
<td>Add or Remove Devices Associated with Policy</td>
</tr>
<tr>
<td>Modify existing CPL policy because it does not behave as intended or has to be improved.</td>
<td>Refine the existing policy.</td>
<td>Refine Existing CPL Policy</td>
</tr>
<tr>
<td></td>
<td>Change the order of policy rules so that the device evaluates correctly.</td>
<td>Change the Order in which Policy Rules are Evaluated</td>
</tr>
<tr>
<td>Verify information about existing policy.</td>
<td>Check information about an existing policy.</td>
<td>View Existing Policy Information</td>
</tr>
</tbody>
</table>

**Manage Attributes**

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Attributes are custom metadata used to refine and describe devices, device groups, policy, and scripts. Attributes can also be used to filter on specific devices, device groups or objects.

**About Attribute Inheritance**

You can designate device and device group attributes as "inheritable." Attributes that are checked as inheritable can "inherit" their attributes from a parent device group.

**Configure Device Group Inheritance**

If you want a group to inherit an attribute's value, you must use a *device attribute*. (Group attributes are used only to add additional meta-data to a group.) To enable group inheritance, see Enable Attribute Group Inheritance. Group hierarchies can also affect inheritance. See Configure Hierarchy for Devices and Device Groups.
Work With Attributes

- Add Attributes
- Edit Attributes
- Add Device Group Attributes
- Set User-Defined Device Attributes for Access Control
- Filter and Keyword Search

Add Attributes

You can define attributes that apply to the devices, device groups, policy and device scripts that you manage in your network. Attributes are custom metadata used to refine and edit devices, device groups, policy, and scripts. Because you have different devices and appliances to manage, those devices require, and are often restricted to, certain attributes. Use these attributes to filter on specific devices, device groups or objects.

1. Select Administration > Attributes.
2. Select one of the following from the Manage Attributes list:
   - Device
   - Device Group
   - Policy
   - Device Script
3. Click Add Attribute. Define the properties of the attribute that you are creating.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description or Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name (*)</td>
<td>Name that displays throughout Management Center.</td>
</tr>
<tr>
<td>Name (*)</td>
<td>This is the name with no spaces.</td>
</tr>
<tr>
<td>Type (*)</td>
<td>Select the data type used for the attribute. See Hide Attribute Value for more information on the Encrypt attribute type.</td>
</tr>
<tr>
<td>Format (*)</td>
<td>Select the format used for String attribute types. For example, Email or Phone.</td>
</tr>
<tr>
<td>Available Values (*)</td>
<td>Display, add, or delete available values for the Picklist attribute type.</td>
</tr>
<tr>
<td>Min Value and Max Value (*)</td>
<td>Specify a minimum or maximum value for the String or Decimal attribute type. The system will not allow attribute values that do not meet or exceed these values.</td>
</tr>
</tbody>
</table>
Management Center - 3.0

<table>
<thead>
<tr>
<th>Property</th>
<th>Description or Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Value</td>
<td>If the attribute has a default value, it is displayed here.</td>
</tr>
</tbody>
</table>
| Mandatory                 | • All attributes that you check as mandatory will appear as options when you create a new policy, device, device group, or device script. When creating the new object, you must enter a value for the mandatory attribute.  
  • Nothing changes to the existing devices, device groups, policy, or scripts when an attribute is marked mandatory.  
  • All mandatory attributes can be filtered on when you Filter by Attributes and Keyword Search.  
  • You can enable variable substitution only if you save the attribute with a default value. See Use Substitution Variables in Policies and Scripts |
| Inheritable               | This attribute applies to devices and devices groups. Attributes that are checked as inheritable can "inherit" their attributes from a parent device group. |
| Displayed as a default column | When enabled, the attribute displays as a column in the Policy Object grid, Script Object grid, or Network dashboard. Even if this option is not enabled, you can still display the attribute by right-clicking the column header, selecting Columns and selecting the attribute to display. See Customize the Network View. |
| Description               | Give a useful description of this attribute to distinguish it from the others when viewing all of the attributes in a list. |

4. Click **Save**.

**NOTE**
You are able to search for specific objects based on the attributes you define. See Filter by Attributes and Keyword Search.

**Edit Attributes**

After you have defined an attribute, you can refine and edit that attribute to apply to any of the devices, device groups, policy and device scripts within your network. Editing an attribute changes the way devices, device groups, policy or script objects can be filtered and searched.

1. Select the **Administration > Attributes** section.
2. From the **Manage Attributes** list, select an attribute to edit from the following attribute types:
   - Device
   - Device Group
   - Policy
   - Device Script
3. Select an attribute from the list and click **Edit**.
4. Change the properties for the attribute.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description or Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name (*)</td>
<td>Name that displays throughout Management Center.</td>
</tr>
<tr>
<td>Name (*)</td>
<td>This is the name with no spaces.</td>
</tr>
<tr>
<td>Type (*)</td>
<td>The format in which users must enter or select attribute values.</td>
</tr>
</tbody>
</table>
### Property Description or Purpose

<table>
<thead>
<tr>
<th>Property</th>
<th>Description or Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Values(*)</td>
<td>The Available Values depend on the Type you selected.</td>
</tr>
<tr>
<td>Default Value</td>
<td>If this attribute has a default value, it is displayed here.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>All attributes that you check as mandatory will appear as options when you create a new policy, device, device group, or device script. All mandatory attributes can be filtered on when you Filter by Attributes and Keyword Search.</td>
</tr>
<tr>
<td>Inheritable</td>
<td>This attribute applies to devices and devices groups. Attributes that are checked as inheritable can &quot;inherit&quot; their attributes from a parent device group.</td>
</tr>
<tr>
<td>Displayed as a default column</td>
<td>When enabled, the attribute displays as a column in the Policy Object grid, Script Object grid, or Network dashboard. Even if this option is not enabled, you can still display the attribute by right-clicking the column header, selecting Columns and selecting the attribute to display. See Customize the Network View.</td>
</tr>
<tr>
<td>Description</td>
<td>Give a useful description of this attribute to distinguish it from the others when viewing all of the attributes in a list.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

### Hide Attribute Value

Hide Attribute Value

There may be times when you do not want the value of an attribute to be shown in policy or scripts. For example, the attribute might contain a device password that should be kept confidential. Management Center provides an **Encrypt** attribute type for these situations.

The encrypted data is stored on Management Center. It is decrypted only when sending to the device.

### Encrypted Attribute Feature Limitations

When using encrypted attributes, be aware that the attribute might be visible in some situations. For example:

- If you include the encrypted attribute in a script and do not structure the script properly, or you include the attribute in a place the device does not expect, the target device can "echo" the plain text value of the attribute in its response.
- If you attempt to install policy that includes an encrypted attribute and the policy installation fails because of a syntax error with the attribute, the target device provides the plain text value of the attribute in the resulting error message.
- If you install the policy to the target and then compare the policy versions, the value of the attribute will be visible in the comparison that shows the policy currently installed on the device.

Because of this, use discretion when assigning permissions for executing policy or scripts.

### Add Encrypted Attributes

1. Select **Administration > Attributes**.
2. Select one of the following from the **Manage Attributes** list:
   - Device
   - Device Group
   - Policy
   - Device Script
3. Click **Add Attribute**.
4. Define the properties of the attribute that you are creating. To hide the value, set the **Type** to **Encrypt**.
You'll notice that you can't even view the value while entering it in the **Default Value**. To ensure the accuracy of your entry, you might want to enter the text elsewhere and cut and paste it into this field.

**NOTE**
The Encrypt attribute type has the same options as the String type. However, it is not meant for long, multi-line strings and does not include an expanded editor.

**NOTE**
See Add Attributes for a description of these properties.

5. Click **Save**.

**Verifying Encrypted Attributes**
After you've added the attribute, you should see a message indicating the value is ***MASKED***.
Device Attributes

If you subsequently add the attribute to policy or to a script, you cannot view the value in previews.

```default
<proxy>
  condition=blacklisted_categories DENY
  $(device.attributes.SG4_PW)
</proxy>
```

Receive Notification When Policy Changes

To use this feature, you must set up a mail server in Administration > Settings > Mail Settings.

Management Center 3.0 and later includes the ability to subscribe to an alert for a policy object that has changed. The alert is sent to an email address (or multiple email addresses) that you specify and includes:

- A diff report of the changes that includes the policy name, reference ID, previous version number, current version number, the user who modified it, the modification time, a description, and a commit comment.
- A description of the previous version
- The ability to specify the format of the diff report as HTML or PDF.

1. Go to Configuration > Policy.
2. Select a policy and click Edit.
3. Click the Notifications tab.
4. Specify the diff notification format: HTML or PDF.
5. Enter one or more, comma-separated, email addresses.
6. Click Save.
7. When the policy is changed, notifications are sent to the specified email addresses.

For example:

```
Management Center: 
Policy: Policy 1
Reference ID: Policy_1
Description: 
Previous Version: 1.5
Previous Version Modified By: admin
Current Version: 1.6
Modified By: admin
Modification Time: Thu Jul 16 10:39:21 UTC 2020
With Comment: Denied fantasy football
```
8. Download the attachment to view the diff.

Compare Different Versions of the Same Policy

As a troubleshooting step or as part of performance evaluation, you might want to identify the changes between an earlier version and a later version of policy. Management Center shows the changes made.

1. Select Configuration > Policy. From the Policy Objects list, select the policy name. If needed, search for the policy object; see Filter by Attributes and Keyword Search.

2. Select the Versions tab.

3. Select the versions of policy to compare (press and hold the Ctrl key while selecting the policy versions).

4. Click Compare. The system displays the Compare Policy dialog.

– CPL Example.
### VPM example.

You can diff the source code of VPM policy. To switch between the Generated CPL and XML views, select the appropriate window.

**NOTE**

To see a full set of comments and the timestamp for any policy changes, to view all text changes, including rule index and timestamp changes, click the **Generated CPL (Verbose)** tab.

The two policies are displayed side-by-side; the web console displays the earlier version on the left and the later version on the right.

- Policy highlighted in red exists in the former version and was removed in the later version.
- Policy highlighted in yellow indicates that a line exists in both versions of policy, but there are differences in the line.
- Policy marked in green does not exist in the former version and was added in the later version.
- Policy highlighted in white means the two copies are identical.

5. (Optional) To restore an earlier version of the policy, see **Restore a Version of Policy**.
6. Click **Close**.

### Export Policy or Shared Objects to Local Disk

You can export policy objects from the **Policy** or **Shared Objects** grid. The policy is exported in JSON format. If you export multiple policy objects, they are collected and exported in a single JSON file.

1. Select **Configuration > Policy** or **Configuration > Shared Objects**.
2. Select one or more policy objects.
3. Click **Export**.

4. Depending on your browser settings, you may be prompted to view or save the file. Click **Save** if prompted. In other cases, the file is automatically saved to local disk (typically, the Downloads folder).

### Restore a Version of Policy

After time, you might find that the policy pushed to devices needs improvement or must change because of changes in business requirements or practices. In such situations, you can modify policy as needed, or revert to an earlier version of policy that is appropriate. When you have determined which version of policy to restore, you can restore it using the version history.

1. Select **Configuration Policy**. From the Policy Objects list, select the policy name. If needed, search for the object; see **Filter by Attributes and Keyword Search**.

2. Click **Edit**. Click the **Versions** tab. Versions of the policy are listed in descending numerical order.

3. From the **Version Control** page, verify that the version you want to restore is the correct one.
   a) Perform one or both of the following as required. Check the version metadata. See **View Existing Policy Information**. Compare versions of policy. See **Compare Different Versions of the Same Policy**.

4. After you identify the version to restore, select it and click **Restore**. The web console displays the Restore dialog.

5. In the **Comment** field, specify the reason for the restore.

6. Click **Restore**. The restored version of the policy is incremented to the latest version in the **Policy** list, and the comment you entered in step 6 is displayed in the **Comments** column.

7. To install the restored policy to associated devices, select the policy and click **Install Policy**. See **Install Policy**.

### Check Consistency between Policy and Devices

You can check if the policy saved in Management Center is different from the policy installed on devices. You can also create a job to check consistency. See **Create Job to Check Consistency of Policy**.

1. To check the consistency of the installed policy with the devices, select **Configuration > Policy** and select a policy object.

2. Select the option by the policy name. Click **Edit**, and then click the **Targets** tab.

3. Select the device that you want to check for consistency against the policy stored in Management Center. Click **Check Consistency**. Select the base policy version by selecting the **The latest policy version** or the **Version** check box.

   **NOTE**
   
   If you don't select any devices, or you select a few and click **Check Consistency**, a consistency check is done on those devices, not just one. No selection of a device is required.

4. Click **Check Consistency**.
If you receive a **Mismatch** error for a device, the policy is inconsistent: either the policy was changed in Management Center and not installed to the device with the error, or the policy on the device was changed outside of Management Center.

5. You can click **Compare Policy** to determine what has changed.

6. (Optional) For each device listed, verify the following:

   **NOTE**
   The Management Center license contains all of the features for which you have purchased a subscription. The documentation covers all features, including ones that you may not have purchased.
   - Policy is enabled (if **Enabled** is selected).
   - Device Name—The name that was entered in Management Center during device registration.
   - Device Count—The number of managed devices is shown in the banner.
   - Device Model—The device hardware model.
   - Installed Version—The version of policy installed on the device. If no version is listed, the device is still associated with policy, but policy has not been installed.
   - OS Type—The operating system on the device.
   - State—The status of the device. See **About Status Indicators**.
Determine Your Next Step

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove associated devices.</td>
<td>Add or Remove Devices Associated with Policy</td>
</tr>
<tr>
<td>Compare different versions of the same policy.</td>
<td>Compare Different Versions of the Same Policy</td>
</tr>
<tr>
<td>Install a policy or policies.</td>
<td>Install Policy or Install Multiple Policies</td>
</tr>
<tr>
<td>View policy information.</td>
<td>View Existing Policy Information</td>
</tr>
</tbody>
</table>

Add or Remove Devices Associated with Policy

Use the following procedure to add targets to associate with the selected policy.

**Web Security Service (WSS) Target Considerations**

Consider the following if you plan to add WSS as a target.

- You cannot add WSS and other devices (for example, a Content Analysis) as targets in the same operation because they have different deployment types. You must add WSS devices in a separate operation.
- Management Center must have a connection to the reference device at the time of installation. When installing policy, Management Center fetches data from the reference device, including non-policy configuration items like ICAP server data, and exception pages referenced by policy.
- For universal policy, appliance-only rules are blanked out before sending to the WSS. The rules are replaced with blank lines.

**Add Targets**

1. Select Configuration > Policy. From the Policy Objects list, select the policy you want to add to devices. If needed, search for the object; see Filter by Attributes and Keyword Search.
2. Select the policy name. Click Edit.
3. Click the Targets tab. To add targets to associate with the selected policy, click Add Targets.
4. From the Add Targets wizard, select the Devices tab. Select the checkbox by the device(s) name (or click Add to add a new device).

**NOTE**
Only those targets that can support the policy selected are shown. This helps to know which policies can be installed on which targets (devices).
5. (Optional) To associate device groups with the policy, click the Groups tab and select Devices. This action immediately populates the Selected list.

6. To remove the selected devices, click Unselect or Unselect All. Click Next. The Add Targets wizard displays the Add Targets: Configure Deployment dialog.

7. From the Deployment Type drop-down list, select one of the following:
– **VPM Slot** - Generated CPL (and the XML markup which persists the state of the VPM UI) pushed to the target's VPM slot.
– **Policy Slot** - The ProxySG appliance's Local, Central, or Forward policy file.
– **WSS** - Used for WSS targets (universal VPM policy) only.
– **Landlord Slot** - Policy rules for tenant determination.
– **Tenant Slot** - Policy specifically for tenants.

**NOTE**
If you select **Tenant Slot** and a tenant is not configured, a "Tenant not configured" warning appears in the Deployment column on the Targets tab.

8. (If you selected Policy Slot) From the **Slot** drop-down list, select **Local**, **Central** or **Forward**.
9. Click **Finish**. A web console message displays the following:

![Add Targets](image)

Add Targets
Successfully added 1 targets to policy object: test\16.

**Remove Targets**
To remove devices associated with a policy, select the device name and click **Remove Targets**. You are asked to confirm that you want to remove the associated device(s). Click **Yes** or **No**.

![Remove Device Associations](image)

Remove Device Associations
Are you sure you want to remove the 1 selected associations?

Yes  No

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>View associated devices (targets)</td>
<td>View Devices Associated with Policy</td>
</tr>
<tr>
<td>Compare policy versions</td>
<td>Compare Different Versions of the Same Policy</td>
</tr>
<tr>
<td>Install a policy</td>
<td>Install Policy</td>
</tr>
<tr>
<td>Compare the policy version installed on the device, with the most</td>
<td>Compare the Device Policy Version with Current Policy Version</td>
</tr>
<tr>
<td>current version saved in Management Center</td>
<td></td>
</tr>
<tr>
<td>Schedule a policy installation</td>
<td>Add a Job</td>
</tr>
<tr>
<td>Install multiple policies to multiple devices</td>
<td>Install Multiple Policies</td>
</tr>
</tbody>
</table>

**Import External Policy**
You can create a job to import a CPL fragment created in an external tool into Management Center. The job can be executed immediately, manually, or on a schedule. This is useful if you want to regularly sync the policy with the version on an external server.
Before you import an external policy, you need to create a policy object in Management Center into which to import the file.

**NOTE**
This operation is not supported in Multistep Device Jobs.

**Prerequisites**

Before you create the Import External Policy job, you need to perform the following tasks:

1. Create the CPL in an external tool.
2. Create a policy object in Management Center. You will be importing the external file into this policy. See Create a CPL Policy Object.
3. (Optional) If you intend to use the URL as an absolute path to the policy target file, select **Use URL as absolute path to file**.
4. If you intend to import policy from a directory that contains UUID .bpf files, do the following:*:
   a. Edit the policy object and go to the Info tab. Record the Unique ID; you must name the external CPL file with this ID.
   b. Name the external policy file with the Unique ID of the Management Center policy.
   Example: `7B6F26F9-94FB-453C-B56F-8AE433ABDBBE.bpf`
5. Store a file that contains the contents of the policy on a web, FTP, or SCP server.
6. Make note of the URL path to the file; you will need to specify the URL when defining the Import External Policy job.

*When the URL is used as an absolute path to the policy target file, Management Center attempts to fetch a file at the URL and store it as the content for the policy target(s) selected. If you have more than one target policy selected for the job, all the targets will be updated with the same content of the file.

The Management Center default treats the URL as a directory and attempts to fetch files that match one of the IDs of the policy target(s). When the job executes, Management Center appends `{id}.bpf` to the URL for each of the policy targets in the job.

**Create Job to Import External Policy**

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Import External Policy**.
3. **Source:**
   - **Import from URL:** The path to the file on the external web, FTP, or SCP server. The filename must be the ID assigned to the target policy.
     - Directory URL Example: `ftp://company.com/policies/
     - Absolute Path to File Example: `ftp://company.com/policies/mypolicy.txt`
   - **Use URL as absolute path to file:** This option is not selected by default. Leave this option unselected if you want to load a large number of policies and do not wish to manage separate jobs for each. Select this option to treat the URL as an absolute path to the policy target(s).
   - **Username:** If authentication to the server is required, enter the name of user with permission to access the server.
   - **Password:** Enter the user's password.

   **NOTE**
   If you have more than one target policy selected for the job, all the targets will be updated with the same content of the file.

4. **Destination:**
   - Select the policies to update.
   - Add multiple policies by selecting the check box next to the name of the policy.
5. **Job Results:**
   - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).
6. **Schedule:**
Choose to trigger job execution using a **Schedule** or an **Event**.

**Schedule**

Use **Schedule** when you want to run the job now or to execute the job at a specific time.
- **Immediate**—automatically runs the job after it is created.
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
- **Run Once Only**—specify the date and time to run the job.
- **Periodic**—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
- **Daily**—runs the job every day at the specified time.
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

See also **Job Scheduling Options**.

**Event**

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See the following note.

7. **Name:**
   - Verify or change the name and add an optional description.
8. Click **Save**.

**Distribute ProxySG Policy to Multiple Devices**

When you want multiple ProxySG appliances to run the same policy, you can create the policy once and then distribute it to all devices that require this same policy. To accomplish this goal, you create and test the policy on a reference device, assign targets to the policy, and then create a job to install the policy on the predefined targets.

1. (Optional) Create a device group for the ProxySG devices to which you want to distribute the same policy. See **Add a Device Group**.
2. Create and test a VPM policy on a single device; this ProxySG is called the *reference device*. See **Select Reference Device for VPM Policy**.
   
   **NOTE**
   
   You can also use CPL to write the policy. See **Create a CPL Policy Object**.
3. Select the target devices to which you want to distribute the policy:
   a. Select **Configuration > Policy**.
   b. Select the policy you created in step 2 and click **Edit**.
   c. Click **Targets > Add Targets**.
   d. Click the **Groups** tab and selected the group created in step 1.
   e. Click **Next** and **Finish**.
4. Create a job to install the policy on the target devices. See **Install Policy**.
5. After Management Center runs the policy installation job, confirm that the policy was installed on the target devices.

**Create Job to Check Consistency of Policy**

This job checks if the policy saved in Management Center is different from the policy installed on devices.
NOTE
This operation is not supported in Multistep Device Jobs. See also Check Consistency between Policy and Devices.

Schedule Consistency Check of Policy
1. Select Jobs > Add > New Job.
2. On the Add New Job page, select Check Consistency.
3. Policy:
   – Policy to check: Select the reference policy to use for comparison. The job will check the policy against all associated targets.
4. Job Results:
   – (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).
5. Schedule:
   Choose to trigger job execution using a Schedule or an Event.
   Schedule
   Use Schedule when you want to run the job now or to execute the job at a specific time.
   – Immediate—automatically runs the job after it is created.
   – No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
   – Run Once Only—specify the date and time to run the job.
   – Periodic—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
   – Daily—runs the job every day at the specified time.
   – Monthly—runs the job once a month on the specified day of the month and specified time of day.
   See also Job Scheduling Options.
   Event
   Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   – Device added to Management Center
   – Device added to Group
   – Device removed from Group
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.
6. Name:
   – Verify or change the name and add an optional description.
7. Click Save.

WARNING
If you receive aMismatch error for a device, the policy is inconsistent: either the policy was changed in Management Center and not installed to the device with the error, or the policy on the device was changed outside of Management Center.

About Universal Policy Enforcement
Management Center can be used in conjunction with the Symantec Web Security Service to create universal policy enforcement (UPE) rules. For more information, see Apply a Single Policy to Both On-Premises and Cloud Users.
Filter by Attributes and Keyword Search

You can search for existing objects by filtering on attributes and then using the keyword search. When you are managing hundreds or policies and scripts across multiple devices, it is important to be able to find a particular object quickly.

**TIP**
You are not limited to the displayed Filter fields. See Customize Object Filters.

1. Click the **Configuration** tab and select **Policy** or **Scripts**. From the Filters list on the right pane, the following fields are available by default.
   - **Name**—Filters by the Object Name
   - **Reference Id**—Filters by the Object Reference Id
   - **Type**—Filters by the Object Type
   - **Description**—Filters by the Object Description
   - **Author**—Filters by who user who last changed the Object

**NOTE**
Additional fields are created when you create a new attribute. See Manage Attributes.

   - **Tenant**—Filters by tenant ID.

2. To filter by a particular type of policy, click the **Type** drop-down list and select a policy type.

3. Two options:
   - Click **Apply Filters**. The **Policy Objects** and **Script Objects** lists only those objects you defined by **Type**. ~or~
   - Filter by particular device type for which you created a script; select the device type from the **Type** drop-down list.

4. Click **Apply Filters**. The **Script Objects** list displays only those scripts you defined by type.

**Search by Keyword**

When searching, Management Center breaks text into keywords and then searches for keywords entered. Management Center's index system has a special case for dot. Although Management Center sees dots as separating letters within a word (for example, Management Center considers dots as a part of a word).

**TIP**
The wildcard symbol is *. Management Center automatically appends an * at the end of your search term but if you want to start with a wildcard search, you have to enter it yourself.

Colons are treated like other non-letters by splitting keywords apart. IPv4 and IPv6 addresses work differently because of colons.

**NOTE**
You cannot search on special characters, such as ^ % | ~ .

1. From the **Keyword Search** field, enter your search term.
2. Press Enter or click the magnifying glass icon.

**Can quotes be used in a search?**

Use quotes when non letters are part of the search term. For example, your search term includes a colon.

**NOTE**
The exception to this search rule is the use of a dot because a dot that is not followed by white space is considered part of the keyword.
How do you search for whole words?
Enter the whole word. If there is more than one word, separate each word with a space. If using special characters, enclose each word in double quotes.

How do you search for partial words?
Enter the partial term, and Management Center attempts to complete the search. For example, enter hi and Management Center matches that to both highlight and high.

Example Searches
IPv4 127.0.0.1
• 127.0.0 — Matches any IPv4 starting with 127.0.0.
• *.0.0.1 — Matches any IPv4 ending in 0.0.1.

IPv6 “0:0:0:0:1”

TIP
Use quotes for IPv6 addresses because IPv6 uses colons instead of dots as the separator.

• “0:0:0” — Matches any IPv6 start with 0:0:0.
• *“0:0:1” — Matches any IPv6 ending with 0:0:1.

Hostnames
• abc.com — Matches a host named abc.com.
• *.com — Matches a hostname ending in .com.
• *”:8080” — Matches a hostname with :8080 as the port.

What if the search finds no match?
If the search finds no match, the right pane displays a message indicating that no objects match the keyword filter. You can search again using a different keyword.

What if the search succeeds in finding matches?
If the search finds matches, the results display in alphabetical order in the Objects list.

How do you clear the search results?
To clear search results and display all objects in the system, click the X in the search field.
Create and Manage Jobs

Management Center allows you to create jobs for running a variety of operations on a defined schedule. For example, you can create jobs for backing up Management Center each day, installing policy on a group of ProxySG appliances immediately, or executing a ProxySG script on a monthly basis. Jobs don't necessarily need a precise schedule, though; if you don't define a schedule for a job, you can run the job manually. In addition, you may override the defined schedule for a job and run it immediately.

NOTE
Scheduling a job and running an operation require different permissions. See Understanding Job Permissions.

1. Plan the job:
   – Determine which operation you want to create a job for. See Job Operations.
   – Which devices do you want to perform the operation on? These will be the \textit{targets} of the job.
   – Decide how often the job should run. This will be the job schedule. See Job Scheduling Options.
2. Create the job. See Add a Job.
3. Monitor scheduled jobs, and run unscheduled jobs as needed. See Monitor Jobs.
4. Monitor jobs as they are running. See View Current Jobs.
5. View job history. See Job History.

Add a Job

This page describes how to add a job using the Jobs > Scheduled Jobs > New Job page.

NOTE
You can also perform operations on individual device, share jobs with another Management Center, or organize jobs in folders.

Composite Jobs
Multistep Device Job
Multistep Job

Device Management
Backup Device
Change Monitoring State
Collect Certificates
Collect SysInfo
Compare Config
Export Backups
Factory Restore Device
Install System Image
Reactivate Statistics Monitoring
Restart Device
Save Config
Set Boot Image

**Policy and Configuration**
- Check Consistency
- Execute Script
- Import External Policy
- Install Policy
- Remove Unused Policy
- Synchronize Devices

**Reports**
- Reporter Report
- SWG-VR Data Collection
- Statistics Monitoring Report
- Schedule Summary Report Job

**System Management**
- Backup Management Center
- Schedule File Transfer

**Add Job That Includes Multiple Jobs (Multistep Job)**

A Multistep Job is a job that includes other jobs you have previously created. The jobs are run in sequence on the target devices specified in each job. This means that you could run a job on a Content Analysis device and a different job on a ProxySG device. You cannot assign target devices while creating a Multistep Job.

If one of the jobs fails, you can continue to execute the rest of the jobs or configure the Multistep Job to abort.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Multistep Job**.
3. **Child Jobs**:
   - Select the jobs to add to the execution list, then click **OK**.
   - Use **Remove**, **Move Up**, and **Move Down** to edit the available jobs and their execution order.
   - Select **Stop on Fail** for any job to stop the execution of the rest of the multistep job should a specific job produce an error. Jobs are executed in the order listed, so you can select as many jobs to stop on as you would like.
   **NOTE**
   Only single jobs are available to embed into a multistep job. To include several job operations in a single job, see **Add Job That Includes Multiple Operations (Multistep Device)**.
4. **Job Results**:
   - Optional—Click **Email results** and select the condition. Then, enter the email(s) of the recipient(s).
5. **Schedule**:
   Choose to trigger job execution using a **Schedule** or an **Event**.
   **Schedule**
   Use **Schedule** when you want to run the job now or to execute the job at a specific time.
– **Immediate**—automatically runs the job after it is created.
– **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
– **Run Once Only**—specify the date and time to run the job.
– **Periodic**—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
– **Daily**—runs the job every day at the specified time.
– **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

See also [Job Scheduling Options](#).

**Event**

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

– **Device added to Management Center**
– **Device added to Group**
– **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See the following note.

**NOTE**

If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. **Name:**

– Verify or change the name and add an optional description.

### Add Job That Includes Multiple Operations (Multistep Device)

The Multistep Device Job ([Jobs > Scheduled Jobs > New Job > Multistep Device Job](#)) enables you to create a job that runs one or more operations on each target device. This is in contrast to the **Multistep Job**, which is a job that contains other discrete jobs.

**TIP**

Use the Multistep Device Job when you want to run operations on multiple devices of the same type. Though a Multistep Device Job can have disparate device targets, all of the operations in the job must be supported by those device types.

Using the Multistep Device Job, you can specify the behavior to occur if a job operation encounters errors. If an operation fails, you have the option to force the job to continue on that device or specify a global recovery action.

**Behavior**

All operations are run in sequence on each target device. All of the selected operations must be able to be performed on the target device type. For example, if one of the job operations is to collect **Sysinfo**, you cannot add a Content Analysis (CA) device target because **Sysinfo** is supported only for ProxySG devices. The system filters out devices that do not support one or more operations in the job. Therefore, if you have mixed device targets, ensure you only add operations that are supported by those devices.

If an operation is marked **Continue on Error**, the job will continue to run even if that operation fails. If you specify a **Recovery** action, that action will be invoked when any operation in the job fails unless the operation is marked **Continue on Error**.

**Add Multistep Device Job**

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Multistep Device Job**.
3. **Operations:**
– Click **Select Operation** to add a job operation. Click **Add another operation** to add additional job operations.
– See **Add a Job** for additional information about each option.
– Use **Remove, Move Up**, and **Move Down** to edit the available jobs and their execution order.
– For each operation, decide whether to continue on error. Click the gear icon and select **Continue on Error**.
– If you add an **Install Policy** job, specify whether to always install the latest version or a specific version.

**TIP**
If you’ve added a lot of operations, save the job and then edit it. When you bring up the editor, all operations will be collapsed, allowing you to view them more easily.

4. **Recovery:**
– Optional—Specify one or more actions to take if one of the operations fails. For example, you can choose to collect Sysinfo for a ProxySG appliance if an operation fails.
  
  This is a global setting that is used when an operation fails on any of the targets. However, the **Recovery** action will not occur if an operation is marked **Continue on Error**.

5. **Targets:**
– Select the **Devices** or **Groups** tab.
– Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
– Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
– If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
– All selected targets appear in **Selected Targets**.

6. **Job Results:**
– (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

7. **Schedule:**
Choose to trigger job execution using a **Schedule** or an **Event**.

**Schedule**
Use **Schedule** when you want to run the job now or to execute the job at a specific time.
– **Immediate**—automatically runs the job after it is created.
– **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
– **Run Once Only**—specify the date and time to run the job.
– **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
– **Daily**—runs the job every day at the specified time.
– **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

See also **Job Scheduling Options**.

**Event**
Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
– **Device added to Management Center**
– **Device added to Group**
– **Device removed from Group**

If you select more than one event type, the job runs if **any** of the conditions are met and the device is an appropriate target. See the following note.

**NOTE**
If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

8. **Name:**
– Verify or change the name and add an optional description.
9. Click **Save**.

**Example**

John Smith’s company has several devices, including ProxySG, Content Analysis (CA), and Malware Analysis (MA) appliances. He creates a Multistep Device Job that includes the following operations:

- Backup
- Install Policy
- Collect Sysinfo
- Restart

John wants the operations to continue even if the backup fails, so he clicks the gear icon in the Backup operation and selects **Continue on Error**.

He has also selected **Monitor/Unmonitor** for the **Recovery** operation, and has configured that option to deactivate the target device if an operation fails.

John continues the job configuration and notices that the **Targets** list does not display his CA and MA appliances. This is because those devices do not support the **Sysinfo** operation.

John completes the job configuration and saves and runs the job. As the job executes, John watches the status of each operations as it runs. The backup operation fails but the job continues to run because he had marked that operation **Continue on Error**. The rest of the operations run successfully. Even though the backup operation failed, the **Recovery** action was never invoked because the Backup operation was marked **Continue on Error**. He remembers that the **Recovery** action only occurs for operations that fail and that are not marked **Continue on Error**.

**Job Scheduling Options**

Define a schedule for each job that you create or edit from the **Schedule** dialog in the Job wizard.

Verify that the time zone is configured for the region in which the job will occur. See Synchronize the System Clock using NTP.

Consider the following scheduling options.

**Immediate**

If you select **Immediate**, the job runs immediately after you finish creating or editing the job. To have the job listed on the **Scheduled jobs** page, select **Save this job in Scheduled Jobs**.

The job displays in **Job History** and **Scheduled Jobs** (if you selected the check box).

**No Schedule**

To run a on-demand job or to define the schedule later, select **No Schedule**.

Although the job does not have a schedule, it still displays in the **Scheduled Jobs** section. When you are ready to run the job, initiate the job manually by selecting **Run Now**. Management Center displays the **Are you sure you want to run the selected job now?** message. Click **Yes**. The **Job History** page displays the completed job.

**Run Once Only**

Certain jobs only need to be run once (for example, when you install policy to a device).

Select **Run Once Only** and then specify the date and time to run the job:

- In the **Run at** field enter the time (using a 24-hour clock) you want to run the job, or use the arrows to adjust the time.
- Click the calendar icon

and select the day.
The job is listed in the Scheduled Jobs section until it runs at the scheduled time.

Periodic
You can schedule a job to run periodically, such as every two weeks or every three days. To specify a periodic schedule, you indicate the frequency the job should run and when you want the first job to run:

- Run every (number) of (minutes, hours, or days)
- Starting at (time) on (a specific date). Enter the time using a 24-hour clock.

The job will be listed in the Scheduled Jobs section.

Daily
You can schedule a job to run every day at a certain time. Specify the time using a 24-hour clock:

- Run at (hh) : (mm)

The job will be listed in the Scheduled Jobs section.

Monthly
You can schedule a job to run monthly. To specify a monthly schedule, you indicate which day of the month to run the job as well as the time of day:

- Run on the (first, second, third, fourth, fifth) (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) of the month.
- Run on day (1-31) of the month.
- Run on the last day of the month.
- Run at (hh):(mm) Enter the time using a 24-hour clock.

The scheduled job will display in the Scheduled Jobs section.

TIP
It is important to remember that if the job that you are scheduling is big (meaning it will take a lot of time and resources), it is recommended you schedule the job to run during off-hours or on weekends.

Change Device Health and Statistics Monitoring State

Devices can be activated or deactivated. Management Center actively monitors the health status of activated devices. Deactivated devices are not monitored.

Whether you choose to activate or deactivate a device depends on your business requirements. For example, you might have already set up a pre-deployed device that is now ready to be activated. Or, you want to deactivate a device that must be taken offline for maintenance.
This job configures devices with a URL to send required configuration and upload statistics to Management Center. The hostname and IP address in this URL is determined by Management Center based on available configuration in the order below:

1. The hostname/IP address defined in Administration > Settings > Device Communication.
2. The virtual IP address configured using the virtual-ip CLI command.
3. The configured IP address on the first available appliance interface.

If you change any of the preceding configurations, you must restart both the management-center and statics-monitoring services (see system-services restart). After the services have been restarted, this job will use the correct hostname and IP address when configuring the URL on a device for statistics export.

**CAUTION**
Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. See Statistics Monitoring Over HTTPS for more information.

**TIP**
This topic describes how to create a job to change the device monitoring state. You can also change the device monitoring state on individual devices. See Enable Device Health and Statistics Monitoring.

**Change Device Monitoring Status**

**TIP**
Deactivating a device is NOT the same as deleting a device. See Stop Managing a Device.

1. Select Jobs > Add > New Job.
2. On the Add New Job page, select Change Monitoring State.
3. **Configuration**:
   - **Change Health Monitoring state**: Select to activate or deactivate health monitoring. If you try to activate the device when the connection parameters are not specified, you receive an error. To specify connections parameters, see Edit a Device.
   - **NOTE**
     Deactivating a device disables all statistics monitoring.
   - **Change Statistics Monitoring state**: Select to change device data collection. You can disable statistics monitoring without deactivating the device. However, Management Center can only collect statistics from activated devices.
     - **NOTE**
       The device status can take up to 30 seconds to change.
4. **Targets**:
   - Select the Devices or Groups tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   - All selected targets appear in Selected Targets.
5. **Job Results**:
   - (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).
6. **Schedule**:
   - Choose to trigger job execution using a Schedule or an Event.

   **Schedule**
   Use Schedule when you want to run the job now or to execute the job at a specific time.
Immediate—automatically runs the job after it is created.

No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.

Run Once Only—specify the date and time to run the job.

Periodic—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.

Daily—runs the job every day at the specified time.

Monthly—runs the job once a month on the specified day of the month and specified time of day.

See also Job Scheduling Options.

Event

Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- Device added to Management Center
- Device added to Group
- Device removed from Group

If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

**NOTE**

If a device cannot be a target for a job (for example, a Content Analysis device in a Collect Sysinfo job), it is ignored.

7. Name:
   - Verify or change the name and add an optional description.

8. Click Save.

Collect Sysinfo

The Collect Sysinfo job extracts the Sysinfo data from the selected ProxySG appliances and outputs it to a file. If the job executes successfully, the files are saved to Jobs > Archived Files as a zip file.

**TIP**

This job requires that Email Results or Generate Archive is selected to save the result.

1. Select Jobs > Scheduled Jobs > New Job and click Collect Sysinfo.

2. Targets:
   - Select the Devices or Groups tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   - All selected targets appear in Selected Targets.

3. Job Results:
   - Click Email results and select the condition. Then, enter the email(s) of the recipient(s).

4. Schedule:
   - Choose to trigger job execution using a Schedule or an Event.

Schedule

Use Schedule when you want to run the job now or to execute the job at a specific time.
– **Immediate**—automatically runs the job after it is created.
– **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
– **Run Once Only**—specify the date and time to run the job.
– **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
– **Daily**—runs the job every day at the specified time.
– **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

See also [Job Scheduling Options](#).

**Event**

Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

– **Device added to Management Center**
– **Device added to Group**
– **Device removed from Group**

If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

**NOTE**

If a device cannot be a target for a job (for example, a Content Analysis device in a Collect Sysinfo job), it is ignored.

5. **Name:**
   – Verify or change the name and add an optional description.

6. Click **Save**.

**Restore Device to Factory Defaults**

This job executes a partial reset to factory defaults; the network settings are not lost and the connection to the device CLI is preserved. This job is supported only on the following devices:

- ProxySG appliance
- Advanced Secure Gateway

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Factory Restore Device**.
3. **Configuration**:
   – Select this option to wait for the device to restart before reporting job success.
4. **Targets**:
   – Select the **Devices** or **Groups** tab.
   – Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   – Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   – If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   – All selected targets appear in **Selected Targets**.
5. **Job Results**:
   – (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).
6. **Schedule**:

   **NOTE**
  
   Symantec recommends that you only run ad-hoc jobs for this option. Do not schedule a factory restore job or trigger it with an event.

Choose to trigger job execution using a **Schedule** or an **Event**.
Schedule
Use Schedule when you want to run the job now or to execute the job at a specific time.
- Immediate—automatically runs the job after it is created.
- No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
- Run Once Only—specify the date and time to run the job.
- Periodic—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
- Daily—runs the job every day at the specified time.
- Monthly—runs the job once a month on the specified day of the month and specified time of day.
See also Job Scheduling Options.

Event
Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
- Device added to Management Center
- Device added to Group
- Device removed from Group
If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

**NOTE**
If a device cannot be a target for a job (for example, a Content Analysis device in a Collect Sysinfo job), it is ignored.

7. Name:
   - Verify or change the name and add an optional description.
8. Click Save.

Schedule Device Restart
If you need to reboot a managed device, use the following procedure to restart it. You can also restart a device from the Network page (Network > select device > Operations).

**NOTE**
See also, Restart a Device.

1. Select Jobs > Add > New Job.
   - On the Add New Job page, select Restart Device.
2. Configuration:
   - Select this option to wait for the device to restart before reporting job success.
3. Targets:
   - Select the Devices or Groups tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - Targets are filtered based on the operations that are chosen. That is, if an operation does not apply to a device, the system does not display those devices.
   - If you select a device group, when the job runs it filters out any devices that do not support all of the selected operations.
   - All selected targets appear in Selected Targets.
4. Job Results:
   - (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).
5. Schedule:
   - Choose to trigger job execution using a Schedule or an Event.
Schedule
Use **Schedule** when you want to run the job now or to execute the job at a specific time.

- **Immediate**—automatically runs the job after it is created.
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
- **Run Once Only**—specify the date and time to run the job.
- **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
- **Daily**—runs the job every day at the specified time.
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

See also **Job Scheduling Options**.

Event
Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:

- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See the following note.

**NOTE**
If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. **Name:**
   - Verify or change the name and add an optional description.

7. Click **Save**.

Save Device Configurations

The **Jobs > Save Config** job saves the configuration settings of a managed device. You can use the **Save Config** job to create a “golden” configuration to be used for comparison with other devices (**Jobs > Compare Config**). The job results are saved to the archive (**Jobs > Archived Files**).

The resulting configuration is saved in JSON format and should only be used with the **Compare Config** job to identify configuration differences. See **Compare Device Configurations** for more information.

Supported Devices

The **Save Config** job supports the following devices:

- ProxySG appliance
- Advanced Secure Gateway
- Content Analysis
- SSL Visibility 4.x
- Malware Analysis

Save a Device Configuration

1. Select **Jobs > Add > New Job**.

2. On the **Add New Job** page, select **Save Config**.

   **Configuration:**
   - Select the device type.
   - Enter the JSON paths to include or exclude, or select individual configuration sections. Use hard returns to enter multiple JSON paths.
If you are not familiar with the JSON paths available in your device configuration, select all of the sections. Then, run the job and view the saved configuration file to determine if additional filtering is required. JSON paths are entered using standard JSON path expressions. For example, enter $.Policy to specify the Policy node at the root level.

The JSON paths you enter override in the Paths to Include section overwrite any of the selected categories. For example, if you enter $.Auth and have selected Tenants, Policy Slots, and PKI in the Sections to Compare, only the Auth configuration will be saved. All categories are ignored.

If you enter one or more JSON paths in the Paths to Exclude section, the checkboxes in Sections to Compare are used, with the exception of any specified in the Paths to Exclude.

3. **Targets:**
   Select the devices or groups for which you want to save configurations. The selected devices must be running the same system image as the source device.
   - Select the Devices or Groups tab.
   - Add multiple devices or device groups by selecting the check box next to the names of devices or device groups.
   - All selected targets appear in Selected Targets.

4. **Job Results:**
   - (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).

5. **Schedule:**
   Choose to trigger job execution using a Schedule or an Event.
   **Schedule**
   - Use Schedule when you want to run the job now or to execute the job at a specific time.
   - Immediate—automatically runs the job after it is created.
   - No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
   - Run Once Only—specify the date and time to run the job.
   - Periodic—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
   - Daily—runs the job every day at the specified time.
   - Monthly—runs the job once a month on the specified day of the month and specified time of day.
   See also Job Scheduling Options.
   **Event**
   - Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
     - Device added to Management Center
     - Device added to Group
     - Device removed from Group
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.
   
   **NOTE**
   If a device cannot be a target for a job (for example, a Content Analysis device in a Collect Sysinfo job), it is ignored.

6. **Name:**
   - Verify or change the name and add an optional description.

7. Click Save.

The system displays the job progress.
View Job Results

To view the job results:

1. Select **Jobs > Archived Files**.
2. Select the job and click **Download**.
3. Locate the JSON file downloaded by your browser and view it using a text editor.

Schedule Reporter Reports

The reports scheduling feature enables you to create scheduled jobs. Some complex reports may take several hours to execute and you can schedule these reports to run during non-business hours. You can also use these features to email a report to users who cannot log into Management Center. Or you could schedule a monthly report that emails the results to interested stakeholders.

This feature creates a scheduled job whose results can be viewed in the **Jobs > Job History** page. All scheduled job reports are saved to the Management Center file archive for later viewing.

- Schedule reports from any of the following pages:
  - **Reports > Reporter**: Select a job and click **Operations > Schedule**.
  - **Reports > Reporter > ReportName**: Run a report and save it if necessary. Click **Actions > Schedule**.
  - **Jobs > Scheduled Jobs > New Job**: Select **Reporter Report**.

**NOTE**

For additional information about these fields, see Create a Custom Reporter Report.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Reporter Report**.
3. **Configuration**:
   - **Database**: Select the Reporter database to use.
   - **Report period**: Specify the date range.
   - **Format**: Select the format, PDF, HTML, or CSV.
     By default, the reports have a Symantec logo. You can replace that with your logo.
   - **Page Orientation**: For PDF, select the orientation, **Portrait** or **Landscape**. (This is not applicable to HTML or CSV.)
   - **Report Rows**: Select the number of rows you want included in the offline report.
   - **Description**: Enter a meaningful description to help you identify or find this job later.
4. **Reports**:
   - Select the reports to run. For more information about the reports, see Reference: Report Descriptions.
5. **Job Results**:
   - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).
6. **Schedule**:
Choose to trigger job execution using a **Schedule** or an **Event**.

**Schedule**
Use **Schedule** when you want to run the job now or to execute the job at a specific time.
- **Immediate**—automatically runs the job after it is created.
- **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
- **Run Once Only**—specify the date and time to run the job.
- **Periodic**—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
- **Daily**—runs the job every day at the specified time.
- **Monthly**—runs the job once a month on the specified day of the month and specified time of day.

See also **Job Scheduling Options**.

**Event**
Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
- **Device added to Management Center**
- **Device added to Group**
- **Device removed from Group**

If you select more than one event type, the job runs if *any* of the conditions are met and the device is an appropriate target. See the following note.

**NOTE**
If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

7. **Name**:
   - Verify or change the name and add an optional description.

8. Click **Save**.

   **NOTE**
   To run a report in the background for later viewing, see **Run a Report to View Later**. To run a report immediately, see **View a Reporter Report**.

**Schedule Summary Report Job**
Management Center enables you to run a Summary Report that provides value-specific information on various security planning, monitoring, and compliance of corporate KPIs.

Use the Summary Report to drill down into the database to find specific information based on the inventory, health, user activity, license state, data from statistics monitoring, and/or device details necessary.

**NOTE**
This operation is not supported in Multistep Device Jobs. See also **Run a Summary Report**.

1. Select **Jobs > Add > New Job**.
2. On the **Add New Job** page, select **Summary Report**.
3. **Report Details**:
   - **Cover Title**: Provide a title for the Summary Report.
   - **Page Header**: Provide an optional page header for the report.
   - **Report Period**: Specify the time period.

   By default, the reports have a Symantec logo. You can replace that with your logo.

4. **Report Content**:
– Sections: Specify the report segments to include. For more information, see Run a Summary Report.
– Database: Select the database from which to run the report. The database is only required for some sections and is inaccessible for the others.

5. Archived File:
– Change the filename of the archived PDF, if wanted. This is automatically populated by what you enter for the Cover Title.

6. Job Results:
– (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).

7. Schedule:
Choose to trigger job execution using a Schedule or an Event.

   Schedule
Use Schedule when you want to run the job now or to execute the job at a specific time.
– Immediate—automatically runs the job after it is created.
– No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
– Run Once Only—specify the date and time to run the job.
– Periodic—runs the job every x number of minutes, hours, or days, starting at the specified time and date.
– Daily—runs the job every day at the specified time.
– Monthly—runs the job once a month on the specified day of the month and specified time of day.
See also Job Scheduling Options.

   Event
Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
– Device added to Management Center
– Device added to Group
– Device removed from Group
If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.

   NOTE
If a device cannot be a target for a job (for example, a Content Analysis device in a Collect Sysinfo job), it is ignored.

8. Name:
– Verify or change the name and add an optional description.

9. Click Save.

Job Operations

When defining a job, additional fields may display, depending on which operation you select. The list below describes each operation and its associated fields.
*designates a required field

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
</table>
| Backup Devices                | Backs up the configuration of the selected device(s) on a defined schedule; any supported type of device can be backed up. Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored. See also Back Up Device Configurations. | Backup Name *  
Backup Description *  
Include Private Data Encrypt Backup |
<p>| Backup Management Center      | Stores a backup of the Management Center configuration to the specified server on a defined schedule. This operation is not supported in Multistep Device Jobs. See also Back Up Management Center.                               | Export to Server - Select the check box. Server URL* - Supported protocols include scp, ftp/ftps, and http/https. Encryption Phrase * - 1 or more characters, alphanumeric. User name Password |
| Change Monitoring State       | Activate or deactivate devices. Management Center actively monitors the health status of activated devices. Deactivated devices are not monitored. Whether you choose to activate or deactivate a device depends on your business requirements. You can also disable statistics monitoring without deactivating a device. See also Monitor Device Health and Statistics. | Change Health Monitoring state - Select the radio button and Activate Devices or Deactivate Devices. Change Statistics Monitoring state -Select the radio button and Enable Statistics Monitoring collection or Disable Statistics Monitoring collection. |
| Check Consistency             | Checks whether the policy installed on selected devices matches the reference policy. This operation is not supported in Multistep Device Jobs. See also Check Consistency between Policy and Devices.                                                         | Policy * - Click ✏ to select the reference policy to use for comparison. Select policy version * - Select the radio button for either The latest policy version or specify a previous Version. |
| Collect Sysinfo               | Extracts the Sysinfo data from the selected ProxySG appliances and outputs it to a file. If the job executes successfully, the files are saved to Jobs &gt; Archived Files as a zip file.                                             | During job creation, ensure that Email Results or Generate Archive are selected. |
| Execute a Script              | Runs the designated script on the selected target ProxySG appliances on a defined schedule. See also Execute a Script.                                                                                      | Device Script * - Click ✏ to select the script to execute |</p>
<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
</table>
| Export Backups          | Saves backup files of the selected target device(s) to the specified server on a defined schedule. Exporting device backups is necessary to save space and is mandatory if you are upgrading the device to a new image.  
Management Center supports configuration backup/restore/import/export of the following device types: ProxySG, Content Analysis, Malware Analysis, and SSL Visibility. Content Analysis 2.1 SNMP trap settings are not backed up or restored. See also Export Device Backups.  
Management Center supports the following key exchange algorithms for SSH/SCP connections: DHGex, DHG, and Curve25519. If a user attempts to export a backup to a server via SCP and the target server does not support the at least one of those key exchange algorithms, the export may fail with the message A connection could not be established or The secure handshake failed during key exchange. This also applies to other Management Center operations that use SSH/SCP.                                                                 | Export to Server - Select the check box.  
Server URL * - Supported protocols include scp, ftp/ftps, and http/https.  
Encryption Phrase * - 1 or more characters, alphanumeric.  
User name  
Password  
Prune Backups - Select this check box if you want to remove the backup from the backup slot when you export the backup.  
Retention Count * - Enter the number of backups to keep.  
Prune Pinned - Select this check box if you want to prune backups that have been pinned (or saved).                                                                                                                                                                                                                   |
| File Transfer           | Transfers a file to the system. If you have previously downloaded a file, such as a configuration, image, license, text, or other file, and you want it on the new system, this option loads it.                                                                                   | Server URL * - Enter the URL of the file.  
Supported protocols include http/https.  
File Type - Specify the file type.  
If the file already exists - Choose what to do if the file already exists.                                                                                                                                                                                                                                               |
| Import External Policy  | Imports the designated ProxySG policy or policy fragment from a web, FTP, or SCP server and merges it into the selected target policy fragment in Management Center.  
This operation is not supported in Multistep Device Jobs.  
See Import External Policy.                                                                                                                                                                                                                                      | Import from URL * - Supported protocols include scp, ftp/ftps, and http/https. The filename must be the ID assigned to the target policy.  
Username  
Password                                                                                                                                                                                                                                                                                                           |
| Install Policy          | Runs the designated policy on the selected target ProxySG appliances on a defined schedule.  
See Install Policy.                                                                                                                                                                                                                                             | Policies * - Click to select the policies to install.  
Force Installation - Select this check box to override any warnings.                                                                                                                                                                                                                                                                  |
| Install System Image    | Upgrades the selected device to the specified image. The file must be uploaded to Management Center (Configuration > Files) and the device type must be specified.  
See Remove Unused Tenant Policy.                                                                                                                                                                                                                                      | System Image - Select the image to install. The file will only be listed here if it has been uploaded to Management Center (Configuration > Files).                                                                                                                                                                           |
<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Unused Policy</td>
<td>Removes tenant policy when there is no policy assigned to the tenant on the appliance. This operation is not supported in Multistep Device Jobs. See Remove Unused Tenant Policy.</td>
<td>No additional fields.</td>
</tr>
<tr>
<td>SWG-VR Data Collection</td>
<td>Used to capture specific information associated with the Value Reporting service offered by Symantec. This job will capture specific information from your SGs attached to a Reporter instance and return a payload suitable for emailing to your SE for analysis. Consult with your SE for more information on this service. This saves the report as an archived file (Jobs &gt; Archived Files). This operation is not supported in Multistep Device Jobs.</td>
<td>Registered</td>
</tr>
<tr>
<td>Summary Report</td>
<td>Runs a summary report. This saves the report as an archived file (Jobs &gt; Archived Files). This operation is not supported in Multistep Device Jobs. See also Run a Summary Report.</td>
<td>Cover Title * - Add a title for the cover page of the report. Sections - Select the sections you want to add to the report on. Database (<em>) - Select the database from which to run the report. The database is only required for some sections and is inaccessible for the others. Filename (</em>) - Change the filename of the archived PDF, if wanted. This is automatically populated by what you enter for the Cover Title. Description - Add a description of the scheduled report.</td>
</tr>
<tr>
<td>Synchronize Devices</td>
<td>Synchronizes configuration settings from one device (the source) to one or more similar devices running the same or later OS versions. Management Center supports synchronization of the following device types: SSL Visibility, Content Analysis, and Malware Analysis. See also Synchronize Devices.</td>
<td>Source Device * - Select the device whose settings you want to copy to other devices. What to synchronize (*) - Varies by source device.</td>
</tr>
</tbody>
</table>

**Share a Job With Another Management Center Appliance (Export/Import)**

In some cases, you might want to share jobs you have created with another Management Center. You can do this by exporting the job(s) from the source Management Center and importing the job(s) on the target Management Center.

Exported jobs are saved in JSON format to allow another Management Center to import the job(s).

**Important Export/Import Notes**
• Symantec strongly recommends that you sync the Management Center "source" appliance's shared objects, policy and script objects, source devices, and so on, with all other Management Center appliances you are sharing jobs with. This is because job imports can fail if shared objects or source devices do not exist on the target Management Center appliance.

• Job data is exported by reference. The operation does not export full objects, for example, an entire script or policy. The system includes sufficient information to match an object with its counterpart on the target device, if it exists. If the counterpart does not exist, the import might fail. See previous bullet.

• Exported policy and script objects must have a reference ID. If they do not, they will fail to export.

• The jobs listed below may require a passphrase if they include sensitive data. For example, if a SWG-VR job contains a registered Reporter, it will not require a passphrase. But if the job contains an unregistered Reporter, a passphrase is required. The passphrase must be provided upon import so the data can be decrypted and re-encrypted by the target Management Center.
  – SWG-VR
  – Import External Policy
  – Backup Management Center
  – Export Backups

If you forget a passphrase, you will need to export the jobs again.

• Reporter Jobs with Role Permissions—If a report job has a server-database-role selection, you must verify the role name and associated permission. Management Center does not check the role permissions when importing or exporting. It imports/exports the Reporter device information, database name, and role name only.

• Multistep Device Job—If any step fails to export, the entire job will fail to export.

• Multistep Job:
  – If any subjob fails to export, the subjobs will still be exported—even if the Multistep Job fails. This also applies to imported Multistep Jobs.
  – If a Multistep Job is selected without selecting its subjobs for export or import, Management Center still tries to export/import all subjobs in the Multistep Job.

• Execute Script—If any script cannot be found, the Job will fail.

Step 1: Export Management Center Job

Exporting one or more jobs is the first step in sharing the job with another Management Center appliance. When you export the job, the system saves it as a JSON file on your local client. To export one or more Management Center jobs:

1. Review the Important Export/Import Notes.
2. Select Jobs and click Export.
   
   NOTE
   If you select jobs in the Jobs list before clicking Export, those jobs will already be selected in the Export wizard.

3. In the Export Jobs window, select the jobs you want to export. If any job requires a passphrase, you will see a text box to enter the passphrase.
4. Enter the passphrase(s) if required and click Next.
5. Review the Export Results and click Download.
   
   NOTE
   If a job exports with errors, it is not included in the JSON file. Jobs exported with warnings are retained.

Step 2: Import Management Center Job

After you have exported jobs from the source Management Center appliance, you can import them onto a different Management Center appliance.

1. Review the Important Export/Import Notes.
2. Select Jobs and click Import.
3. In the Import Job File window, drag and drop the exported JSON files or click **Browse** to select them.
4. If any of the imported jobs requires a passphrase, enter it and click **Next**.
5. The system runs a simulated import to determine if the jobs can be successfully imported.
6. In the Choose Jobs window, review the results of the **Success** tab.
   If a job with the same name already exists, the system prompts you to update an existing job or to create a new job.
7. Review the results in the **Error** tab, to determine if you can fix the problems.
   The system displays the number of errors. Click the + symbol to expand the error description. Record the errors, and if necessary, exit the Import to fix the problems.
   Errors can be caused for a number of reasons, including an incorrect passphrase. For example, if a job lists source devices that are not present on the Management Center, you will have to add those devices before the import will succeed. If target devices are missing, the import will succeed if there is at least one valid target. See **Important Export/Import Notes** for more information.,
8. After reviewing the errors and making the appropriate changes, ensure that **Import Job** is selected for each job you want to import and click **Next**. The system now imports the selected jobs.
9. Review the results of the import and click **Finish**.

**Reference: How Objects are Referenced**

The following list describes the exported data that is used to look up objects on the target device. It is not a comprehensive list of everything exported.

<table>
<thead>
<tr>
<th>Job</th>
<th>Exported Data</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>• Name (for informational purposes only, not used for lookup)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Serial number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Port</td>
<td></td>
</tr>
<tr>
<td>Device Group</td>
<td>• Hierarchy name</td>
<td>The system matches this against the full path and hierarchy on the target device.</td>
</tr>
<tr>
<td></td>
<td>• Group path from the selected group up to the base group</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>• Name</td>
<td>The policy job is matched against the reference ID, content type, and if applicable, the version. Targets are matched according to their contents. If a target contains both a device and device group, then it will be matched against the device within the device group on the target.</td>
</tr>
<tr>
<td></td>
<td>• Reference ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Content type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Targets (A list of objects containing a device group and/or a device export)</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>• Name (informational purposes only)</td>
<td>The system matches this against the canned ID. Custom reports are not supported at this time.</td>
</tr>
<tr>
<td></td>
<td>• Canned ID</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>• Name (informational purposes only)</td>
<td>The system matches this against the same data (version may or may not apply) on the target device.</td>
</tr>
<tr>
<td></td>
<td>• Reference ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Version</td>
<td></td>
</tr>
</tbody>
</table>
Monitor Jobs

Scheduled Jobs list all the jobs that have been created and are either scheduled to run or have no schedule and must be run manually. Use this screen to see when scheduled jobs will run next, when jobs have last run, how many times each job has run, and who created the job.

1. Select Jobs > Scheduled Jobs.
2. From this list of scheduled jobs, you can select a job and perform any of the following tasks on the job:
   - **Edit**—Change any of the job parameters (basic information, operation parameters, targets, schedule). See Edit a Job.
   - **Delete**—Permanently remove the job from the list of scheduled jobs
   - **Enable**—Re-enable a job that has been disabled
   - **Disable**—Disable the job so that it will not run as scheduled
   - **Run Now**—Initiate the operation of the job; any job can be manually run — unscheduled as well as scheduled

You can also right-click a job and select the task from the menu.

By default, jobs are sorted alphabetically by name. To sort by a different column:

1. Hover the mouse on the column heading you want to sort by, on the right edge of the column.
2. Click the triangle and select Sort Ascending or Sort Descending.

Edit a Job

You can edit any job listed on the Scheduled Jobs page.

1. Select Jobs > Schedule Jobs.
2. Select the name of the job that you want to edit. Click Edit.
3. Make your changes.
4. Click Save.

View Current Jobs

The Current Jobs section displays all currently running jobs. To view jobs that have already occurred, View Job History. To view all scheduled jobs, see Monitor Jobs. To cancel a currently running job, see Cancel a Currently Running Job.

1. Select Jobs > Current Jobs. The top pane displays the following details:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This is the name you gave the job when you created it. See Add a Job.</td>
</tr>
<tr>
<td>Status</td>
<td>This is the current status of the job. The status of a job changes from Running to Complete.</td>
</tr>
<tr>
<td>Progress</td>
<td>This progress bar is constantly updating. You can view in real-time the progress of the current job. The color of the progress bar correlates with the top of the web console banner.</td>
</tr>
<tr>
<td>Start Time</td>
<td>This shows the start time (in a 24-hour clock format) of the current job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The shows the end time (in a 24-hour clock format) of the current job.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Description</td>
<td>This is the description you gave the job when you created it. Although entering a description is optional, the description (and name) help differentiate versions of the similar jobs. For example, a common job is &quot;Backup&quot;, but without a good description it is difficult to see which devices are currently being backed up.</td>
</tr>
</tbody>
</table>

**NOTE**
Each time you start a job manually a Job Progress window displays. If you want to run the script in the background (and get rid of the window) while you do other tasks in Management Center, click **Continue in Background**.

2. If you select a name of a currently running job in the top pane, the details of that job appear in the two bottom panes.

3. The **Job Progress Summary** pane includes filters for the device on which the job is currently running. To cancel a currently running job, click **Cancel**.

If you have too many jobs going to keep track of, you can filter the results by:

- **Complete** = Green
- **Error** = Red (Hover your mouse over all jobs with errors to view the details of the error)
- **Warning** = (Hover your mouse over all jobs with warnings to view the details of the warning)
- **Running** = Grey (Grey signifies inactivity)

For more information on colors and status indicators, see **About Status Indicators**.

**Cancel a Currently Running Job**

To cancel a currently running job, select **Jobs > Current Jobs**.

1. Select the job you want to cancel.
2. Click **Cancel**.

**NOTE**
Some steps of a job that are currently in progress will run to completion instead of being canceled.

3. Ensure that the job running is canceled by checking the **Status** column and the **Job Results** pane. Check for errors, which appear with a red exclamation mark in the Status column:

```
<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>! Error: The operation has failed</td>
</tr>
</tbody>
</table>
```

4. All jobs that you successfully cancel are obvious in the web console. Canceled jobs appear as such in the Status column.

**WARNING**
Some jobs have multiple commands running on multiple devices. The more complex a job is, the more errors may occur when you choose to cancel a running job.

**View and Manage Job History**

View all past jobs and their status. The Job History section is similar to the Current Jobs list, but the Job History displays thousands of results of jobs that have already occurred. The Current Jobs section displays currently running jobs. To view currently running jobs, see **View Current Jobs**. To view all scheduled jobs, see **Monitor Jobs**. You can view more details of a completed job from Job History.

1. Select **Jobs > Job History**.
2. The Job History top pane displays the following details about each completed job:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This is the name you gave the job when you created it. See Add a Job.</td>
</tr>
<tr>
<td>Status</td>
<td>This is the status of the job. More details are available about the job.</td>
</tr>
<tr>
<td>Progress</td>
<td>This progress bar displays completed jobs, with the latest job that was run always on top.</td>
</tr>
<tr>
<td>Start Time</td>
<td>This shows the start time (in a 24-hour clock format) of the selected job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The shows the end time (in a 24-hour clock format) of the selected job.</td>
</tr>
<tr>
<td>Description</td>
<td>This is the description you gave the job when you created it. Although entering a description is optional, the description (and name) help differentiate versions of the similar jobs. For example, a common job is &quot;Backup&quot;, but without a good description it is difficult to the different backups that occurred.</td>
</tr>
</tbody>
</table>

3. If you select a name of a job in the top pane, the details of that job appear in the two bottom panes. The job Name and the Job Results are detailed in the bottom panes. You can copy and paste the text in these panes. The text in the Status field is especially useful for debugging.

WARNING
Management Center can be down while a job is running. The jobs that run while Management Center is down never appear in Current Jobs but they will appear in Job History when Management Center is back up and running.

4. To delete any jobs from the history, select the job(s) from the main list and click Delete.

View and Filter Job Progress

The Job Progress Summary pane includes filters for the device on which the jobs have run or are currently running. If you need to filter the Job History results, you can filter the results by:

- **Job Name:** Any part of the name of the job(s), such as searching for any job that includes "Backup" in the title.
- **Description:** Any keywords that may be in the description of the job(s).
- **Owner:** The current owner of the job(s).
- **Started by:** The user who first initiated the job(s).
- **Job Status:** The specific status of available jobs. The available statuses include:
  - Canceled
  - Complete
  - Failed to start
  - Interrupted
  - Missed Execution
  - Prepared Running
Each status also includes a colored icon, indicating the progress through the task.
• **Complete** = Green (Green indicates that the job is running or has already run successfully)
• **Error** = Red (Red signifies that the job did not run because of an error. Select the job name to drill down for the details)
• **Warning** = Yellow (Yellow signifies the job ran, but issues occurred. Select the job name to drill down for the details)
• **Running** = Green or Grey (Grey signifies inactivity)

**Step Status:** The specific status of step(s) within multistep jobs. Step statuses include:
- Canceled
- Complete
- Continue Error
- Error
- Pending
- Running
- Skipped

**Date:** The start and/or end date for the range desired.

**TIP**
When the Job Progress window displays a currently running job that is taking a long time, you have the option to **Continue in Background**.

For more details on the use of color and status indicators, see [About Status Indicators](#).

**NOTE**
You cannot delete a job from Job History, you can only **Cancel a Currently Running Job**.

### Organize Jobs with Folders
To make it easier to find your policy, you can logically organize your jobs using folders.

1. Go to **Jobs > Jobs**.
2. Click **Add > Add Folder**.

   ![Add Folder](image)

   **NOTE**
   This system does not display the **Add Folder** option unless the **Folders** option is enabled.

3. Provide a name and optional description and click **Save**.
   The system displays the folder in the left pane. If you don't see the folder list, toggle the **Folders** option.

### Policy Objects

4. Drag and drop the job(s) you'd like to move to the folder.
5. Optional—If you want to make the folder a sub-folder of another folder, drag and drop it to any folder (except itself).
View Archived Files

The Jobs > Archived Files page contains files created from various sources, for example, job results or running a Reporter report to archive. You can download or delete files from this page.
Management Center allows you to consolidate data from all, or a group of, ProxySG appliances you have added as managed network devices. Management Center offers Statistics Monitoring and Reporter reports.

Statistics Monitoring Reports
Statistics Monitoring reports consolidate statistics from your managed ProxySG devices. There are two categories of Statistics Monitoring reports:

- Devices: a variety of reports about the network traffic seen by a single ProxySG device, ProxySG appliances in a device group, or all ProxySG devices
- WAN Optimization: reports for ProxySG appliances with a Proxy or MACH5 Edition license.

View Statistics Monitoring Reports
For descriptions of each report, refer to Reference: Statistics Monitoring Reports in Management Center.

Reporter Reports
If you have integrated Symantec Reporter into Management Center, additional sets of reports are available to you. Reporter reports are grouped into the following categories:

- Security: reports that reveal activity on the network that may pose security or liability concerns.
- Web Applications: reports that provide insight into the web applications being accessed on your network, as well as the riskiness of these applications.
- User Behavior: reports that give you insight into the websites and categories of web traffic users are viewing or are blocked from viewing, and the amount of web traffic for different time periods.
- Bandwidth Usage: reports that analyze hourly, daily, and monthly bandwidth usage on the network, and estimate the time and data cost of that usage.

Integrate Reporter into Management Center
For descriptions of each of these reports, see Reference: Reporter Report Descriptions.

View Consolidated Reports
When using Management Center to manage and monitor ProxySG devices, you can produce reports that consolidate the data from all these devices or a group of devices, allowing you to get a complete picture of activity on your network. For example, you can view the bandwidth savings for all MACH5 appliances or get a list of the top web applications seen on the networks your ProxySG appliances are connected to.

Device Reports
To view reports about the network traffic seen by a group of ProxySG devices, or by all ProxySG devices managed in Management Center:

1. (Optional) Create device groups for the ProxySG devices you want to report on. See Add a Device Group.
2. Decide which Devices report to view (such as Traffic Mix or Traffic Statistics). For descriptions of each report, see Devices Reports.
3. Select Reports > Statistics Monitoring and choose the report from the Devices panel. By default, the report displays data from all ProxySG devices managed in Management Center.
4. (Optional) To narrow down the consolidated report to a group of devices:
   a. Click Device Filter: All Devices or click the Options button. The Filters dialog displays.
b. From the Filter drop-down, select Device Group.
c. Click and select the device group.
d. Click Save.

WAN Optimization Reports

To display consolidated reports for ProxySG appliances with Proxy or MACH5 Edition licenses:

1. (Optional) Create device groups for the ProxySG devices you want to report on. See Add a Device Group.
2. Decide which WAN Optimization report to view. For descriptions of each report, see WAN Optimization Reports.
3. Select Reports > Statistics Monitoring and choose the report from the WAN Optimization panel. By default, the report displays data from all ProxySG devices with a Proxy or MACH5 Edition license that are being managed in Management Center.
4. (Optional) To narrow down the consolidated report to a group of devices:
   a. Click Device Filter: All Devices or Options. The Filters dialog displays.
   b. From the Filter drop-down, select Device Group.
   c. Click and select the device group.
   d. Click Save.

Reporter Reports

If you have integrated Symantec Reporter into Management Center, the following additional categories of reports are available: Security, Web Applications, User Behavior, Log Detail, and Bandwidth Usage. The Reporter reports consolidate data from all ProxySG appliances in the selected Reporter database.

1. Make sure you have added Reporter as a managed device in Management Center. See Integrate Reporter into .
2. Select Reports > Reporter > Database and select the database from which you want to produce a consolidated report.
3. Decide which Reporter report to view. For descriptions of each report, see Reference: Reporter Report Descriptions.

Integrate Reporter into Management Center

Prerequisites

- Configure your Reporter Enterprise Server to receive logs from one or more ProxySG appliances. Refer to Upload Access Logs From ProxySG Appliance and Upload Access Logs to the Reporter Server for more information.
- Obtain or verify administrator access to Reporter Enterprise Server 10.1.x or later.
- Verify that Reporter Enterprise Server is deployed inline with ProxySG appliances within your network.
- Ensure that you have access to a Reporter Enterprise Server (username and password).
- To be able to view Reporter reports on managed devices, you will need to add a Reporter Enterprise Server from the Network tab.

Procedure

To integrate Reporter so that you can view Reporter reports in the Management Center web console:

1. Verify prerequisites above.
2. Add Reporter as a managed device in Management Center.
View a Reporter Report

Reporter reports can only be viewed if you have already added the Reporter Enterprise Server as a managed device.

You can view one of the built-in reports as described below, or create your own custom reports and groups.

The procedure below documents an example of how to view a Reporter report. This example uses the Security report Trend of Blocked Requests.

1. Select Reports > Reporter.
2. Select a role and the Reporter database from the Database drop-down list at the top of Reports Home. The database you select determines the list of available reports.

   ![Reports Home](image)

   **NOTE**
   If the database you want is not available, see Determine Why A Reporter Database Does Not Display.

   Reporter has the following report categories:
   - Security
   - User Behavior
   - Log Detail
   - Bandwidth Usage
   - Web Applications

3. In this example, select Trend of Blocked Requests in the Security list. A default line graph is displayed with Average Requests and a Normal Request Range. Line graphs show how data for the trend changes over time. Average Requests represent the average number of blocked requests specific to your organization. The Normal Request Range is a calculation that produces a "normal" range of blocked requests specific to your organization.

4. (Optional) Change the date filter to display a different time range on the report. The default time range for this report is 7d (7 days).

   ![Date Filter](image)

   You can also use the arrows
   ![Arrows](image)
   to filter the date and time. When you change the date range, the dates are expanded or contracted along the bottom of the report.

5. (Optional) Most report data is generated in UTC time. To ensure the report you're viewing is relevant to the time zone where the users are located, you can set a time zone by clicking
The Profile dialog appears, with Reporter Time Zone selected. Select your preferred time zone from the drop-down menu and click **Save**.

6. (Optional) From the **Quick Pick** drop-down, select a type of relative date filter, for example, **Before** or **Since**.

7. (Optional) Change the graph type by selecting the button next to **Actions**.

![Graph types](image)

Graph types include:

- **Area** - An area graph displays graphically quantitative data. It is based on the line chart. The area between axis and line are commonly emphasized with colors and textures. Commonly used area graphs compare one area with two or more areas.

- **Bar** - A bar graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted horizontally and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped bar graphs display bars clustered in groups of more than one bar graph.

- **Column** - A column graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted vertically and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped column graphs display bars clustered in groups of more than one column graph.

- **Line** - Line graphs show how data for one data type changes over time.

- **Pie** - A pie graph is a circular statistical graphic, divided into slices to illustrate numerical proportion. In a pie graph, the arc length of each slice (and thus the central angle and area), is proportional to the quantity it represents. The pie chart displays the value name and metric when a user hovers the mouse over a section.

8. The default overlay for the Trend of Blocked Requests report is **Requests**. (Optional) To add or change overlays, select an overlay from the legend on the right of the report. Each overlay is represented by a different color and pattern. For example:

![Overlay options](image)

9. (Optional) Click each data type, (Requests, Page Views, Browse Time, etc.) to have them appear in the open report. To remove data types from the graph, click the appropriate entry again.
10. (Optional) Save the customized report you have open by clicking Actions > Save As. The Save As Dialog appears. You can also share the report with other users.

11. (Optional) Save the current report view in PDF, HTML, or CSV format for offline viewing. Click Actions > Download. The web console displays the Download dialog.

   By default, the reports have a Symantec logo. You can replace that with your logo.
a. Select the format, **PDF**, **HTML**, or **CSV**.

b. For PDF, select the orientation, **Portrait** or **Landscape**. (This is not applicable to HTML or CSV.)

c. Select the number of rows you want included in the offline report. Leave the default value, **Visible**, if you would like the report to contain only the data that appears on screen.

d. Click **Download**. Click **Close** to cancel.

12. (Optional) To view a report that is currently open, select that report from the menu on the left of the page. When multiple databases are available, open reports are separated by database.

13. (Optional) In addition to a graph, each report includes a table that displays the data used in the graph. You can drill down into this data to display additional reports. For example, if a **Category** report is displayed, you can click one of the categories in the data grid and drill down to find out what sites are being viewed and who is viewing them. There are three ways to drill down in a report:

   a. Highlight the entry in the table and click the arrow in the **Explore** column.
b. Click the text in the data field that you want to drill down into. The **Overview** report for that element, (URL, Category, User, etc.) displays.

c. Right-click any field in the table at the bottom of a report to display a list of fields. The menu will display fields common to the type of report you are viewing. In the below example, a Category report offers Site as the most common option, to display the sites listed in the selected category. Select your preferred field from the More Fields menu item to view drilled-down reports for other data fields.
14. (Optional) Generate an **Overview** report of items in the data grid. To see more information about an item in the report, click the hyperlink to launch an **Overview** report for that item. For example, if you click the hyperlink for CNN, the Overview report will show a daily trend of traffic to CNN, the top users and Client IPs accessing CNN, and a breakdown of the protocols used to access CNN.
15. (Optional) Filter or change the report criteria.

Create Geovisual Reporter Reports

The Color Map, Bubble Map, and Pie Map reports (Reports > Reporter > New Report) provide a geographically-based view of report data. Currently, you can create these reports only by grouping by Destination Country. Hover the cursor over the colored map areas to view relevant information.

NOTE
To view these reports, you must select a database that contains access logs generated by a ProxySG with an Advanced Web Security license.

Color Map

Bubble Map

Geo Pie Map

Create GeoVisual Maps

1. Select Reports > Reporter.
2. Select a Reporter database. To view these reports, you must select a database that contains access logs generated by a ProxySG with an Advanced Web Security license.
4. In Grouping Level, select One Level for Color or Bubble maps. Select Two Level for Geo Pie maps.
5. In Group By, select Destination Country. For two-level reports, Destination Country must be specified for the 1st level.
6. Select the chart type.

   For two-level reports, the system displays the following:

7. Select the desired time frame, columns, and filters. See Create a Custom Reporter Report for more information.
8. Click Run Report.
Run a Summary Report

Management Center enables you to run a Summary Report (Reports > Reporter > New Report > Summary Report) that provides value-specific information on various security planning, monitoring, and compliance of corporate KPIs.

Use the Summary Report feature to drill down into the database to find specific information based on the inventory, health, user activity, license state, data from statistics monitoring, and/or device details necessary.

1. Select **Summary Report** from the **New Report** menu.

2. Add and select the information and sections for the report.

<table>
<thead>
<tr>
<th>Report Content</th>
<th>Notes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Activity</td>
<td>Requires Reporter 10.x appliance</td>
<td>Provides a summary of Network Activity Metrics, Network Traffic Top 5s, and Traffic Trend.</td>
</tr>
<tr>
<td>Device Inventory</td>
<td>Requires Management Center only</td>
<td>Provides a summary of health status, device types, license state and expiry, and ProxySG appliance license components.</td>
</tr>
<tr>
<td>User accounts</td>
<td>Requires Management Center only</td>
<td>Provides a summary of Management Center user accounts and their roles and permissions. For more information, see View All Users and Associated Roles and Permissions.</td>
</tr>
<tr>
<td>Device Performance</td>
<td>Requires statistics monitoring service</td>
<td>Provides a summary of Services, Trend of Services, CPU, and Memory.</td>
</tr>
<tr>
<td>WAN optimization</td>
<td>Requires statistics monitoring service</td>
<td>Provides a summary of Bandwidth Savings and Effective Bandwidth.</td>
</tr>
<tr>
<td>Certificate Status</td>
<td></td>
<td>Lists certificate status based on the expiration (expired, 30 days, 60 days).</td>
</tr>
<tr>
<td>Certificate Inventory</td>
<td>Requires Management Center only</td>
<td>Full list of all certificates and the devices they are associated with. This is helpful to use as a complete inventory of PKI.</td>
</tr>
</tbody>
</table>

**NOTE**
The database is required (and available) only for reports that include specific section(s).
3. Click Run Report. When the job is finished, the system provides a link to the report in PDF format. By default, the reports have a Symantec logo. You can replace that with your logo.

4. Click Download to save the file locally.

You can also access the PDF report by going to the archive in Configuration > Jobs > Archived Files.

**TIP**

Alternately, you can click Create Job... to run the report as a job.

Management Center saves the reports under the Jobs tab, on the Archived Files page. The total amount of space allocated to the archive is 10% of the available disk space.

Use the filters to sort through the archived reports. You can sort by:

- Filename
- Extension (example: PDF)
- Created By
- Source

**View Reporter Report Details**

In addition to a graph, each report includes a table that displays the data used in the graph. You can drill down into this data to display additional reports. For example, if a Category report is displayed, you can click one of the categories in the data grid and drill down to find out what sites are being viewed and who is viewing them. There are three ways to drill down in a report:

- Highlight the entry in the table and click the arrow in the Explore column.
- Click the text in the data field that you want to drill down into. The Overview report for that element, (URL, Category, User, etc.) displays. For example, if you click the hyperlink for CNN, the Overview report will show a daily trend of traffic to CNN, the top users and Client IPs accessing CNN, and a breakdown of the protocols used to access CNN.
- Right-click any field in the table at the bottom of a report to display a list of fields. The menu will display fields common to the type of report you are viewing. In the below example, a Category report offers Site as the most common option, to display the sites listed in the selected category. Select your preferred field from the More Fields menu item to view drilled-down reports for other data fields.
Schedule SWG-VR Data Collection

The SWG-VR data collection is used to capture specific information associated with the Value Reporting service offered by Symantec. This job captures specific information from the ProxySG appliances attached to a Reporter instance and returns a payload suitable for emailing to your SE for analysis. Consult with your SE for more information on this service. This job saves the report as an archived file (Jobs > Archived Files).

NOTE
This operation is not supported in Multistep Device Jobs.

1. Select Jobs > Add > New Job.
2. On the Add New Job page, select SWG-VR Data Collection.
3. **Reporter:**
   – Specify the Reporter to collect the data from. Select **Registered** if the device is managed by Management Center or **Unregistered Reporter** to specify the connection details for another Reporter instance.
   
   **NOTE**
   Use **Not Registered** if using Reporter 9.x or higher. Manually enter the credentials to connect.

4. **Job Results:**
   – (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. **Schedule:**
   Choose to trigger job execution using a **Schedule** or an **Event**.

   **Schedule**
   Use **Schedule** when you want to run the job now or to execute the job at a specific time.
   – **Immediate**—automatically runs the job after it is created.
   – **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
   – **Run Once Only**—specify the date and time to run the job.
   – **Periodic**—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
   – **Daily**—runs the job every day at the specified time.
   – **Monthly**—runs the job once a month on the specified day of the month and specified time of day.
   
   See also **Job Scheduling Options**.

   **Event**
   Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   – **Device added to Management Center**
   – **Device added to Group**
   – **Device removed from Group**
   
   If you select more than one event type, the job runs if **any** of the conditions are met and the device is an appropriate target. See the following note.

   **NOTE**
   If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.

6. **Name:**
   – Verify or change the name and add an optional description.

7. **Click** **Save**.

**Run a Reporter Report in the Background (Or to Archive)**

This topic describes how to create a report that can be run and archived to **Jobs > Archived Files**. You can also choose to run the report in the background. Though this operation does not create a scheduled job object, the results can be viewed in the **Jobs > Job History** page and are saved to **Jobs > Archived Files** for later viewing.

**NOTE**
This operation creates an ad hoc job. You cannot email the results of this type of job. If you want to email results, select **Create Job** in the Schedule Reports: Reports dialog. See **Schedule Reporter Reports**.

1. **Select Reports > Reporter.**
2. **Select a Reporter database to use for the reports.**
3. **Select the check box next to one or more reports and click **Operations > Run.**

4. In the Schedule Reports: Reports dialog, select any other reports to run.
5. In the Schedule Settings dialog, specify any other reports to schedule.
   a. Select the database from which you want to schedule the report.
   b. Select the time span for the report.
   c. Select a report format: PDF, HTML, or CSV.
   d. Select the page orientation.
   e. Select the number of report rows.
   f. Optional: Add a description.

6. Click Run Now. The system runs the report.

7. Click Continue in Background button at the bottom of the Job Progress: Run Report dialog to continue running the report for later viewing. When the report completes, the system provides a notification that includes a link to view the report.

The Job Progress dialog shows the status of the job. If the job is successful, click the Download link next to the report to view it. You can also access the files by navigating to Jobs > Archived Files.

Reference: Report Descriptions

The following report groups are available if you have integrated Reporter 10.1.x or later with Management Center:

   NOTE
   Some reports require Reporter versions later than 10.1.2.x. These requirements are noted in the report description.

   • Security
   • User Behavior
   • Bandwidth Usage
   • Web Applications
   • Log Detail

From the Database drop-down list, select the Reporter database to use in your reports. The information displayed in the report group will differ according to the database selected. For example, WAF database reports contain an Actions report in the Security group. That report is not displayed for other databases.

The following tables briefly describe the default graph in each of the Reporter reports. In addition to a graph, each report has a data grid displaying the statistics used in the graph, you can drill-down into this data for more details. Note that you have many options for customizing reports: displaying just the graph, displaying just the data grid, changing the graph type, specifying a date filter, and selecting/unselecting overlays. See Generate a Reporter Report for details.

   NOTE
   Reporter reports in Management Center are derived from Reporter database log files, and these reports may be different or enhanced from similar reports in Reporter Enterprise Server.

Security
The **Security** reports reveal activity on the network that may pose security or liability concerns. The available reports may differ depending on the selected database type.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentially Infected Clients - Unified</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database. Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing results from the Symantec Content Analysis (CA) appliances and Malware Analysis (MA) appliances that are deployed as part of your SGOS proxy security solution. These reports are called <em>Unified</em> reports. Displays an area, bar, column, or pie chart of the client IP addresses that might be infected by malicious content, as found by sandboxing, file reputation, predictive analysis score, anti-virus, and WebPulse. By default, the report lists each IP address, sorted by the number of risky requests.</td>
</tr>
<tr>
<td>Potential Malware Infected Clients</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a bar chart of the client IP addresses that might be infected by malicious content, as found by sandboxing, file Reputation, anti-virus, WebPulse. By default, the report lists each IP address, sorted by the number of risky requests.</td>
</tr>
<tr>
<td>Malware Detected Names</td>
<td>Displays a bar chart of the names of the malware detected by Content Analysis/ Proxy AV. To view this report, you must add a Reporter appliance running 10.1.3.x or later. <em>Note:</em> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Blocked Users</td>
<td>For each user, this report shows a bar chart of the number of requests that were blocked due to the URL being from one or more of the following categories: Spyware, Suspicious, Phishing, or Malicious. <em>Note:</em> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Blocked Request by User Agent</td>
<td>For each user agent (browser + version), the report shows a bar chart of the number of blocked web requests to URLs from one of the following categories: Spyware, Suspicious, Phishing, or Malicious.</td>
</tr>
<tr>
<td>Threat Sites Blocked</td>
<td>Displays a a bar chart of the websites that had blocked web requests to URLs from any of the following categories: Spyware, Suspicious, Phishing, or Malicious. The sites with the most blocked web requests appear at the top of the report.</td>
</tr>
<tr>
<td>Trend of Risky Requests</td>
<td>Displays a line graph that shows the number of risky web requests (for example, requests to URLs of malware categories) over the specified time period. The graph contains a shaded area that represents the normal requests range, which is a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of risky web requests during the last month.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trend of Risky Users</td>
<td>Displays a line graph that shows the number of users making requests to URLs of risky categories (Spyware, Suspicious, Phishing, or Malicious) over the specified time period. The graph contains a shaded area that represents the normal count range, which is a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of users making risky web requests during the last month. <strong>Note:</strong> User drill-downs are blank if user name data isn't available in the Reporter log file.</td>
</tr>
<tr>
<td>Trend of Blocked Requests</td>
<td>Displays a line graph that shows the number of web requests that were blocked over the specified time period. The requests could be blocked for a variety of reasons, such as due to deny policies on the ProxySG. The graph contains a shaded area that represents the normal requests range, which is a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of risky web requests blocked during the last month.</td>
</tr>
<tr>
<td>Trend of Blocked Users</td>
<td>Displays a line graph that shows the number of users who were blocked over the specified time period. The users could be blocked for a variety of reasons, such as due to deny policies on the ProxySG. The graph contains a shaded area that represents the &quot;normal count range,&quot; a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of users blocked during the last month. <strong>Note:</strong> User drill-downs are blank if user name data isn't available in the Reporter log file.</td>
</tr>
<tr>
<td>Trend of Risky Clients</td>
<td>Displays a line graph that shows the number of client IP addresses that accessed URLs in the following categories: Spyware, Suspicious, Phishing, or Malicious. The graph contains a shaded area that represents the &quot;normal count range,&quot; a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of client IPs that were potentially infected during the last month.</td>
</tr>
<tr>
<td>Threats</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a bar chart that provides details for the number of threats discovered by each detection method (Sandboxing, File Reputation, Anti-virus, WebPulse).</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Threats - Unified</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database. Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing results from the Symantec Content Analysis (CA) appliances and Malware Analysis (MA) appliances that are deployed as part of your SGOS proxy security solution. These reports are called <strong>Unified</strong> reports. Displays an area, bar, column, or pie chart that provides details for the number of threats discovered by each detection method (sandboxing, file reputation, predictive analysis score, anti-virus, WebPulse). If Malware Analysis processing results in a detonation, the Malware Analysis sends that result to the Content Analysis, which notifies the SGOS proxy device. The SGOS proxy device caches the result and blocks subsequent requests that match. However, the log entries for these cache block actions do not contain the sandboxing vendor or score. Because of this, you might not see the Malware Analysis benefits reflected in the reports. For example, the SGOS proxy device might block 20 requests that match a cached result; the Malware Analysis is credited with only one result (the one that resulted in the cache entry). However, when the SGOS proxy device receives a clear cache action (for example, when new AV patterns are loaded), the Malware Analysis action re-occurs on the next request.</td>
</tr>
<tr>
<td>Trend of Threats</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a column chart that shows the trend over time for each detection method (Sandboxing, File Reputation, Anti-virus, WebPulse).</td>
</tr>
<tr>
<td>Trend of Threats - Unified</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database. Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing results from the Symantec Content Analysis (CA) appliances and Malware Analysis (MA) appliances that are deployed as part of your SGOS proxy security solution. These reports are called <strong>Unified</strong> reports. Displays an area, bar, column, or pie chart that shows the trend over time for each detection method (sandboxing, file reputation, predictive analysis score, anti-virus, WebPulse).</td>
</tr>
<tr>
<td>Threats - WAF</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of threats by category (attack family or anti-virus). Each colored section represents a threat type and corresponding number of incidents.</td>
</tr>
<tr>
<td>Trend of Threats - WAF</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for anti-virus and attack family threats.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Actions</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows action-related data. This data includes requests, page views, browse time, cost (time), cost (bytes), total bytes, bytes sent, bytes received, cache bytes, server bytes, bytes saved.</td>
</tr>
<tr>
<td>Methods</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows data per HTTP method. These actions include requests, page views, browse time, cost (time), cost (bytes), total bytes, bytes sent, bytes received, cache bytes, server bytes, bytes saved.</td>
</tr>
<tr>
<td>Attack Families</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of requests per attack type (for example, SQL injection). The data corresponds to that recorded for the x-bluecoat-waf-attack-family log field. Each slice represents an attack type. The chart displays only the top ten attack types.</td>
</tr>
<tr>
<td>Attack Families Per Country</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the total number of attacks per country. The bar is segmented; each color represents a different attack type. The chart displays only the top ten countries. The data is based on geolocation data and is only shown when either x-bluecoat-waf-attack-family or x-virus-id does not include &quot;-&quot;.</td>
</tr>
<tr>
<td>Sandboxing Risk Score</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</td>
</tr>
<tr>
<td>Trend of Sandboxing</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for each risk score.</td>
</tr>
<tr>
<td>Trend of Predictive Analysis</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for each predictive analysis score.</td>
</tr>
<tr>
<td>Trend of File Reputation</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for each file reputation score.</td>
</tr>
<tr>
<td>File Risk Score</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</td>
</tr>
<tr>
<td>File Risk Score</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.</td>
</tr>
</tbody>
</table>
**Report** | **Description of Default Graph**
---|---
## URL Threat
To view this report, you must add a Reporter appliance running 10.1.5.4 or later. Displays a pie chart that shows the risk threat level (a rating between 1 and 10) of URLs. Malicious sites rank higher (for example, a 9 or 10) while a site that may be questionable, yet not malicious, may rank lower (for example, a 4 or 5). You can use the report to filter out specific risk levels. You can also see the users who visit the higher risk sites more frequently.

## Risky Sites per Country
To view this report, you must add a Reporter appliance running 10.1.5.4 or later. Displays which sites in countries are getting the most risky traffic (a web threat level of 7 or greater). This provides the ability to drill down to more specific information, such as which sites are being viewed by country.

## Risky Clients per Country
To view this report, you must add a Reporter appliance running 10.1.5.4 or later. Displays which clients are visiting the riskiest sites (a web threat level of 7 or greater). The report gives the ability to view specific client risk information, such as which clients are requesting the riskiest sites, and even the clients they are speaking to.

## Attack Families by Site
To view this report, you must add a WAF database from a Reporter appliance running 10.1.5.4 or later. Two-level report that displays each protected web site and the corresponding number of requests per attack type. The data corresponds to that recorded for the x-bluecoat-waf-attack-family log field. Each slice represents an attack type. The chart displays only the top ten attack types.

## Allowed - No WAF Detection
To view this report, you must add a WAF database from a Reporter appliance running 10.1.5.4 or later. Can be used to on a non-production system to test WAF policy. After you set up your WAF policy, you can send malicious traffic through your test device to see if the policy is working; this report list the requests that were allowed to pass without being detected.

### User Behavior
The User Behavior reports give you insight into the websites and categories of web traffic users are viewing or are blocked from viewing, and the amount of web traffic for different time periods.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked Requests by Site</td>
<td>Displays a bar graph that shows the number of web requests that were blocked on each website. The sites with the most blocked requests appear at the top of the report.</td>
</tr>
<tr>
<td>Blocked Requests by Category</td>
<td>Displays a bar graph that shows the number of web requests that were blocked in each URL category. The categories with the most blocked requests appear at the top of the report.</td>
</tr>
<tr>
<td>Blocked Requests by User</td>
<td>Displays a bar graph that shows the number of web requests that were blocked for each user. The users with the most blocked requests appear at the top of the report. <strong>Note:</strong> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Filtering Verdict Trend by Day</td>
<td>Displays a stacked column graph that shows the number of web requests that triggered specific policy verdicts. By default, all verdicts are selected; you will want to select just the policy verdicts you are interested in (such as connect_method_denied and policy_denied).</td>
</tr>
<tr>
<td>Sites</td>
<td>Displays a bar graph that lists the websites with the most page views. For each website, the graph illustrates the number of page views during the specified time period. The site with the most page views appears at the top of the report.</td>
</tr>
<tr>
<td>Categories</td>
<td>Displays a pie chart that shows the categories with the most page views; all other categories are combined into an Other slice.</td>
</tr>
<tr>
<td>Categories per User</td>
<td>Displays a bar graph that lists the names of the most active users and indicates the most accessed URL categories for the pages they viewed. The graph shows the number of pages viewed in each category for each user.</td>
</tr>
<tr>
<td>Note:</td>
<td>This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Users</td>
<td>A bar graph that shows the users with the most page views during the specified time period. The user with the most page views appears at the top of the report.</td>
</tr>
<tr>
<td>Note:</td>
<td>This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Client IPs</td>
<td>Displays a bar graph that shows the client IP addresses with the most page views during the specified time period. The client IP with the most page views appears at the top of the report.</td>
</tr>
<tr>
<td>User Agent Families</td>
<td>In releases prior to 2.4.1.1, you must add a WAF database from a Reporter appliance running 10.1.3.x or later to view this report. In 2.4.1.1 and later, this report is available for Main and Unified databases if you are using a Reporter 10.1.5.x database.</td>
</tr>
<tr>
<td>Note:</td>
<td>Displays an area, bar, column, or pie chart that shows the top 10 client user agent families (not user agent strings). For example, Firefox.</td>
</tr>
<tr>
<td>Countries</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the top ten countries per number of requests (based on geolocation data).</td>
</tr>
<tr>
<td>Protocols</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of number or requests per protocol. The chart shows only the top 10 protocols.</td>
</tr>
<tr>
<td>Days</td>
<td>Displays an area graph that shows the number of web requests for each day in the selected time period.</td>
</tr>
<tr>
<td>Days of Week</td>
<td>Displays a column graph that shows the number of web requests for each day of the week in the selected time period. For example, the Monday column reflects the total of all requests that were made on Mondays during the time period. This report allows you to see how the trends in web browsing differ by day of the week.</td>
</tr>
</tbody>
</table>
Management Center - 3.0

Description of Default Graph

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours of Day</td>
<td>This column graph totals web requests for each hour of the day. For example, every Web page request that occurred at 9am, 10am, and so on. This allows you to analyze which hours are consistently the heaviest with Web requests. Network administrators might use this data to adjust bandwidth policy.</td>
</tr>
<tr>
<td>Months</td>
<td>This report totals web requests for each month. For example, every web page request that occurred in January, February, and so on. This allows you to drill down each month and analyze trends.</td>
</tr>
<tr>
<td>Trend of Discovered Users</td>
<td>Displays the number of unique users per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
</tbody>
</table>

**Bandwidth Usage**

Use the **Bandwidth Usage** reports to analyze hourly, daily, and monthly bandwidth usage on the network, and to estimate the time and data cost of that usage.

The cost-related reports calculate bandwidth cost based on the **Cost per MB** and **Cost per Hour** settings in Reporter. For example, if **Cost per Hour** is set to $10, the Cost (Time) value is calculated by multiplying the time spent web browsing by $10. Or if **Cost per MB** is set to $4, the Cost (Bytes) value is calculated by multiplying the number of megabytes of traffic by $4.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
</table>
| Cost per User               | The data in this bar graph approximates the cost accrued per user based on total bytes of throughput and time spent web browsing. Reporter lists each user, sorted by the total cost of bandwidth.  
  **Note:** This report are blank if user name data isn’t available in the Reporter log file. |
| Cost per User and Site      | Displays a bar graph that shows the total bandwidth cost for the websites each user visited during the selected time period. The users with the highest bandwidth cost appear at the top of the graph.  
  **Note:** This report are blank if user name data isn’t available in the Reporter log file. |
| Cost per Hour of Day        | Displays a column chart that shows the total cost of time and bandwidth for each hour of the day. For example, total cost at 9am, 10am, and so on. This allows you to analyze which hours have the most traffic and are therefore most expensive. Network administrators might use this data to adjust bandwidth policy. |
| Cost per Day                | Displays an area chart that shows the cost of time and bandwidth each day in the specified time period.                                                                 |
| Cost per Day of Week        | Displays a column graph that shows the total cost of time and bandwidth each day of the week in the selected time period. For example, the Monday column reflects the total cost on Mondays during the time period. This report allows you to see how the cost of web usage differs by day of the week. |
| Cost per Month              | This area graph totals time and bandwidth costs for each month. For example, total costs in January, February, and so on. This allows you to drill down each month and analyze trends.                                      |
### Bandwidth per Hour of Day
This column chart shows the total bytes sent and received for each hour of the day. For example, total bandwidth usage at 9am, 10am, and so on. This allows you to analyze which hours have the most traffic. Network administrators might use this data to adjust bandwidth policy.

### Bandwidth per Day
This area chart shows the total bytes sent and received each day in the specified time period, allowing you to see a trend of bandwidth usage over time.

### Bandwidth per Day of Week
This column graph shows the total bytes sent and received each day of the week in the selected time period. For example, the Monday column reflects the amount of bandwidth used on Mondays during the time period. This report allows you to see how the trends in web usage differ by day of the week.

### Bandwidth per Month
This area chart shows total bandwidth used each month. For example, total bytes in January, February, and so on. This allows you to drill down each month and analyze trends.

### Server IPs
To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of requests per server IP address. You can also select other data, including requests, page views, browse time, cost (time), cost (bytes), total bytes, bytes sent, bytes received, cache bytes, server bytes, and bytes saved.

### Log Detail
The Log Detail reports provide information about the bcreporterwarp_v1 access log fields.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Log Details</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a grid report of the access log fields associated with the selected database. For example, if a WAF database is selected, this report shows data for the bcreporterwarp_v1 access log.</td>
</tr>
<tr>
<td>Blocked Log Details</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a grid report of the access log fields for blocked requests associated with the selected database. For example, if a WAF database is selected, this report shows data for the bcreporterwarp_v1 access log.</td>
</tr>
</tbody>
</table>

### Web Applications
The **Web Application** reports provide insight into the web applications being accessed on your network, as well as the riskiness of these applications.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Applications</td>
<td>A bar graph that shows the number of requests for each web application during the specified time period. The web applications having the most web requests appear at the top of the report. Use this report to see what types of web application traffic are running on your network.</td>
</tr>
<tr>
<td>Web Applications by Users</td>
<td>Displays a pie chart of the top web applications as calculated by the number of users accessing the content over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Web Applications by Client IPs</td>
<td>Displays a pie chart of the top web applications as calculated by the number of unique IP addresses accessing the content over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Blocked Web Applications</td>
<td>Displays a bar graph that shows the number of web requests denied by a policy verdict (that is, blocked) for each web application during the specified time period. The web applications with the most blocked requests appear at the top of the report. Use this report to confirm that policies are being enforced properly.</td>
</tr>
<tr>
<td>Trend of Active Web Applications</td>
<td>Displays the number of unique web applications per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Trend of Web Application Traffic</td>
<td>Displays total bytes sent, bytes received, and the number of requests per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.</td>
</tr>
<tr>
<td>Web Application Groups</td>
<td>An application group contains applications with similar functionality (email, social media, games, and so forth). This report shows the total number of web requests for all applications in each application group during the specified time period. The application groups with the most web requests appear at the top of the report.</td>
</tr>
<tr>
<td>Web Application Operations</td>
<td>Displays a bar graph that shows the number of requests for different web application operations (such as Play Video, Download Files, Upload Media) during the specified time period.</td>
</tr>
<tr>
<td>Users of Risky Applications</td>
<td>Risky applications are those with risk scores greater than 70. (You can change the filter to make the number higher or lower.) Ranked by total bytes received, this report lists users who have accessed web applications that are widely deemed as risky for business network use. <strong>Note:</strong> This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Report</td>
<td>Description of Default Graph</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Web Applications per Risk      | Displays a pie chart that shows the number of requests for web applications at each risk score (1 to 10). For example, the report shows a bar for each risk score with different color segments representing different web applications. The length of each segment corresponds to the number of requests for that application. Tips:  
  • Sort the values in the Web Application column to alter the pie chart to show the corresponding data.  
  • You may want to turn off the Other overlay, if this segment has a significant number of requests. |
<p>| Users Per Risk Score           | Shows the number of users per risk score (1 to 10) over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.                                                                          |
| Risk Distribution              | Displays a pie chart that shows the percentage of requests at each risk level. Each slice represents a risk level.                                                                                                                                                                      |
| Risk Distribution Per User     | Displays a color-coded bar chart that shows the amount of traffic (hits and bytes) for each risk score (1 to 10) per user over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.                                        |
| Trend of Risk Distribution     | Displays a color-coded bar chart representing the amount of traffic (hits and bytes) for each risk score (1 to 10) per day over the selected time period. To view this report, you must add a Reporter appliance running 10.1.2.x or later.                                      |
| Social Media Activity          | Displays a bar graph that shows the number of requests for each operation (such as Post Messages and Upload Media) used in social networking web applications. The operations that have the most activity appear at the top of the report.                                      |
| Social Media Applications      | Displays a bar graph that shows the number of requests for each social networking application (Facebook, Twitter, Pinterest, and so on). The social networking applications with the most requests appear at the top of the report. With this report, you can see how much social media traffic your network has and which applications are most popular. Depending on company policy, you may decide to put controls on social networking after viewing this report. |
| Facebook Users                 | Displays a bar graph that shows the number of Facebook requests by each user. The names of the users with the most Facebook requests appear at the top of the report. This report allows you to see who the most active Facebook users are. Note: This report will be blank if user name data isn’t available in the Reporter log file. |
| Facebook Categories            | Displays a bar chart that shows the amount of traffic attributed to different categories of Facebook traffic (other than social networking). For example, you can see the number of Facebook requests that are for games or messaging.                                                               |
| Mail Activity                  | Displays a bar graph that shows the number of requests for various email operations. For example, you can see the number of requests for Send Email, Download Attachment, and Upload Attachment operations for email web applications.                                               |</p>
<table>
<thead>
<tr>
<th>Report</th>
<th>Description of Default Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Applications</td>
<td>Displays a bar graph that shows the number of requests for web mail applications (Gmail, Yahoo Mail, Hotmail, and so on). The email applications with the most requests appear at the top of the report. This report allows you to determine the most popular web mail applications on your network.</td>
</tr>
<tr>
<td>Top Mail Senders</td>
<td>Displays a bar graph that shows, for each user, the number of requests for Send Email or Send Attachment operations. This report allows you to see which users are the biggest web mail consumers. The IP addresses of the users with the most web mail traffic appear at the top of the report.</td>
</tr>
<tr>
<td>Search Terms</td>
<td>Displays a bar graph that displays top search terms that users enter in browser search engines (Google, Yahoo, Bing, and so forth). You can drill down to find the user(s) who searched for the term and which search engine was used.</td>
</tr>
<tr>
<td>Search Applications</td>
<td>Displays a bar graph that displays the number of requests for each search engine (Search Engines/Portals category).</td>
</tr>
</tbody>
</table>

**How Many Open Reports Can I Have?**

You can open up to 250 reports or 200 obfuscated reports.

**Search for Specific Report Data (Search and Forensic Report)**

Management Center enables you to search for specific report data using a simple search or by executing a forensic report.

**Use Simple Search**

The *Reports > Reporter* page includes a simple search field in the top right-hand corner, as shown below.

1. By default, a search term entered here searches all criteria. If you want to run a search on a specific database, select the menu icon on the search box. This brings up a more detailed search page that has other search options in a drop-down menu.
2. Select a search type from the menu. The available criteria differs, depending on the selected database.
3. Enter a search term and click the magnifying glass (or press Enter).

4. The search results display in a new tab on the left.

5. Click the search result to view detailed data about that item.

Run Forensic Report

Use the Forensic Report feature to drill down into the database to find specific information based on the source, destination, and verdict properties of one or more requests. The Forensic Report option is located directly beneath the Management Center banner in the New Report menu.
1. Select **Forensic Report** from the **New Report** menu. The system opens the Run Forensic Report window.

2. Select (or enter) the search criteria from the available data or enter a transaction ID.

3. Select a time duration.
4. Click Run Report. The system displays the search results in the Full Log Details report.

Details for virus_detected
Verdict is "virus_detected"

<table>
<thead>
<tr>
<th>Date and Time</th>
<th>Client IP</th>
<th>Status</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 22, 2015 8:29:19 PM</td>
<td></td>
<td>200</td>
<td>No U</td>
</tr>
</tbody>
</table>

http://www.eicar.org/download/eicar.com.txt
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Ch

5. Click links in the search result to view detailed data about that item.

**Reporter Graph Types and Views**

Reporter graph types depend on the type of data represented in the report. The available graph types are:

- **Area** - An area graph displays graphically quantitative data. It is based on the line chart. The area between axis and line are commonly emphasized with colors and textures. Commonly used area graphs compare one area with two or more areas.
- **Bar** - A bar graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted horizontally and show comparisons among categories. One axis of the graph shows
the specific categories being compared, and the other axis represents a discrete value. Grouped bar graphs display bars clustered in groups of more than one bar graph.

- **Column** - A column graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted vertically and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped column graphs display bars clustered in groups of more than one column graph.

- **Line** - Line graphs show how data for one data type changes over time.

- **Pie** - A pie graph is a circular statistical graphic, divided into slices to illustrate numerical proportion. In a pie graph, the arc length of each slice (and thus the central angle and area), is proportional to the quantity it represents. The pie chart displays the value name and metric when a user hovers the mouse over a section.

Drill down on specific data within a report by clicking the down arrow in the **Explore** column (or by selecting a line the column portion in the report and right-clicking) and selecting from the available options. Drilling down is most helpful when you know what you are looking for. For example, if you are viewing a **Trend of Risky Users** report, you can drill down on the username or risk categories to find the sites that the user is visiting the most. The following is an example of data that is available when you are drilling down in a report:

### Create a Custom Reporter Report

If you can't find a standard Reporter report that suits your needs, you can design and save a custom report using Management Center's flexible and powerful report designer. When designing your report, you choose one or two metrics to report on, select the type of chart (such as pie or bar), define the report time frame (such as one day or one year), select the columns of data (for example, Page Views and Bytes Sent), and configure one or more filters (such as a particular URL category or a range of risk scores). As you design your report, it dynamically displays in the preview window with sample data so that you can get a good picture of what it will look like.

Once you have finished designing the report, you can save it for future use and run it at any time.

#### Step 1: Create the Report

1. Select **Reports > Reporter**.
2. Select a Reporter database.
4. (Optional) To enlarge the Preview window, hover on the divider line between panes and drag to the left.
5. From the Group By drop-down list, select the main metric that Management Center will use to present the data.
If a Reporter administrator had created custom log fields in Reporter 10.x, these fields will be displayed in the list along with the standard built-in fields.

6. In the **Display** field, specify the number of items to display in the chart.

7. If you want to report on two metrics:
   a. Select **Two Level** for the **Group Type**. An additional row displays so that you can choose a second metric.
   
   ![Group By](image)

   b. In the **Then By** drop-down, select the secondary metric to report on.
   c. Select the number of items to **Display**.

8. As you set options, watch the report build in the Preview window pane.

**Step 2: Select the Chart Type**

Horizontal bar is the default chart type. The following chart types are available:

- **Area** - An area graph displays graphically quantitative data. It is based on the line chart. The area between axis and line are commonly emphasized with colors and textures. Commonly used area graphs compare one area with two or more areas.

- **Bar** - A bar graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted horizontally and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped bar graphs display bars clustered in groups of more than one bar graph.

- **Column** - A column graph presents grouped data with rectangular bars with lengths proportional to the values that they represent. The bars are plotted vertically and show comparisons among categories. One axis of the graph shows the specific categories being compared, and the other axis represents a discrete value. Grouped column graphs display bars clustered in groups of more than one column graph.

- **Line** - Line graphs show how data for one data type changes over time.

- **Pie** - A pie graph is a circular statistical graphic, divided into slices to illustrate numerical proportion. In a pie graph, the arc length of each slice (and thus the central angle and area), is proportional to the quantity it represents. The pie chart displays the value name and metric when a user hovers the mouse over a section.

After you click a chart type, the Preview window pane displays the report with the selected type of chart.
NOTE
If you selected a two-level report in Step 1, be sure to choose bar or column for the chart type. These are the only chart types that represent both levels of data in two-level reports. When a two-level report is selected, the column and bar charts display as stacked columns and stacked bars.

Step 3: Define the Time Frame

Define the reporting period for the report using any of the methods below:

- Choose one of the standard time periods, such as 30d or 1y. The default time period is 24h.
- Use the arrows
  
  to select the date or date range.
- From the Quick Pick drop-down, select a type of relative date filter, for example, Before or Since.
- To specify a custom range of dates, choose Custom from the Quick Pick drop-down, enter the beginning and ending date, and click Apply.

Step 4: Choose Report Columns

A statistical table appears below the chart in the custom report. For example, if User is the metric selected in the Group By field, the table includes statistics for each user.
Warning: this is a report preview for display purposes only, data displayed here will not match the actual report.

Current and previous 23 hours

<table>
<thead>
<tr>
<th>User</th>
<th>Requests</th>
<th>Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>27,529</td>
<td>179.1 MB</td>
</tr>
<tr>
<td>No User</td>
<td>2,726</td>
<td>26.8 MB</td>
</tr>
<tr>
<td>acr0q3e</td>
<td>2,476</td>
<td>21.6 MB</td>
</tr>
<tr>
<td>admin</td>
<td>1,109</td>
<td>19.0 MB</td>
</tr>
<tr>
<td>abs0qwl</td>
<td>669</td>
<td>9.1 MB</td>
</tr>
<tr>
<td>adf03ye</td>
<td>1,999</td>
<td>3.1 MB</td>
</tr>
<tr>
<td>acg0b6w</td>
<td>465</td>
<td>1.7 MB</td>
</tr>
<tr>
<td>acr0o7n</td>
<td>462</td>
<td>1.6 MB</td>
</tr>
<tr>
<td>abr0c5y</td>
<td>499</td>
<td>867.2 KB</td>
</tr>
<tr>
<td><strong>Report Totals:</strong></td>
<td>275,290</td>
<td>1.7 GB</td>
</tr>
</tbody>
</table>
NOTE
The default statistics are Requests and Total Bytes. Note that the Preview window only shows two statistical columns, but the full report when generated will show all selected columns.

Step 5: Add Filters
You can narrow down what is displayed in a report by setting up filters.

Step 6: Save the Custom Report
So that you can run the report in the future, without having to recreate it, you should save it into a report group.

1. In the Save Report section, select Save report for running later.

2. Enter a Name for the report.
3. (Optional) Enter a Description up to 1024 characters. In the description mention the report settings such as the type of chart, the time period, filters used, and so forth.
4. Select the Group to save the report in or share the report with other users. If you haven't created the group yet, you can select the New Group option from the Group drop-down and define the group name at that time.
5. Click Save and Run to save the settings and view the full report.

Edit Custom Reporter Reports
After designing and saving a custom report, you may want to tweak some of the settings.

TIP
For more information about any of these settings, see Create a Custom Report.

Modify Report Settings
1. Select Reports > Reporter.
2. Click the name of the custom report you want to modify; this runs the report.
3. To modify the **Group By** fields and/or **Filters**, click the gear settings icon.

4. To modify the chart type, click the chart icon and select the desired type.

5. The Time Frame can be changed using the time toolbar at the top of the report.

6. To modify the columns:
   - In the report table below the chart, hover the mouse on the right side of a column heading until you see the triangle, then click.
   - Select **Columns**.
c. Select the columns you want to include in the report.
7. To save the custom report modifications, select Actions > Save.

Delete a Custom Report

1. Select Reports > Reporter.
2. Select the check box by each report name you want to delete.

4. Click Delete to confirm.

Additional Information

- To rename a custom report, select the check box next to the report name and issue the Operations > Rename command.
- To copy a built-in or custom report, run the report and issue the Actions > Save As command.

Customize Reporter Report Options

Starting with Management Center 1.6, you can now customize every Reporter report. In some cases, these reports can take significantly take longer to run than the standard reports available on Management Center. You can create your own custom reports and save them by using the Save As button and providing the report with a name. See Create a Custom Report for more information.

In addition to the options in this topic, you can alter what is reported in the following ways:
Change the number of items displayed per page

1. In the Group By section, change the Display value.

2. Change other options as desired.
3. Click Run Report.

Change the grouping of the report (that is, change the focus of the report).

1. In the Group By section, choose the field you want to focus the report on from the Group By drop-down list. This field is the main metric that Management Center uses to present the data.
NOTE
If a Reporter administrator had created custom log fields in Reporter 10.x, these fields will be displayed in the list along with the standard built-in fields.

2. Change other options as desired.
3. Click **Run Report**.

When you change the **Group By** field, a new report is generated and the name of the report is changed to match your selection. The previous report is still available in the left pane.

**Create a two-level report**

1. In the **Group By** section, click **Two Level** for the Summary Type.

2. Select the two values to report. In the following example, the report is grouped by **Day** and then by **Verdict**.
3. Change other options as desired.

Create Custom Report Groups

Reporter-based reports are grouped into five groups: Security, Bandwidth Usage, User Behavior, Log Detail, and Web Applications. These groups are static and cannot be modified. However, you can create your own report groups and save custom reports you create into these new groups.

1. Select Reports > Reporter.

3. Enter a Name for the report group.
4. (Optional) Enter a Description up to 1024 characters.
5. Click Save. The container for the new group displays at the bottom of the Reporter page, underneath the built-in groups. You can now create and save custom reports to this group.
Additional Information

- To modify the name or description of a custom report group, click the gear icon in the group’s title bar.
- To delete a custom report group, click the delete (X) icon in the group’s title bar. Note that you cannot delete a group that contains custom reports; you must delete the reports before you can delete the group.
- To move a custom report from one group to another, select the check box next to the report name and issue the Operations > Move command.

**Set Time Zone for Reporter Reports**

Associate a custom time zone with your user profile. That time zone is then used for all Reporter reports. Each user can set a different time zone without affecting other user’s views.

1. In the web console banner, click and select your username.

   ![Username Selection](image)

   **NOTE**
   
   The username for the standard Admin login is "Management Center."

2. Select the **Reporter Time Zone** tab.

   ![Reporter Time Zone Tab](image)

3. Select the new time zone.

4. Click **Save**.

5. When you open a Reporter report, verify your settings by opening a Reporter report and hovering over the time zone icon.
6. (Optional) Once set, you can change the time zone by clicking the time zone icon.

**Determine Why A Reporter Database Does Not Display**

If you try to run reports and the database you want is not available in the **Database**: drop-down menu (**Reports > Reporter**), click **Status** to display that database’s current status.

1. Click **Reports > Reporter**.
2. Click the **Database**: drop-down. The system displays the available databases.
3. If the database you want is not in the menu or you want to see the current status of the Reporter servers and all associated databases, click **Status**.

4. If a Reporter server is available (and you have permissions to view it), you can click the plus symbol to display the associated database(s).

Use the status information to help you determine why the database is not available.
An organization without an effective monitoring system is susceptible to issues such as unplanned downtime and performance degradation; thus, the ability to monitor network activity is crucial for capacity planning and quick responses to potential problems. By analyzing report data, organizations can plan for scalability and anticipate future requirements.

**CAUTION**
Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. See Statistics Monitoring Over HTTPS for more information.

**CAUTION**
Management Center keeps up to 12 months of per hour data and 7 days of per minute data for all devices that have statistics monitoring enabled. To purge this data from Management Center, see Purge Statistics.

As an administrator, it is critical that you be aware of issues, changes, and trends that could arise in your network. In Management Center, you can report on key metrics such as CPU usage, connection counts, bandwidth gains and losses, and other statistics of managed appliances. Statistics Monitoring reports provide you with visibility into network performance. With reports, you can identify trends such as:

- Usage patterns
- Bandwidth savings
- Peak numbers of concurrent users
- Statistics averaged over weeks and months

To ensure that your data analysis is accurate and timely, identify the metrics that are most important to you and run reports regularly.

You can monitor the health of your devices without generating a report. See Monitor Device Health and Backups.

**Prerequisites**
You can generate reports on ProxySG appliances that:

- Run SGOS 6.3.x and later
- Have a Proxy or MACH5 Edition license (Note: this is a requirement for WAN Optimization reports, not Device reports)
- Have the latest trust package installed
- Have statistics collection enabled in device properties (see Add a Device)

You can still manage ProxySG appliances that do not meet these requirements, but their statistics will be unavailable from Statistics Monitoring.

**View Statistics Monitoring Reports**

To view Statistics Monitoring reports:

1. Select **Reports > Statistics Monitoring**.
2. Select a report from **Device Performance** or **WAN Optimization**. See Reference: Statistics Monitoring Reports in Management Center for descriptions.
3. From a dashboard widget, you can also Display a Full Report.
4. Refine reports to make them more useful:
   - Display data for a specific time period. See Change the Scope of a Report.
   - Add metrics to focus on specific data. See Modify Options for Statistics Monitoring Reports.
5. (Optional) Save the current report view in PDF, HTML, or CSV format for offline viewing. Click Actions > Download. The system displays the Download dialog.
   By default, the reports have a Symantec logo. You can replace that with your logo.

**Save a Custom Statistics Monitoring Report and Assign to a Group**

1. Select **Reports > Statistics Monitoring**.
2. Generate a report by clicking the desired report link.
3. Optional—Modify the report to suit your requirements (date range, etc.).
4. Select Actions > Save As.

5. Name the report and provide an optional description.
6. Assign the report to an existing group or select New Group and follow the prompts.
7. Click Save.

**Move, Rename, or Delete Statistics Monitoring Reports**

You can only move, rename, or delete custom reports. If you select a custom report and a report residing within the Device Performance or WAN Optimization groups, these options will not be available.

2. Select one or more reports and click Operations.
3. Select the desired operation.

**Run Now or Schedule Report Execution**

- Select Reports > Statistics Monitoring.
- Select one or more reports and click Operations.
- Select one or more reports and click Run and Archive Now or Schedule.
- Complete the job settings and run or save the job.

**Troubleshooting Statistics Monitoring Reports**

If the statistics monitoring dashboard shows an incorrect number of devices, see Remove Orphan Device Count in Statistics Monitoring Dashboard.

**Reference: Statistics Monitoring Reports in Management Center**

The following Statistics Monitoring reports are available in Management Center.

**Device Performance Reports**
Device reports show statistics on network traffic seen by a single ProxySG device, ProxySG appliances in a device group, or all ProxySG devices.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Report Format</th>
<th>Field</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Displays the percentage of CPU being used. By default, data shown in this report is an average of CPU usage across all devices.</td>
<td>Line graph</td>
<td>Memory, Users</td>
<td>CPU, Users</td>
</tr>
<tr>
<td>Memory</td>
<td>Displays the percentage of memory being used. By default, data shown in this report is an average of memory usage across all devices.</td>
<td>Line graph</td>
<td>CPU, Users</td>
<td></td>
</tr>
<tr>
<td>Active Sessions</td>
<td>Provides an immediate picture of the client-server sessions and the associated proxies, services, bytes, savings, and other statistics.</td>
<td>Line graph</td>
<td>CPU, Memory</td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td>Displays the total number of bytes or packets sent or received through ProxySG appliance network ports. Select the device for which you want to view interface information; the data renders as a pie chart, where each segment represents one interface.</td>
<td>Circle graph</td>
<td>Bytes Received, Bytes Sent, Packets Received, Packets Sent</td>
<td></td>
</tr>
<tr>
<td>Interfaces Detail</td>
<td>Displays the bytes sent and received and packets sent and received through ProxySG appliance network ports. The information is presented in a grid; you can sort data by column headers or hide some columns to limit the information displayed.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trend of Interfaces</td>
<td>Displays the trend of bytes or packets sent or received through ProxySG appliance network ports over the specified period of time.</td>
<td>Stack graph</td>
<td>Bytes Received, Bytes Sent, Packets Received, Packets Sent</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>Displays a comparison of the traffic through specified ProxySG appliances measured in bytes.</td>
<td>Circle graph</td>
<td>Bypassed Bytes, Server Bytes, Client Bytes</td>
<td></td>
</tr>
</tbody>
</table>
### WAN Optimization Reports

The **WAN Optimization** reports display statistics for ProxySG appliances with a Proxy or MACH5 Edition license.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Report Format</th>
<th>Field</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Savings (bytes)</td>
<td>Displays bandwidth savings in bytes received from monitored devices.</td>
<td>Line graph</td>
<td>CPU, Memory, Users</td>
<td></td>
</tr>
<tr>
<td>Bandwidth Savings (cost)</td>
<td>Displays bandwidth savings expressed in terms of cost.</td>
<td>Line graph</td>
<td>CPU, Memory, Users</td>
<td></td>
</tr>
<tr>
<td>Bandwidth Savings (percent)</td>
<td>Displays bandwidth savings expressed as a percentage.</td>
<td>Line graph</td>
<td>CPU, Memory, Users</td>
<td></td>
</tr>
<tr>
<td>Bandwidth Gain</td>
<td>Displays bandwidth gains (including negative gains) for a specified interval.</td>
<td>Line graph</td>
<td>CPU, Memory, Users</td>
<td></td>
</tr>
<tr>
<td>Effective Bandwidth</td>
<td>Compares effective and actual bandwidth, measured in bytes.</td>
<td>Line graph</td>
<td>CPU, Memory, Users</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Report Format</td>
<td>Field</td>
<td>Overlays</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Services</td>
<td>Compares specified services.</td>
<td>Circle graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>Services Detail</td>
<td>Displays bandwidth savings for different services in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trend of Services</td>
<td>Displays the trend of the specified service over a period of time.</td>
<td>Stack graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>Proxies</td>
<td>Breaks down the total number of server bytes through different proxies.</td>
<td>Circle graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
<tr>
<td>Proxies Detail</td>
<td>Displays bandwidth savings in bytes, actual bandwidth, effective bandwidth, and the bandwidth gain.</td>
<td>Table chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trend of Proxies</td>
<td>Displays the trend of proxies versus the Server Bytes by default aggregated across all devices.</td>
<td>Stack graph</td>
<td>Bypassed Bytes, Bandwidth Savings, Bandwidth Savings Percentage, Bandwidth Gain, Effective Bandwidth, Client Bytes, Server Bytes, New Intercepted Connections, Peak Intercepted Connections</td>
<td></td>
</tr>
</tbody>
</table>
### Modify Options for Statistics Monitoring Reports

By default, a **Statistics Monitoring** report displays data for the last seven days for all ProxySG devices but you can customize the report by changing the start date and interval, choosing which devices or device group to report on, and adding overlays of additional statistics.

**NOTE**  
To have the reports on the **Statistics Monitoring** dashboard to automatically refresh the displayed reports, select **Options** and click the **Auto-refresh** box to select it. The default is set to 5 minutes, though you can set it to any desired interval of minutes (up to 59) or hours (up to 24).

To customize the reports:

1. Select **Reports > Statistics Monitoring**.
2. Select a report from **Devices** or **WAN Optimization**. See Reference: Statistics Monitoring Reports in Management Center for descriptions.
3. After you select the report, the report opens in a new tab.
4. To open the Filters dialog, click the gear settings icon within the report.
5. Filter the report data using the options described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>The date and time from which report data begins. The interval you select is based on the start date. For example, if you specify the 13th of the month for the start date and an interval of 7 days, the report shows data from the 13th through the 19th. Specify the date in MM/DD/YY format, or click the calendar to pick a date.</td>
</tr>
</tbody>
</table>
| Interval         | The number of hours or days after the start date for which the report shows data.  
Note: The start date and interval in conjunction might result in future days on the report. For example, if you want data from only the last four days, selecting a start date from four days ago results in three future days on the report. To avoid confusion, you can select a start date that is earlier than required so that future days do not display.  
Select the interval from the drop-down list. Intervals can include 60 minutes, 24 hours, 7 days or 31 days.  
If you select 60 minutes, the time field is available. Select a time from the drop-down list. Times are available in one-hour increments. |
| Filter           | Select a filter from the drop-down list. If you select Device or Device Groups, use the to select multiple ProxySG devices or a single device group.                                                                |
| Graph (This option is not available for all reports) | Changes how the data is displayed. You can graph the data as the mean average for all devices (single data line) or as individual metrics for each device (one line per device). Hover the mouse cursor over a graph line to get additional information. |
| Field (This option is not available for all reports)  | The source for which to show trending data.  
Select the specific item that you want to report on (by default, the first item in the drop-down list is displayed when you first open the report). The report displays the data for your selection. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overlays (This option is not available for all reports)</td>
<td>Metrics that you can add to the report to help you interpret the data. You can add overlay(s) to the report. When you add overlays, the additional data displays in a legend at the bottom of the report. Use the legend to identify the appearance and color of each data type. The following is an example of the legend for the Bandwidth Savings (bytes) report:</td>
</tr>
</tbody>
</table>

### Change the Scope of a Statistics Monitoring Report

By default, Statistics Monitoring reports and report widgets display data for the last seven days. For example, if you select a report on April 14th, the report opens with Last 7 Days selected for the date range at the bottom left corner. The start date or time of the selected rate range is displayed between < >.

To view data from a broader or narrower time frame, select an interval from the Quick Pick drop-down list. The report data updates immediately to reflect your selection.

Refer to the following table to understand how the date range affects the report data; assume that the current date and time is Tuesday, October 15th at 09:05.

<table>
<thead>
<tr>
<th>Selected Date Range</th>
<th>Description</th>
<th>Report shows data for this period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Hour</td>
<td>The current hour.</td>
<td>09:00 - 10:00</td>
</tr>
<tr>
<td>Today</td>
<td>The current day.</td>
<td>October 15th</td>
</tr>
<tr>
<td>Current Week</td>
<td>The current calendar week, starting on Monday.</td>
<td>October 14th - October 20th</td>
</tr>
<tr>
<td>Current Month</td>
<td>The current calendar month, starting on the 1st.</td>
<td>October 1st - 31st</td>
</tr>
<tr>
<td>Yesterday</td>
<td>The previous day.</td>
<td>October 14th</td>
</tr>
<tr>
<td>Previous Week</td>
<td>The previous calendar week, starting on Monday.</td>
<td>October 7th - 13th</td>
</tr>
<tr>
<td>Previous Month</td>
<td>The previous calendar month, starting on the 1st.</td>
<td>September 1st - 30th</td>
</tr>
<tr>
<td>Last 7 Days</td>
<td>The period of time starting 7 days ago and ending today.</td>
<td>October 8th - October 15th</td>
</tr>
<tr>
<td>Last 31 Days</td>
<td>The period of time starting 31 days ago and ending today.</td>
<td>September 14th - October 15th</td>
</tr>
</tbody>
</table>

To view data from different points in time, use the date range and < > in conjunction. Using < > causes the report to go back and forward, respectively, at the interval specified in Date Range. For example, if the date range is Last 7 Days and the report shows data from October 8th to October 15th, clicking < causes the report to display data from October 1st to October 8th. If you change the date range to Today and click <, the report displays data from the previous day. You can use > to return to more recent dates and times.

For more information about report dates, see Date Filters.
NOTE
It is possible to display future days in reports if you use >. If a report abruptly shows no data while you are changing the dates or times, check the dates/times that have no data and exclude them from your analysis (or change the date range again).

Filter on Devices or Device Groups
To view a report of data from multiple devices or from a particular device group:
1. Display the desired Statistics Monitoring report.
2. Click the Options button.
3. Change the Start Date and Interval, if desired.
4. Use the Filter drop-down list to select individual devices or specify a device group.
5. To choose from the available devices or device groups, click:
   – Device: Select one or more devices and click OK.
   – Device Group: Select one group and click OK.
6. Click Save.
After you save your changes, the report data updates immediately. The Device Filter displays the names (or IP addresses) of the devices filtered in the reports. See Refine Statistics Monitoring Reports.

Zoom In and Out on Reports
In reports that display changes over time, it is useful to see more detail on a specific data point. For example, if you are looking at a report with Current Week as the date range, zooming in on a specific day displays the report for the day at hourly intervals. Zooming in on a specific hour displays the report for the hour at five-minute intervals.
1. In the report, hover over the data point you want to see in greater detail. The data point expands slightly.
2. Click the data point and select Zoom In. The report displays the data at the new level.
3. To return to the previous level, click any data point and select Zoom Out.

Display a Full Statistics Monitoring Report
Display a full report from a statistics monitoring widget.
2. Do one of the following:
   – If the report you want has a widget on the dashboard, expand the widget if necessary and then click View Full Report at the bottom of it.
   – If the report does not have a widget on the dashboard, click Report > Statistics Monitoring. Available reports are displayed in two lists: Devices and WAN Optimization.
3. Select the report you want to view. The report opens in a new tab.

NOTE
If you leave a report open for an extended period of time, you can refresh it to ensure that no stale data is displayed. To refresh a report, click

at the bottom of the report.
**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to accomplish?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about different graph types.</td>
<td>Statistics Monitoring Graph Types</td>
</tr>
<tr>
<td>See the report for different dates or times.</td>
<td>Change the Scope of a Report</td>
</tr>
<tr>
<td>Change the metrics and other data that display on the report.</td>
<td>Modify Options for Statistics Monitoring Reports</td>
</tr>
<tr>
<td>View descriptions of the Statistics Monitoring reports.</td>
<td>Reference: Statistics Monitoring Reports in Management Center</td>
</tr>
<tr>
<td>Schedule Statistics Monitoring reports.</td>
<td>Schedule Statistics Monitoring Reports</td>
</tr>
</tbody>
</table>

**Statistics Monitoring Graph Types**

Statistics Monitoring graph types depend on the type of data represented in the report. Some reports consist of a combination of these formats.

- Line graphs show how data for one data type changes over time. You can hover over the line graphs for extra tool tips that can include data such as the date, percentage, total number, etc.
- Stack graphs show changes in a set of data, for both for the individual data types and the total of the individual items. Each color in a stack graph represents one type of data changing over time.
- Circle graphs show the proportions of specific data with a set of data. **Example:** The Effective Bandwidth graph in the Traffic Mix report shows the proportion (in percentage) of effective bandwidth for different traffic types. Hover over a segment in the graph to display the number of bytes for each traffic type.
- Table charts arrange data in rows to compare data from multiple sources. **Example:** The Devices Detail report widget shows the actual bandwidth versus effective bandwidth for all devices in the system.

**Schedule Statistics Monitoring Reports**

Use this procedure to create a job to schedule or run one or more statistics monitoring reports. For more information about the reports see Reference: Statistics Monitoring Reports in Management Center.

**NOTE**

You can also schedule or run statistics monitoring reports from the Statistics Monitoring page. See View Statistics Monitoring Reports.

1. Select Jobs > Add > New Job.
3. Configuration:
   - **Report period:** Specify the date range.
   - **Format:** Select the format, PDF, HTML, or CSV.
     By default, the reports have a Symantec logo. You can replace that with your logo.
   - **Page Orientation:** For PDF, select the orientation, Portrait or Landscape. (This is not applicable to HTML or CSV.)
4. Reports:
   - Select the reports to run. For more information about the reports, see Reference: Statistics Monitoring Reports in Management Center.
5. Job Results:
   - (Optional)—Click Email results and select the condition. Then, enter the email address(s) of the recipient(s).
6. **Schedule:**
   Choose to trigger job execution using a Schedule or an Event.

   **Schedule**
   Use Schedule when you want to run the job now or to execute the job at a specific time.
   - Immediate—automatically runs the job after it is created.
   - No Schedule—no specific time or day is specified; when you are ready to run the job, use the Run Now button to execute the job.
   - Run Once Only—specify the date and time to run the job.
   - Periodic—runs the job every \( x \) number of minutes, hours, or days, starting at the specified time and date.
   - Daily—runs the job every day at the specified time.
   - Monthly—runs the job once a month on the specified day of the month and specified time of day.
   See also Job Scheduling Options.

   **Event**
   Use Event when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
   - Device added to Management Center
   - Device added to Group
   - Device removed from Group
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.
   
   **NOTE**
   If a device cannot be a target for a job (for example, a Content Analysis device in a Collect Sysinfo job), it is ignored.

7. **Name:**
   - Verify or change the name and add an optional description.

8. Click **Save**.

Statistics monitoring reports are saved to Jobs > Archived Files. You can also download the report from the Job Progress dialog.

**Remove Orphan Device Count in Statistics Monitoring Dashboard**

One or more “orphan” devices can be shown in the Statistics Monitoring Dashboard if the following is true:

- A user replaced a monitored device on the network with a different device that used the same IP address, without completing the RMA Device operation.

This caused Management Center to retain information about removed device in Statistics Monitoring Database. You can now remove these orphan devices using the following CLI command.

**Syntax**

```
# service-action purge-statistics-monitoring-orphans
```

After you execute the command, Management Center deletes the orphans and writes the results to syslog.

**Statistics Monitoring Over HTTPS**

Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. Because of this change, the statistics monitoring for all ProxySG appliances will not function after upgrade to 1.7 or
later (because port 9009 is blocked). To re-enable statistics monitoring on all monitored ProxySG appliances, you must do one of the following:

- Create a job on Management Center to enable statistics monitoring and manually select all target ProxySG appliances (Jobs > Scheduled Jobs > New Job).
- Deactivate, and then reactivate, all ProxySG appliances that previously had statistics monitoring enabled. Upon reactivation, statistics monitoring will be correctly configured. During that process Management Center does the following on the ProxySG appliance:
  - Uploads a new certificate required to enable the ProxySG appliance to trust the connection (Configuration > SSL > CA Certificates)
  - Creates a central management CCL that includes the new certificate (Configuration > SSL > CA Certificates > CA Certificate Lists)
  - Creates a new device profile that includes the CCL (Configuration > SSL > Device Profiles)

If you subsequently change the certificate by importing (security ssl import external-certificate) or generating (security generate-ssl-certificate) a new one, statistics monitoring will fail until you re-enable statistics monitoring using one of the procedures above.

Work with Reports

Report

See the following for information about working with Reporter reports:

- Generate a Reporter Report
- Customize Reporter Report Options
- Reporter Graph Types and Views
- Create Geovisual Reports
- Date Filters
- Search for Specific Report Data (Search and Forensic Report)
- Set Time Zone for Reports

Statistics Monitoring

See the following for information about working with Statistics Monitoring reports:

- View Statistics Monitoring Reports
- Change the Scope of a Statistics Monitoring Report
- Statistics Monitoring Graph Types
- Modify Options for Statistics Monitoring Reports
- Date Filters

Create a Shared Statistics Monitoring or Reporter Custom Report

In 2.3 and later, Management Center provides a way for you to share custom reports with other users. Any user who previously had permission to view Reporter or Statistics Monitoring reports will be able to view the shared reports.

Though everyone with the correct permissions can view the reports, they cannot add, delete, or update them unless they have either the admin role or the Shared Custom Report permission with the appropriate action assigned to their role. To allow a user (or group or users) to perform one or more of those operations, edit their role (Administration > Roles > Edit) and assign the Shared Custom Reports permission along with the correct associated Action.
NOTE
After upgrade to 2.3, only the admin role has full permissions to add, delete, or update shared reports.

Allowed User Operations
The allowed operations for shared custom reports are as follows:

- Any user that can view statistics monitoring or Reporter reports can view shared custom reports.
- By default, users with the admin role can add, delete, or update shared custom reports.
- Other users can perform one or more of those operations, depending on the settings configured for their role.
- Even if a user does not have a delete or update permission, they can still perform those operations on reports they have created.
- Shared custom reports cannot be moved.

Find Shared Custom Reports
Two shared report groups are automatically created upon upgrade to Management Center 2.3. These groups are named as follows:

- Reporter: **Shared Custom Reporter Report**
- Statistics Monitoring: **Shared Custom Reports**

All shared custom reports are saved to one of these groups.

Create a Shared Custom Report
Users that have the **Share Custom Report Add** permission are able to create new shared custom reports.

1. If the user does not have the **Share Custom Report** permission, assign it to their role.
   See **Define Roles** and **Reference: Permissions Interdependencies** for more information.
2. Create a custom report by editing one of the canned reports.
   See **Create a Custom Reporter Report** and **Modify Options for Statistics Monitoring Reports** for more information.
3. When you are satisfied with your report, click **Save As**.
4. Edit the name of the report as desired.
5. In the **Save As** dialog, select **Groups > Shared Custom Reports**.
Add a Custom Logo to Downloaded Reports

By default, downloaded reports include the Symantec logo at the top of each report page. In Management Center 2.3 and later, you can add your corporate (or other) logo to your downloaded reports.

The new logo will be applied to the following reports:
• Reporter Reports
• Statistics Monitoring reports
• Summary reports

Logo Size

When adding a logo, ensure that the logo size is commensurate with the page header:
• Maximum width: 295 pixels
• Maximum height: 32.5 pixels

If your image is too big, the system should scale it to the proper size.

Procedure—Add Custom Logo to Reports

1. Select Administration > Settings > Branding.
2. Click inside the Branding logo text box. The system prompts you to browse for the file.
3. Click Select File and locate the custom logo.
4. Click Upload.
5. Click Save.

Remove Custom Logo

To remove a custom logo, select Administration > Settings > Branding. In the Branding log field, click Remove.
Filter and Keyword Search

Apply filters to any object within Management Center. Objects can include:

- Attributes
- Audited Objects
- Authentication
- Devices
- Policy Objects
- Policy Device Assignment
- Roles
- Script Objects

Filter on attributes and then use the keyword search. When you are managing hundreds or thousands of policies across multiple devices, it is important to be able to find a particular policy or configuration quickly.

You are not limited to the Filter fields displayed. You can customize your filters.

Procedure

Default fields are dependent upon the type of object that you are filtering. For example:

- Name - Filters by the object name
- Type - Filters by the object type
- Description - Filters by the object Description
- Author - Filters by who created the object

1. To filter by a particular type of policy, click the Type drop-down list. Select a Policy Type:
   - CPL
   - CPL Fragment
   - VPM
2. Click Apply Filters.
3. The Object list displays all of the Objects by Type. After you have applied filters, search for specific objects using the Keyword Search.
4. From the Policy Objects listed by Type, search for a specific Policy using the Keyword Search.

   **TIP**
   The logic is Filter *and* Keyword Search.

Search by Keyword

When searching, Management Center breaks text into keywords and then searches for keywords entered. Management Center's index system has a special case for dot. Although Management Center sees dots as separating letters within a word (i.e. Management Center considers dots as a part of a word).

**NOTE**
You cannot search on special characters such as `^ % | ~`.

Colons are treated like other non-letters by splitting keywords apart. IPv4 and IPv6 addresses work differently because of colons.

**NOTE**
The wildcard symbol is `*`. Management Center automatically appends an `*` at the end of your search term but if you want to start with a wildcard search, you have to enter it yourself.
Can quotes be used in a search?
Use quotes when non letters are part of the search term. For example, your search term includes a colon. The exception to this search rule is the use of a dot because a dot that is NOT followed by white space is considered part of the keyword.

How do you search for whole words?
Enter the whole word. If there is more than one word, separate each word with a space. If using special characters, enclose each word in double quotes.

How do you search for partial words?
Enter the partial term, and Management Center attempts to complete the search. For example, enter hi and Management Center matches that to both highlight and high.

Example Searches

IPv4 127.0.0.1
• 127.0.0 – matches any IPv4 starting with 127.0.0
• *.0.0.1 - matches any IPv4 ending in 0.0.1

IPv6 “0:0:0:0:0:1”

TIP
Use quotes for IPv6 addresses because IPv6 uses colons instead of dots as the separator.
• “0:0:0” – matches any IPv6 start with 0:0:0
• “0:0:1” – matches any IPv6 ending with 0:0:1

Hostnames
• abc.com - matches a host named abc.com
• *.com – matches a hostname ending in .com
• **:8080” – matches a hostname with :8080 as the port

Search
1. From the Keyword Search field, enter your search term.
2. Press Enter or click the magnifying glass icon.

What if the search finds no match?
If the search finds no match, the right pane displays a message indicating that objects match the keyword filter. You can search again using a different keyword.

What if the search succeeds in finding matches?
If the search finds matches, the results display in alphabetical order in the Objects list.

How do you clear the search results?
To clear search results and display all objects in the system, click the X in the search field.
About Database Filtering to Restrict Report Data

You can apply a database filter to restrict report data. To begin, specify a database and then add one or more filter criteria.

Here are several examples of filters you can create:

**Example 1**
If the administrator selects the filter **Site**, the operator **contains**, and enters **facebook** for the value, the report returns only sites that contain the string "facebook."

**Example 2**
If the administrator selects the filter **Client IP**, the operator **matches**, and enters the IP address range **10.1.1.0/22**, the report includes all addresses in that network mask.

**Example 3**
If the administrator selects the filter **Hours of Day**, the operator **in between**, and selects the hours **9 a.m.** and **5 p.m.**, the report includes data only for the time between 9 and 5.

Use a Database Filter to Restrict Report Data

If users have report permission filters that apply to the role they're using to run the report, they will not be able to filter on any fields specified in those permission filters unless the Reporter is running 10.5 or higher.

Restrict report data using a database filter. This action allows access to reports you have not restricted but removes data according to the fields specified in the filter. For each filter you want to add, follow the steps below.

**NOTE**
For filtering examples, see About Database Filtering to Restrict Report Data.

1. In the **Filters** section, click **Add Filter**.

2. Select a field.
3. Select the appropriate operator. The available operators change depending on the selected field.

4. Select or enter a value.
5. Click Finish, then Save.

**Date Filters**

When filtering by date, different time increments may display, depending on the type of date filter that you select. The list below describes each date filter and its associated time increments. User date filters for both reports and dashboards.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Time Increments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Pick</td>
<td>1 Day7 Day30 Day90 DayYTD</td>
<td>Displays the time increment of data selected starting from the current date. For example: If you select 30 Day, the report displays 30 days of data from the current date.</td>
</tr>
<tr>
<td>Current</td>
<td>hourdayweekmonthyear</td>
<td>Displays the current time increment of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the report displays a month of data for the current month of May.</td>
</tr>
<tr>
<td>Previous</td>
<td>hourdayweekmonthyear</td>
<td>Displays the previous time increment of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the report displays a month of data for the previous month of April.</td>
</tr>
<tr>
<td>Current and Previous</td>
<td>hourdayweekmonthyear</td>
<td>Displays the current and previous time increment of data based on the beginning and ending cycle of that increment. For example: If you filter on the current and previous month, and the current month is May, the report displays two months of data for both April and May.</td>
</tr>
<tr>
<td>Before</td>
<td>Calendar picker</td>
<td>Displays an absolute date on a calendar. Displays all data for that report that exists in the database before the date chosen.</td>
</tr>
<tr>
<td>Since</td>
<td>Calendar picker</td>
<td>Displays an absolute date on a calendar. Displays all data for that report that exists in the database after the date chosen.</td>
</tr>
<tr>
<td>Custom</td>
<td>Calendar picker</td>
<td>Displays a calendar picker to choose the beginning and end of the data.</td>
</tr>
<tr>
<td>All Dates</td>
<td>No dates are filtered</td>
<td>Displays all data for all dates stored in the database. When choosing this option, all absolute dates disappear and no calendar picker is available.</td>
</tr>
</tbody>
</table>

**Customize Report Widgets**

Widgets on the Dashboard and Reports tabs can be customized based on the type of data that you want to view.
**Collapse Report Widgets**
You can collapse report widgets if you have limited room on the dashboard, or if you prefer not to see all of the widgets expanded at once.

- To expand a report widget, click the down arrow in the widget title bar.
- To collapse a collapsed widget, click the up arrow in the widget title bar.

**Move Report Widgets**
You can move report widgets. Because widgets align themselves automatically when you move them, you can put them in groups.

1. Hover over a widget title bar. The pointer changes to a multi-directional arrow.
2. Drag the widget to its new location.

**Remove Report Widgets**
To remove a report widget, click the X on the top right corner of the widget.

To add the widget to the dashboard again, click **Add Report** and select the widget from the list.

**Change Date Range for Reporter Widgets**
To change the date for a Reporter widget, click the gear icon in the top-right corner of the widget.

**Add Reports**
The amount of report widgets that you can add and customize is wholly dependent upon whether you have integrated Reporter 10.x into your network.

**Close a Report**
When you no longer need to view a report, close it using one of the following methods.

**Close the Active Report**
Click **Close** to close the report.

Alternatively, close the report by clicking the X on the tab at the bottom of the screen.

**Close a Report on Another Widget**
If you have multiple reports open, you can close a report other than the active one by clicking the X on the appropriate tab at the bottom of the screen.
View Raw Report Data

The Source Data Viewer displays a report in raw data format, which breaks down specific data types that Management Center collects from devices. If the interaction of data in a standard report seems wrong or misleading, you can view the data in isolation from other metrics.

1. Select **Reports > Statistics Monitoring**.
2. Click **Source Data Viewer**. The Source Data Viewer opens on a new tab.
3. In the tree on the left, browse to the data you want to display and select it. The report opens on a new tab on the right.

**Example**

In this example, you want to see how much traffic was received on the 1:0 interface for all appliances on the previous day.

1. In the Source Data Viewer, select `tpcip > interface > 1 > 0 > bytes-received`. The report opens. Only the bytes-received metric is graphed.
2. (Optional) Add data to the report. See Modify Report Options.
3. (Optional) Change the interval or date range for the report. See Change the Scope of a Report for instructions. The following example shows the report with the Memory overlay selected.

Modify Display of Table Data

You can modify the view of table data as described below. Each table supports specific actions; all actions may not be available.

**Show Available Actions**

Click the arrow to the right of the column headings to show the available actions.

**Change Columns**

Hover over **Columns** to change the displayed columns.

**Group Table Data**

Select **Group by this field** to group the table data in accordance with that column heading.
The data is then grouped. In the example below, the Type column was grouped.

Deselect Show in groups on the dropdown menu to put data back into a plain list.

**Reports: Save as PDF**

Most Management Center reports can now be saved and downloaded to your local client as a PDF file.

1. To download the current report as a PDF, click **Download PDF**. The web console displays the **Download** dialog.

2. Select the orientation, **Portrait** or **Landscape**.

3. Optional—Change the report title or file name. Click **Download**. Click **Close** to cancel.

Some reports do not have the PDF option. These include detail reports or reports that include source data. For example:

- Interfaces Detail
- Devices Detail
- Intercepted Traffic Savings
- Traffic Mix
- Traffic Statistics
- Services Detail
- Proxies Detail
- ADN History

**Monitor Device Health**

Management Center collects health status information on device components including system resources, license validity, and user-defined health checks, and displays the aggregate health status in several areas.

If Management Center is configured to use a server certificate issued by a Certificate Authority, the certificate chain (intermediate/top CA) needs to be added to the **management-center** CA Certificate List (CCL). For Statistics Monitoring, Management Center will install this chain of trust to manage each device in order for it to establish a secure channel with Management Center.

Device health is always represented by status colors: **Error** (red), **Warning** (yellow), and **OK** (green). A device’s health status is determined by system-defined thresholds on the device: if a service or other monitored component exceeds a threshold, the device goes into a Warning or Error state.
If you cannot get the device out of the **Error** state, regardless of what you try, you may need to RMA the device. See [Perform an Operation on a Managed Device](#).

A gray status color indicates an absence of health status and represents an **Inactive** device. Some jobs and operations cannot occur on inactive or pre-deployed devices.

See [About Status Indicators](#) for more information on status colors in various areas of the web console.

**TIP**
For more information on monitoring health status on the ProxySG appliance, refer to the [SGOS Administration Guide](#).

### View Device Health Status on the Dashboard

The Dashboard displays overall health status information in widgets. Two widgets display by default, but you can close them by clicking the X in the top right corner.

The **Device Health** widget gives an overall picture of the health of monitored devices in a circle graph.

**TIP**
If you have removed a widget from the Dashboard, you can display it again. See [Customize the Dashboard View](#) for instructions.

Click a status icon below the chart to see the devices that have that status.

The **Top Problem Devices** widget lists the devices that are consistently displaying with errors or warnings.

For example, if you edit the first SG300 Series device, the **Dashboard** tab displays the health status as red with the specific errors and warnings for each device value.

### View Health Status in the Banner

In the web console banner, look for the device status icons.

![Status Icons](#)

Click a status icon to see the devices that have that status. These totals are the same as the device status totals that display under the Device Health widget on the Dashboard; because these are in the banner, they are visible to you no matter which tab you are working on. See also [Web Console Overview](#).

### View Device Health Status

1. Select **Network** and a device or group you want to view. By default the **Health** page is the default view. From here, you can review the information in the **Status** column to view the device health status. If you are viewing group details, the system displays the aggregate health by status.
2. To review all devices by their licensing status, click **Licensing**.
3. To view certificate information for the devices, click **Certificates**.
4. To receive more details, edit the device whose health you want to view. See [View and Edit Device Information](#).
5. Review the errors and warnings, system metrics, and health checks for the selected device. Each device type provides unique health details.

**NOTE**
Note: As of Management Center 1.11.1, SSL Visibility appliances running version 4.0 or later support health reporting for **License**, **Load**, **Network**, and **System** attributes with the Up/Down column. Earlier versions of SSL Visibility do not support this functionality.
View Device Statistics

Management Center provides dynamically generated device statistics for each monitored device.

1. Select the **Network** tab.
2. Edit the device whose health you want to view and click **Statistics**.

The system displays a variety of important device statistics. For example:

When **Auto Refresh** is enabled the statistics refresh every 60 seconds. If Auto Refresh is disabled, you can manually refresh the statistics by clicking the refresh icon.

Device Statistics Notes

- Content Analysis (CA) 2.1+ appliances include on-board Malware Analysis (MA). If the MA is licensed and enabled, the dashboard for CA 2.1 displays 7 additional panels for internal sandboxing data.
- The Dashboard is not supported for Security Analytics devices in Central Manager (CMC) mode.
- SSL Visibility devices running version 3.x do not display dashboard information.

Metrics

The metrics may be displayed in one of several different ways:

- **Counters**: Displays a count for a specific time period.
  - Examples: **Object Count**, **Total Scan**.
- **State**: Displays a text value.
  - Examples: **Condition** - Green/Yellow/Red condition indicator.
- **Series**: Displays values over a period; this presentation may be in an area display, a bar, a column, a pie chart, or a donut chart.
  - Examples: **CPU**, **ICAP Scan**.

Device Statistics Notes

- Content Analysis (CA) 2.1+ appliances include on-board Malware Analysis (MA). If the MA is licensed and enabled, the dashboard for CA 2.1 displays 7 additional panels for internal sandboxing data.
- The Dashboard is not supported for Security Analytics devices in Central Manager (CMC) mode.
- SSL Visibility devices running version 3.x do not display dashboard information.

Resolve Device Errors

See **Resolve Device Errors** for more information.

Enable Device Health and Statistics Monitoring

Devices can be activated or deactivated. Management Center actively monitors the health status of *activated* devices. Deactivated devices are not monitored. Whether you choose to activate or deactivate a device depends on your business requirements. For example, you might have already set up a pre-deployed device that is now ready to be activated, or want to deactivate a device that must be taken offline for maintenance.

**CAUTION**

Appliance statistics collection over HTTP port 9009 is disabled by default in 1.7 and later. The new default is HTTPS port 9010. See **Statistics Monitoring Over HTTPS** for more information.
TIP
Any of the **Change Monitoring Status** actions can be saved to a job and scheduled. See [Change Device Health and Statistics Monitoring State](#) for more information.

**Change Health Monitoring Status**

TIP
Deactivating a device is NOT the same as deleting a device. See [Stop Managing a Device](#).

1. Select the **Network** tab.
2. Locate the device you want to activate or deactivate. See [Filter Devices or Device Groups in a Permission](#).
3. Select the device or group, and click the **Operations** drop-down list.
4. Select **Change Monitoring Status**...
5. Select one or more devices and click **Next**.

6. Verify that **Change Health Monitoring state** is selected and do one of the following:
   a. To activate a deactivated device, select **Activate Device**.
   b. To deactivate an activated device, select **Deactivate Device**.

**NOTE**
Deactivating a device disables all statistics monitoring.

If you try to activate the device when the connection parameters are not specified, you receive an error. To specify connections parameters, see [Edit a Device](#).
7. Click **Run Now**. The system displays the Activate Devices - Job Results window.

![Activate Devices - Job Results](image)

**NOTE**
The device status can take up to 30 seconds to change.

**Enable or Disable Statistics Monitoring**

Use these options to enable or disable statistics monitoring. You can disable statistics monitoring without deactivating the device. However, Management Center can only collect statistics from activated devices.

1. Select the **Network** tab.
2. Locate the device you want to activate or deactivate. See Filter Devices or Device Groups in a Permission.
3. Select the device, and click the **Operations** drop-down list.
4. Select **Change Monitoring Status**...
5. Select one or more devices and click Next. The system displays the Change Monitoring Status: Operation States dialog.
6. Verify that Change Statistics Monitoring state is selected and do one of the following:
   a. To enable statistics monitoring, select Enable Statistics Monitoring collections.
      NOTE
      You can only enable statistics monitoring for activated devices.
   b. To disable statistics monitoring, select Disable Statistics Monitoring collections.
7. Click Run Now. The system displays the Activate Devices - Job Results window.
NOTE
The device status can take up to 30 seconds to change.

About Pre-Deployed and Deactivated Devices

You can manage devices in Management Center even if you do not have the ability to monitor their activity and statistics. These devices have an Inactive status in the system; when you select them, the System Metrics and Health Checks tabs at the bottom of the screen display no data.

To look for inactive devices in the system, click the Network tab and clear all the statuses beside Filter by except Inactive:

The Network tab displays only the Inactive devices.

Inactive devices consist of two types: pre-deployed devices and deactivated devices. The following are examples of why you might need to manage inactive devices:

• You add a device that has not arrived in your organization yet or is not set up. In this scenario, in the Add Device wizard, you select Unavailable (pre-deployment) for the deployment status. Connection parameters are not required when you select the pre-deployment status, so you must specify them before you activate the device later.

• To allow for scheduled maintenance or other scenarios where devices must be powered off. In this scenario, to prevent error alert messages, you could deactivate the affected devices by selecting them and clicking Deactivate. Then, reactivate the devices when maintenance is complete.

For more information about device status and the use of color in the web console, see About Status Indicators.

View System Metrics

In Management Center, device metrics refer to key hardware components such as CPU usage, disk status, fan status, and motherboard temperature. Refer to these metrics to verify availability and performance of system resources.

1. Select the Network tab. Select a device to view metrics.
2. At the bottom of the screen, click the up arrow

   The monitor window expands from the bottom of the screen.
3. The web console displays the Overview, System Metrics, and Device Health and Backup tabs.
4. (Optional) If the device is always in an error state (yellow or red) and you are unable to update the license or restore a good configuration, you may need to perform an RMA for the device. See RMA Device.

5. Click System Metrics. The web console displays information about the system resources. If available, scroll down to see all of the metrics available for the selected device. To see device details in the overview tab, see Verify Device Details.

   **NOTE**
   Management Center can collect metrics only from activated devices. If you select a deactivated or pre-deployment device, the Overview, System Metrics, Health Checks and Backup tabs display no information.

**The System Metrics Tab**

The Systems Metrics tab provides a snapshot glance of the disk status as well as the percentage that both the CPU and Memory are currently being used, and the threshold settings for both Warning and Critical. To configure warning and critical thresholds displayed in the System Metrics tab, see Hardware Monitor Settings. An example of a ProxySG appliance is displayed in the table shown below.

<table>
<thead>
<tr>
<th>Metric Description</th>
<th>Status</th>
<th>Current Value</th>
<th>Warning Threshold</th>
<th>Critical Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Utilization</td>
<td>OK</td>
<td>3%</td>
<td>80%</td>
<td>95%</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>OK</td>
<td>25%</td>
<td>90%</td>
<td>95%</td>
</tr>
<tr>
<td>Disk 1 Status</td>
<td>OK</td>
<td>present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk 2 Status</td>
<td>OK</td>
<td>present</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**The Health Checks Tab**

The Health Checks tab displays information based on the type of device that you have selected. An example of an SSL Visibility appliance is displayed in the table shown below. The top row displays General with the number of health checks that are routinely performed on the device. To see other places within the web console to view device health, see Monitor Device Health and Backups.

<table>
<thead>
<tr>
<th>Name</th>
<th>Info</th>
<th>State</th>
<th>UP/DOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>- General (4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License</td>
<td>OK</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>Load</td>
<td>OK</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>OK</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>OK</td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>

**The Backup Tab**

The Backup tab displays all of the device backups for the selected device. The Backup tab also displays whether a device backup has been exported to an external server, and whether it has been restored. Perhaps most importantly, you can pin a backup to ensure that it doesn't get deleted when Management Center deletes old backups when performing routine disk maintenance. When importing a backup, Management Center will not replace pinned backups unless specified when you Import Device Backups. You must select a backup from the list to View, Restore, or Delete a backup.
See Monitor Device Health and Backups. An example of a ProxySG appliance backup information is displayed in the table shown below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Date/Time</th>
<th>Device Type</th>
<th>OS Version</th>
<th>Exported Date</th>
<th>Restored Date</th>
<th>Pinned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>SG in Dallas</td>
<td>7/3/15 8:05 PM GMT</td>
<td>ProxySG</td>
<td>SGOS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>SG in Tuscon</td>
<td>6/3/15 7:58 PM GMT</td>
<td>ProxySG</td>
<td>SGOS 6.5.5.410</td>
<td>7/11/15 1:58 AM GMT</td>
<td>7/12/15 3:30 PM GMT</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Joe's SG</td>
<td>5/3/15 8:01 PM GMT</td>
<td>ProxySG</td>
<td>SGOS 6.5.5.410</td>
<td>5/23/15 6:01 AM GMT</td>
<td>5/27/15 4:12 PM GMT</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Matt's SG</td>
<td>5/3/15 8:03 PM GMT</td>
<td>ProxySG</td>
<td>SGOS 6.5.5.410</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export device backups to an external server.</td>
<td>Export Backups</td>
</tr>
<tr>
<td>Verify device details in the Overview tab.</td>
<td>Verify Device Details</td>
</tr>
<tr>
<td>View device backup in a text editor.</td>
<td>Monitor Device Health and Backups</td>
</tr>
</tbody>
</table>

**View Device License Information**

Management Center allows you to monitor the health status of a device's license and its associated components. Devices are polled hourly for license changes.

**NOTE**
Some unmonitored devices may show licensing information while others do not. If you disable statistics collection on a device that was previously monitored, it will show the last license data. Devices that were never monitored show no license data.

1. Select the **Network** tab.
2. Select the device group in the left pane.
3. Select the **Licenses** tab. The system displays the license information for all applicable devices in the group, including the licensed components, time to expiration, and the expiration date.
4. To review the license details for a specific device, click the + symbol next to the device's IP address.

   The system then displays the same details for each associated license and component.
5. Optional: Click **Export Data** to save the data to a .csv file.
# Manage Dashboards

Dashboards allow you to quickly view important device data. This data is represented by widgets. Widgets represent data from managed devices. Dashboards are highly customizable and can help you quickly view the information you deem important.

To monitor devices from a single screen, add dashboards and add widgets to those dashboards using the options on the **Dashboards > Manage Dashboards** page.

<table>
<thead>
<tr>
<th>Order</th>
<th>Name</th>
<th>Type</th>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3, etc. The order is displayed from left to right on the dashboard tab beginning with 1 on the left.</td>
<td>The name of the dashboard as it appears on the Dashboard tab.</td>
<td>Reporter - displays only Reporter widgets on the dashboard. WAF Reporter - displays only WAF widgets on the dashboard Mixed - Can display data from all widgets on the dashboard. Statistics Monitoring - displays only Statistics Monitoring widgets on the dashboard.</td>
<td>Each dashboard can display multiple widgets. For a quick reference of what is displayed on each dashboard, view the widget count for each dashboard.</td>
<td>The description helps to differentiate the dashboard type, and the widgets within the dashboard.</td>
</tr>
</tbody>
</table>

## Notes

- Dashboards are dependent on the reports that you can generate for each managed device. To generate advanced reports and view advanced real-time data within dashboards, see **Integrate Reporter into Management Center**.

## Add a Dashboard

To accommodate your screen size or personal preference, you can change the number of dashboards that display, as well as define the layout of the dashboards. You must also define the dashboard type. Layouts arrange widgets in one to four columns of equal width, with the columns expanding to fit the width of the screen. When you select a layout, your change persists (beyond the current session) until you change the layout again.

**NOTE**

Although you can add multiple dashboards, remember that dashboards display data from databases that may not be the only database available. For example, a Reporter Enterprise Server can provide data from multiple databases. When adding Reporter widgets to dashboards, you can choose from the available databases.

1. From **Dashboards > Manage Dashboards**, click **Add Dashboard**.
2. Enter a descriptive **Dashboard Name** and **Description**.
3. Choose a **Type**:
   - **Mixed** - A dashboard that displays both ProxySG appliance and Reporter widgets
   - **Reporter** - A dashboard that displays Reporter widgets

   If you select Reporter as the dashboard **Type**, from the **Template** drop-down list, select from the following templates to pre-populate widgets:
Welcome to Management Center 3.0!

- **Web Application Usage**
- **Threat Detection**
- **Content Filtering**
  - **WAF Reporter** - A dashboard that displays Reporter Web Application Firewall (WAF) widgets. If you select **Reporter WAF** as the dashboard type, select **Web Application Firewall** from the Template dropdown list.
  - **Statistics Monitoring** - A dashboard that displays ProxySG appliance widgets.

4. Select the auto-refresh rate.
   Select the Layout for the dashboard.
5. Click **Save**. The saved dashboard is displayed in the **Dashboard** drop-down with the name that you gave it.

**NOTE**
After you have created a dashboard, you cannot edit the type.

### Reorder Dashboard List

When you add a new dashboard, the most recently added dashboard is appended to the end of the list. For example if you have three dashboards and add one, the new dashboard becomes the fourth dashboard on the list and will appear to the right of the previously added dashboards. To change the order dashboards are displayed:

1. From **Dashboards > Manage Dashboards**, select the dashboard you want to move.
2. Click **Move Up** or **Move Down** to change the order.

### Duplicate a Dashboard

To use a dashboard as a template for a dashboard that you may want to clone (and perhaps edit later), you can duplicate a dashboard that already exists. You are unable to change the type of dashboard when you duplicate.

1. From **Dashboards > Manage Dashboards**, click **Duplicate**.
2. From the Duplicate Dashboard dialog, give the dashboard a unique name.
3. Click **Duplicate**. The duplicated dashboard is displayed under **Manage Dashboards**.

### Dashboards and Widgets

The **Dashboards** section of Management Center enables you to get a quick view of your device health and statistics.

#### Dashboards

A **dashboard** provides a simplified view of data in **widgets**. Management Center displays the following default dashboards after users Log into the Web Console:

- **Home Dashboard**
  - The home dashboard displays when you log into the web console by default. The dashboard displays **Device Health** and **Top Problem Devices** widgets by default, but you can add and remove widgets to any dashboard.
- **Statistics Monitoring Dashboard**
  - The web console displays the Statistics Dashboard when you select **Dashboards > Statistics Monitoring**. It displays widgets that provide a simplified view of the statistics monitoring data in a full report.

  **NOTE**
  - When you open or view the **Statistics Monitoring** dashboard it does not display filtered data from the last session. Each new session opens with no filters applied.

For help with managing dashboards, see the following:
• Manage Dashboards
• Change the Dashboard Layout or Refresh Rate
• Web Console Overview
• Display a Full Statistics Monitoring Report
• View Statistics Monitoring Reports
• Change the Scope of a Statistics Monitoring Report
• Schedule Statistics Monitoring Reports
• Monitor Device Health
• Enable Device Health and Statistics Monitoring
• View and Edit Device Information

Widgets
A widget is a graphical representation of information, designed to provide a quick overview of statistics or other important information. The variety of widgets available to add to dashboards is dependent upon dashboard Type. See Manage Dashboards.

For help with managing widgets, see the following:
• Add a Widget to the Current Dashboard
• Customize Report Widgets
• Add the Bookmarked Devices Widget
• Monitor Device Health

Add a Widget to the Current Dashboard

1. Select the Dashboards tab.
2. Click Add Widgets.

   NOTE
   The available widgets are controlled by the report permissions associated with a user's role. Users cannot add widgets for restricted fields.

3. (Optional) From the report groups in the left pane, select the group that contains the report widget you want to add: Bandwidth Usage, Devices, Health, Security, User Behavior, WAN Optimization, Web Applications. The right pane updates with the list of report widgets for the selected report type.
4. Select the report widget you want to add.
5. For Reporter widgets, select the Database, Layout, and Date Filter.
6. Click Add Widget Now.
7. Repeat steps 3 to 6 to add more widgets, and then click Close.

To customize the layout and widgets of your dashboard, see Change the Dashboard Layout.

Add the Bookmarked Devices Widget

The Home dashboard displays the Device Health and the Top Problem Devices widgets by default after you log in. To add a widget specifically to view real-time data for favorite devices, add the Bookmarked Devices widget to a dashboard.

1. From the Home dashboard, select Add Widgets. The web console displays the Add Widgets wizard.
2. Scroll to Health and select Bookmarked Devices.
3. Select **Add Widget Now**. Click **Close**. The dashboard displays an empty widget.

4. Select **Add Devices**. Give the widget a name and select the devices that you want to monitor in the dashboard.

5. Select the devices that you want to "bookmark" as your favorite devices and click **OK**. The new widget displays the selected devices.
Change the Dashboard Layout or Refresh Rate

To accommodate your screen size or personal preference, you can change the layout of the main Dashboard tab and define the dashboard type and refresh rate. Layouts arrange widgets in one to four columns of equal width, with the columns expanding to fit the width of the screen.

When you select a layout, your change is saved beyond the current session until you change the layout again.

1. Select the Dashboard tab. To customize the layout and type, click Options. The web console displays the Layout Options dialog. You can change the following:
   - Dashboard name
   - Description
   - Dashboard Type
     - Mixed - A dashboard that displays both ProxySG appliance and Reporter widgets
     - Reporter - A dashboard that displays Reporter widgets
     - Statistics Monitoring - A dashboard that displays ProxySG appliance widgets
   - Auto-refresh rate.
   - Layout
2. Click Save.

After you add a dashboard, you cannot change the dashboard type.

Date Filters

When filtering by date, different time increments may display, depending on the type of date filter that you select. The list below describes each date filter and its associated time increments.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Time Increments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Pick</td>
<td>1 Day 7 Day 30 Day 90 Day YTD</td>
<td>Displays the current &lt;time increment&gt; of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the data that is displayed in the report reflects a month's data for the current month of May.</td>
</tr>
<tr>
<td>Current</td>
<td>hour day week month year</td>
<td>Displays the previous &lt;time increment&gt; of data based on the beginning and ending cycle of that increment. For example: If you filter on the current month, and the current month is May, the data that is displayed in the report reflects a month's data for the previous month of April.</td>
</tr>
<tr>
<td>Filter</td>
<td>Time Increments</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Current and Previous</td>
<td>hour, day, week</td>
<td>Displays the current &lt;time increment&gt; and the previous &lt;time increment&gt; of data based on the beginning and ending cycle of that increment. For example: If you filter on the current and previous month, and the current month is May, the data that is displayed in the report reflects data for both April and May.</td>
</tr>
<tr>
<td>Before</td>
<td>Calendar picker</td>
<td>Displays an absolute date on a calendar. Displays all data for that report that exists in the database before the date chosen.</td>
</tr>
<tr>
<td>Since</td>
<td>Calendar picker</td>
<td>Displays an absolute date on a calendar. Displays all data for that report that exists in the database after the date chosen.</td>
</tr>
<tr>
<td>Custom</td>
<td>Calendar picker</td>
<td>Displays a calendar picker to choose the beginning and end of the data.</td>
</tr>
<tr>
<td>All Dates</td>
<td>No dates are filtered</td>
<td>Displays all data for all dates stored in the database. When choosing this option, all absolute dates disappear and no calendar picker is available.</td>
</tr>
</tbody>
</table>
Administrate Management Center

- Define Management Center Settings
- Configure General System Settings
- Upgrade Management Center
- Downgrade Management Center
- Back Up the Configuration
- Encrypt Sensitive System Data
- Restore a Management Center Backup Configuration
- Configure Management Center Failover

Management Center Documentation Resources

Symantec provides technical and solution documentation in different formats. This page provides a resource locator.

Management Center Documentation

- Management Center Help (online help system)
  The online help system is intended to contain the same information as the Configuration Guide, but it is not updated as frequently. The content in the Management Center Configuration Guide on the Broadcom Tech Docs Portal supersedes the content in the online help.

Release Notes, Software Images, MIBs

To download software images and license keys, you need the serial number of the appliance:

- The serial number of your appliance To locate the serial number, go to the banner and click About. View the serial number under Chassis FRU Info. The serial number can also be found on the front panel LCD screen.

  ![About button screenshot]

  - For more instructions, refer to the Getting Started guide.
Access the Management Center CLI

You can access the Management Center CLI from the pull-down in the user interface banner.

![Open CLI Shell](image)

**NOTE**
You can also Access the CLI of a Managed Device.

**Requirements**

Users must have the <Management Center, CLI> permissions to use this feature.

**Procedure**

1. Go to the Management Center home or dashboard

![Symantec Management Center](image)

2. In the banner, click the pull-down and select **Open CLI Shell**.
   
   A new browser window opens.

3. Manually log into the Management Center CLI shell.

**Specify Explicit Proxy Settings**

If you have configured an explicit proxy server in your environment, you can specify the settings in Management Center. These settings are used for all outgoing HTTP requests and other functions such as licensing, heartbeats, and support case reports.

1. Select **Administration > Settings > HTTP Proxy**. Fields marked with a red asterisk (*) are required settings.
2. Specify explicit proxy settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable*</td>
<td>Specify whether an explicit proxy is configured.</td>
<td>false</td>
</tr>
<tr>
<td>HTTP Proxy IP or hostname</td>
<td>Specify the IP address or hostname of proxy server.</td>
<td>Example: https://&lt;IP_address&gt;</td>
</tr>
</tbody>
</table>
### Add Packages to Management Center

Use the **Administration > Packages** page to load add-ons to Management Center. Currently, the page only supports downloads for the new Blue Coat ProxySG appliance Admin Console package. However, other downloads will be supported in future releases.

See [Install the ProxySG Admin Console](#) for more information.

**NOTE**
You can limit the actions users are allowed to perform on this page by adding the **Settings - View** or **Settings - Update** permission to a new or existing role. See [Grant Permissions](#) for more information.

**NOTE**
Management Center replaces special characters in file names.

#### Add a Package

1. Select **Administration > Packages**.
2. Add the file using one of the following methods:
   - By browsing:
     a. Click **Add Package**.
     b. Click **Select File** and browse to the file(s).
     c. Select the file.
     d. Click **Open**.
     e. Click **Upload**.
   - By dragging and dropping one or more files:
     a. Click **Add Package**.
     b. Drag and drop the files into the **Upload From Browser** window.
     c. Click **Upload**.
   - By specifying a URL:
     
     **NOTE**
     To add packages from a URL, you must first enable HTTP. For information on enabling HTTP, see [security](#). At this time, Management Center does not challenge you when downloading from a secure web site.
     a. Click **Add Package**.
     b. In the **URL** field, specify the location of the package.
     c. Click **Upload**.

#### Delete Uploaded Packages

To delete a file, select the file and click **Delete**.
Define Management Center Settings

Use the Administration > Settings page to modify Management Center device-specific settings, for example, diagnostic settings, SNMP, and authentication settings.

- **General**
  Configure General Settings about managed devices, policy revisions and users and backups.

- **Alerts**
  Configure alerts for device errors.

- **LDAP**
  Authenticate users against LDAP.

- **Active Directory LDAP**
  Authenticate users against Active Directory.

- **RADIUS**
  Authenticate users against RADIUS.

- **SMTP Alerts**
  Configure SMTP communication settings.

- **SNMP Alerts**
  Configure SNMP communication settings.

- **HTTP Proxy**
  Configure proxy settings.

- **Diagnostics**
  Configure the Logging level for logs (collected from devices).

- **Housekeeping**
  Configure auditing and job execution settings.

- **SNMP Settings**
  Configure SNMP community settings.

- **Mail Settings**
  Configure mail server settings.

- **Consent Banner**
  Specify consent banner settings.

- **Hardware Monitor Settings**
  Set hardware monitoring thresholds.

- **Device Communication**
  Identify the hostname used in Management Center's HTTPS server certificate.

Configure General System Settings

Configure Management Center general settings about bandwidth cost, the number of backup slots for Management Center backups and the maximum number of policy and script revisions to store. You can also create a password reset email and configure settings to apply to Management Center users.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

1. Select Administration > Settings.
2. From System Settings, select General on the left.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth Cost per GB</strong></td>
<td>See Set Bandwidth Cost for Reports</td>
</tr>
<tr>
<td><strong>Device Polling Interval</strong></td>
<td>See Set the Device Polling Interval</td>
</tr>
<tr>
<td><strong>Number of backup slots</strong></td>
<td>Set the Number of Backup Slots</td>
</tr>
<tr>
<td><strong>Maximum number of policy revisions to store</strong></td>
<td>Set the Maximum Number of Policy Versions to Store in Management Center</td>
</tr>
<tr>
<td><strong>Maximum number of script revisions to store</strong></td>
<td>Set the Maximum Number of Script Revisions to Store in Management Center</td>
</tr>
<tr>
<td><strong>Inactivity timeout (minutes)</strong></td>
<td>Specifies the number of minutes before an inactive user is logged out. Users are warned 30 seconds before they are logged out.</td>
</tr>
<tr>
<td><strong>Inactivity timeout exclusions</strong></td>
<td>text: Enter comma-separated usernames</td>
</tr>
<tr>
<td><strong>Is Reset Password enabled?</strong></td>
<td>false</td>
</tr>
<tr>
<td><strong>Reset Password Email Subject</strong></td>
<td>text: Management Center Reset Password</td>
</tr>
<tr>
<td><strong>Reset Password Email Message</strong></td>
<td>text: Enter the body text of the email that will be sent upon a user's request of a password reset. Click OK.</td>
</tr>
</tbody>
</table>

4. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

5. Instruct users to log into the web console with their existing username and password. After a user logs in, you can manage their account in Management Center.

### Set Bandwidth Cost for Reports

Statistics Monitoring reports require that you specify a bandwidth cost to display data. The bandwidth cost is a multiplier and is thus not expressed in a specific currency unit. For example, you can enter a value to represent on average how you pay per gigabit for data usage on your network.

1. Select **Administration > Settings**. Select **General**. General fields display on the right.
2. Enter a decimal value.
3. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

### Set the Number of Backup Slots

By default, Management Center stores up to five backups per device, with each backup placed in a **slot**. After five backups, Management Center prunes (deletes) an **unpinned** backup to make room for the new backup. (Backups that
are pinned are preserved and cannot be manually deleted or automatically pruned.) If you want Management Center to store more or fewer backups per device, you can adjust the number of backup slots.

1. Click the Administration tab and select Settings.
2. Select General on the left.
3. In the Number of backup slots enter a new value.
4. Click Save.

NOTE
You can override the default number of backups that are retained for a device by entering a Retention Count when exporting backups. See Export Device Backups.

Configure Mail Settings

The settings on the Administration > Settings > Mail Settings page are for configuring the server that Management Center uses to send alerts related to users of the system, for example, password resets.

NOTE
The options on this page do not enable alerts for managed devices. To receive monitored device event notifications via email, you must configure SMTP alerts. Management Center stores the settings so that SMTP alerts (emails) can be transmitted and received correctly.

1. Select Administration > Settings.
2. Select Mail Settings. Mail settings display on the right.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server*</td>
<td>The SMTP mail server to use for outgoing mail.</td>
<td>Example: smtp.organization.com</td>
</tr>
<tr>
<td>Mail Server Port*</td>
<td>The Port that the SMTP mail server uses.</td>
<td>Example: 25</td>
</tr>
<tr>
<td>From address*</td>
<td>The e-mail address from which e-mails are sent.</td>
<td>Example: <a href="mailto:bccm@organization.com">bccm@organization.com</a></td>
</tr>
<tr>
<td>Username</td>
<td>The User name used to access the SMTP mail server.</td>
<td>Example: joe.admin</td>
</tr>
<tr>
<td>Passphrase</td>
<td>The password required to access the SMTP mail server.</td>
<td>Example: admin123</td>
</tr>
</tbody>
</table>

4. Click Save and then Activate to cause the server to load and apply the currently saved configuration.

Configure SNMP Agent Settings

You can configure your SNMP agent to use SNMPv2 or SNMPv3, or both.

TIP
The Simple Network Management Protocol (SNMP) itself does not define which variables a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBS). The MIBs are available on the Downloads page. Refer to the Management Center Release Notes for information on MIBs. See Access Management Center Software Downloads and Documentation for more information about accessing Symantec downloads.

SNMPv2 Settings

1. Select Administration > Settings.
2. Select **SNMP Settings** on the left.
3. Click the **Enabled** check box.
4. Enter the password in the **Community** text field. This password must be entered as alpha-numeric with no special characters. For more information on the **Community** field, see Configure SNMP Alerts.
5. Click **Save**.

**SNMPv3 Settings**

1. Select **Administration > Settings**.
2. Select **SNMP Settings** on the left.
3. Click the **Enabled** check box.
4. Enter a **User**.
5. Enter the authentication protocol: SHA or MD5.
6. Enter the authentication password.
7. Optionally, choose to encrypt the SNMP agent data and provide the encryption method and password.
8. Click **Save**.

**Configure Consent Banner**

A Notice and Consent banner provides consent information to users of computer networks, computers, and other systems and resources. Users are required to accept the terms in the banner prior to authentication. The banner is presented to users before a login process, and it requires users to acknowledge and agree to the message before they can log in or access resources on the network.

Implement the consent banner to do some or all of the following:

- Obtain users' notice of, and consent to, lawful monitoring of usage and data collection.
- Notify users that they must concede certain expectations of privacy in order to access the network.
- Ensure users' compliance with organization-specific policies.

Staring with Management Center1.10.1.1, the controls also allow for simple formatting within the consent field. If you are familiar with Markdown, you can use the simple options to create and format the content.

The logo displays centered above the banner text. The banner text displays within an uneditable text box. A blue **Accept** button displays below and to the right of the banner text, as shown in the example below.
Procedure

1. Select Administration > Settings.
2. Click Consent Banner to open the editing options.
3. To activate the banner, select the box next to Show consent banner.
4. Edit what displays for the consent content. The options available include:
   a. **Company Logo or Consent Image**: Click in the Consent image field. Select a file from your local system to upload. This image appears above the consent text box. (Alternatively, you can download a copy of the currently loaded image by clicking the download button, or delete the image by clicking the remove button.)
   b. **Text Formatting**: In the Consent text box, enter the text to present to users upon login to Management Center. Format the text as needed, either with Markdown (a simple formatting code) or by using the format controls at the top of the text field. The text field displays the formatting along with the formatting code for your reference.
      
      **NOTE**
      The code in the editing box does not show on the consent banner when you finish.
   c. **Inline Images and/or Icons**: The format controls include a button to add images. Any images you use must first be uploaded to Management Center. See Upload Files to Management Center for more information.

Editor Example
5. Once finished with the editing, click **Save**. (Or click **Cancel** to reset the last saved settings.)

### Configure Hardware Monitor Settings

To better understand how each device is reporting disk and memory usage, configure hardware monitor settings and the Disk and Memory Critical and Warning Levels.

1. Select **Administration > Settings**.
2. Select **Hardware Monitor Settings**. Hardware monitor fields display on the right.
3. Specify the hardware Hardware Monitor threshold settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Input Value/Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Enabled</td>
<td>Enable or disable hardware monitor</td>
<td>true/false</td>
</tr>
<tr>
<td>Monitor Interval (min)</td>
<td>The threshold at which the hardware monitor polls the device (in minutes).</td>
<td>5</td>
</tr>
<tr>
<td>Disk Usage - Warning</td>
<td>The threshold at which the monitor polls the device for disk usage events.</td>
<td>85</td>
</tr>
<tr>
<td>Disk Usage - Critical</td>
<td>The threshold at which the monitor polls the device.</td>
<td>95</td>
</tr>
<tr>
<td>Disk Usage - Shutdown on critical?</td>
<td>Shuts down the web console when the threshold for Critical is reached.</td>
<td>true/false</td>
</tr>
<tr>
<td>Memory Usage - Warning</td>
<td>The threshold at which the monitor polls the device for memory usage events.</td>
<td>95</td>
</tr>
</tbody>
</table>
4. Click **Save** and then **Activate** to cause the server to load and apply the currently saved configuration.

   **NOTE**
   If you enable the hardware monitor and also enable **Disk Usage - Shutdown on critical?**, the web console shuts down when the threshold for critical is reached. The Management Center CLI is still available.

   If you have unsaved changes, the edited settings are marked with a red triangle. See the "Pending changes" text at the top left of the dialog as an example.

### Automate Password Reset Process

As an administrator on Management Center, you need to configure settings so that users can request a password reset if they forget their password.

The password reset process requires that you configure three different settings:

- You must enable the password reset feature (**Administration > Settings > General**).
- You must configure the email server (**Administration > Settings > Mail Settings**).
- Each user must set up a security question in their user profile (**Banner >**).

These actions are described in the following section.

#### Enable Password Reset

1. Select **Administration > Settings > General**.
2. Check the box in the **Is Reset Password enabled?** field.
3. For **Reset Password Email Subject**, modify the email subject line, if desired.
4. For **Reset Password Email Message**, modify the body of the email that is automatically sent to users when they click the **Reset Password** link. For example, you can add a person's name to the signature instead of the generic Management Center.

   **NOTE**
   The message contains two substitution variables: `{fullname}` and `{link}`. Management Center automatically replaces `{fullname}` with the user's first and last name and replaces `{link}` with a password reset URL.

5. Click **Save** and then **Activate**.
6. Make sure an email server is configured. See **Configure Mail Settings**.
7. Ensure that all users have added a security question to their **user profile**. Users are challenged to answer their security question during the password reset process.
8. Optional—To capture log data, configure the **Security Logging Level** to **INFO** or a higher severity (**Administration > Settings > Diagnostics**). See **Configure Diagnostics Logging**.
Management Center Mail Settings

Management Center has three different email settings.

<table>
<thead>
<tr>
<th>Function</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device health notifications</td>
<td>SMTP alerting</td>
<td>These options configure the mail server for sending device health monitoring notifications from Management Center.</td>
</tr>
<tr>
<td>Management Center health notifications</td>
<td>SMTP (CLI)</td>
<td>This CLI option configures Simple Mail Transfer Protocol (SMTP) settings for Management Center core health monitoring notifications.</td>
</tr>
<tr>
<td>Password reset notifications</td>
<td>Mail Settings</td>
<td>These options configure the server that Management Center uses to send alerts related to users of the system, for example, password resets.</td>
</tr>
</tbody>
</table>

Back Up the Management Center Configuration

Symantec recommends that you back up the Management Center configuration often. The backup contains Management Center database, settings, and, optionally, device reporting statistics. To save disk space on the appliance, you can export the backup to an external server as part of the backup job. Exporting backups to an external server is required before upgrading or downgrading the software image. See Upgrading Management Center.

Important Backup Notes

Backups are not compatible or transferable between FIPS and Non-FIPS mode, for the following reasons:

- Encryption differences between FIPS/Non-FIPS mode
- Non-FIPS backup cannot be restored to FIPS appliance without omitting certain backup portions.

Backup Requirements

Back up the Management Center configuration requires specific permissions. Sensitive data is encrypted with an encryption key. See the topic Understanding Job Permissions in the Management Center Configuration and Management Guide.

Back Up Management Center

To back up the Management Center configuration, you must create a job for it. You can either schedule the job to run on a regular basis, run immediately, or on-demand at a time that you want to create a backup.

NOTE

This operation is not supported in Multistep Device Jobs.

1. Select Jobs > Add > New Job.
2. On the Add New Job page, select Backup Management Center.
3. Configuration:
   - If you want the backup file to be exported to an external HTTP, FTP, or SCP server, select the Export to Server check box and fill in the server details:
• **Server URL**: Enter the protocol (SCP, FTP, FTPS, HTTP, HTTPS) and server name and path. For example: `ftp://mycompany.com/backups`

• **Encryption Phrase**: This option is required for exporting the archive. - 1 or more characters, alphanumeric

• **Username**

• **Password**
  – (Optional) Select the **Exclude Statistics Monitoring Trend Data** check box to exclude device reporting statistics. By excluding these statistics, the backup is substantially smaller (perhaps by hundreds of gigabytes). Keep in mind, however, that the restored backup will not have any statistics data.

4. **Job Results**:
   – (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).

5. **Schedule**:
   Choose to trigger job execution using a Schedule or an Event.
   - **Schedule**—Use **Schedule** when you want to run the job now or trigger the job execution at a specific time.
     - **Immediate**—automatically runs the job after it is created.
     - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job manually.
     - **Run Once Only**—specify the date and time to run the job.
     - **Periodic**—runs the job every x number of minutes, hours, or days, starting at the specified time and date.
     - **Daily**—runs the job every day at the specified time.
     - **Monthly**—runs the job once a month on the specified day of the month and specified time of day.
   
   – **Event**—Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
     - **Device added to Management Center**
     - **Device added to Group**
     - **Device removed from Group**
   
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target.
   If a device cannot be a target for a job (for example, a Content Analysis device in a Collect Sysinfo job), it is ignored.
   If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target.

6. **Name**:
   – Verify or change the name and add an optional description.

7. **Click Save**.

**CAUTION**

Management Center retains only five backups. When the sixth backup occurs (such as in a recurring job), the oldest backup is deleted. This method is a rolling five backup retention and cannot be configured. To retain extra backup configurations, you can export the backup to an external server as part of the backup job, or you can export backups later using the `backup export` CLI command.

**Back Up Management Center Using the CLI**

1. Log in to the CLI. See **Access the Management Center CLI**.

2. Enter privileged mode. See **Privileged Mode Commands**.

3. At the command prompt, type the following command and press Enter:
   ```
   # backup create
   ``
   
   The CLI indicates that the backup is being created. You should see a response similar to the following output:
Upgrade Management Center

CAUTION
Always back up your Management Center configuration before upgrading or downgrading. Then, store the backup off-box. If you experience problems with upgrading or downgrading, backing up the configuration ensures that you can restore it.

Upgrade Best Practice
When upgrading or downgrading the version of Management Center, you must stay within two versions of what is running. Refer to this article for more information.

Manage Management Center System Images
When new features and improvements are made to Management Center, you can download a system image from Symantec and can upgrade the appliance. If you ever experience issues with a new image, you can activate an older image to downgrade the appliance.

Management Center stores up to six images on the system. For Management Center virtual appliances, this number also depends on the image size and boot partition (limited to 4 GB by default). The image that is marked as the default image will be loaded the next time that the appliance is rebooted.

If the maximum number of images are stored on your system and you download another image, Management Center deletes the oldest unlocked image to make room for the new image. To prevent an image from being deleted or replaced, you can lock the image.

You perform image management using Management Center CLI commands. See installed-systems for a description of the commands for adding, deleting, locking, unlocking, and viewing images.

Special Notes Regarding Management Center 3.x Software Image Installation:
Due to some major changes to the underlying systems Management Center relies on, there are several important points to be aware of:

• Backups are not compatible or transferable between FIPS and Non-FIPS mode, for the following reasons:
  – Encryption differences between FIPS/Non-FIPS mode
  – Non-FIPS backup cannot be restored to FIPS appliance without omitting certain backup portions.
• The SSH RSA host key used for port 22 on Management Center no longer changes with upgrades.
• The initial upgrade may take a long time to complete. Wait for the upgrade to complete—any interruption in the upgrade process may result in instability.

Upgrade Management Center Failover Pair
During replication, configuration for both the primary and secondary failover partners is limited. Replication requires that both the primary and secondary partners run the same version of Management Center. To ensure they are on the same version, the installed-systems CLI command is disabled on both failover partners (to deny installing and changing system images).

To upgrade a Management Center failover pair, you must first back up the configuration, export it off box, and then disable the failover pair. For full details, refer to About Management Center Failover.
Upgrade from 2.3.x or 2.4.x

Management Center supports upgrade from two previous versions of what is running. (In this case, 2.3.x and 2.4.x).

1. Before you begin, backup your Management Center configuration and export it off-box. If you must recover from a failed upgrade, you use this backup.
2. Access the Broadcom Support portal.
   Follow the instructions in the Getting Started guide to learn how to download your software and retrieve license keys.
   
   **NOTE**
   If you are upgrading Management Center on AWS, use only aws.bcsi images.
3. Download the desired image.
   a. Transfer the image directly to Management Center. Select Configuration > Files and transfer the image using the Transfer File button.
   b. Download the image to a local drive, select Configuration > Files, and upload the image to Management Center. Alternatively, you can store the image file on a web server that the Management Center appliance can access. The add image process works with any HTTP server, and HTTPS servers configured with trusted certificates. If your HTTPS server does not have a trusted certificate, place the file on an internal HTTP server.
   
   **NOTE**
   If you require HTTP service, enable it using the following command: (config)# security http enable For security reasons, you should immediately disable the HTTP service after retrieving the system image.
4. Add the system image using the \# installed-systems load <URL> command.
   
   **NOTE**
   By default, the URL provided is in HTTPS. If your Management Center does not have a signed HTTPS certificate, installation of the image from the HTTPS URL provided will fail. If that is the case, follow step 4b to modify the provided URL To use HTTP and port 8080 instead.
   
   where <URL> is the location of the image on a web server, in the following format:
   
   http://host/path, for example, http://webserver.mycompany.com/images/542386.bcsi
   
   If the image was uploaded to Management Center, complete the following steps:
   
   a. Copy the file URL. In the Configuration > Files page, select the image and click Copy URL. The file has a format similar to the following example:
      
      https://10.131.38.36:8082/fs/download/6c80d3a2cc124347aedb2a688da3859e
   b. Change the protocol to HTTP and the port to 8080. The URL should now look like this:
      
      http://10.131.38.36:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e
      
      If HTTP access to Management Center is disabled, you should change the URL to the following format:
      
      http://localhost:8080/fs/download/6c80d3a2cc124347aedb2a688da3859e
   c. Execute the installed-systems load command and wait for upgrade to complete.
5. Reboot the hardware appliance to run the new image:
   
   \# restart
   
   When the appliance restarts, the network connection closes. If boot failure occurs upon an upgrade, Management Center downgrades to the previous version automatically.
6. Access the web-based management console at https://management_center_ip/8082
7. Access the CLI using an SSH client.
8. If necessary, disable TLS versions prior to TLSv1.2:
   
   (config)# ssl edit ssl-context default

   (config ssl-context default)# protocols view

   tlsv1.2 tlsv1.1 tlsv1
(config ssl-context default)# protocols remove tlsv1

  ok

(config ssl-context default)# protocols remove tlsv1.1

  ok

**Downgrade Management Center**

Downgrading has the following special guidelines that you must follow:

- Downgrades cannot be performed from Management Center 3.x to 2.x or 1.x.
- All maintenance/patch releases of a version are treated as equivalent. For example, 1.6.2.1 would be the same as any other 1.6.x release.
- Upon downgrade, newer data (data from the upgraded image that is not supported in the older version) is lost.
- Upon downgrade, newer configuration settings (settings from the upgraded image that are not supported in the older version) are lost.
- Data and configuration settings that are common to the upgraded image and downgraded image are seamlessly maintained, regardless of schema differences between versions.
- Administrator access and permissions are required to downgrade Management Center.

To downgrade:

1. **Back up** Management Center
2. Decide which installed image to revert to. (Make sure to follow the guidelines noted previously regarding release numbers.)
   
   # installed-systems view
   
   Make note of the index value next to the image you want to revert to.
3. Make an older image the default image. (Make sure to follow the guidelines noted previously regarding release numbers.)
   
   # installed-systems default <index_number>
   
   Replace <index_number> with the image's index ID value.
4. Reboot the hardware appliance to activate the default image:
   
   # restart

**Restore a Management Center Backup Configuration**

You can restore a configuration backup after reinstalling, upgrading, or downgrading Management Center or if you want to revert to a previous configuration. You perform this operation using the command-line interface.

**NOTE**

Restoring a backup requires shutting down services; you should perform the restore during off hours.

**Restore Management Center Backup**

Before you restore a backup, you should view the backup files currently stored on the system to make sure that you restore the correct version. If the backup you want to restore was exported to an external server, you should import the backup file before the restore process.

1. **Access the Management Center CLI.**
2. Enter enable mode, then configuration terminal mode.
3. At the command prompt, type the following command and press Enter: 

```
(config)# backup view
```

The CLI displays a list of all the backups that were created for this instance of Management Center. You should see a response similar to the following:

```
Statistic Monitoring Trend Data : false, Size : 4.6 MB
Description : none
2. Version : 2.0.0.0 (214174-Debug), Creation Time : 2018-02-23 19:03:00 UTC
Statistic Monitoring Trend Data : false, Size : 2.7 MB
Description : before upgrade to 2.0
3. Version : 2.0.0.0 (216160), Creation Time : 2018-03-27 13:26:56 UTC
Statistic Monitoring Trend Data : false, Size : 2.7 MB,
Description : none
```

The backups are listed in descending chronological order; for example, the backup with index number 1 is more recent than index 2. Each backup indicates the date and time when the backup was created, the build version, and in parentheses, the build number.

4. Once you identify the backup you want, make note of the index number.

5. (Optional) If the backup you want to restore was exported to a server and is not on the list of backups stored on the appliance, you can import it to Management Center.

```
(config)# backup import <URL>
```

<URL> is the URL of the server and path to the backup file. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP.

6. At the command prompt, type the appropriate command.
   - To determine the restore point you want to use:
     `(config)# backup restore view`
   - To restore a specific version: 
     `(config)# backup restore <index_number>` where `<index_number>` is the index number of the backup.

7. Press Enter. The CLI indicates that you are about to restore a backup and asks you to confirm the action:

```
Warning, restoring a backup replaces all Management Center configuration.
Do you wish to proceed with restoring the backup taken on 2018-Mar-29 03:33:00 UTC? [yes, no]
```

8. Type Y to proceed. The CLI displays the progress of the restore:

```
Restoring backup ...
Decompressing ...
Verifying backup contents ...
Shutting down services ...
Restoring database ...
Restoring configuration ...
Restarting services ...
Completed restoring backup.
```

### Upload Files to Management Center

Use the Configuration > Files page to add files to Management Center. These files can be used for various operations, including upgrading Management Center.

All file types except .exe can be uploaded. If you upload a file with one of these extensions: .bcl, .bcsi, .nru, .nsu, .pac, .patch, .si, .txt; the file is automatically associated with the proper file type—config, image, license, text. If the file type is not one of the preceding, Management Center labels it as unknown.

You can limit the actions users are allowed to perform on this page by adding the File permission to a new or existing role.

**NOTE**

Management Center replaces special characters in file names.
Upload Files

1. Select **Configuration > Files**.
2. Add the file using one of the following methods:
   - By browsing:
     a. Click **Add File**.
     b. Click **Select File** and browse to the file(s).
     c. Select the file.
     d. Click **Open**.
     e. Click **Upload**.
   By dragging and dropping one or more files:
     a. Click **Add File**.
     b. Drag and drop the files into the **Upload Files** window
     c. Click **Upload**. If a file with same name already exists, the system prompts you to choose whether to upload and replace the existing file, skip the download, or to keep both and upload the file with a new name. If the upload will exceed the available space on disk, you are prompted to delete files to make room for the new file.
3. Management Center indicates the progress of the upload.

Transfer Files

Click **Transfer File** to retrieve files from a URL.

Files

1. Click **Transfer File**. The system displays the File Transfer window.
2. Enter the URL into the Server URL field.
3. Select the File Type.
4. Select the behavior to occur if the file already exists.
5. Click Run Now to start the job immediately or create a scheduled job.

**Associate File with Device Type**

If you upload an image file with the intention of upgrading one of your managed devices, you must associate the file with a device type.

1. Select the file.
2. Right click the Device Type field in that row and click Edit.

The system displays the Edit File window.
3. Select the device type from the Device Type drop-down.

Show screen.
4. Click **Save**.

**Other Operations**

**Edit Uploaded File**
See [Edit Uploaded File Properties](#).

**Change the File URL**
See [Change File URL](#).

**Set File Access Control**
See [Set File Access Control](#).

**Sort, Group, and Modify Uploaded File Data**
Click the arrow to the right of the column headings to sort and group uploaded files.
Hover over **Columns** to change the displayed columns. Select **Group by this field** to group the table data in accordance with that column heading. Deselect **Show in groups** to put data into a plain list.

**Delete Uploaded Files**

To delete a file, select the file and click **Delete**.

**Copy File URL**

To copy the file's URL, click **Copy URL**. The URL opens in a small sub-window. You can then right-click the URL and select **Copy** or enter CTRL-C to copy the URL. You can then paste the URL into Management Center CLI commands (for example, installing a new image), and other options or operations that accept URLs.

**Edit Uploaded File Properties**

1. This topic describes how to edit files contained in **Configuration > Files**. To edit a file, select the file and click **Edit**. The system displays the **Edit File** dialog. Here, you can edit the following:

   - **Display Name**
   - **File Type**
   - **Device Type**
   - **Resource ID**

   For the **Resource ID**, you must enter a string of alpha numeric characters (maximum of 36 characters) which can be used to reference the file.
• The Resource ID needs to be unique; you can't have the same resource ID for two separate files.
• The resource ID can't be an empty string.
• Special characters are not allowed.
• The changes you make in this field are reflected in the file URL.

• Access Control
  For information on setting access control, see Set File Access Control.

• Description

2. After making the desired changes, click Save.

Set File Access Control
This topic describes how to set access control for files contained in Configuration > Files. You can only set access controls for downloading files. File uploads are always over HTTPS and authenticated.

1. Select the file and click Edit.
2. Click the Access Control pulldown menu and select the desired permission.
   • ALL: This setting allows downloading using HTTPS or HTTP without authorization. (The default setting is All.)
   • AUTHENTICATED: This setting only allows file downloading over HTTPS. To download files, you must be authenticated to Management Center. If you have generated an API token for your user ID, you can use your API credentials.
   • NONE: This setting blocks all access to download files from /fs/download. The Copy URL setting is not available on the UI when the access is set to NONE.

3. Click Save.

Change File URL
This topic describes how to change the file URL for files contained in Configuration > Files. By default, the last part of the file URL is a random string of alphanumeric characters. For example: https://198.51.100.24:8082/fs/download/a57a1aed5ac64c399a8d1877fc15bd8f
To make the URL more user friendly or descriptive, enter descriptive text in the Resource ID field.

1. Select the uploaded file and click **Edit**.
2. Add or change the text to the Resource ID field.
3. Click **Copy URL**. The URL should now reflect the text you entered in step 2.

### Schedule File Transfer

Transfers a file to the system. If you have previously downloaded a file, such as a configuration, image, license, text, or other file, and you want it on the new system, this option loads it.

1. Select **Jobs > Add > New Job**.
2. On the Add New Job page, select **File Transfer**.
3. **Configuration**:
   - **Server URL**: Enter the URL of the file. Supported protocols include http/https.
   - **File Type**: Specify the file type.
   - **If the file already exists**: Choose what to do if the file already exists.
4. **Job Results**:
   - (Optional)—Click **Email results** and select the condition. Then, enter the email address(s) of the recipient(s).
5. **Schedule**:
   - Choose to trigger job execution using a **Schedule** or an **Event**.
   - **Schedule**
     - Use **Schedule** when you want to run the job now or to execute the job at a specific time.
     - **Immediate**—automatically runs the job after it is created.
     - **No Schedule**—no specific time or day is specified; when you are ready to run the job, use the **Run Now** button to execute the job.
     - **Run Once Only**—specify the date and time to run the job.
     - **Periodic**—runs the job every $x$ number of minutes, hours, or days, starting at the specified time and date.
     - **Daily**—runs the job every day at the specified time.
     - **Monthly**—runs the job once a month on the specified day of the month and specified time of day.
   - See also **Job Scheduling Options**.
   - **Event**
     - Use **Event** when you want to trigger the job execution when something happens, such as adding a device to a specific group. You can select one or more of the following events:
     - **Device added to Management Center**
     - **Device added to Group**
     - **Device removed from Group**
   - If you select more than one event type, the job runs if any of the conditions are met and the device is an appropriate target. See the following note.
     - **NOTE**
       If a device cannot be a target for a job (for example, a Content Analysis device in a **Collect Sysinfo** job), it is ignored.
6. **Name**:
   - Verify or change the name and add an optional description.
7. Click **Save**.
About Management Center Failover

Management Center supports failover using two physical appliances. One appliance is delegated as the *primary* and the other as the *secondary*. After failover is configured, the secondary replicates data from the primary appliance. During continuous replication, users can perform all normal operations on the primary failover partner. Users cannot access the secondary failover partner—its sole purpose is to replicate actions occurring on the primary node so that it can take over if something happens to primary node.

Because the secondary failover partner replicates the data on the primary partner, it is ready to take over if the primary failover partner becomes unresponsive.

Management Center supports three failover methods:

- The vMotion feature of ESX: This method is recommended. If you have vMotion in your installation, Symantec recommends that you use it instead of the manual failover support that is described in this topic. See Verify VMware Requirements for more information.
- Manual failover mode: If you use this method, you must manually log into the secondary failover partner and configure it to be the primary failover partner.
- Automatic failover mode: If you choose this method, failover automatically occurs after the timeout value (set during failover configuration) expires.

Virtual IP Address Support

Using a virtual IP address allows users and devices to access the correct Management Center appliance in all cases—whether an appliance has failed over or not. A common use case is statistics monitoring (see View Statistics Monitoring Reports), in which devices are configured with a virtual IP address to send data back to Management Center. Assigning a virtual IP address is not required for failover. However, using a virtual IP address enables the secondary failover partner to accept requests on that virtual IP-address when the primary failover partner is unresponsive.

Virtual IP address assignments are supported for on-premises and AWS deployments. Adding a virtual IP address is described in Configure the Primary Failover Partner and Configure the Secondary Failover Partner.

Important Failover Notes

- A one-time authorization token is required to set up failover in Management Center 2.x and later. The token is generated during the configuration of the primary partner and is good for 24 hours. See Configure Failover.
- For systems setup in failover, the data encryption key is kept in sync between the primary and secondary devices.
- Management Center supports multiple network interfaces. Symantec recommends that failover partners communicate over a separate channel.
- You can use IPv6 for failover communication in Management Center 2.x and later.
- If you intend to upgrade the failover pair, you must first disable failover. After upgrade, you can then reestablish failover.
- A Management Center assigned as the secondary partner can only be accessed by users logging in with the admin account. For example, to make the secondary partner the primary, you must be logged in with the admin account. See Add Local Users for more information.

Failover Limitations

This topic describes limitations with Management Center failover.

Failover Configuration Limitations

During replication, configuration for both the primary and secondary failover partners is limited. Replication requires that both the primary and secondary partners run the same version of Management Center. To enforce this, the installed-
CLI command is disabled on both failover partners (to deny installing and changing system images). If, for any reason, the system images do not match on the primary and secondary partners – replication is paused until the problems are resolved.

The secondary failover partner has stricter restrictions on what can be configured. In addition to not being able to manage system images, the following CLI commands are disabled on the secondary partner:

- `backup` (all commands)
- `license` (all commands)
- `http-proxy` (all commands)
- `service db-maintenance`
- `service purge-vpm-cache`
- `snmp` (all commands)
- `statistics-monitoring` (all commands)

Device Limitations

Because Web Security Service (WSS) devices are initially registered through a connection established only with the primary partner (which subsequently discards the credentials), WSS connections will fail if an event causes a failover to the secondary partner. In that event, you must re-authenticate to those WSS devices (Network > Edit Device > Connection Parameters).

Data Replicated Between Failover Partners

What is Replicated?

The following data is replicated on the failover partner:

- Device data stored in the database
- Files in the Management Center file store
- Policy and scripts (along with historical versions)
- Device backups
- PDM data from ProxySG appliances
- Data protection key
- Trusted certificates for servers; root CA installed by a user
- The following configuration settings in Administration > Settings:
  - General
  - Housekeeping
  - Mail Settings
  - Consent Banner
  - Hardware Monitor Settings

Optional Replication

The user can also choose to replicate the following settings on the secondary failover partner:

- Authentication (Active Directory/LDAP/RADIUS) configuration
- Logging and SNMP/SMTP alert configuration
- Access Control List (ACL) configuration

See failover for more information.

Data Not Replicated

- Licensing and system settings
- Backups for Management Center
- Network-related configuration, with exception of virtual IP addresses
Configure Management Center Failover

Management Center Failover Prerequisites

To prepare for failover:

- Determine your failover mode: automatic or manual.
- Identify a Management Center appliance to act as the primary failover partner. Record the IP address and password of the "admin" account of this device.
- Identify a Management Center appliance to act as the secondary failover partner. Record the IP address and password of the "admin" account of this device.
- Determine whether to use a virtual IP address in your manual or automatic failover configuration. If you want to use a virtual IP address, obtain an unused IP address within the primary subnet of the failover partner. Use the virtual-ip command to create a virtual IP address on the primary failover partner. Then, assign that same virtual IP address as the primary IP address of the secondary failover partner.
- If you assign a virtual IP address to the primary failover partner, you must allow the Virtual Router Redundancy Protocol (VRRP) to be used between the failover nodes.
- AWS: If you are deploying automatic failover within AWS, the AWS role that is attached to your instance must allow you to assign or unassign private IP addresses. Otherwise, the virtual IP address will not switchover during a failover event. For example:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```
• Ensure you have a method for recording the one-time authorization token that is generated while configuring the primary appliance. This token is required for configuring the secondary appliance.
• Ensure that port 2025 is open between the primary and secondary partners. Management Center failover employs an SSH connection.
• Ensure that DNS is working properly. SSH connections use RDNS; you must have a valid DNS setup for the pair when using failover.

Configure Management Center Failover:
1. Configure the **primary failover partner**.
2. Configure the **secondary failover partner**.

**Configure the Primary Failover Partner**

See [Configure Management Center Failover](#) for a list of prerequisites. You should decide whether you want to assign a virtual IP address to the primary failover partner. A good reason to configure a virtual IP address is that you do not need to reactivate statistics monitoring after you promote the secondary failover partner.

1. Use an SSH client to log into the CLI of the Management Center appliance that is to be the primary failover partner.
2. Enter Enable mode:
3. Enter Configuration mode:
4. Optional: If you want to configure a virtual IP address to the primary failover partner, do the following:
   The primary IP address can be any available IP address in the primary failover partner's subnet.
   ```
   (config)# virtual-ip address ip_address
   ```
   For example:
   ```
   (config)# virtual-ip address 192.0.2.24
   ```
   ```
   Virtual-ip:
   Status: running, this node has virtual-ip
   Address: 192.0.2.24
   Interface: 0:0
   Peer: not defined
   ```
5. Confirm that failover has not already been configured on the appliance:
   ```
   (config)# failover view
   ```
   ```
   Failover: Status: Disabled
   Primary*: 198.51.100.20
   Secondary: 0.0.0.0
   Token Expires: Mar 28, 2018
   Last status update 1 second(s) ago
   (*) this Management Center
   ```
   Please record authentication token for setup with primary and press Enter.
6. Make this appliance the primary failover partner. This process generates a one-time authentication to be used for configuring the secondary partner.

   The command output is similar to the following:
   ```
   One-time initial authentication token for secondary node: 58f1ddaa6f878f96
   ```

   ```
   Failover:
   Status: ERROR: Secondary not configured
   Primary*: 198.51.100.20
   Secondary: 0.0.0.0
   Token Expires: Mar 28, 2018
   Last status update 1 second(s) ago
   (*) this Management Center
   ```
   Please record authentication token for setup with primary and press Enter.

   Because the secondary failover partner has not been configured, the failover icon displays with an exclamation mark:
NOTE
This icon also displays if failover has been configured and the secondary is unresponsive.

Configure the Secondary Failover Partner

Complete all tasks that are required for the secondary appliance to service requests (set up authentication, and so on), before beginning this procedure. You must also have the token that is generated by the primary appliance during failover configuration. For more information about the token and other prerequisites, see Configure Management Center Failover.

1. Use an SSH client to log into the CLI of the Management Center appliance that is to be the secondary failover partner.
2. Enter Enable mode: `# enable`
3. Enter Configuration mode: `# configure`
4. Confirm that failover has not already been configured on the appliance:
   ```
   (config)#
   failover view
   Failover: Status: Disabled
   ```
5. Enter the following command to begin configuring the secondary failover partner:
   ```
   (config)#
   failover make-secondary
   ```
6. When prompted for the value of 'primary-ip', enter the IP address of the primary failover partner.
   Example:
   ```
   Value for 'primary-ip' (<IP address>): 198.51.100.20
   ```
7. Enter the token generated by the primary appliance during failover configuration. For more information, see Configure Management Center Failover.
   ```
   Value for 'token' (): ****************
   ```
8. Specify the type of failover mode, automatic or manual.
   ```
   Value for 'failover mode' (automatic, manual):
   ```
   If you specify automatic, you must now choose a timeout value:
   ```
   Please enter the minutes to wait if primary goes down before automatically switching to secondary. [1 - 120] minutes?
   ```
9. When prompted to continue, enter Yes and wait for failover setup to complete.
   ```
   Warning: Initial failover data transfer may take a long time to complete. To complete the failover setup, allow for transfer to finish and do not disable failover on 198.51.100.20 (primary) or 198.51.100.21 (secondary) during this operation.
   Are you sure you want to continue? [yes, no] yes
Configuring primary...done.
Stopping services on secondary...done.
Retrieving content repository and file artifacts...done
Preparing database for replication...done

(!) Authorization changes completed - forcing logout.

Failover:
  Status:          Healthy (100% of initial sync complete. Sequence IDs: [EEB2C68, EEB2C68])
  Primary:         198.51.100.20
  Secondary*:      198.51.100.21
  Replicating:
    ACL Configuration:        false
    Authentication Configuration: false
    Diagnostics Configuration: false
    Mode:                      automatic
    Timeout (minutes):         4
    Virtual IP:                checking status...
  Last status update 0 second(s) ago

(*) this Management Center
(config-failover)# Connection to 198.51.100.21 closed.

10. Verify that failover has been successfully configured:
(config-failover)# view
Failover:
  Status:          Healthy (1 second replication delay)
  Primary+:        10.47.192.80
  Secondary*:      10.47.192.81
  Replicating:
    ACL Configuration:        false
    Authentication Configuration: false
    Diagnostics Configuration: false
    Mode:                      manual
    Virtual IP:                true
    Address:                  10.47.192.85
    Interface:                0:0
  Last status update 3 second(s) ago

(*) this Management Center
(+) has virtual-ip

If failover has been successfully configured, the failover icon displays in the web UI banner:

![Failover Icon](image)

You can also mouse over the failover icon to review the failover status.
11. Optional—Use the CLI to configure other replication settings.

```
# failover replicate ?
```

See `failover` for more information.

**Manual Failover: Switch to Secondary When the Primary is Unresponsive**

**On the Secondary Failover Partner:**

1. Log into the secondary failover partner using the CLI admin account of the device. See Add Local Users for more information.

2. Enter Configuration mode and issue the `failover make-primary` command to make the secondary appliance the primary failover partner. If the original primary device later becomes responsive, you can make it the secondary failover partner, thus preserving the failover capability.

   ```
   (config)# failover make-primary
   System is configured as secondary, promoting state to primary will break replication.
   Are you sure you want to promote state to primary? [y/N]
   Restoring operational data...done. Failover: Status: ERROR: Secondary not configured
   Primary*: 198.51.100.24
   Secondary: not configured
   Last status update 2 second(s) ago (*) this Management Center
   ```


   **NOTE**
   You do not have to reactivate statistics monitoring if a virtual IP address was configured on the primary failover partner and managed devices are configured to use a virtual IP address to send statistics data to Management Center (see Reactivate Statistics Monitoring). For additional information, see About Management Center Failover.

Reactivate the statistics monitoring job after making the secondary failover partner active. This job instructs devices that have PDM Export (statistics monitoring) enabled to send updates to the new primary device.

a) Select **Jobs > Scheduled Jobs**.
b) Click **New Job**. The system displays the New Job: Basic Info dialog.
c) In the Basic Info dialog, enter a name for your job. Enter a description of the job. Good descriptions help to differentiate jobs when they have similar names.
d) Click **Next**.
e) In the Operation dialog, select **Reactivate Statistics Monitoring**.
f) Click **Next**. The system displays the **Targets** dialog. Management Center automatically finds all applicable targets.
g) Click **Next**. The system displays the **Schedule** dialog.
h) Optionally, enter a schedule.
i) Click **Finish**.

**On the Original Primary Device:**
4. Fix the problem on the original primary failover partner.

5. On the original primary failover partner, enter Configuration mode and make it (the device that was unresponsive) the new secondary failover partner:

   (config)# failover make-secondary

**Automatic Failover: Switch to Secondary When the Primary is Unresponsive**

**Automatic Failover With a Virtual IP Address**

If you have configured a virtual IP address on the primary failover partner, no other actions are required to promote the secondary failover partner to primary. Everything is done automatically.

**Automatic Failover Without a Virtual IP Address**

If you have not configured a virtual IP address on the primary failover partner, you must create a job to reactivate statistics monitoring (PDM export).

1. To reactivate statistics monitoring, select Jobs > Scheduled Jobs.
2. Click New Job. The system displays the New Job: Basic Info dialog.
3. In the Basic Info dialog, enter a name for your job. Enter a description of the job. Good descriptions help to differentiate jobs when they have similar names.
4. Click Next.
5. In the Operation dialog, select Reactivate Statistics Monitoring.
6. Click Next. The system displays the Targets dialog. Management Center automatically finds all applicable targets.
7. Click Next. The system displays the Schedule dialog.
8. Optionally, enter a schedule.
9. Click Finish.

**Configure SNMP Trap or SMTP Notification for Failover Alerts**

You can configure an SNMP alert and/or SMTP notification to notify you when there is an error in the failover state. When configured, the health check runs every 60 seconds to determine the health of the failover configuration. Possible error states include:

- Secondary not configured
- Host that is not configured as failover partner
- Partner IP address is not active

If the health check encounters a failover error, it checks two more times before it confirms the error. If the health check confirms the error, a trap is sent and the health check resumes. When the failover pair is healthy again, the health check sends another trap indicating that the problem has been resolved.

**NOTE**
The failover health check can be configured only from the Management Center CLI. You cannot configure this option using the user interface.

**Configure Failover Health SNMP Trap**

To receive an SNMP trap when the health check detects a failover error, you must configure the following settings from the Management Center CLI: SNMP community name, vacm view, vacm, group, vacm access, notify target name, and notify target IP address. Then, you must enable the SNMP agent.

Example SNMP Trap Configuration
(config)# snmp community public
(config-community-public)# exit
(config-snmp)# vacm view bc subtree 1.3 included
(config-snmp)# vacm group public member public sec-model v2c
(config-snmp)# vacm group public access v2c no-auth-no-priv notify-view bc read-view bc write-view bc
(config-snmp)# notify target1 type trap tag target1
(config-snmp)# target target1 ip 192.0.2.14 tag target1 udp-port 162 v2c sec-name public
(config-snmp)# agent enable

NOTE
The SNMP failover health trap uses the BLUECOAT-SG-HEALTHMONITOR-MIB, which is included in the BLUECOAT-MIB. You can download these MIBs on the Download site.

Configure Failover Health SMTP Notification
To receive an SMTP trap when the health check detects a failover error, you must configure the following settings from the Management Center CLI:

(config)# smtp
(config-smtp)# destination-address add address
(config-smtp)# from-address address
(config-smtp)# gateway gateway

Example SNMP Trap Configuration

(config)# snmp community public
(config-community-public)# exit
(config-snmp)# vacm view bc subtree 1.3 included
(config-snmp)# vacm group public member public sec-model v2c
(config-snmp)# vacm group public access v2c no-auth-no-priv notify-view bc read-view bc write-view bc
(config-snmp)# notify target1 type trap tag target1
(config-snmp)# target target1 ip 192.0.2.14 tag target1 udp-port 162 v2c sec-name public
(config-snmp)# agent enable

NOTE
The SNMP failover health trap uses the BLUECOAT-SG-HEALTHMONITOR-MIB, which is included in the BLUECOAT-MIB. You can download these MIBs on the Download site.
Upgrade the Failover Pair

Upgrading is a complex procedure. Please review the document Upgrade Management Center before starting this procedure.

1. Back up the primary partner.
   Back up the Primary partner's configuration and export it off-box to a secure location before upgrading your failover pair. See Back Up the Management Center Configuration. You do not need to back up the Secondary partner.

2. Disable Failover on the primary and secondary partners.
   Complete the following procedure on both the Primary and Secondary failover partners before upgrading.
   a) Log into the CLI, enter configuration mode and enter the following command: (config)# failover
      b) Enter the following command to disable the Primary partner: (config-failover)# disable
         The system terminates the CLI session when you run the disable command.

3. Log back into the CLI and enter the following command to verify that failover has been disabled: (config-failover)# view

4. Download the system image on both primary and secondary partners using one of the following methods:
   - Transfer the image directly to Management Center. Select Configuration > Files and transfer the image using the Transfer File button.
   - Download the image to a local drive, select Configuration > Files, and upload the image to Management Center.
   - Alternatively, you can store the image file on a web server that the Management Center appliance can access. The add image process works with any HTTP server, and HTTPS servers configured with trusted certificates. If your HTTPS server does not have a trusted certificate, place the file on an internal HTTP server.
     If you require HTTP service, enable it using the following command: (config)# security http enable. For security reasons, you should immediately disable the HTTP service after retrieving the system image.

5. Upgrade both primary and secondary partners.
   Follow the procedures in Upgrade Management Center to upgrade the Primary and Secondary partners.

6. Re-enable failover on both primary and secondary partners.
   Follow the procedures in Configure Management Center Failover to re-enable failover on the Primary and Secondary partners.

Disable Failover

Use the failover disable command to disable failover.

(config)# failover disable

   Failover: Status: Healthy (0 second replication delay)
   Primary: 198.51.100.20
   Secondary*: 198.51.100.24
   Last status update 2 second(s) ago  (*) this Management Center
   Are you sure you want to disable failover? [y/N]
   Restoring operational data...done. Failover: Status: Disabled

View Failover Health Check Logs

Navigate to the following directory to view failover health check logs:
/var/log/user_syslog
Update the Management Center License

NOTE
The Management Center license contains all of the features for which you have purchased a subscription. The documentation covers all features, including ones that you may not have purchased.

NOTE
The Management Center license contains all of the features for which you have purchased a subscription. The documentation covers all features, including ones that you may not have purchased.

NOTE
The Network Protection Licensing Portal (NPLP) has been replaced by MySymantec.

You can update your existing license from MySymantec, download the license from a web server or workstation, or install it manually.

License Update Procedure

1. To view license status or to update or install a license, select Administration > License.
2. To view detailed license component information, select the License Components tab.
   
   NOTE
   Use the passphrase field when you are installing a license you generated with a passphrase; the passphrase is required for VA Offline licensing.

3. Install the license using one of the methods shown in the Install New License tab.
   See Install the license from MySymantec using the Management Center web console, Install the license from URL, or Paste license text from a text editor for instructions.

4. (Optional) To troubleshoot the license installation, do the following:
   – To check the status of a license, run the CLI command licensing view.
   – To verify network settings, run the following CLI commands:
     • # show running-config interface
     • # show running-config ip
     • # show running-config dns
   – To verify site accessibility, run the CLI command ping with the following sites:
     • ping bto-services.es.bluecoat.com
     • ping validation.es.bluecoat.com
   – To update the license, run the CLI command (config)# licensing load.
   – Try to update the license again, after running the CLI command #restart.

5. (Optional) From a web browser, log into Management Center. If the web console loads, the license was installed successfully. If the web console does not load, run the CLI command #licensing view to determine if the license was installed and is valid.

Install the license from MySymantec using the Management Center web console

1. Select Administration > License.
2. Click the Install New License tab.
3. Select Install from NPLP.
4. Enter your MySymantec (formerly known as NPLP) user ID and password.
5. Click Install License.
6. Click Refresh to display the updated license information in the License Components table.

Manually download the license key from MySymantec

If your Management Center appliance does not have Internet access, follow the procedure below to manually download the license key from MySymantec. For more information on downloading a license, refer to the Getting Started web page.
Locate the appliance serial number in your shipping alert email.

1. Log in to your MySymantec account.
2. In the My Products list, locate the serial number of the appliance you want to license.
3. Generate a new key; this downloads the license file.

You can then Install the license from URL or Paste license text from a text editor.

**Install the license from URL**

Before you can install your license you must first get the license file (*.bcl or *.bin) from MySymantec (as described above) and save it to a location on a web server or workstation that the VA can access.

1. Select Administration > License.
2. Click the Install New License tab.
3. Select Install from URL. The web console displays a text field.
4. Enter the location (a valid URL) of the license file into the field.
5. Click Install License.
6. Click Refresh to display the updated license information in the License Components table.

**Paste license text from a text editor**

Before you can install your license you must first get the license file (*.bcl or *.bin) from MySymantec (as described above) and save it to a local directory. Open the license file in a text editor (such as Notepad) and make sure you save the file.

1. Select Administration > License.
2. Click the Install New License tab.
3. Select Paste license text. The web console displays a text box.
4. Copy and paste the license from the text editor to the box.
5. Click Install License.
6. Click Refresh to display the updated license information in the License Components table.

**Verify License Components from the Web Console**

Management Center has a flexible license model. Components can be licensed, and are exposed dependent upon the license type and component name. You can view the validity of licensed components, add more devices to your license, and view the serial number and appliance model of the hardware appliance. Install or update your licenses directly from NPLP while logged into the web console.

1. To verify the license components, type and status, log in to the web console.
2. Select Administration > License. From the License Component tab you verify the following General Information about the license:
   - Manufacturer (Symantec: A Division of Broadcom)
   - Number of Maximum Devices allowed
   - Serial Number
   - Appliance Model
   - Appliance Identifier (Enterprise licensed appliances only)
   - Status
   - Component Name
   - Activation date
   - Expiration date
   - License Type

**Next steps**

If you are deploying AWS, go to Step 5: Disassociate User Data from the Instance.
Migrate From Director to Management Center

To migrate a Symantec Director device hierarchy (including overlays) into Management Center, you need to export the device metadata from Director, placing the migration file in a location that Management Center can access.

Prerequisites:

• Obtain or verify access to the Symantec Director CLI.
• Obtain or verify access to an HTTP, SCP, or FTP server, and ensure that you have access privileges to upload data to it.
• Obtain or verify access to the Management Center web console.

Migration recommendations and limitations:

• Before you begin, push all pending policy changes from Director to your devices to ensure that all devices have the latest configuration.
• Remove any devices from your Director configuration that are no longer in use.
• Remove any overlays that include policy, as Management Center cannot import them. Once migrated, Management Center can pull existing policy from these devices.
• Make note of jobs that you run on a regular basis, as Director jobs will not import to Management Center.
• Profiles are also not imported in the migration from Director to Management Center. Rather, this functionality can be recreated using scripts to create a proper image of your devices to use as a generic source for your configuration file updates.
• Device configurations can be imported into a Management Center script directly from each device post-migration.

Export Metadata from Director as an Encrypted File

1. Log into the Director CLI and go into config mode.
2. Type the following command to generate the migration file:
   (config)# mc-migration generate
   The CLI prompts you to enter a passphrase. You will be required to enter this passphrase to generate the metadata and import it in the Management Center application.
3. Enter a passphrase consisting of at least four characters and press Enter.
   The CLI generates the device metadata. The metadata is encrypted and compressed in a Gnu Privacy Guard (GPG) encrypted (*.tgz.gpg) file. For example: SGME-Director-to-MC-Migration-2015.03.13-154907.tgz.gpg. Make note of the filename.
4. Upload the compressed and secured file to an external HTTP, SCP, or FTP server. Enter the command:
   (config)# mc-migration upload file server
   where:
   file is the filename you recorded in the previous step.
   server is the hostname or IP address of an external server:
   http://hostname_or_address[:port]/path_and_filename
   ftp://hostname_or_address/path_and_filename
   scp://hostname_or_address//path_and_filename

   NOTE
   If necessary, copy or move the file to a location that Management Center can access.

Import Director Metadata as Scripts into Management Center

From the Management Center web console, import the device metadata file that is currently saved on an external server.

1. Log into the Management Center web console.
2. Click the **Network** tab.
3. Select **Operations > Import from File**. The web console displays the Import from File dialog.

**Show screen.**

4. Select the **Import from file exported from an external system** check box, then click **Launch Import Wizard**.
5. On the Import from File: Select File dialog, select the file that you want to import. The **GPG encrypted file** check box is selected by default for (*.gpg) files. Clear the check box if your file is not encrypted (*.tar.gz or *.tgz format).

**NOTE**
Files must have the extensions *.gpg* (Gnu Privacy Guard [GPG] encrypted compressed file), *.tar.gz, or *.tgz (unencrypted compressed files).

6. If necessary, enter the passphrase that you specified when generating an encrypted file, then click **Next**.
7. Select devices and device groups to import from a hierarchy. If any device is not a member of a hierarchy, a **pseudo-hierarchy** is available, named **Unassigned**. If any errors or warnings exist, for any device, the status is shown on the right. To select all devices in all hierarchies, select **All Hierarchies**.
NOTE
A device can only exist in one group for a given, distinct hierarchy. Devices can be members of different hierarchies.

8. The available scripts show on the Import from File: Select Scripts dialog. By default, all scripts are selected. Clear the check box for any script you do not want to import. When finished selecting scripts, click **Import**.
Any ProxySG appliances that are running SGOS 5.x are imported in a deactivated (pre-deployment) status.

9. The Import from File wizard displays the Device Import Status dialog. The Overlays Summary and list of imported overlays show at the bottom. When finished viewing the import status, click Close.

10. View the successfully migrated devices, device groups, and hierarchies in the Management Center Network tab.

11. View imported overlays by selecting Configuration > Scripts

(Optional) Delete Migration File in Director
After you have successfully imported devices from Director, you can delete the migration metadata file from Director.

1. Log in to the Director CLI.
2. Type the following command:
   
   (config)# mc-migration delete file

   where file is the name of the migration file.

After the file is deleted, the CLI displays the (config)# prompt again.

**Determine Your Next Step**

<table>
<thead>
<tr>
<th>What do you want to do next?</th>
<th>Refer to this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that all devices belong to a hierarchy and group</td>
<td>Ensure Devices Belong to Device Groups</td>
</tr>
<tr>
<td>Change device information</td>
<td>Edit a Device</td>
</tr>
<tr>
<td>Check device metrics</td>
<td>View System Metrics</td>
</tr>
</tbody>
</table>

**Display Local Time on Management Center**

Use the options on this page to display the local timezone on the Management Center user interface Dashboard.

**NOTE**

This setting applies only to displaying the local time on the Management Center dashboard. It does not affect any other time zone settings on Management Center.

**Display Local Time on Management Center User Interface**

1. Go to Administration > Settings > Time Zone.
2. Select Display local time on Dashboard.
3. Set the desired time zone in the Local time zone option.
4. Click Save.
5. Navigate back to the Management Center Dashboard to view the changes.

**Management Center: SNMP Monitoring Best Practices**

Systems and network administrators are challenged with ensuring the reliability, stability, and availability of mission-critical systems in the corporate network. SNMP has made that task easier by making devices simpler to monitor, maintain, and upgrade. The network administrator is alerted about situations that require administrative attention, but even the best of appliances will need closer monitoring and observation when problems arise either in the network or in the application.

Management Center offers specific features (SNMP elements), which allow close resource monitoring for day-to-day informational use. It also provides information that allows users to prioritize network needs and to focus and allocate resources to maximize reliability.

Administrators need to determine when their Management Center is utilizing resources outside of normal operation ranges or is approaching the resource capacity limits of the system so that they can take appropriate corrective action.
This document defines a set of metrics that help characterize load conditions on Management Center appliances running MC 2.x or later and identifies the SNMP sources of statistics that enable monitoring of these resources.

**MIBs Used With Management Center**

Management Center uses private and standard MIBs. This document does not describe all of these MIBs. The information in this document provides information only about the MIBs that provide the best data for monitoring Management Center resources.

Refer to Management Center MIB Files for more information about the MIBs and how to download them.

**BLUECOAT-SG-SENSOR-MIB**

The SENSOR-MIB monitors the values of the various environmental sensors present on the appliance.

Parameters that you can monitor with the SENSOR-MIB include:

- Bus Temperature
- CPU Temperature
- Fan
- CPU Fan
- Bus Voltage
- CPU Voltage
- Power Supply

The SENSOR-MIB trap variables and their values are described in the following table.

<table>
<thead>
<tr>
<th>Trap Variable</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>deviceSensorName</td>
<td>The textual name of the sensor</td>
<td>---</td>
</tr>
<tr>
<td>deviceSensorUnits</td>
<td>The units of sensor measurements.</td>
<td>other(1), truthvalue(2), specialEnum(3), volts(4), celsius(5), rpm(6)</td>
</tr>
<tr>
<td>deviceSensorValue</td>
<td>Reports the most recent measurement seen by the sensor. Measurements are interpreted based on the deviceSensorUnits value.</td>
<td>other(1) - a measure other than those listed below truthvalue(2) - true(1), false(2) specialEnum(3) - user defined enumerated values volts(4) - electrical potential as a fixed point number celsius(5) - temperature as a fixed point number rpm(6) - revolutions per minute in nonnegative numbers</td>
</tr>
<tr>
<td>Trap Variable</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>deviceSensorCode</td>
<td>Interprets the deviceSensorValue.</td>
<td>ok(1) unknown(2) notInstalled(3) voltageLowWarning(4) voltageLowCritical(5) noPower(6) voltageHighWarning(7) voltageHighCritical(8) voltageHighSevere(9) temperatureHighWarning(10) temperatureHighCritical(11) temperatureHighSevere(12) fanSlowWarning(13) fanSlowCritical(14) fanStopped(15)</td>
</tr>
<tr>
<td>deviceSensorStatus</td>
<td>Indicates the operational status of the sensor.</td>
<td>ok(1) unavailable(2) nonoperational(3)</td>
</tr>
</tbody>
</table>

The error messages produced by the deviceSensorCode are described in the following table.

<table>
<thead>
<tr>
<th>Message</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK(1)</td>
<td>Normal</td>
</tr>
<tr>
<td>voltageLowCritical(5) noPower(6) voltageHighCritical(8) voltageHighSevere(9) temperatureHighCritical(11) temperatureHighSevere(12) fanSlowCritical(14) fanStopped(15)</td>
<td>Critical-Immediate attention is required.</td>
</tr>
<tr>
<td>unknown(2) notInstalled(3)</td>
<td>Minor</td>
</tr>
<tr>
<td>voltageLowWarning(4) voltageHighWarning(7) temperatureHighWarning(10) fanSlowWarning(13)</td>
<td>Warning</td>
</tr>
</tbody>
</table>

**Listing SENSOR-MIB Values From the CLI**

The Management Center CLI lists the current SENSOR-MIB values from the `enable` command level:

```
# enable Password: # show BLUECOAT-SG-SENSOR-MIB
```

```
<table>
<thead>
<tr>
<th>DEVICE</th>
<th>SENSOR</th>
<th>DEVICE</th>
<th>SENSOR</th>
<th>DEVICE</th>
<th>SENSOR</th>
<th>DEVICE</th>
<th>SENSOR</th>
<th>TIME</th>
<th>DEVICE</th>
<th>SENSOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDEX</td>
<td>TRAP</td>
<td>UNITS</td>
<td>SCALE</td>
<td>VALUE</td>
<td>Code</td>
<td>Status</td>
<td>STAMP</td>
<td>NAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>1</td>
<td>false</td>
<td>specialEnum 0 0</td>
<td>notInstalled</td>
<td>notInstalled</td>
<td>2677</td>
<td>PWR button1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>false</td>
<td>specialEnum 0 0</td>
<td>ok</td>
<td>ok</td>
<td>2677</td>
<td>PSU 2 status1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>false</td>
<td>specialEnum 0 16</td>
<td>noPower</td>
<td>ok</td>
<td>2677</td>
<td>PSU 1 status1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>false</td>
<td>specialEnum 0 0</td>
<td>notInstalled</td>
<td>notInstalled</td>
<td>2677</td>
<td>CPU CATERR1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>false</td>
<td>specialEnum 0 128</td>
<td>notInstalled</td>
<td>notInstalled</td>
<td>2677</td>
<td>CPU status1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>false</td>
<td>specialEnum 0 0</td>
<td>notInstalled</td>
<td>notInstalled</td>
<td>2677</td>
<td>Chassis opened1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>false</td>
<td>specialEnum 0 0</td>
<td>notInstalled</td>
<td>notInstalled</td>
<td>2677</td>
<td>BIOS2 Boot Fail1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>false</td>
<td>specialEnum 0 0</td>
<td>notInstalled</td>
<td>notInstalled</td>
<td>2677</td>
<td>BIOS1 Boot Fail1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>false</td>
<td>volts 0 0</td>
<td>notInstalled</td>
<td>notInstalled</td>
<td>2677</td>
<td>SSL VPTX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>I</th>
<th>Volts</th>
<th>RPM</th>
<th>Temp</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>false</td>
<td>0</td>
<td>0</td>
<td>notInstalled</td>
<td>SSL PLL</td>
</tr>
<tr>
<td>11</td>
<td>false</td>
<td>0</td>
<td>0</td>
<td>notInstalled</td>
<td>SSL core</td>
</tr>
<tr>
<td>12</td>
<td>false</td>
<td>-4</td>
<td>18228</td>
<td>ok</td>
<td>SAS IO</td>
</tr>
<tr>
<td>13</td>
<td>false</td>
<td>-3</td>
<td>1048</td>
<td>ok</td>
<td>SAS core</td>
</tr>
<tr>
<td>14</td>
<td>false</td>
<td>-3</td>
<td>1528</td>
<td>ok</td>
<td>PCH SAS</td>
</tr>
<tr>
<td>15</td>
<td>false</td>
<td>-2</td>
<td>112</td>
<td>ok</td>
<td>PCH core</td>
</tr>
<tr>
<td>16</td>
<td>false</td>
<td>-3</td>
<td>752</td>
<td>ok</td>
<td>Memory SAS</td>
</tr>
<tr>
<td>17</td>
<td>false</td>
<td>-3</td>
<td>1528</td>
<td>ok</td>
<td>Memory I/O</td>
</tr>
<tr>
<td>18</td>
<td>false</td>
<td>-3</td>
<td>1064</td>
<td>ok</td>
<td>CPU VT</td>
</tr>
<tr>
<td>19</td>
<td>false</td>
<td>-4</td>
<td>9212</td>
<td>ok</td>
<td>CPU sys agent</td>
</tr>
<tr>
<td>20</td>
<td>false</td>
<td>-3</td>
<td>1813</td>
<td>ok</td>
<td>CPU PLL</td>
</tr>
<tr>
<td>21</td>
<td>false</td>
<td>-4</td>
<td>9114</td>
<td>ok</td>
<td>CPU core</td>
</tr>
<tr>
<td>22</td>
<td>false</td>
<td>-3</td>
<td>1264</td>
<td>ok</td>
<td>BMC PLL</td>
</tr>
<tr>
<td>23</td>
<td>false</td>
<td>-3</td>
<td>1568</td>
<td>ok</td>
<td>BMC memory</td>
</tr>
<tr>
<td>24</td>
<td>false</td>
<td>-3</td>
<td>3072</td>
<td>ok</td>
<td>Battery</td>
</tr>
<tr>
<td>25</td>
<td>false</td>
<td>-4</td>
<td>50232</td>
<td>ok</td>
<td>+5V standby</td>
</tr>
<tr>
<td>26</td>
<td>false</td>
<td>-4</td>
<td>50508</td>
<td>ok</td>
<td>+5V main bus</td>
</tr>
<tr>
<td>27</td>
<td>false</td>
<td>-2</td>
<td>331</td>
<td>ok</td>
<td>+3.3V standby</td>
</tr>
<tr>
<td>28</td>
<td>false</td>
<td>-3</td>
<td>3328</td>
<td>ok</td>
<td>+3.3V main bus 2</td>
</tr>
<tr>
<td>29</td>
<td>false</td>
<td>-2</td>
<td>1196</td>
<td>ok</td>
<td>+12V main bus 1</td>
</tr>
<tr>
<td>30</td>
<td>false</td>
<td>-2</td>
<td>1196</td>
<td>ok</td>
<td>+1.1V standby</td>
</tr>
<tr>
<td>31</td>
<td>false</td>
<td>3</td>
<td>7</td>
<td>ok</td>
<td>Sys fan 6 rear</td>
</tr>
<tr>
<td>32</td>
<td>false</td>
<td>2</td>
<td>81</td>
<td>ok</td>
<td>Sys fan 6 front</td>
</tr>
<tr>
<td>33</td>
<td>false</td>
<td>3</td>
<td>7</td>
<td>ok</td>
<td>Sys fan 5 rear</td>
</tr>
<tr>
<td>34</td>
<td>false</td>
<td>3</td>
<td>8</td>
<td>ok</td>
<td>Sys fan 5 front</td>
</tr>
<tr>
<td>35</td>
<td>false</td>
<td>2</td>
<td>69</td>
<td>ok</td>
<td>Sys fan 4 rear</td>
</tr>
<tr>
<td>36</td>
<td>false</td>
<td>2</td>
<td>81</td>
<td>ok</td>
<td>Sys fan 4 front</td>
</tr>
<tr>
<td>37</td>
<td>false</td>
<td>3</td>
<td>7</td>
<td>ok</td>
<td>Sys fan 3 rear</td>
</tr>
<tr>
<td>38</td>
<td>false</td>
<td>2</td>
<td>81</td>
<td>ok</td>
<td>Sys fan 3 front</td>
</tr>
<tr>
<td>39</td>
<td>false</td>
<td>2</td>
<td>68</td>
<td>ok</td>
<td>Sys fan 2 rear</td>
</tr>
<tr>
<td>40</td>
<td>false</td>
<td>2</td>
<td>81</td>
<td>ok</td>
<td>Sys fan 2 front</td>
</tr>
<tr>
<td>41</td>
<td>false</td>
<td>2</td>
<td>69</td>
<td>ok</td>
<td>Sys fan 1 rear</td>
</tr>
<tr>
<td>42</td>
<td>false</td>
<td>2</td>
<td>81</td>
<td>ok</td>
<td>Sys fan 1 front</td>
</tr>
<tr>
<td>43</td>
<td>false</td>
<td>0</td>
<td>28</td>
<td>ok</td>
<td>DC PSU 2 fan R</td>
</tr>
<tr>
<td>44</td>
<td>false</td>
<td>0</td>
<td>28</td>
<td>ok</td>
<td>DC PSU 2 fan F</td>
</tr>
<tr>
<td>45</td>
<td>false</td>
<td>0</td>
<td>28</td>
<td>ok</td>
<td>DC PSU 1 fan R</td>
</tr>
<tr>
<td>46</td>
<td>false</td>
<td>0</td>
<td>28</td>
<td>ok</td>
<td>DC PSU 1 fan F</td>
</tr>
<tr>
<td>47</td>
<td>false</td>
<td>3</td>
<td>12</td>
<td>ok</td>
<td>AC PSU 2 fan</td>
</tr>
<tr>
<td>48</td>
<td>false</td>
<td>0</td>
<td>0</td>
<td>notInstalled</td>
<td>AC PSU 1 fan</td>
</tr>
<tr>
<td>49</td>
<td>false</td>
<td>0</td>
<td>28</td>
<td>ok</td>
<td>System R temp</td>
</tr>
<tr>
<td>50</td>
<td>false</td>
<td>0</td>
<td>25</td>
<td>ok</td>
<td>System L temp</td>
</tr>
<tr>
<td>51</td>
<td>false</td>
<td>0</td>
<td>31</td>
<td>ok</td>
<td>System C temp</td>
</tr>
<tr>
<td>52</td>
<td>false</td>
<td>0</td>
<td>0</td>
<td>notInstalled</td>
<td>SSL card temp</td>
</tr>
<tr>
<td>53</td>
<td>false</td>
<td>0</td>
<td>35</td>
<td>ok</td>
<td>SAS card temp</td>
</tr>
<tr>
<td>54</td>
<td>false</td>
<td>0</td>
<td>17</td>
<td>ok</td>
<td>PSU inlet temp</td>
</tr>
<tr>
<td>55</td>
<td>false</td>
<td>0</td>
<td>21</td>
<td>ok</td>
<td>PSU 2 core temp</td>
</tr>
<tr>
<td>56</td>
<td>false</td>
<td>0</td>
<td>0</td>
<td>notInstalled</td>
<td>PSU 1 core temp</td>
</tr>
<tr>
<td>57</td>
<td>false</td>
<td>0</td>
<td>44</td>
<td>ok</td>
<td>PCH temp</td>
</tr>
<tr>
<td>58</td>
<td>false</td>
<td>1</td>
<td>2</td>
<td>ok</td>
<td>Midplane temp R</td>
</tr>
<tr>
<td>59</td>
<td>false</td>
<td>0</td>
<td>16</td>
<td>ok</td>
<td>Midplane L temp</td>
</tr>
<tr>
<td>60</td>
<td>false</td>
<td>0</td>
<td>17</td>
<td>ok</td>
<td>Midplane C temp</td>
</tr>
<tr>
<td>61</td>
<td>false</td>
<td>0</td>
<td>13</td>
<td>ok</td>
<td>Front panel temp</td>
</tr>
</tbody>
</table>
Management Center includes support for the HOST-RESOURCES-MIB, an internet standard that is detailed in RFC 2790: https://tools.ietf.org/html/rfc2790

http://www.net-snmp.org/docs/mibs/host.html

Management Center does not display all of the information available in the HOSTRESOURCES-MIB. The displayed information is limited to the following values:

- System up time
- Memory size
- CPU load per core

The following example shows the results of snmpwalk on an S-400 appliance:

```
HOST-RESOURCES-MIB::hrSystemUptime.0 = Timeticks: (263841) 0:43:58.41
HOST-RESOURCES-MIB::hrMemorySize.0 = INTEGER: 32791168 KBytes
HOST-RESOURCES-MIB::hrProcessorLoad.196608 = INTEGER: 20
HOST-RESOURCES-MIB::hrProcessorLoad.196609 = INTEGER: 12
HOST-RESOURCES-MIB::hrProcessorLoad.196610 = INTEGER: 12
HOST-RESOURCES-MIB::hrProcessorLoad.196611 = INTEGER: 4
HOST-RESOURCES-MIB::hrProcessorLoad.196612 = INTEGER: 3
HOST-RESOURCES-MIB::hrProcessorLoad.196613 = INTEGER: 1
HOST-RESOURCES-MIB::hrProcessorLoad.196614 = INTEGER: 1
HOST-RESOURCES-MIB::hrProcessorLoad.196615 = INTEGER: 1
```

You can also view this information from the Management Center CLI:

```
# show HOST-RESOURCES-MIB

HOST-RESOURCES-MIB hrSystem hrSystemUptime 456987
HOST-RESOURCES-MIB hrStorage hrMemorySize 32791168
HR	HR
DEVICE	PROCESSOR
INDEX	LOAD
-------------------
196608	20
196609	11
196610	12
196611	4
196612	1
196613	1
196614	1
196615	1
```
Management Center includes support for the Interfaces Group MIB (also known as the IF-MIB), an internet standard detailed in RFC 2863: https://tools.ietf.org/html/rfc2863

http://www.net-snmp.org/docs/mibs/interfaces.html

As with the HOSTRESOURCES-MIB, Management Center limits the information that it displays. Consider the following example (note the 4 interfaces on the S-400 appliance):

```
bash-4.1# snmpwalk -v2c -c testsnmp localhost .1.3 | grep IF-MIB
IF-MIB::ifNumber.0 = INTEGER: 4
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifDescr.1 = STRING: 0:0
IF-MIB::ifDescr.2 = STRING: 1:0
IF-MIB::ifDescr.3 = STRING: 2:0
IF-MIB::ifDescr.4 = STRING: 2:1
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 1500
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
IF-MIB::ifMtu.4 = INTEGER: 1500
IF-MIB::ifSpeed.1 = Gauge32: 1000000000
IF-MIB::ifSpeed.2 = Gauge32: 0
IF-MIB::ifSpeed.3 = Gauge32: 0
IF-MIB::ifSpeed.4 = Gauge32: 0
IF-MIB::ifPhysAddress.1 = STRING: 0:d0:83:9:69:26
IF-MIB::ifPhysAddress.2 = STRING: 0:d0:83:9:69:27
IF-MIB::ifPhysAddress.3 = STRING: 0:d0:83:9:69:28
IF-MIB::ifPhysAddress.4 = STRING: 0:d0:83:9:69:29
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifAdminStatus.3 = INTEGER: up(1)
IF-MIB::ifAdminStatus.4 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: down(2)
IF-MIB::ifOperStatus.3 = INTEGER: down(2)
IF-MIB::ifOperStatus.4 = INTEGER: down(2)
IF-MIB::ifLastChange.1 = Timeticks: (57013) 0:09:30.13
IF-MIB::ifLastChange.2 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.3 = Timeticks: (57013) 0:09:30.13
IF-MIB::ifLastChange.4 = Timeticks: (0) 0:00:00.00
IF-MIB::ifInOctets.1 = Counter32: 2702197
IF-MIB::ifInOctets.2 = Counter32: 0
IF-MIB::ifInOctets.3 = Counter32: 25283
IF-MIB::ifInOctets.4 = Counter32: 0
IF-MIB::ifInUcastPkts.1 = Counter32: 17871
IF-MIB::ifInUcastPkts.2 = Counter32: 0
IF-MIB::ifInUcastPkts.3 = Counter32: 227
```
You can also view IF-MIB information from the Management Center CLI. The following output is from an S400 appliance:

```
# show IF-MIB

IF-MIB interfaces ifNumber 4
IF-MIB ifTable ifEntry 1
```
ifDescr 0:0
ifType ethernetCsmacd
ifMtu 1500
ifSpeed 1000000000
ifPhysAddress 00:d0:83:09:69:26
ifAdminStatus up
ifOperStatus up
ifLastChange 57013
ifInOctets 2725695
ifInUcastPkts 18120
ifInNUcastPkts 3065
ifInDiscards 183
ifInErrors 0
ifInUnknownProtos 0
ifOutOctets 392678
ifOutUcastPkts 2609
ifOutNUcastPkts 0
ifOutDiscards 0
ifOutErrors 0
ifOutQLen 0
ifSpecific 0.0
IF-MIB ifTable ifEntry 2
  ifDescr 1:0
  ifType ethernetCsmacd
  ifMtu 1500
  ifSpeed 0
  ifPhysAddress 00:d0:83:09:69:27
  ifAdminStatus up
  ifOperStatus down
  ifLastChange 0
  ifInOctets 0
  ifInUcastPkts 0
  ifInNUcastPkts 0
  ifInDiscards 0
  ifInErrors 0
  ifInUnknownProtos 0
  ifOutOctets 0
  ifOutUcastPkts 0
  ifOutNUcastPkts 0
  ifOutDiscards 0
  ifOutErrors 0
  ifOutQLen 0
  ifSpecific 0.0
IF-MIB ifTable ifEntry 3
  ifDescr 2:0
  ifType ethernetCsmacd
  ifMtu 1500
  ifSpeed 0
  ifPhysAddress 00:d0:83:09:69:28
  ifAdminStatus up
  ifOperStatus down
  ifLastChange 57013
  ifInOctets 25283
SNMPv2-MIB

Management Center uses a standard implementation of the SNMPv2-MIB, RFC 3418:


The SNMPv2-MIB is the Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), the document that defines managed objects which describe the behavior of a Simple Network Management Protocol (SNMP) entity.

The following output is from a BASH shell `snmpwalk`:

bash-4.1# snmpwalk -v2c -c testsnmp localhost .1.3 | grep SNMPv2-MIB
SNMPv2-MIB::sysDescr.0 = STRING: Symantec Management Center
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.14501.6
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00

ifInUcastPkts  227
ifInNUcastPkts  48
ifInDiscards   0
ifInErrors     0
ifInUnknownProtos  0
ifOutOctets    468
ifOutUcastPkts  6
ifOutNUcastPkts 0
ifOutDiscards  0
ifOutErrors    0
ifOutQLen      0
ifSpecific     0.0
IF-MIB ifTable ifEntry 4
ifDescr        2:1
ifType          ethernetCsmacd
ifMtu           1500
ifSpeed         0
ifPhysAddress   00:d0:83:09:69:29
ifAdminStatus   up
ifOperStatus    down
ifLastChange    0
ifInOctets      0
ifInUcastPkts   0
ifInNUcastPkts  0
ifInDiscards    0
ifInErrors      0
ifInUnknownProtos  0
ifOutOctets     0
ifOutUcastPkts  0
ifOutNUcastPkts 0
ifOutDiscards   0
ifOutErrors     0
ifOutQLen       0
ifSpecific      0.0
Management Center - 3.0

SNMPv2-MIB::snmpInPkts.0 = Counter32: 2198
SNMPv2-MIB::snmpInBadVersions.0 = Counter32: 0
SNMPv2-MIB::snmpInBadCommunityNames.0 = Counter32: 0
SNMPv2-MIB::snmpInBadCommunityUses.0 = Counter32: 0
SNMPv2-MIB::snmpInASNParseErrs.0 = Counter32: 0
SNMPv2-MIB::snmpEnableAuthenTraps.0 = INTEGER: disabled(2)
SNMPv2-MIB::snmpSilentDrops.0 = Counter32: 0
SNMPv2-MIB::snmpProxyDrops.0 = Counter32: 0
SNMPv2-MIB::snmpSetSerialNo.0 = INTEGER: 2103378064

bash-4.1#

You can display similar information from the Management Center CLI:

# show SNMPv2-MIB
SNMPv2-MIB system sysDescr "Symantec Management Center"
SNMPv2-MIB system sysObjectID 1.3.6.1.4.1.14501.6
SNMPv2-MIB system sysUpTime 831609
SNMPv2-MIB system sysServices 72
SNMPv2-MIB system sysORLastChange 0
SNMPv2-MIB snmp snmpInPkts 1400
SNMPv2-MIB snmp snmpInBadVersions 0
SNMPv2-MIB snmp snmpInBadCommunityNames 0
SNMPv2-MIB snmp snmpInBadCommunityUses 0
SNMPv2-MIB snmp snmpInASNParseErrs 0
SNMPv2-MIB snmp snmpSilentDrops 0
SNMPv2-MIB snmp snmpProxyDrops 0
SNMPv2-MIB snmpSet snmpSetSerialNo 2103378064

BLUECOAT-INFO-MIB

The INFO MIB is used to provide general information about the appliance—product information, version, serial number.

bash-4.1# snmpwalk -v2c -cpublic localhost 1.3.6.1.4.1.3417.2.19
SNMPv2-SMI::enterprises.3417.2.19.1.1.0 = STRING: "Blue Coat Management Center"
SNMPv2-SMI::enterprises.3417.2.19.1.2.0 = STRING: "2.4.1.1"
SNMPv2-SMI::enterprises.3417.2.19.1.3.0 = STRING: "0000000000"

You can display similar information from the CLI:

# show BLUECOAT-INFO-MIB
BLUECOAT-INFO-MIB blueCoatInfo blueCoatSoftware "Blue Coat Management Center"
BLUECOAT-INFO-MIB blueCoatInfo blueCoatVersion 2.4.1.1
BLUECOAT-INFO-MIB blueCoatInfo blueCoatSerialNumber 0000000000

BCSI-MC-RESOURCES-MIB

The BCSI-MC-RESOURCES-MIB shows the current memory utilization.

bash-4.1# snmpwalk -v2c -cpublic localhost 1.3.6.1.4.1.14501.6.2
BCSI-MC-RESOURCES-MIB bccmResMonSystem bccmResMonMemoryUsedPercentage 63

You can display similar information from the CLI:

# show BCSI-MC-RESOURCES-MIB
BCSI-MC-RESOURCES-MIB bccmResMonSystem bccmResMonMemoryUsedPercentage 63
**SNMP Traps**

SNMP traps send notification to the SNMP management server when appropriate conditions or thresholds are met. You configure Management Center SNMP traps using the user interface settings on the **Administration > Alerts** page. The alerts conform to the format described in the BCSI-MANAGEMENT-CENTER-MIB.

Refer to **Receive Error Notifications** to get more information about the types of alert notifications that can be sent with traps.

**Additional Information**

Additional information and resources are listed under the support section of the Symantec website at:


**Reference: Management Center MIB Files**

You can set up and receive SNMP notifications about Management Center. Download the management information bases (MIBs) that Management Center supports from: https://support.broadcom.com/security.

For instructions on configuring SNMP, refer to **Configure SNMP Alerts** and **Configure the SNMP Agent Password**.

**Management Center MIBs**

Management Center uses public and private MIBs.

**Private MIBs**

Management Center uses the following private MIBs:

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCSI-MIB</td>
<td>A root MIB module for Symantec. This is the root MIB module for Blue Coat Systems, which was acquired by Symantec. It defines the parent OID for Blue Coat products, BCSI-MANAGEMENT-CENTER-MIB requires it.</td>
</tr>
<tr>
<td>BLUECOAT-MIB</td>
<td>A root MIB module for Symantec. The enterprise number is that of CacheFlow, Blue Coat System's former corporate name. This MIB defines the parent OID for older Blue Coat products (SG product line).</td>
</tr>
<tr>
<td>BCSI-MANAGEMENT-CENTER -MIB</td>
<td>The MIB module for Management Center, which describes trap notifications sent from Management Center.</td>
</tr>
<tr>
<td>BLUECOAT-SG-SENSOR-MIB</td>
<td>The MIB module for hardware sensor data.</td>
</tr>
<tr>
<td>BLUECOAT-INFO-MIB</td>
<td>The INFO MIB is used to provide general information about the appliance—product information, version, serial number.</td>
</tr>
<tr>
<td>BCSI-MC-RESOURCES-MIB</td>
<td>The BCSI-MC-RESOURCES-MIB shows the current memory utilization.</td>
</tr>
<tr>
<td>BLUECOAT-SG-HEALTHMONITOR-MIB</td>
<td>Not implemented.</td>
</tr>
</tbody>
</table>

**Standard MIBs**
Management Center also supports several variables in the following standard MIBs. The suggested source for these files is http://www.ietf.org.

<table>
<thead>
<tr>
<th>RFC</th>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2790</td>
<td>HOST-RESOURCES-MIB</td>
<td>Monitors the values of Management Center system resources like CPU and memory</td>
</tr>
<tr>
<td>RFC 2863</td>
<td>INTERFACES-GROUP-MIB (IF-MIB)</td>
<td>Describes network interface parameters and state.</td>
</tr>
<tr>
<td>RFC 3418</td>
<td>SNMPv2-MIB</td>
<td>Describes generic objects for managed entity.</td>
</tr>
<tr>
<td>RFC 3415</td>
<td>SNMP-VIEW-BASED-ACM-MIB</td>
<td>Describes objects for View-based Access Control Model.</td>
</tr>
</tbody>
</table>

**Send Usage Data to Broadcom**

This topic describes options on the Administration > System Settings > Usage Data page.

Use the options on this page to send daily usage data to Broadcom.

**IMPORTANT**
If you have a Portfolio License Agreement (PLA) with Broadcom, you are required to send daily usage data to Broadcom. You can do that using this option or by another means negotiated with Broadcom.

The usage data information is securely transmitted to the Broadcom Portal. The data includes the number of devices that are being monitored. No Personally Identifiable Information (PII) covered under GDPR is transmitted. You can view the data that is sent by looking at the usage.log. Go to Administration > Logs to view the log.

**NOTE**
If you are not in a PLA with Broadcom, you can defer sending usage data. In that case, the system still creates a daily log of the data but the log is not sent to Broadcom.

1. Select Administration > System Settings > Usage Data.
2. Click Send Data to Broadcom.
3. Site ID: Do not enter a value in this option unless Broadcom support directs you to.
4. Click Save, then Activate.
5. To test the connection, click Test.
   The system displays a pass or fail message. If the test fails, check your Management Center proxy settings and the firewall settings in your deployment.
Troubleshoot and Resolve Issues

This section discusses troubleshooting steps and advanced procedures for Management Center.

The following topics provide information for resolving common issues:

- VM Workaround for vSphere 6.5.x
- Reset or Restore Admin Account Passwords
- Encrypt Sensitive System Data
- Back Up the Management Center Configuration
- Upgrade Management Center
- Downgrade Management Center
- Restore a Management Center Backup Configuration

"Multi-tenant policy support is not enabled for this device" when installing policy

Problem: Attempts to install policy to a ProxySG appliance fail and you receive the message "Error: Multi-tenant policy is not enabled for this device".

Resolution 1: Multi-tenant policy was introduced in SGOS 6.6.x; if the device is running an earlier version of SGOS, you cannot install multi-tenant policy to it. If the device is running SGOS 6.6.x, proceed to the next resolution.

Resolution 2: The device does not have the Multi-Tenant Policy license or the license is invalid. If this is the case, contact your Symantec sales point of contact or Symantec customer care for assistance.

To determine if the appliance has the license:
1. Log in to the ProxySG Management Console.
2. Select Maintenance > Licensing.
3. In the list of Licensed Components, look for Multi-Tenant Policy. If the license is installed and valid, proceed to the next resolution.

Resolution 3: Multi-tenant policy is not enabled on the device. To enable it, enter the following commands:

```
#(config) general

#(config general) multi-tenant enable

ok
```

User has "access denied" error when running a job

Problem: A user runs a job manually (through the Run Now option) or using the Immediate schedule option, but the job completes with an "access denied" error.

Resolution: Check the user's permissions; if they do not have sufficient permissions for the operation, they cannot run a manual or immediate job for the operation. For more information, see Understanding Job Permissions.
User has "does not support" error when adding target device to edited policy

Problem: Before pushing policy to targets ProxySG Appliances, a user adds a target device. While the targeted device is selected, select Compare Policy. The expected result is comparison table of the version of policy stored on Management Center and the version already installed on the device. An error is displayed instead: "x.x.sgos6x.policy.command.x.x." does not support version 5.5.11.7.

Resolution: The ProxySG appliance SGOS version was downgraded after it was added to Management Center. Upgrade the SGOS version to 6.3.x or later before continuing.

A Device is Unassigned to a Device Group

Problem: At times a device is not a member of a device group. This can happen when no groups were selected when the device was added to Management Center, or if the groups to which the device was assigned were deleted.

Resolution: Ensure Devices Belong to Device Groups

"Local Changes Detected" error when installing policy

Problem: When you click Install Policy, the Policy Editor displays a Local Changes Detected message:

This message means that the policy on a device has changed outside of Management Center. It could have been changed on the ProxySG appliance itself, or through an overlay installation if you also use Symantec Director to manage devices.

Resolution: To resolve this conflict, click Compare to see the differences between the policy on the device and the policy you want to install. See Compare the Device Policy Version with Current Policy Version for information.

Then, click Install Policy to overwrite the version on the device, or click Cancel to keep the version on the device.

"Import batch contains duplicate device name violation" when importing multiple devices

Problem: When you import devices, you receive the error "Import batch contains duplicate device name violation."

Resolution: Each device in the import file must have a unique name. Management Center detects duplicate device names even if you select only one or none of the devices for importing, and regardless of their placement in the hierarchy.

Rename duplicate devices in the import file and import them again. Alternatively, remove devices that you do not want to add from the file and import devices again.

"Could not enable statistics collection due to unexpected server failure" when activating a device

Problem: When you activate a device, you receive the alert "Statistics collection failed. Could not enable statistics collection on <device> due to unexpected server failure". When you added the device, you had selected Collect statistics for this device.

Resolution 1: Statistics collection requires SGOS 6.3.x. If the ProxySG appliance is not running SGOS 6.3.x or later, disable statistics collection by editing the device details and clearing Collect statistics for this device. You can enable statistics collection for the device again later if you upgrade SGOS to a supported version.

Resolution 2: Connection settings are incorrect. Verify device connection parameters and edit the device details.
Can't Connect to Device After Upgrading to 2.x

Problem: You were able to connect to and manage a device prior to upgrading to 2.x. After upgrading to 2.x, you can no longer connect to the device.

Resolution: Check that the “#” symbol does not appear in any of the following:

- The proxy name
- The SSH banner page
- The password

The # symbol is not supported for these in 2.x.

Read Messages and Alerts

In the web console banner, the Messages icon displays alerts to communicate that a change was made, such as a confirmation of device activation. Alerts indicate the severity level of the change; for example, Messages displays a green Message-level alert when you add a device and a red Error-level message when device activation fails.

If you have unread alerts, the Messages icon in the banner displays the number of unread alerts and the status of the alert with the highest severity level.

To read messages, in the web console banner, click Messages.
To filter alerts, click **Errors**, **Warnings**, or **Messages** at the bottom of the dialog. To understand more about colors and status, see [About Status Indicators](#).

**TIP**
To manage alerts, click on the Alerts icon 🗣️ to get to the Alerts page. See [Manage Alerts](#) for more information.

**TIP**
When you navigate to another screen, Message-level alerts are removed from the Messages dialog, but Errors and Warnings remain on the dialog until you read them.

## Configure Diagnostics Logging

Use this page to set the logging levels. The Master Log includes all of the General and Device Plugin data. To reduce the size of the Master Log or to produce a targeted log, configure the levels accordingly. The level you choose determines the amount of information provided in each log. For example, debug logs can later be used to send diagnostic information to Support. The logging levels are described in the following table.

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEBUG</td>
<td>Logs detailed informational events and is most useful when you are attempting to diagnose problems.</td>
</tr>
<tr>
<td>INFO</td>
<td>Logs high-level informational messages only.</td>
</tr>
<tr>
<td>WARN</td>
<td>Logs potentially harmful events.</td>
</tr>
<tr>
<td>ERROR</td>
<td>Logs all errors that do not cause the system to restart.</td>
</tr>
<tr>
<td>OFF</td>
<td>Disables logging. The Master Log cannot be disabled.</td>
</tr>
<tr>
<td>ALL</td>
<td>Logs everything. Applicable only to the Master Log.</td>
</tr>
</tbody>
</table>

When you enable a log, data is written to a specific log file. For example, if the Master log is set to INFO or above, messages are written to `log.log`. If the Master Log is set to DEBUG, all messages are written to `debug.log` and also to `log.log` (messages for INFO and above). All other logs send data to a log of the same name, for example, `security.log` and `network.log`.

**Configure Diagnostic Logging**

1. Select **Administration > Settings > Diagnostics**. The system displays the Diagnostics window.

2. Specify the **Master Logging Level**, **General**, and **Device Plugin** settings.

3. Do one of the following:
   - Click **Save** to store the settings on the server. If you are unable to save your changes, make sure that all required settings are specified.
   - Click **Activate** to cause the server to load and apply the currently saved configuration.

## Determine Which Management Center Version You are Using

To aid in troubleshooting, you might need to determine the version and build of Management Center that is currently running.
NOTE
Refer to the Management Center  *Release Notes* to identify issues or limitations that your build might include.

1. In the web console banner, click
   > About. The web console displays the Management Center - About dialog. The dialog displays information about the Management Center version. See the table following this procedure.
2. Click Close to close the dialog.

### Build Information Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The Management Center version.</td>
</tr>
<tr>
<td>Build</td>
<td>The number of the installed build.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the appliance.</td>
</tr>
</tbody>
</table>

### # service

The service command allows you to view disk usage and troubleshoot the following:

- Disk space or possible file corruption issues
- Enable verbose logging
- Upload diagnostic data to Symantec using an open support case
- Possible VPM cache corruption issues

**View Disk Usage**

View your current disk usage before performing disk maintenance.
Syntax

# service disk-usage

Perform Disk Maintenance

Clean your disk by using the # service db-maintenance command and subcommand. This is used for manual database cleanup and re-indexing. While running this maintenance command, both Management Center and statistics monitoring are unavailable.

Syntax

# service db-maintenance

NOTE
Automated disk space cleanup occurs when Management Center reaches 85% of disk utilization. This automated cleanup removes backed up dump files and all but the latest Management Center backup. This automated cleanup is not as thorough as performing disk maintenance manually. Management Center and statistics monitoring remain available and running.

Enable Verbose Logging

To enable verbose debug logging, execute the command # service enable-verbose-logging. When you have completed capturing what you want, stop the logging by executing the command # service disable-verbose-logging. You can then export the debug log from the web console or include the log in a support case upload.

Syntax

# service enable-verbose-logging
# service disable-verbose-logging

NOTE
You should enable verbose logging to include more debug-level details in system logs, which can be used to troubleshoot issues you may have encountered. Because the system log is included in the diagnostics upload to Symantec Support, enabling verbose logging includes debug-level logs in the diagnostics archive.

Start or Stop Service

Start or stop Management Center services.

# service stop-service [ management-center | report-generator | statistics-monitoring ]

Stops the specified service.

# service start-service [ management-center | report-generator | statistics-monitoring ]

Starts the specified service.

Use the show status command to view the current status of the services.

Management Center# show status Configuration: Memory installed: 7858 megabytes Memory free: 3274 megabytes CPUs installed: 2 MAC: 00:50:56:b5:8a:e1 Birth Certificate: Installed General status: System started: 2017-02-24 06:50:58MST CPU utilization: 0 Service status:

Upload Diagnostics Data

Upload diagnostics data to a destination server or directly to Symantec if you have an open support case.

Syntax

```
# service upload-diagnostics [subcommands]
```

Subcommands

```
# service upload-diagnostics [subcommands]
```

<table>
<thead>
<tr>
<th>SCP:</th>
<th>scp://&lt;host&gt;/&lt;path&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP:</td>
<td>ftp://&lt;host&gt;/&lt;path&gt;</td>
</tr>
<tr>
<td>FTPS:</td>
<td>ftps://&lt;host&gt;/&lt;path&gt;</td>
</tr>
<tr>
<td>HTTP:</td>
<td>http://&lt;host&gt;/&lt;path&gt;</td>
</tr>
<tr>
<td>HTTPS:</td>
<td>https://&lt;host&gt;/&lt;path&gt;</td>
</tr>
</tbody>
</table>

```
# service upload-diagnostics <case_number>
```

Upload the diagnostics to Symantec Support with your existing case number.

*<case_number>* is the number for your open Symantec Support case.

Purge VPM Cache

If you receive a message when starting the Visual Policy Manager Editor from the web console that a jar mismatch exists, you will need to purge the VPM cache. This happens rarely, such as if there is a network failure while jars are being transferred between devices.

Purge all Visual Policy Manager .jar files by using #purge-vpm cache command.

Syntax

```
# purge-vpm cache
```

Configure Management Center to Trust Its Image Store

This topic describes how to configure Management Center to establish SSL trust when installing images from its own file store. Consider the following system image installation error:

```
# installed-systems load https://198.51.100.8:8082/fs/download/bccm_main-235430.bcsi
failed
% ErrorCode : -14500
% ErrorMessage : Connection error
% Reason : Invalid server certificate
```
This error means that the default SSL certificate is not trusted by Management Center (it has not been added to the browser-trusted certificate list). If you receive this error, complete the following procedure.

1. Access the Management Center CLI.
2. Log into enable mode.
3. View the Management Center default certificate:
   ```
   # ssl view certificate default
   ```

   ```
   -----BEGIN CERTIFICATE-----
   MIIEcjCCAvKgAwIBAgIJAOHKNes6SjX6MA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
   VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAsTDU1vdW50YS1vdW50YXJpYXMg
   BgNVBAoTG0JsdWUgQ29hdCBNYW5hZ2VtZW50IENlbnRlcjETMBEGA1UEAxMKMTAw
   snIodWwuY29yc3QgW291bnQgUGFzc2V0IHRoZSBDdW50YXJpYXMgUmVhdmluaW5n
   MjEuODIwMDAwMDAwMDAwMDAwMDAwMjEuMDAwMDAwMDAwMDAwMDAwMjEuMDAwMDAw
   1jXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXj
   -----END CERTIFICATE-----
   ```

4. Copy the certificate.
5. Enter the following command to view the certificate names in the Management Center CA chain (if any are installed):
   ```
   # ssl view ccl management-center
   ```

   For example:
   ```
   # ssl view ccl management-center
   Certificates:
   customer-ca-1
   customer-ca-2
   ```

6. View and copy each certificate.
   ```
   # ssl view certificate cert_name
   ```

   For example:
   ```
   # ssl view certificate customer-ca-1
   ```

7. Enter SSL configuration mode and use the inline command to paste the certificates. For example:

   ```
   #ssl view certificate default
   ```

   ```
   -----BEGIN CERTIFICATE-----
   MIIEcjCCAvKgAwIBAgIJAOHKNes6SjX6MA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
   VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAsTDU1vdW50YS1vdW50YXJpYXMg
   BgNVBAoTG0JsdWUgQ29hdCBNYW5hZ2VtZW50IENlbnRlcjETMBEGA1UEAxMKMTAw
   snIodWwuY29yc3QgW291bnQgUGFzc2V0IHRoZSBDdW50YXJpYXMgUmVhdmluaW5n
   MjEuODIwMDAwMDAwMDAwMDAwMDAwMjEuMDAwMDAwMDAwMDAwMDAwMjEuMDAwMDAw
   1jXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXjXj
   -----END CERTIFICATE-----
   ```

   ```
   -----END CERTIFICATE-----
   ```
# configure terminal
(config)# ssl

(config-ssl)# inline ca-certificate mc_server_cert

Enter the certificate below and end it with a Ctrl-D

-----BEGIN CERTIFICATE-----
MIIECjCCAvKgAwIBAgIJAOHKNes6SjX6MA0GCSqGSIb3DQEBCwUAQIGEMQswCQYD
VQQGEwJVUzELMAkGA1UECFMCQX0ExFjAUGFBgNVBAcTDU1vdW50YWluIFZpZXcw
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5ePZJuz1lpN5aFbO51y
l5nQ+FvQcywF8p7fTm/C+KZyFZeVt9D3Dm3y7Lb8jKJM6u+31Y7vzo6ouH0pNwi
3x2nDy9T4/f+0P9w8eBPu5JmIzUo3GmX+Vw7oQAi4v0t2sL4b0WQ+Bf3cFRX0Z6
Z8yvAHlrz0mJxvrW4IFK+iXOD4LupJ6wzsv89bQc9gVn81oDGT+ehk9+jUqmcnO
OCp6RjWw8zYf1Ea8hPjPz514s6DyM4spvI7Z0vB6ZD2GtFbrycJm7VXkZyi2Gz
-----END CERTIFICATE-----

ok

Repeat for each certificate you recorded in the previous steps.

8. Add each certificate to the Certificate Authority Certificate List (CCL). For example:
   (config-ssl)# edit ccl browser-trusted
   (config-ccl-browser-trusted)# add mc_server_cert
   ok

You should now be able to install the Management Center image.

Install Management Center Certificates on Content Analysis toEstablish SSL Trust

If you attempt to retrieve a system image from Management Center using the Content Analysis (CA) CLI, image installation will fail unless the Management Center certificates have been added to the CA browser-trusted CCL. This topic
describes how to collect the Management Center certificate chain and install it onto the CA appliance so it will trust the HTTPS URL when loading a software image from Management Center.

**Step 1: Collect Management Center Certificates**

1. **View the Management Center default certificate**:

   ```
   # ssl view certificate default
   -----BEGIN CERTIFICATE-----
   MIIECjCCAvKgAwIBAgIJAOHKNes6SjX6MA0GCsGS1b3DQEBCwUAMIGEMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcgbVBlZSExMD<decltype(Step1)>.#ssl view certificate default
   -----BEGIN CERTIFICATE-----
   LE+2ljaus61ibvHpJacksonxahdh2+8uAldvaE2zhb70qfTkxMmVF+wt3DnNET5Elm7E0jGTItP9z8S9bVoay9cQ7AOMD34PrJ3MregionU2+3Pj543439e0Yr268AVgg35D2cz0cmkxrippxExI+oUxlmkzz+dda1844l1j+fVCCAK1148nupfhr0Kn1s8d9K8v8a2gSNHJ33R/1D4uHusYtM28Rc/9unQx82 SAfuy7Ud121gmpq55vblHyphol1vVGh74/7jZ5f5Hh49eCr8bmt2Rduitgk3BAG1f7TMB768G1udEqQ1MaHAbqgFVnF4FQVDR0TB1wADaadBqvNH5UEFJAUbgpBqEFqocpAjkJkWBBHUAeWQYqVDR0B0BBY1EF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyAQo+M/n666V3n3RA1DlWhQMBaF0Py+TLUljyyA
   -----END CERTIFICATE-----
   ```

2. Copy the default certificate.

3. Enter the following command to view the certificate names in the Management Center CA chain (if any are installed):

   ```
   # ssl view ccl management-center
   ```

**Step 2: Install Management Center Certificate(s) on the Content Analysis Appliance**

1. Access the Content Analysis CLI and enter configuration mode.

2. Install the Management Center certificates you recorded in Step 1.
Management Center - 3.0

(config)# ssl inline ca-certificate ca-name

For example:

(config)# ssl inline ca-certificate mc-default

Enter the certificate below and end it with a Ctrl-D

-----BEGIN CERTIFICATE-----
MIIECjCCAvKgAwIBAgIJAMrmxW4MVDv/MA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAoTDU1vdW50YWluIENlbnRlcm1l
MTQxNzpxMDEvMjAxOTIyMzQ3NzI4MjIyNzEwMTQ0MFoX
DTIzMDIwMTE5MQQ4MFowQjEAMA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAoTDU1vdW50YWluIENlbnRlcm1l

CA certificate mc-default is added successfully.

3. Repeat step 2 for each Management Center certificate you have recorded.
4. Add each certificate authority to the browser-trusted CCL:

(config)# ssl ccl browser-trusted

(config-ccl-browser-trusted)# ca-certificate cert_name

5. Verify that the certificate(s) have been added to the browser_trusted CCL:

# show running-config ssl ccl browser-trusted
Stop or Restart Services

To troubleshoot some issues, you might need to stop or restart Management Center services. You will need to restart the services after you install or update a Management Center license.

Stop Management Center Services

You can start or stop the Management Center, report generator, or statistics monitoring services.

1. Go to the Management Center CLI, as described in Access the Management Center CLI.
2. Enter privileged mode by typing `enable` at the command prompt.
3. Enter your enable password and press Enter.
4. At the `#` prompt, type the following command and press Enter:
   ```
   # system-services stop [management-center | report-generator | statistics-monitoring]
   
   The CLI displays the command prompt.
   ```

Restart Services

1. Go to the Management Center CLI, as described in Access the Management Center CLI.
2. Enter privileged mode by typing `enable` at the command prompt.
3. Enter your enable password and press Enter.
4. At the `#` prompt, type `system-services restart ?` and enable each service.
   ```
   # system-services restart management-center
   # system-services restart report-generator
   # system-services restart statistics-monitoring
   
   WARNING
   You cannot access the web console while the services are restarting; however, you can try accessing the web console a few minutes after issuing the command.
   ```

Test Network Connectivity

Verify that your network is set up correctly by using the `ping` command or the `tracepath` command in the CLI. Be sure to specify a hostname or IP address that you know is reachable and working.

1. Access the Management Center CLI.
2. Enter Privileged mode. Privileged Mode Commands.
3. Ping an IP address: `# ping <hostname or IP address>
4. Trace the path between the host and a destination IP address: `# tracepath <destination>`

If you receive an error message, check your network configuration.

Upload System Diagnostics

To help Symantec Technical Support troubleshoot a Management Center issue, you can send diagnostics information to an external server using a supported protocol (FTP, HTTP, HTTPS, or SCP).

1. Log in to the CLI. See Access the Management Center CLI.
2. Enter the privileged mode password and press Enter.
3. Enter the appropriate command to upload the diagnostics:
   ```
   Using Your SR Case Number
   
   # diganostics service-info send<case_number>
   ```
Upload the diagnostics to Symantec Support with your existing case number.

```
FTP
# diagnostics service-info send url ftp://host:port/path
username <username> password <password>
```

where `username` and `password` are the username and password to authenticate to the server. If the FTP server does not require authentication, these values are not required.

**View Hardware Diagnostics and Memory Resources**

Use the Hardware Diagnostics screen to check on how much memory and storage space is being used by Management Center system components and processes. In addition, you can monitor various hardware sensors to spot potential problems with CPUs, fans, power supplies, and so forth (not applicable to virtual appliances).

- **System Metrics** — Details about memory usage of the CPUs and Management Center processes
- **Storage Usage** — Additional memory settings
- **Data Storage** — Amount of data used by each feature
- **Database Storage** — Amount of storage used for each database (Management Center, Device Statistics, Reporter)
- **Temperature Sensors** — The results of temperature monitoring for the chassis, CPU, and other components that produce heat in the appliance
- **RPM Sensors** — Reports the speed at which the fans on the appliance spin
- **Voltage Sensors** — Reports the voltage, status and state of components for which the appliance has a voltage sensor such as CPU cores, power supply, and others
- **Other Sensors** — Reports status of optional hardware components, such as extra power supplies

**NOTE**
Byte counts for memory usage are approximations, not precise values.

To view hardware diagnostics for your appliance:

1. Select **Administration > Hardware Diagnostics**.
2. Click **Refresh** to view the most current appliance status totals and usage.
Reference: Understanding Job Permissions

A job is distinct from the operation (such as backing up devices and installing policy) that the job executes. When users create a job, they define its operation, targets, and schedule. If a user has permissions to add or update jobs, that user can configure and save any job.

Users can run jobs in Management Center in the following ways.

**User runs a job immediately after configuring it or manually using Run Now**

- The job executes as the user.
- The Audit Log displays the event as a Job Execution and lists the username as the Operating User.
- The job information shows that it was started by the user.

**NOTE**

As long as the user has the job permissions, running a job immediately or manually always results in a completed job. In the previous scenario, if the user has permissions to perform the operation, the job completes without errors; if the user has insufficient permissions to perform the operation, the job completes with errors.

**User configures a job scheduled in the future**

- The job executes as the system.
- The Audit Log displays the event as a Job Execution and lists SYSTEM as the Operating User.
- The job information shows that it was started by the system.

Because the job executes as the system, which can perform all operations, users with permissions to schedule jobs can create jobs for an operation that they do not have permissions to perform. Allowing more users than necessary to schedule jobs is a potential security risk.

**TIP**

Consider granting the Scheduled Job - Run Now permission to most users who require the ability to run jobs. Reserve the Scheduled Job - Add and Scheduled Job - Update permissions for the most senior users.
Reference: Permissions Interdependencies

When adding permissions to roles, remember that users can access an object as long as they have a role with the required permission. For example, if a user is added to a role which allows access to only one device group and a role that has View permissions for all devices, the user can see all devices in all groups.

Refer to the following permission objects to determine specific dependencies.

**NOTE**
The View permission is implied in all higher permission levels except for Add. To reduce the number of permissions in a role, you can remove the View permission if a higher-level permission for the same object exists in the role. For example, if a role already has the Policy - Update permission for importing policy, you do not have to add the Policy - View permission for adding policy jobs.

### All objects

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all functions in all areas of the web console</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View all areas of the web console</td>
<td>None</td>
</tr>
</tbody>
</table>

### Attribute Definition

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Add, delete, and edit attributes</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Add attributes</td>
<td>Attribute Definition - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete attributes</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Edit attributes</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View attributes</td>
<td>None</td>
</tr>
</tbody>
</table>

### Audit

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all audit log functions</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to audit log records</td>
<td>None</td>
</tr>
</tbody>
</table>

### Backup Image

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Import, export, delete, and restore image backups</td>
<td>Management Center - View Management Center - Update</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete backups</td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Export backups</td>
<td></td>
</tr>
<tr>
<td>Import</td>
<td>Import backups</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Restore backups</td>
<td>Management Center - View Management Center - Update</td>
</tr>
<tr>
<td>Permission action</td>
<td>Allows access to these areas/functions</td>
<td>Requires these permissions to be useful</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>View</td>
<td>View information about existing backups</td>
<td></td>
</tr>
<tr>
<td>View Contents</td>
<td>View the backup contents</td>
<td></td>
</tr>
</tbody>
</table>

### Device

**NOTE**
When using filters with a specified value, make sure that the value exactly matches the value in the device properties. See Set User-Defined Device Attributes for Access Control and Reference: Permissions Filters.

<table>
<thead>
<tr>
<th>Permission Action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All device functions</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td>To see the effective policy for a device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To change membership in device properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Group - Change</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Membership</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - Change</td>
<td>To add devices by importing from a file:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Membership</td>
<td>Device - Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td>Device - Update</td>
</tr>
<tr>
<td>Backup</td>
<td>Back up devices</td>
<td>Device - Manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup Image - Update</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Delete devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td>Manage</td>
<td>Activate and deactivate devices</td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - Manage</td>
<td></td>
</tr>
<tr>
<td>Execute Scripts</td>
<td>Execute scripts on devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - Manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Script – View</td>
<td></td>
</tr>
<tr>
<td>Install Policy</td>
<td>Install policy to devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - Manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - Update</td>
<td></td>
</tr>
<tr>
<td>Restore</td>
<td>Restore configuration backups to devices</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Group - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup Image - View</td>
<td></td>
</tr>
<tr>
<td>Permission Action</td>
<td>Allows access to these areas/functions</td>
<td>Requires these permissions to be useful</td>
<td>Grant these permissions for more functions</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Update</td>
<td>Edit device basic information, connection parameters, and attributes</td>
<td>Hierarchy - View Device Group - View</td>
<td>To change membership in device properties: Device Group - Change Membership To add devices by importing from a file: Device - Add Device - Update</td>
</tr>
<tr>
<td>View</td>
<td>View device information</td>
<td>Hierarchy - View Device Group - View</td>
<td></td>
</tr>
</tbody>
</table>

**Device Group**

**NOTE**

When using filters with a specified value, make sure that the value exactly matches the value in the device group properties. See Set User-Defined Device Attributes for Access Control and Reference: Permissions Filters.

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all device group functions</td>
<td>Hierarchy - View</td>
<td>To see the devices in groups: Device - View</td>
</tr>
<tr>
<td>Add</td>
<td>Add device groups</td>
<td>Hierarchy - View Device Group - Change Membership</td>
<td>To associate devices while adding a group: Device - View To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update</td>
</tr>
<tr>
<td>Change Membership</td>
<td>Change associated groups in device properties</td>
<td>Hierarchy - View Device - Update</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Delete device groups</td>
<td>Hierarchy - View Device - View</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Edit device groups' basic information and attributes</td>
<td>Hierarchy - View</td>
<td>To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update</td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to device groups</td>
<td>Hierarchy - View</td>
<td></td>
</tr>
</tbody>
</table>

**Device Script**
Prior to Management Center 2.0, Device - Manage was required to execute scripts on a device. In 2.0 and later, Device Script enables you to execute scripts on a device without requiring the Device-Manage permission. This means you can limit users to only being able to manage and execute scripts, without providing them with additional device permissions.

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All functions related to script</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Add script objects</td>
<td>Device Script - View Device - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete script objects</td>
<td>None</td>
</tr>
<tr>
<td>Edit Metadata</td>
<td>Edit script object attributes and information</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Edit and execute script content</td>
<td>Device - View Device - Execute Script</td>
</tr>
<tr>
<td>View</td>
<td>View script</td>
<td>None</td>
</tr>
</tbody>
</table>

**Note:** Compare Versions of the Script is available at this level.

### File

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for ancillary functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Add, delete, and edit files</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Add file</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete files</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Edit Metadata</td>
<td>Edit file attributes and information</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View files</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

### Hierarchy

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for ancillary functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Add, delete, and edit hierarchies</td>
<td>Device Group - All operations</td>
<td>To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update</td>
</tr>
<tr>
<td>Add</td>
<td>Add hierarchies</td>
<td>Hierarchy - View Device Group - All operations</td>
<td>To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete hierarchies (except for the predefined hierarchies)</td>
<td>Device Group - Delete</td>
<td>To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update</td>
</tr>
<tr>
<td>Update</td>
<td>Edit hierarchies</td>
<td>Device Group - Update</td>
<td>To add device groups or hierarchies by importing from a file: Device Group - Add Device Group - Update</td>
</tr>
<tr>
<td>View</td>
<td>View hierarchies</td>
<td>Device Group - View</td>
<td>To see devices: Device - View</td>
</tr>
</tbody>
</table>
### Management Center

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all Management Center functions.</td>
<td>None</td>
</tr>
<tr>
<td>Backup</td>
<td>Perform Management Center backup and restore.</td>
<td>Scheduled Job - Add Scheduled Job - View</td>
</tr>
<tr>
<td>CLI</td>
<td>Use Management Center CLI.</td>
<td>None</td>
</tr>
</tbody>
</table>

### PKI

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all operations pertaining to the Management Center data protection key.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>View Administration &gt; Data Protection tab and view and change the Management Center data protection key.</td>
<td>None</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete Management Center data protection key.</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>For future use.</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>For future use.</td>
<td>None</td>
</tr>
</tbody>
</table>

### Policy

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All functions related to policy</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add policy objects</td>
<td>Policy - View</td>
<td>To assign targets while adding a policy object: Policy - Assign Target Device - View</td>
</tr>
<tr>
<td>Assign Targets</td>
<td>Add and remove target devices</td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td>CPL - Add Section</td>
<td>Add policy sections to existing policy objects</td>
<td>None</td>
<td>To add policy sections while adding a new policy object: Policy - Add</td>
</tr>
<tr>
<td>CPL - Delete Section</td>
<td>Delete policy sections</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CPL - Edit Default</td>
<td>Edit the default sub-section in policy sections</td>
<td>* CPL - Edit Override - Consider granting this permission to senior roles only. Granting this permission allows users to edit the Override sub-section in all policy sections, which could have unintended results.</td>
<td></td>
</tr>
<tr>
<td>CPL - Edit Mandatory</td>
<td>Edit the mandatory sub-section in policy sections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPL - Edit Override*</td>
<td>Edit the override sub-section in policy sections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPL - Move Section</td>
<td>Move policy sections within policy objects</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CPL - Update Section</td>
<td>Edit the name and purpose of sections</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Delete policy objects</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Permission action</td>
<td>Allows access to these areas/functions</td>
<td>Requires these permissions to be useful</td>
<td>Grant these permissions for more functions</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Edit Contents</td>
<td>Restore previous versions of policy and edit policy</td>
<td>None</td>
<td>To select a reference device: Device - View</td>
</tr>
<tr>
<td>Edit Metadata</td>
<td>Edit policy object attributes and information</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Import</td>
<td>Import policy from devices</td>
<td>Device - View Policy - Edit Contents <em>Note: Because Management Center imports policy as one section, it might be useful to grant some policy section permissions in some cases (for example, to allow users to break down the imported policy into sections and sub-sections).</em></td>
<td></td>
</tr>
<tr>
<td>Publish</td>
<td>Install policy on target devices</td>
<td>None</td>
<td>To add/remove target devices to policy before installing: Device - View Device - Manage Device - Install Policy Policy - Assign Targets</td>
</tr>
<tr>
<td>View</td>
<td>View policy <em>Note: Edit &gt; Check Consistency is available at this level.</em></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**REST API**

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Grants access to all REST API functions.</td>
<td>This permission must be used in conjunction with other permissions to get access to the data. For example, to read a device using the API, you also need Device View.</td>
</tr>
<tr>
<td>Add</td>
<td>Users can perform POST/GET/PUT operations.</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Users can perform DELETE operations.</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Users can modify API methods.</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>Users can view API methods.</td>
<td></td>
</tr>
</tbody>
</table>

**Role**

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>All role functions</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Users can add roles</td>
<td>Role - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Users can delete roles</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Users can update roles</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to roles</td>
<td>None</td>
</tr>
</tbody>
</table>

**Scheduled Job**
NOTE
Job permissions are distinct from the operational permissions. If you have unexpected results or 'access denied' errors when running jobs, see Understanding Job Permissions.

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Add, edit, delete, enable, disable, and run jobs; view job progress, current jobs, and job history</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add jobs</td>
<td>Scheduled Job - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> Scheduled Job - Add is an elevated permission. See Understanding Job Permissions.</td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(For policy jobs) Policy - View</td>
<td></td>
</tr>
<tr>
<td>Cancel Running Job</td>
<td>Cancel all active, running jobs</td>
<td>Scheduled Job - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device - View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(For policy jobs) Policy - View</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Delete jobs</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Run Manually</td>
<td>Run jobs manually using the <strong>Run Now</strong> option</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Edit jobs’ information and schedule; enable/disable jobs</td>
<td>None</td>
<td>To view devices and add/remove targets:</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> Scheduled Job - Update is an elevated permission. See Understanding Job Permissions.</td>
<td></td>
<td>Device - View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To add/remove policies from a job:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy- View</td>
</tr>
<tr>
<td>View</td>
<td>View all scheduled and current jobs and job history</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All users can see the <strong>Jobs</strong> tab in the web console, even if they do not have a Scheduled Job - View permission.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Session

**NOTE**
Session permissions are specifically to control access to user sessions.

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>View, kill, disable logins</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View active sessions</td>
<td>None</td>
</tr>
<tr>
<td>Kill Session</td>
<td>Kill an active session</td>
<td>None</td>
</tr>
<tr>
<td>Enable/Disable User Login</td>
<td>Enable or Disable logins to Management Center</td>
<td>None</td>
</tr>
</tbody>
</table>
### Settings

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all settings functions in Administration Settings (Hardware Diagnostics is always read-only)</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Edit Management Center Settings</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View Management Center Settings, and Hardware Diagnostics</td>
<td>None</td>
</tr>
</tbody>
</table>

### Statistics

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all Appliance Monitoring reports and functions</td>
<td>None</td>
<td>To filter reports and report widgets by device or device group: Device Group - View Device - View</td>
</tr>
<tr>
<td>View</td>
<td>Read-only access to reports</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

### Tenant

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires these permissions to be useful</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Allows access to the tenant definitions in Management Center.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Users can add tenants</td>
<td>None</td>
</tr>
<tr>
<td>Delete</td>
<td>Users can delete tenants</td>
<td>None</td>
</tr>
<tr>
<td>Update</td>
<td>Users can edit tenants</td>
<td>None</td>
</tr>
<tr>
<td>View</td>
<td>View Configuration &gt; Tenants</td>
<td>None</td>
</tr>
</tbody>
</table>

### User

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all user functions</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add users and specify basic information</td>
<td>User - View</td>
<td>To assign roles while adding a user Role - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete users</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Update users' basic information and change/expire user passwords</td>
<td>None</td>
<td>To add or remove roles from a user: Role - View</td>
</tr>
<tr>
<td>View</td>
<td>View users</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
# User Group

<table>
<thead>
<tr>
<th>Permission action</th>
<th>Allows access to these areas/functions</th>
<th>Requires permissions to be useful</th>
<th>Grant these permissions for more functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations</td>
<td>Perform all user group functions</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Add user groups</td>
<td>User Group - View</td>
<td>To add or remove group roles while adding a user group: Role - View To add or remove group roles while adding a user group: User - View</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete user groups</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Update user groups' basic information</td>
<td>None</td>
<td>To add/remove users from groups: User - View</td>
</tr>
<tr>
<td>View</td>
<td>View user groups</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Management Center tips and use cases:

- Organize Scripts by Attribute
- Restrict Access Only to a Specific Object Included in a VPM Layer
- `$(if)` `$(else)` Logic in Scripts and Policy

### Restrict Access Only to a Specific Object Included in a VPM Layer

This topic describes how to restrict user access to an object included in the VPM Web Access Layer. The intention of the policy is to allow users to edit the allowlist, but preclude them from altering other policy in the VPM.

Although this can be accomplished with CPL, it is easier to create a shared object, restrict access to that object, and then include the object in the VPM policy.

**Step 1---Create the URL List Object**

1. Select **Configuration > Shared Objects**.
2. Click **Add Object**. The web console displays the Create New Shared Object wizard.
3. Fill in required fields.
   a. **Object name** (*) - Required name
   b. **Object type** (*) - From the drop-down list, choose **URL List**.
   c. **Reference ID** (*) - Enter a Reference ID that you can filter for when building policy.
   
   **NOTE**
   
   The Reference ID must begin with a letter and must contain only letters, numbers, and "_".
   
   d. **Description** - Enter a meaningful description to help you when reusing this fragment.
4. Click **Next**. The Create New Shared Object wizard displays the **Attributes** dialog. If you defined a policy attribute as mandatory, you can choose the attribute's value for this policy fragment. See **Add Attributes**.
5. Click **Finish**. The URL list displays in the editor.

**Step 2---Add URLs**

1. Select **Configuration > Shared Objects**.
2. Select or edit the desired URL list. The system displays the URL list editor.
3. Enter the URL in the URL field and click **Add**.

   **NOTE**
   The system displays the text entered into the Description field as a comment in the generated policy.

4. Alternatively, paste in multiple URLs:
   a. Click **Paste URLs**. The system opens the Paste URLs: Enter URLs dialog.
   b. Copy the URLs into the Paste URLs: Enter URLs dialog. Press CTRL+V or right-click and click **Paste**. The URLs are added to the list.
   c. Click **Next**. The system opens the Paste URLs: Validate dialog.
   d. Click **Finish**.

5. Click **Save**.

**Step 3—Add an Allowlist Editing Role**

1. Select **Administration > Roles** and click **Add Role**.
2. In the **Add Role: Basic Info** dialog, enter a name for the role. In this example, you might use "Allowlist Editor."

   **NOTE**
   If you authenticate users against LDAP, Active Directory or RADIUS, create a role in sync with the directory service.

3. (Optional) Enter a description.
4. Click **Next**.
5. In the **Add Role: Permissions** dialog, click **Add Permission**.
6. From the **Object** drop-down list, select **Policy**.
7. From the **Action** drop-down list, delete **All Operations** and select **Edit Contents**.
8. In the **Filter** drop-down list, use the pencil to select the URL allowlist you created in steps 1 and 2.

9. Click **Finish**.

**Step 4—Assign Users to the Allowlist Editing Role**

1. Select **Administration > Users**.
2. In the **Users** left pane, select the user whose roles you want to change. The user's details display.
3. Click **Edit**. The web console displays the Edit User dialog.
4. Click **Assign Roles**. The dialog displays a list of all the roles in the system. Roles to which the user is not assigned are listed under **Available Roles**. Roles to which the user is currently assigned are listed under **Assigned Roles**.
5. Select the **Allowlist Editor** role from **Available Roles** and, using the arrow, add it to the **Assigned Roles** list.
6. Click **Save**. The web console banner displays an alert indicating that the user was saved.

   **NOTE**
   Roles are linked to user sessions. If you edit users' roles while they are logged in to the web console, instruct them to log out and log in again to see the effects of the change.
Step 5—Create the VPM Policy Object

NOTE
Skip to step 6 if you are going to add your URL list to an existing policy object.

To add a VPM policy object, complete the following steps.

1. Select Configuration > Policy.
2. Click Add Policy. The system displays the Create New Policy: Basic Information dialog.
3. Enter a name for the policy object.
4. Select VPM for the Policy Type.
5. Enter a Reference ID. Although entering a reference ID is not required, it is useful for filtering objects when building policy. If you do not enter a reference ID, the system assigns a default ID based on the policy name you enter. Imported policy objects are assigned a default ID.
   NOTE
   The Reference ID must begin with a letter, and must contain only letters, numbers and ".".
6. Enter a description in the Description field. Although entering a description is not required, the description helps differentiate versions of the same policy.
7. If you are to include shared objects, verify that Replace Substitution Variables is enabled. See Use Substitution Variables in Policies and Scripts for more information.
8. Click Next.
9. Enter or select values for the defined attributes.
10. Click Finish.

Step 6—Add the URL List to the VPM Policy

1. Select Configuration > Policy.
2. From the Policy Objects list, select the desired VPM policy.
3. Review the Included Objects section.
4. Any lists already included in the policy are displayed in the Included Objects list. You may only reference shared objects if they are associated with the policy. To add available lists:
   a. Click Add Object.
   b. Select the additional lists to add to the policy, then click OK.
   TIP
      You can search for lists using the Keyword Search.
5. Make note of the reference ID for the object(s) you want to set.
6. (Optional) If you want to limit the lists to specific revisions in order to avoid unintentional changes, you can lock the revision version.
   a. Select an object.
   b. Click Select Version.
   c. Select Use specific version.
   d. Select the version number from the menu.
   e. Click Save.
7. (Optional) Select any lists to remove and click Delete.
   NOTE
   If any of the lists are in use, you need to launch the VPM Editor to remove or change the rules that reference them in the policy.
8. Once finished editing the available shared objects for the policy, click Save.
9. Click Launch VPM Editor.
   NOTE
   The following steps are shown using the legacy VPM editor. If you use the web-based editor, see Web-Based VPM Shared Include Example and Launch Web-Based VPM.
10. Select or create the desired policy layer.

11. On the desired line number, right click the field under **Destination** and select **Set** from the menu.

12. Select the desired list:
   - By the reference ID from the objects list.
   - For a category, select any VPM object that lists categories.

   **NOTE**
   Shared objects are read-only. You cannot use the **Edit** option when setting the destination object. If you do try to edit it, it gets overwritten the next time you open the VPM editor.

13. (Optional) Set the desired action condition by right-clicking under the **Action** field.

14. When finished setting the destination and conditions, click **Save policy**. (Optional) To exit the VPM Editor without saving changes, close the VPM Editor and then click **Do not Save Policy**.

15. Enter a brief description of the policy changes in the **Save Changes** field, click **OK**, then click **Close**.

16. Close the VPM Editor.

17. Back in Management Center, on the VPM policy, click the **Info** tab.

18. Ensure that **Replace substitution variables** is selected, then click **Save**.

For more information about adding or editing VPM Shared Objects, see **Create Shared Objects**.

You are now ready to install the policy. From this point on, any user with the correct permissions can edit the list as needed without having to open the VPM.
Management Center REST API

Management Center 1.6.1.1 and later include a new REST API. You can use this API if you want to access Management Center without using the UI or want to trigger Management Center operation without using the UI. This REST API has the ability to:

- Access and raise alerts.
- View registered devices, device health, and other monitoring variables.
- View jobs and job execution status.
- Start and cancel jobs.
- Show basic device information like version, disk usage, name of device.

No special policy or licensing is required to use this feature. API activities are recorded in the audit log.

Limitations

The REST API has the following requirements:

- JSON is the only supported payload.
- HTTPS is required to access the API.
- BASIC authentication is the only supported authentication method for providing user credentials for the API.
- You cannot add devices. A bulk device import already exists.

Documentation

Access the REST API documentation at the following URL:

https://MC_IP:8082/help/api

For example:

https://198.51.100.18:8082/help/api or click this link.

Or extract this archive package on your network or local workstation for offline viewing.

Troubleshooting

Confirm that the user has the proper permissions:

- REST API permissions (included in default administrator role).
- Appropriate permissions for the data or operation. For example, the user must have the Device permission if they want to use the Device API to list devices.
CLI Command Reference

Management Center includes a command-line interface (CLI) that allows you to perform administrative tasks. A PDF of the Management Center CLI command documentation is available in the documentation section of the Symantec support site.

• "Access the Management Center Command Line Interface (CLI)" —Describes how to access the CLI via an SSH connection.
• "Command Line Overview"—Describes the standards and conventions in the Management Center CLI.
• "CLI URL Syntax" —Describes the valid syntax for commands that require a URL path.
• CLI Output Processing—Describes how to modify CLI output.
• "CLI Command Reference: List"—Navigate links to view command descriptions and syntax.

Command Line Overview

The command-line interface (CLI) provides a UNIX-like interface for accessing the software. All of the functions available via the management console are also accessible with CLI commands. In addition, a number of CLI commands support special features and diagnostic tasks that are not incorporated in the browser interface.

Command Usage Conventions

A few basic conventions apply to commands:

• Commands are case sensitive—that is, you must enter them in lowercase characters. Some parameters must be entered in uppercase.
• A command can be abbreviated by entering the minimum number of characters required to uniquely distinguish it from other commands. For example, instead of typing event-log you can type ev and press spacebar or Tab to complete the command.
• Command syntax can be verified by typing a ? after the command. For example:

  (config-proxy-settings) ?

  Possible completions:
  {disable}
  disable disable configuration
  enable enable configuration
  host proxy setting host name
  password proxy setting password
  port proxy setting port
  username proxy setting user name
  view view the proxy config setting
  ---
  exit exit from current mode
  help provide help information
  no Negate a command or set its defaults

• To issue multiple commands from a single command line, separate the commands with a semicolon (;). The semicolon is the equivalent of pressing the Enter key. For example:

  show version;show timezones

• To negate a command or set it to its default, type no before the command. For example:

  (config)#no proxy-settings username
  (config)#no alert-settings email-alerts server-settings
About the Comment ! Character

The Management Center CLI interprets the exclamation mark ! as a comment character. If a password has an exclamation mark, you must surround the password in quotes when entering it into the CLI or it will be ignored during command execution. For example, the following command will fail because the password is not quoted:

```
# backup export 1 scp://198.51.38.42:2024/home/jsmith passphrase example123 username jsmith password !abc
```

The following command will succeed:

```
# backup export 1 scp://198.51.38.42:2024/home/jsmith passphrase example123 username jsmith password "!abc"
```

Typographical Conventions

The following typographical conventions are used for command syntax:

<table>
<thead>
<tr>
<th>Boldface in monospace font</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Square brackets]</td>
<td>Optional arguments in a command line</td>
</tr>
<tr>
<td>&lt;angle brackets in italic&gt;</td>
<td>Required arguments for which you will supply a value</td>
</tr>
<tr>
<td>Pipe character (</td>
<td>)</td>
</tr>
</tbody>
</table>

Command Prompts

The CLI has three major modes—standard, privileged (enable), and configure:

- Standard mode: Initial mode; use to monitor the service. Prompt: >
- Privileged (enable) mode: View, manage, and change the appliance settings. Prompt: #
- Config mode: Configuration mode, used to configure a service. Prompt: (config)#

Certain configuration commands also have modes that change the command prompt. For example:

- authentication configuration mode: (config-authentication) prompt
- health monitoring mode: (config-health-monitoring)# prompt
- NTP configuration mode: (config-ntp)# prompt
- SSL configuration mode: (config-ssl)# prompt

To exit out of the current mode, type exit; you may need to type exit multiple times to return to the desired mode.

Edit Previously Entered Commands

If you make a typing mistake in your command, you don't need to retype it—you can redisplay the command and edit it. This capability is available when logged in to the appliance via SSH, but not via a direct console serial connection.

<table>
<thead>
<tr>
<th>Display a previously entered command</th>
<th>Press up arrow until the command you want is displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scroll down through the command history</td>
<td>Press down arrow</td>
</tr>
<tr>
<td>Move cursor to the left</td>
<td>Press left arrow</td>
</tr>
<tr>
<td>Move cursor to the beginning of the line</td>
<td>Press Ctrl+A</td>
</tr>
<tr>
<td>Move cursor to the right</td>
<td>Press right arrow</td>
</tr>
<tr>
<td>Insert characters</td>
<td>Position cursor and start typing</td>
</tr>
<tr>
<td>Delete character to the left of cursor</td>
<td>Press Backspace</td>
</tr>
</tbody>
</table>
NOTE
If the arrow keys aren't working, make sure your remote login utility is emulating VT100 arrows. You may need to enable this option in your client.

**CLI Output Processing**
You can process command output using an output redirect. The pipe command | character is used for this purpose. The commands can be chained to achieve more complex processing. For more information, see CLI Output Processing.

**Access the Management Center Command Line Interface (CLI)**
Log on to the CLI through an SSH connection or through the VMware, KVM, or Hyper-V console.

**TIP**
For hardware appliances, access the CLI through the serial console.

**Log on using SSH**
1. Install an SSH client. This procedure uses PuTTY as an example; your steps might be slightly different.
2. Open PuTTY and specify the following information:
   - **Host Name (or IP address)**—The IP address that you specified for Management Center
   - **Port**—22
3. (Optional) Specify a name for the connection and click **Save** to save the settings.
4. Click **Open**. The SSH window opens, with a login prompt.
5. At the **login as:** prompt, type **admin** and press Enter.
6. At the **admin@IP_address's password:** prompt, type your password and press Enter. The console displays the CLI banner.

**Log on through the VMware console**

**NOTE**
Use the VMware console or SSH if you are logging into a Virtual Appliance.

1. In the VMware client, browse to the VM in the inventory.
2. Select the VM, right-click, and select **Open Console**. The console displays the CLI console and prompts you to press Enter three times.
3. Press Enter three times. The console displays the CLI banner.

**KVM: Log on using SSH**

See Log on using SSH.

**Log on through the KVM (virsh) console**

1. Login to the CentOS server.
2. Enter the following command to open the console on the Management Center KVM instance:
   ```bash
   # virsh console mc_vm_name
   ```
3. Press **Enter** three times. The console displays the CLI banner.
4. To exit a virsh console session, type **CTRL + ]**.
Log on From Hyper-V Manager

1. Open the Hyper-V Manager and select the specific VM.
2. Right click the Hyper-V instance and click **Connect**.
   The client displays the console.
3. Press Enter three times.
   The console displays the CLI banner.

**CLI URL Syntax**

All CLI commands that accept a URL as a download source or upload destination are formatted as:

```
protocol://host/path
```

For example, the SCP protocol must use the format:

```
scp://host/path
```

If path is a directory, it must end with a forward slash (/). The following protocols are supported, although some commands do not support all of the protocols:

- `ftp://hostname[:port]/path`
- `ftps://hostname[:port]/path`
- `http://hostname[:port]/path`
- `https://hostname[:port]/path`
- `scp://hostname[:port]/path`

**Notes**

- URLs cannot contain spaces. If the hostname or path contains a space, you must use the URL-encoded characters instead: `%20`.
  For example, enter the following URL

  `http://yourserver.com/d/backup 2.tgz.gpg`

  as


**CLI Output Processing**

You can process command output using an output redirect. The pipe command `|` character is used for this purpose. The commands can be chained to achieve more complex processing.

**Syntax**

```
(config)# cli_command | processing_options
```

**Example**

```
# show health-monitoring | ?
```

Possible completions:

- `begin` Begin with the line that matches
- `count` Count the number of lines in the output
The following table describes these redirect targets.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `begin` | Begin with the line that you have specified. For example:  
  ```
  # show history | begin 08-22
  08-22 21:53:32 -- show configuration | count
  08-22 21:54:00 -- show configuration | count
  08-22 21:54:52 -- show configuration commit | count
  08-22 21:55:07 -- show configuration
  08-22 21:55:36 -- show configuration commit list | count
  08-22 22:05:14 -- show configuration commit list
  08-22 22:06:09 -- show
  08-22 22:06:15 -- show history
  ``` |
| `count` | This redirect target counts the number of lines in the output. For example:  
  ```
  (config)# show configuration commit list | count
  Count: 39 lines
  ``` |
| `display` | Set display options. For example:  
  ```
  # show timezone current | display json
  {
    "result": "Local time: 2019-08-22 22:22:24+00:00 UTC 
    
    
    
    "TimeZone": "UTC"
  }
  ``` |
### exclude

Exclude the specified lines. For example:

```
# show clock local

local-time: 2019-08-22T22:25:27+0000
year: 2019
month: 08
day: 22
hour: 22
minute: 25
second: 27
ntp ntp: false
ntp-synchronized ntp-synchronized: false
```

```
# show clock local | exclude ntp

local-time: 2019-08-22T22:25:53+0000
year: 2019
month: 08
day: 22
hour: 22
minute: 25
second: 53
```

### include

Show only lines that include the specified lines. For example:

```
# health-monitoring view current | include Memory
2019-09-09 18:42:34 | Memory Utilization
```

### linnum

Enumerate lines in the output. For example:

```
# diagnostics heartbeat view | linnum
1: {
2:   "machine_status" : {
3:     "partitions" : [ {
4:       "name" : "/dev/mapper/live-rw",
5:       "used" : "1452520",
6:       "free" : "42486540"
7:     }, {
8:       "name" : "/dev/mapper/vg_persist-cache--data",
9:       "used" : "10232",
10:      "free" : "44740744"
11:     }, {
```

```
```json
"machine_status": {
  "partitions": [
    {
      "name": "/dev/mapper/live-rw",
      "used": "1452520",
      "free": "42486540"
    },
    {
      "name": "/dev/mapper/vg_persist-cache-data",
      "used": "10232",
      "free": "44740744"
    },
    {
      "name": "/dev/mapper/vg_persist-core",
      "used": "23044",
      "free": "49626420"
    },
    {
      "name": "/dev/mapper/vg_persist-data",
      "used": "5027900",
      "free": "454578448"
    },
    {
      "name": "/dev/mapper/vg_persist-data",
      "used": "5027900",
      "free": "454578448"
    }
  ]
}
```
Enforce table output. For example:

```
show running-config interface | tab
```

<table>
<thead>
<tr>
<th>DEVICE</th>
<th>MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>IP ADDRESS</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>0:0</td>
<td>enable</td>
</tr>
<tr>
<td>10.9.47.12</td>
<td>255.255.252.0</td>
</tr>
</tbody>
</table>

End with the line that matches.

```
# show history | until 19:03
08-27 20:44:31 -- en
08-27 20:44:34 -- con
09-09 18:40:50 -- en
09-09 18:41:17 -- health-monitoring view
09-09 18:41:26 -- health-monitoring view current
09-09 18:43:18 -- health-monitoring view current |
    include Memory
09-09 18:47:46 -- ssh view
09-09 18:47:54 -- ssh view | linenum
09-09 18:48:12 -- event-log view
09-09 18:48:18 -- event-log
09-09 18:48:36 -- event-log view log
09-09 18:48:44 -- event-log view log | linenum
09-09 18:49:29 -- show licenses | linenum
09-09 18:52:14 -- smtp view
09-09 18:52:37 -- diagnostics view
09-09 18:52:59 -- diagnostics heartbeat view
09-09 18:53:09 -- diagnostics heartbeat view |
    linenum
09-09 18:57:11 -- diagnostics heartbeat view | more
09-09 19:00:56 -- diagnostics heartbeat view |
    nomore
09-09 19:01:55 -- failover view
09-09 19:02:10 -- system-services status
09-09 19:03:46 -- view
```

**Syntax**

```
(config)#
    cli_command | processing_options
```

**Example**

```
# show health-monitoring | ?
```
The following table describes these redirect targets.

<table>
<thead>
<tr>
<th>Possible completions:</th>
<th>Begin with the line that you have specified. For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>begin</td>
<td># show history</td>
</tr>
<tr>
<td>count</td>
<td>08-22 21:53:32 -- show configuration</td>
</tr>
<tr>
<td></td>
<td>08-22 21:54:00 -- show configuration</td>
</tr>
<tr>
<td></td>
<td>08-22 21:54:52 -- show configuration commit</td>
</tr>
<tr>
<td></td>
<td>08-22 21:55:07 -- show configuration</td>
</tr>
<tr>
<td></td>
<td>08-22 21:55:36 -- show configuration commit list</td>
</tr>
<tr>
<td></td>
<td>08-22 22:05:14 -- show configuration commit list</td>
</tr>
<tr>
<td></td>
<td>08-22 22:06:09 -- show</td>
</tr>
<tr>
<td></td>
<td>08-22 22:06:15 -- show history</td>
</tr>
<tr>
<td>display</td>
<td>This redirect target counts the number of lines in the output. For example:</td>
</tr>
<tr>
<td></td>
<td>(config)# show configuration commit list</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Count: 39 lines</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>notab</td>
<td>Set display options. For example:</td>
</tr>
<tr>
<td></td>
<td># show timezone current</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;result&quot;: &quot;Local time: 2019-08-22 22:22:24+00:00 UTC \nTimezone: UTC&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
### Exclude

Exclude the specified lines. For example:

```markdown
# show clock local

local-time:        2019-08-22T22:25:27+0000
year:        2019
month:        08
day:        22
hour:        22
minute:        25
second:        27
ntp ntp:        false
ntp-synchronized ntp-synchronized:        false

# show clock local | exclude ntp

local-time:        2019-08-22T22:25:53+0000
year:        2019
month:        08
day:        22
hour:        22
minute:        25
second:        53
```

### Include

Show only lines that include the specified lines. For example:

```markdown
# health-monitoring view current | include Memory

2019-09-09 18:42:34 | Memory Utilization
```

### Linnum

Enumerate lines in the output. For example:

```markdown
# diagnostics heartbeat view | linnum

1: {  
2:   "machine_status" : {  
3:     "partitions" : [ {  
4:       "name" : "/dev/mapper/live-rw",  
5:       "used" : "1452520",  
6:       "free" : "42486540"  
7:     }, {  
8:       "name" : "/dev/mapper/vg_persist-cache--data",  
9:       "used" : "10232",  
10:      "free" : "44740744"  
11:     }  
12: }  
13: }
```
# diagnostics heartbeat view | more

```json
{
  "machine_status": {
    "partitions": [
      {
        "name": "/dev/mapper/live-rw",
        "used": "1452520",
        "free": "42486540"
      },
      {
        "name": "/dev/mapper/vg_persist-cache--data",
        "used": "10232",
        "free": "44740744"
      },
      {
        "name": "/dev/mapper/vg_persist-core",
        "used": "23044",
        "free": "49626420"
      },
      {
        "name": "/dev/mapper/vg_persist-data",
        "used": "5027900",
        "free": "454578448"
      },
      {
        "name": "/dev/mapper/vg_persist-data",
        "used": "5027900",
        "free": "454578448"
      }
    ]
  }
}
```

# show running-config | nomore

# show subscriptions | repeat ?

--- repeat refresh ---

```
subscriptions
application-protection
  license-type Subscription
  licensed-until 2020-11-27
  subscription-validity Valid
  data-validity Valid
  data-version 20190808
  last-download-info
    time 2019-09-09T19:20:03.394+0000
    url https://subscription.eu.bluecoat.com/
  application-protection/database
    status "Not modified"
```
Configure Mode Commands

The following commands are available in configure mode. This mode offers commands that change the configuration of the appliance.

To enter configure mode, type `configure` at the enable prompt (#). The prompt will change to (config)#. To see a list of commands available in configure mode, type `help` or `?` at the (config)# prompt.

```bash
acl
Create firewall rules—access control lists—for accessing services on the appliance.

Syntax
(config)# acl
```
**Management Center - 3.0**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disable the user-defined access control list. This command is useful when locked out of the interface with a misconfigured access list.</td>
</tr>
<tr>
<td>enable</td>
<td>Enable the user-defined access control list.</td>
</tr>
<tr>
<td>rule &lt;source IP&gt; &lt;service&gt;</td>
<td>Define the IP addresses (individual, range, or subnet) that are allowed to access an appliance service (such as Management or SNMP).</td>
</tr>
</tbody>
</table>

**Notes**

- The subcommands listed above can either be entered in acl configuration mode (at the config-acl prompt) or in configuration mode (at the config prompt).
- To see the access control list, use the show full-configuration acl command.
- To remove a rule, enter no rule followed by the rule definition.
- Up to 1000 ACL rules can be entered in the access control list.
- The access control list only apply to incoming connections. Connections originating from the appliance are not subject to the access control list.
- Changes take effect immediately after a new rule is added or removed. It's not necessary to reboot.
- Existing connections that are allowed under a access control list are not affected when the rule is removed.
- The access list is not interface specific; the list applies to all interfaces.

**Examples**

```plaintext
(config)# acl

(config-acl)# rule 10.167.9.0/24 Management

(config-acl)# rule 10.167.9.129 255.255.255.0 SNMP

(config-acl)# no rule 10.167.9.0/24 Management
```

**appliance-name**

Assign a unique name to the appliance. The appliance name is used when alerts are sent out to recipients, plus in other elements such as the command-line prompt and SNMP logs. Consider using a geographic or other location-based name to ensure each appliance in your network can be identified easily. The name defined here also appears in the top bar in the Management Center Web UI.

**Syntax**

```plaintext
(config)# appliance-name <name>
```
Notes

• While in the CLI, the name change occurs right away, s restart of the appliance is required for the name change to appear in the web Management Console.
• Unless it is further changed by the user, the appliance name does not change after it has been manually configured except when Management Center is downgraded to a version that does not support a configurable appliance name.
• After upgrading from a build that does not allow appliance name configuration to one that does, the SNMP sysname defaults to 'BCMC' which differs from the default appliance name. The SNMP sysname will retain this value until an appliance name is configured, after which the SNMP sysname will correspond with the configured appliance name.
• After downgrading to a build that does not allow appliance name configuration, the SNMP sysname defaults to 'BCMC' and the appliance name returns to the default value for that build.
• The default appliance name for Management Center builds that do not support a configurable appliance name is based on the build version and changes when the user upgrades or downgrades the appliance.
• The appliance name is not included with the backup data. You must manually configure the appliance name after restoring the appliance configuration.
• After upgrading the appliance from a version that does not support appliance name configuration to one that does, the default appliance name will be the same as the default appliance name of the first image that was ever run. Exceptions to this are listed below and whichever occurred most recently will be the one in effect:
  – A factory reset was previously executed while running image X: the default appliance name after the upgrade will be the appliance name from image X.
  – The appliance was previously downgraded from an image Y that supported appliance name configuration to image Z that does not. In this instance the default appliance name after the current upgrade will be the same as the default appliance name of image Z.

Examples
ManagementCenter(config)# appliance-name management_center_main

  management_center_main(config)#

device-communication

Sets the hostname/IP that managed devices use to contact Management Center. Setting the hostname is necessary when multiple IP addresses are configured on the appliance. For devices to be able to validate SSL connections, the specified hostname must match the common name (CN) field in the certificate, or the x509 extension for hostname on Management Center’s server certificate. If no value is provided for device-communications, Management Center uses the CN value from the default server certificate that is used to secure HTTPS connections.

CAUTION
If you are using PDM data collection, specify a hostname. If no hostname is specified, PDM data collection may fail.
Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>device-communication hostname value</code></td>
<td><code>value</code> represents either the IP address of the interface on which management connections are expected, the common name (CN) or the hostname from an x.509 certificate extension.</td>
</tr>
<tr>
<td><code>device-communication ssh regenerate-key</code></td>
<td>Regenerate the RSA key used to authenticate to the ProxySG or ASG device. For more information, see Add a Device.</td>
</tr>
<tr>
<td><code>device-communication ssl-context context_name</code></td>
<td>Set the SSL context to be used for device communication. For more information, see Configure Device Connection Security Level (SSL Context).</td>
</tr>
</tbody>
</table>

Example

MC_Draper(config)# device-communication hostname managementcenter1

dns

Configure servers and domains for the domain name system (DNS).

Syntax

```plaintext
(config)# dns ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name-server &lt;IP address&gt;</code></td>
<td>IP address of a DNS server. Enter one or more IP addresses, each separated by a space.</td>
</tr>
<tr>
<td><code>domain-list &lt;domain&gt; &lt;domain&gt; ...</code></td>
<td>A list of DNS domain names of which this appliance will consider itself to be a member. DNS queries which use a short name will append these domains, in turn, until a match is found.</td>
</tr>
</tbody>
</table>

Notes

- To clear these settings, use the no command. For example, `no dns name-server`.
- To view the current settings, type `show full-configuration dns`.

Examples

```plaintext
(config)# dns name-server 10.2.2.10 10.2.2.11
```

installed-systems

Manage images installed on the system. Up to six images can be installed on the system. If your system already has six images installed and you add another image, the oldest unlocked image will be replaced with the new image, unless you have designated a particular image to be replaced.
**Syntax**

# installed-systems ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Cancel the download process of an image that is currently downloading</td>
</tr>
<tr>
<td>default &lt;image#&gt;</td>
<td>Specify the image that will be run the next time the system is restarted.</td>
</tr>
<tr>
<td></td>
<td>Tip: Use the installed-systems view command to identify the image number.</td>
</tr>
<tr>
<td>delete &lt;image#&gt;</td>
<td>Delete an image from the system. Use the installed-systems view command to</td>
</tr>
<tr>
<td></td>
<td>identify the image number to delete.</td>
</tr>
<tr>
<td></td>
<td>Note: You cannot remove a locked image or the current running image.</td>
</tr>
<tr>
<td>load &lt;URL&gt;</td>
<td>Download and install an image on the system. &lt;URL&gt; is the path to an image</td>
</tr>
<tr>
<td></td>
<td>on a web server that the appliance has access to.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="http://webserven.mycompany.com/images/542386.bcs">http://webserven.mycompany.com/images/542386.bcs</a></td>
</tr>
<tr>
<td></td>
<td>Management Center always uses the HTTP proxy if it is enabled.</td>
</tr>
<tr>
<td></td>
<td>Therefore, if you are attempting to load an image from localhost, disable</td>
</tr>
<tr>
<td></td>
<td>the HTTP proxy first.</td>
</tr>
<tr>
<td></td>
<td>To enforce failover replication, the installed-systems CLI command is</td>
</tr>
<tr>
<td></td>
<td>disabled on both failover partners (to deny installing and changing</td>
</tr>
<tr>
<td></td>
<td>system images).</td>
</tr>
<tr>
<td></td>
<td>To upgrade, you must first disable failover. For more information, refer</td>
</tr>
<tr>
<td></td>
<td>to the failover documentation in the Configuration and Management Guide.</td>
</tr>
<tr>
<td>lock &lt;image#&gt;</td>
<td>Lock an image to protect it from accidental deletion.</td>
</tr>
<tr>
<td>replace &lt;image#&gt;</td>
<td>Designate which image will be replaced next (if the system already</td>
</tr>
<tr>
<td></td>
<td>has six installed images and you load another image). If you do not</td>
</tr>
<tr>
<td></td>
<td>specify an image to be replaced, the oldest unlocked image on the system</td>
</tr>
<tr>
<td></td>
<td>will be replaced.</td>
</tr>
<tr>
<td>unlock &lt;image#&gt;</td>
<td>Unlock an image that you no longer want to protect from deletion.</td>
</tr>
<tr>
<td></td>
<td>You have to unlock a locked image before you can remove it.</td>
</tr>
<tr>
<td>unset-replace</td>
<td>Unset image to be replaced next. When a replacement image is not</td>
</tr>
<tr>
<td></td>
<td>designated, the oldest image will be replaced when you load a seventh</td>
</tr>
<tr>
<td></td>
<td>image.</td>
</tr>
<tr>
<td>view</td>
<td>Show a list of installed images along with their image numbers, software</td>
</tr>
<tr>
<td></td>
<td>versions, release IDs, whether the image is locked or unlocked, whether</td>
</tr>
<tr>
<td></td>
<td>it has ever been booted, creation date/time, and boot date/time. The</td>
</tr>
<tr>
<td></td>
<td>summary at the bottom of the list indicates which image number is the</td>
</tr>
<tr>
<td></td>
<td>current running system, the default system to run the next time the appliance is restarted, and the image number that will be replaced next.</td>
</tr>
</tbody>
</table>

**Examples**

# installed-systems view

```
1. Version : 2.0.0.0, Release ID : 218372, Locked : false, Booted : true
   DisplayName : Blue Coat Management Center 2.0.0.0, Release ID: 218372
```
configure the interface settings (such as IP address) on the appliance.

**Syntax**

```
(config)# interface <interface number> ?
```

where `<interface number>` is the interface (0:0, 1:0, 1:1, and so forth) that you want to configure.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description <code>&lt;text&gt;</code></td>
<td>Description of the interface; enclose in quotes if the description contains spaces.</td>
</tr>
<tr>
<td>disable</td>
<td>Disable the interface.</td>
</tr>
<tr>
<td>enable</td>
<td>Enable the interface.</td>
</tr>
<tr>
<td>ip-address <code>&lt;ip address&gt;</code></td>
<td>Set the static IP address of the interface.</td>
</tr>
<tr>
<td>mtu-size <code>&lt;size&gt;</code></td>
<td>Specify Maximum Transmission Unit (MTU) size (default=1500 bytes).</td>
</tr>
<tr>
<td>speed <code>&lt;speed&gt;</code></td>
<td>Set the speed of the interface (for example, 1gb,10gb,100mb). The default setting is auto.</td>
</tr>
</tbody>
</table>

**Notes**

- The sub-commands listed above can either be entered in interface configuration mode (for example, at the `config-interface-1:0` prompt or in configuration mode (at the `config` prompt).
- Use the `show full-configuration` command in interface configuration mode to display the interface settings. (See example below.)
- An interface can have both an IPv4 and IPv6 address (dual-stack).

**Examples**

```
(config)# interface 0:0

(config-interface=0:0)# ip-address 203.0.113.17 255.255.248.0

(config-interface=0:0)# ip-address FE80::0202:B3FF:FE1E:8329/64 ok

(config-interface=0:0)# show full-configuration
interface 0:0
description "management interface"
enable
speed auto
```
Configuration settings:
- duplex auto
- mtu-size 1500
- ip-address 203.0.113.17 255.255.248.0
- ip-address fe80::202:b3ff:fe1e:8329/64

**ip**

Configure the interface settings (such as IP address) on the appliance.

**Syntax**

```
(config)# ip ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp &lt;IP address&gt; &lt;MAC address&gt;</td>
<td>Add a static IPv4 or IPv6 address to the Address Resolution Protocol (ARP) table, correlating the specified MAC address to the IP address.</td>
</tr>
<tr>
<td>default-gateway &lt;IP address&gt;</td>
<td>Change the IP address of the default gateway used by Management Center.</td>
</tr>
<tr>
<td>neighbor &lt;IPv6 address&gt; &lt;MAC address&gt;</td>
<td>Configure static IPv6 neighbor entries (similar to a static ARP entry for IPv4). The IPv6 address and the hardware MAC address must be provided.</td>
</tr>
<tr>
<td>route &lt;prefix IP&gt;(/&lt;mask bits&gt;</td>
<td>&lt;subnet mask&gt;) &lt;next hop IP&gt; [device-name &lt;interface&gt;] [metric &lt;value&gt;]</td>
</tr>
</tbody>
</table>

**Examples**

```
(config)# ip arp 1.1.1.1 01:23:45:67:89:ab

(config)# ip route 10.64.0.0/16 10.63.158.213 device-name 0:0 metric 10

(config)# ip route 2001:db8::/32 2001:0db8:0000:0000:0000:0000:ff00:0042:8329 metric 20

(config)# ip route 10.63.0.0 255.255.0.0 10.63.158.213 metric 30

(config)# ip neighbor 2001:db8::ff00:42:8329 01:23:45:67:89:ac
```

**Example: Force Failover Node Communication Through a Second Network Interface**

```
(config)# ip route 10.169.21.63 255.255.255.255 10.169.21.1 device-name 1:0
```
Equivalent with Mask Bits

(config)# ip route 10.169.21.63/32 10.169.21.1 device-name 1:0

ipv6

Enable or disable support for IPv6 networking. Once enabled, IPv6 support is available in configuration sections for Packet Captures, Backups, Failover, Ping, Traceroute, SNMPWALK, Syslog, and in networking and interface configuration. To enable IPv6, add an IPv6 address to the interface.

Syntax

(config)# ipv6 [enable|disable]

Examples

(config)# ipv6 enable

(config)# show full-configuration ipv6
ipv6 enable
#show running-config ipv6
ipv6 enable

(config)# interface 0:0

(config-interface-0:0)# ip-address 203.0.113.17 255.255.248.0

(config-interface-0:0)# ip-address FE80::0202:B3FF:FE1E:8329/64

The previous commands add an IPv4 and an IPv6 address to interface 0:0.

login-banner

Configure a banner message to appear before users log in to the appliance. The message will appear before users log in to the CLI (via serial console and SSH) and the web user interface. This feature meets the security technical implementation guideline STIG V-3013. Messages can contain up to 2,047 characters and can be defined using multi-byte UTF-8 characters.

Syntax

# login-banner ?

disable
enable
inline message

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disable the login banner message.</td>
</tr>
<tr>
<td>enable</td>
<td>Enable the login banner message. (You cannot enable the feature until you define the message.)</td>
</tr>
<tr>
<td>inline message</td>
<td>Define the login banner message. You will be prompted to enter the message text and press Ctrl-D when finished.</td>
</tr>
</tbody>
</table>
view message | status

Show the currently defined message and feature status (enabled vs. disabled).

Examples

# login-banner inline message
Enter the login banner message below and end it with a Ctrl+D

This is a banner message.
ok

# login-banner enable

# login-banner view message
This is a banner message.

# login-banner view status
Login banner is enabled.

licensing

Configure licensing, including the loading of licenses on to the appliance.

Syntax

(config)# licensing

(config-licensing)#

| inline license-key [passphrase <value>] | Import a license from terminal input (typically by pasting the license content with a right-click). Include the passphrase to decrypt the private key if the license has birth-cert and birth-key in it. Press Ctrl-D after pasting the certificate content. |
| load [username <value>] [password <value>] | Enter your MySymantec credentials to download the appliance license from the Network Protection Licensing Portal (NPLP). **Note**: MySymantec Credentials are only required for Management Center Virtual Appliances. |
| load url <url> passphrase <value> | Download a license from the specified URL. |
| view [status|configuration] | Display the license install status or licensing configuration details. |

**NOTE**

The sub-commands listed above can either be entered in licensing configuration mode (at the config-licensing prompt) or in configuration mode (at the config prompt).

Examples

To load a license from the Symantec licensing server from a Virtual Appliance installation of Management Center:

(config)# licensing load username john.smith@test.com password helloworld
To load a license from the Symantec licensing server from a hardware appliance:
(config)# licensing load

To load a license from a URL other than NPLP:
(config)# licensing load http://test.server.com/license.txt

To view the currently installed license:

(config-licensing)# view
Appliance Serial Number : 100041XXXX
Licensable component information:
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Policy Management
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Device Configuration
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Management Center
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Device Inventory
Serial Number : 100041XXXX
Part Number : 076-02019
Expiration Date : 2018-08-09
Expiration Type : Subscription
Product Description : Management Center VA, 1 year monitoring & management subscription, 300 devices
Activation Date : 2015-09-04
Component Name : Performance Monitoring
**ntp**

Configure Network Time Protocol (NTP) settings. Use NTP to synchronize the time on the appliance with another server or reference time source. You can configure up to 10 NTP servers.

**Syntax**

```
(config)# ntp ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Stops the NTP service on the appliance. The NTP service is configured to not start when the appliance is rebooted.</td>
</tr>
<tr>
<td>enable</td>
<td>Starts the NTP service on the appliance. The NTP service is configured to start automatically when the appliance is rebooted. At least one NTP server must be defined in order to enable the NTP service.</td>
</tr>
<tr>
<td>server &lt;hostname or IP address&gt;</td>
<td>Domain name or IP address of the NTP server. The default NTP servers are ntp.bluecoat.com and ntp2.bluecoat.com.</td>
</tr>
<tr>
<td>symmetric-key key-id &lt;value 1-65534&gt; algorithm &lt;sha1&gt; [encrypted-secret &lt;value&gt;</td>
<td>secret &lt;string&gt;]]</td>
</tr>
<tr>
<td>update-now</td>
<td>Forces the NTP service to update the appliance's clock.</td>
</tr>
</tbody>
</table>

**Notes**

- Type `ntp` to enter NTP configuration mode. The prompt will display as `(config-ntp)#`.  
- Use the `no server` command in the NTP configuration mode to remove a configured server. (See example below.)  
- Use the `show full-configuration` command in the NTP configuration mode to display the NTP settings. (See example below.)

**Examples**

```
(config)# ntp server ntp.bluecoat.com

(config)# ntp enabled

(config)# ntp

(config-ntp)# show full-configuration
ntp
   enabled
   server ntp.bluecoat.com
   server ntp2.bluecoat.com

(config-ntp)# no server ntp2.bluecoat.com
```

```
577
```
To view the current configuration:

# show running-config ntp
ntp
enable
symmetric-key 1 algorithm sha1
symmetric-key 1 encrypted-secret $AES256-CBC$4dQX+DOtMmVdhtM4PG/+g==
$gFDz7v2vFOM0A1DqgjzLPB5jfqgsEZhdoy8Ee1tvkY=+$kkZd4y09r3hNnlhziLWrw==
$eR4tJbJSB7309qcDCQ+jmLnCXUhfz7gQAcwvHdwFyERfZUX5QyKprrQ1LGj2jRwveM5UXcmem43v65eZan/
WGzBow8YjdwLZNOcoN8?xhdfN45638w8sKsmd/60dhzVOM5k3PQs1nQbCtmAn1BreBsrh2L/9zaJF18C1Hrd5AYZpNokiakrMjxvwv01EawxsagCflqqr2+iwXRoUKMoWO4P3j0SSF3ihHMzZNweCoXby3nA2e/WY0u/8UhqJauz/+d1v56H/809VCLASR4PL0Ntx2V10wJG25WYuZNe+hQ==
server ntp.bluecoat.com
server ntp2.bluecoat.com
server symmetric-key
!

password-policy

Configure password rules for administrative users. For example, you can require that the password contain at least one uppercase letter, one number, and one special character. By default, the password length and prohibit-common-words rules are defined. The default minimum password length is six characters.

NOTE
After the initial upgrade to Management Center 2.0.x, any admin passwords that were defined in MC 1.x that do not adhere to the default password policy are respected. When they are changed, however, or when new administrator passwords are defined, these rules apply.

Syntax

```text
(config)# password-policy ?
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min-digits &lt;value&gt;</td>
<td>Set the minimum number of digits required in a password. Range: 0-255. By setting this rule to 0 (the default), numbers are not required in a password.</td>
</tr>
<tr>
<td>min-groups &lt;value&gt;</td>
<td>Set the minimum number of password rules (min-digits, min-lowercase, min-special, min-uppercase) that must be met. Range: 0-4. By setting this rule to 0 (the default), the password does not have to meet a minimum number of rules. For example, if you set min-digits and min-special rules, you would set min-groups to 2. Note: min-length is not counted as a rule for the purposes of the min-groups command.</td>
</tr>
<tr>
<td>min-length &lt;value&gt;</td>
<td>Set the minimum number of characters required in a password. Range: 0-255. The default password length is 6, but the password can have any length.</td>
</tr>
<tr>
<td>min-lowercase &lt;value&gt;</td>
<td>Set the minimum number of lowercase letters required in a password. Range: 0-255. By setting this rule to 0 (the default), lowercase letters are not required in a password.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>min-special &lt;value&gt;</td>
<td>Set the minimum number of special characters (symbols) required in a password. Range: 0-255. By setting this rule to 0 (the default), special characters are not required in a password. Here are some supported examples of special characters: !&quot;#$%&amp;'() * +,-./;&lt;=?&gt;@[]^_`{</td>
</tr>
<tr>
<td>min-uppercase &lt;value&gt;</td>
<td>Set the minimum number of uppercase letters contained in a password. Range: 0-255. By setting this rule to 0 (the default), uppercase letters are not required in a password.</td>
</tr>
<tr>
<td>prohibit-common-words builtin</td>
<td>Don't allow common dictionary words to be specified in passwords.</td>
</tr>
<tr>
<td>prohibit-whitespace true</td>
<td>false</td>
</tr>
</tbody>
</table>

**Notes**

- The sub-commands listed above can either be entered in password-policy configuration mode (at the config-password-policy prompt) or in configuration mode (at the config prompt).
- Use the show password-policy-configuration command to display the password policy settings.
- To remove a rule, type no before the rule command. For example: no min-lowercase
- If you configure multiple password policy rules but don't configure the min-groups command, the rules will not take effect; only the min-length rule will be enforced.

**Examples**

To require a password to have at least 8 characters, and have at least one number, one symbol, and one uppercase letter, set the following rules:

```
(config)# password-policy

(config-password-policy)# min-length 8

(config-password-policy)# min-digits 1

(config-password-policy)# min-special 1

(config-password-policy)# min-uppercase 1

(config-password-policy)# min-groups 3

(config)# show password-policy-configuration
min-uppercase: 1
min-groups: 3
prohibit-whitespace: false
min-special: 1
min-digits: 1
min-length: 8
min-lowercase: 0
prohibit-common-words: No dictionary defined
```
After these rules are configured and a user tries to specify "test" for the user password, the following message will appear:

```plaintext
(config local-user-list john_jones)# password test
Please enter a valid password.
Password must contain at least 1 uppercase characters.
Password must contain at least 1 special characters.
Password must contain at least 1 digit characters.
Password matches 0 of 3 character rules, but 3 are required.
Password must be at least 8 characters in length.
```

**proxy-settings**

Configure an HTTP proxy server in situations where your network requires all servers to connect through a proxy to access Internet resources.

**Syntax**

```plaintext
(config)# proxy-settings enable|disable host <hostname or IP address> password <string> port <value>
username <string>
(config)# proxy-settings view
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Turn the proxy settings off.</td>
</tr>
<tr>
<td>enable</td>
<td>Turn the proxy settings on.</td>
</tr>
<tr>
<td>host &lt;hostname or IP address&gt;</td>
<td>Configure the HTTP proxy host name or IPv4/IPv6 address.</td>
</tr>
<tr>
<td>password &lt;string&gt;</td>
<td>Enter the password for the HTTP proxy server.</td>
</tr>
<tr>
<td>port &lt;value&gt;</td>
<td>Define the port number of the HTTP proxy server (0-65535).</td>
</tr>
<tr>
<td>username &lt;string&gt;</td>
<td>Enter the user name for the HTTP proxy server.</td>
</tr>
<tr>
<td>view</td>
<td>View the HTTP proxy config settings</td>
</tr>
</tbody>
</table>

You can enter all the subcommands in one line, or enter each command on a separate line.

**Examples**

```plaintext
(config)# proxy-settings enable host 10.10.12.11

(config)# proxy-settings enable

(config)# proxy-settings host 10.10.12.11

(config)# proxy-settings port 8008

(config)# proxy-settings view
enabled: true
host: 10.10.12.11
port no: 8008
username: becky
```
security

Specify security options for Management Center, including where administrators can access the appliance from, what client certificates they require (if enabled) and whether they can access the appliance by HTTP or not.

CAUTION

The options and subcommands listed here are applicable when the security command is run from a (config)# prompt. You may also run this command from an enable prompt, but the primary focus of that is to view your existing security configuration.

Syntax

(config)# security [subcommands]

| allowed-hosts [add | delete | view] | Add, remove, or view the IP addresses that are allowed to access Management Center. |
|-----------------------------------------|----------------------------------------------------------------------------------|
| crls | client-authentication [disable | Set restrictions for how Management Center challenges administrative users to use X.509 client certificates to login. |
| password-requirement <enable/disable> | set-regex <value>]                                                              |
| hsts [disable | enable | view] |
| enable | view] | Enable, disable, or view support for HTTPS Strict Transport Security (HSTS) protocol. |
| http | Enable, disable, or view the current setting for HTTP management console access on ports 8080 and 9009. |

Example

(config)# security allowed-hosts

TIP

Changes to this security command will take effect the next time Management Center is restarted.

Subcommands:

# security allowed-hosts add
# security allowed-hosts delete
# security allowed-hosts view

Limits access to a specific host such that it can be accessed only by the specified hostname, and not its IP address. For example, consider a Management Center instance with the following properties:

- Hostname: mc.example.com
- IP address: 192.0.2.10

The administrator then enters the following command:

(config)# security allowed-hosts add mc.example.com

After the preceding command is run, users will only be able to access the Management Center by typing mc.example.com in the browser address bar. If users type 192.0.2.10 in the address bar, they will receive a 403 Forbidden error.

You can also specify an IP address instead of a hostname. If you specify an IP address, users can only access the device using the IP address and will receive an error if the hostname is used.
NOTE

The security allowed-hosts command has no effect on Management Center failover pairs.

```plaintext
(config)# security client-authentication disable
```

Disable X.509 client authentication.

```plaintext
(config)# security client-authentication password-requirement
```

Subcommands:

```plaintext
(config)# security client-authentication password-requirement enable
(config)# security client-authentication password-requirement disable
```

Enables or disables the requirement for users to enter their password during SSL mutual authentication. The behavior is as follows:

- **enable**: All users are forced to enter their password when accessing Management Center.
- **disable**: When the password requirement is disabled, a user does not have to enter a password to access Management Center if the system determines the certificate is valid, and finds the user in the local user database or the LDAP system, if configured.

The default is **enable**.

This method only supports the local or LDAP authentication schemes. You can use active directory but only if you set it up using the LDAP settings (Administration > Settings > LDAP). This is because a service account is needed to look up users because the system no longer has the user password.

To validate certificates, you must create a regular expression to evaluate the information in the certificate's `SubjectAlternativeName` field. The `SubjectAlternativeName` data is compared to a regex set by the `security ssl client-authentication set-regex` command, which is used to extract the portion of the value to use as the user’s identity. That value is then used to find the user in the local or LDAP authentication service. Refer to the following topics in the Configure Users, Roles, and Attributes section of this guide for more information:

- Use LDAP Subject Alternative Name Data for Certificate Validation
- Authenticate Users with SSL Mutual Authentication

```plaintext
#security client-authentication set-mandatory
```

Users must use X.509 client authentication. If X.509 client authentication fails, no connection is established.

When configured, all traffic requires a certificate. For example, to access file service requests and API's, client authentication is mandatory.

```plaintext
# security client-authentication set-optional
```

If X.509 client authentication fails, users can log in using the standard Management Center login page. Issuing this command requires Management Center to restart.

```plaintext
# security client-authentication set-regex
```

Sets the regex command used to extract the certificate’s name or data set in the certificates `SubjectAlternativeName` (`subjAltName`); the default is `CN=(.*?), .`.

Subcommand:
default

Resets the principal regex to the default.

Subject alternative name example:

```
(config)# security client-authentication set-regex "'(1\.3\.|1\.|4\.|1\.|311\.|20\.|2\.|3,\s[0-9]*\.(.*?))'"
```

Refer to Use LDAP Subject Alternative Name Data for Certificate Validation for more information.

```
# security client-authentication view
```

View current X.509 client authentication settings.

```
(config)# security hsts [enable | disable | view]
```

Enable, disable, or view the HTTPS Strict Transport Security (HSTS) protocol and adds Strict-Transport-Security header to responses. Support for HSTS depends on your client software and its support of this feature.

**WARNING**

Before enabling this option, ensure that your Management Center appliance has a DNS record, that all administrators access it using the hostname associated with that DNS record, and that an SSL certificate that has been signed by a trusted certificate authority (CA) is installed. See Statistics Monitoring over HTTPS for steps to install a CA-signed certificate.

```
(config)# security http
```

Subcommands:

```
# security http enable
# security http disable
# security http view
```

Enables or disables HTTP access to port 8080. The command also controls access to statistics monitoring port 9009. By default, HTTP is disabled. You can enable HTTP in the following cases:

- You want to install system images without a secure connection on managed devices.
- You want to monitor appliances over HTTP port 9009.

**NOTE**

If you enable HTTP after using HTTPS, you must delete the HTTPS cookie from your browser to be able to use the HTTP connection for the UI.

**TIP**

Changes to this security command will take effect the next time Management Center is restarted.

# service-action

The service-action command allows you to view disk usage and troubleshoot the following issues:

- Disk space or possible file corruption issues
- Cache repository index issues
- Possible VPM cache corruption issues
**Perform Disk Maintenance**

Clean your disk by using the `# service-action db-maintenance` command and subcommand. This command performs a manual database cleanup and re-indexing. Management Center and statistics monitoring are unavailable while running this maintenance command.

**Syntax**

```
# service-action db-maintenance
```

**NOTE**

Automated disk space cleanup occurs when Management Center reaches 85 percent of disk utilization. This automated cleanup removes backed up dump files and all but the latest Management Center backup. This automated cleanup is not as thorough as performing disk maintenance manually. Management Center and statistics monitoring remain available and running.

**Take Memory Dumps for Management Center Services**

The `service-action memory-dump` command enables you to take memory dumps for the following services:

- Management Center (web UI, device management, policy management, scheduled jobs, reporting, alerts, and so on)
- Report Generator (for offline reports)
- Statistics Monitoring

Access the memory dumps in the UI here: Administration > Logs. You can also upload the memory dumps to support using the `diagnostics service-info send options` command. All memory dumps are deleted whenever Management Center restarts. The deletion is done to preserve disk space.

**Syntax**

```
#service-action memory-dump management-center | report-generator | statistics-monitoring
```

**Purge VPM Cache**

If you receive a message when starting the Visual Policy Manager Editor from the web console that a jar mismatch exists, purge the VPM cache. The error happens rarely, such as if there is a network failure while jars are being transferred between devices.

Purge all Visual Policy Manager .jar files by using `#service-action purge-vpm cache` command.

**Syntax**

```
#service-action purge-vpm cache
```

**Rebuild Cache Repository Index**

Management Center maintains an index of device backups, policy, scripts, and other configuration elements. If issues arise with this index, Management Center may behave in an unexpected manner. As directed by Symantec support staff, run this command to rebuild the cache repository index.

**Syntax**

```
#service-action rebuild-repository-index
```
Remove Orphan Device Count in Statistics Monitoring Dashboard

If the following scenario is true, one or more "orphan" devices can be shown in the Statistics Monitoring Dashboard:

- A user replaced a monitored device on the network with a different device that used the same IP address, without completing the RMA Device operation.

This caused Management Center to retain information about removed device in Statistics Monitoring Database. You can now remove these orphan devices using the following CLI command.

**Syntax**

```
# service-action purge-statistics-monitoring-orphans
```

After you execute the command, Management Center deletes the orphans and writes the results to syslog.

**shutdown**

**Syntax**

```
# shutdown
```

**snmp**

Configure Secure Network Management Protocol (SNMP).

**Syntax**

```
(config) # snmp ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent</td>
<td>Configure the SNMP agent. When an SNMP manager polls a device for information, the SNMP agent on the device responds to the queries. See snmp agent.</td>
</tr>
<tr>
<td>community</td>
<td>Define the community strings for SNMP v1/v2c. See snmp community.</td>
</tr>
<tr>
<td>system</td>
<td>System configuration (contact, location, name). See snmp system.</td>
</tr>
<tr>
<td>usm local</td>
<td>Define an SNMP local user entry. See snmp usm local.</td>
</tr>
<tr>
<td>usm remote</td>
<td>Define a user or a management system that receives notification of SNMPv3 traps and informs. See snmp usm remote.</td>
</tr>
<tr>
<td>vacm</td>
<td>Configure view-based access control model. See snmp vacm group access and snmp vacm group member.</td>
</tr>
</tbody>
</table>

**snmp agent**

When an SNMP manager polls a device for information, the SNMP agent on the device responds to the queries.
### Syntax

(config) snmp agent ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disable the agent</td>
</tr>
<tr>
<td>enabled</td>
<td>Enable the agent</td>
</tr>
<tr>
<td>max-message-size &lt;value&gt;</td>
<td>The maximum length of SNMP message the agent can send or receive. Range: 484-214748364. Default=50000.</td>
</tr>
<tr>
<td>version v1</td>
<td>v2c</td>
</tr>
</tbody>
</table>

### Examples

(config)# snmp agent enabled
(config)# snmp agent version v3

---

**snmp community**

Define community strings for SNMP v1/v2. The community string acts as a password for accessing statistics on the device. Equipment usually ships with a read-only community string set to public but network managers typically change the community string to a customized value. Each system that polls your appliance could potentially have a different community string.

**NOTE**

SNMP community strings are used only by devices that support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

### Syntax

(config)# snmp community <string>

After defining the community string, the command prompt changes, indicating the community string. For example, for a community string public, the prompt looks as follows: (config-community-public)#

The following sub-commands are available in community string configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name &lt;string&gt;</td>
<td>Necessary only when the community string is not the same as the index.</td>
</tr>
<tr>
<td>sec-name string &lt;value&gt;</td>
<td>Initially set to the value of 'index.'</td>
</tr>
<tr>
<td>target-tag &lt;target_name&gt;</td>
<td>Limit access for this community to the specified target(s). See snmp target for more information.</td>
</tr>
</tbody>
</table>

### Examples

(config)# snmp community public
(config-community-public)# target-tag v1target
**snmp system**

Configure SNMP system settings to identify the contact name, location, and fully-qualified domain name of the appliance.

**Syntax**

```
(config) snmp system ?
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>contact &lt;name&gt;</td>
<td>The name of the person managing the appliance; &lt;name&gt; can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.</td>
</tr>
<tr>
<td>location &lt;place&gt;</td>
<td>The physical location of the appliance (room, floor, building), where &lt;place&gt; can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.</td>
</tr>
<tr>
<td>name &lt;fqdn&gt;</td>
<td>The appliance's fully-qualified domain name for SNMPv1, where &lt;fqdn&gt; can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.</td>
</tr>
</tbody>
</table>

**Examples**

```
(config)# snmp system contact "Gail Jellison"

(config)# snmp system location "building B, 1st floor"
```

**snmp usm local**

Define an SNMPv3 local user entry.

**Syntax**

```
(config)# snmp usm local user <user_name>
```

After defining the local user name, the command prompt changes, indicating you are in configuration mode for the local user. You can then define authentication and/or privacy keys that a management system can use to access the appliance.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth [md5</td>
<td>sha {key &lt;key&gt;</td>
</tr>
<tr>
<td>priv [aes</td>
<td>des {key &lt;key&gt;</td>
</tr>
</tbody>
</table>

**Examples**

```
(config)# snmp usm local user altman

(config-user-altman)# auth md5 password Gquw4321

(config-user-altman)# priv aes password Gquw4321
```
**snmp usm remote**
Define the remote engine ID that receives notification of SNMPv3 traps and informs.

**Syntax**
```
(config)# snmp usm remote
```

**snmp vacm group access**
Define access for an SNMP group. Each group is defined by a name, a security model (and level), and a set of views that specifies which types of MIB data that access group can read or write.

**Syntax**
```
(config)# snmp vacm group <group_name> access {usm | v1 | v2c} {auth-no-priv | auth-priv | no-auth-no-priv}
```

<table>
<thead>
<tr>
<th>Access Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-no-priv</td>
<td>A connection that is secured with a passphrase and authentication but no encryption.</td>
</tr>
<tr>
<td>auth-priv</td>
<td>A connection that is secured with both authentication and encryption.</td>
</tr>
<tr>
<td>no-auth-no-priv</td>
<td>A connection that uses a simple passphrase (known as a shared secret) to secure the communication.</td>
</tr>
</tbody>
</table>

After defining the access rights for the group, the command prompt changes, indicating the security level. For example:
```
(config-access-v1/auth-no-priv)#
```
You then need to specify the name of the MIB view for each type of access.

<table>
<thead>
<tr>
<th>MIB View Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>notify-view &lt;MIB_view&gt;</td>
<td>Specify the name of the MIB view of the SNMP context authorizing notify access. For example, in Content Analysis the view is named cas-view (and is not user-definable).</td>
</tr>
<tr>
<td>read-view &lt;MIB_view&gt;</td>
<td>Specify the name of the MIB view of the SNMP context authorizing read access. Note that SNMPv1 is not permitted in read-view.</td>
</tr>
<tr>
<td>write-view &lt;MIB_view&gt;</td>
<td>Specify the name of the MIB view of the SNMP context authorizing write access. Note that write-view is not implemented in all products.</td>
</tr>
</tbody>
</table>

**Examples**
```
(config)# snmp vacm group cas-group-v2c access v2c auth-no-priv

(config-access-v1/auth-no-priv)# read-view cas-view
```

**snmp vacm group member**

**Syntax**
```
(config)# snmp vacm group <group_name> member <member_name> {sec-model usm | v1 | v2c}
```
Examples

```
(config)# snmp vacm group cas-group-2vc member member1 sec-model v2c
(config)# snmp vacm group cas-group-2vc member member2 sec-model v2c
```

After defining members, you can define the access rights for the group. See `snmp vacm group access`.

splunkforwarder

Manages the Splunk forwarder service. Forwarders collect data (primarily log events) from employee endpoints and servers, and deliver the data to Splunk Enterprise or Splunk Cloud for indexing and analysis. For Management Center (MC), the Splunk forwarder forwards MC system-specific logs. Essentially, this is the MC syslog.

Syntax

```
(config)# splunkforwarder ?
```

```
host <host name or ip address>  Configure the host name or IP address of the Splunk forwarder.
port <number>  Define the Splunk forwarder's listening port number.
reload  Reload configuration and restart Splunk forwarder service.
status  Display the status of the Splunk forwarder service (running or stopped).
stop  Stop the Splunk forwarder service.
```

Examples

```
(config)# splunkforwarder host 10.10.10.10
(config)# splunkforwarder port 9997
(config)# splunkforwarder status
```

running

ssh-console

Syntax

```
(config)# ssh-console ciphers add | demote | promote | remove | reset | set | view  Add, remove, or change the order of Cipher Block Chaining (CBC) ciphers. By default, CBC ciphers are disabled. Promote and demote change the cipher order.
(config)# ssh-console delete  Delete SSH objects, for example, client keys.
(config)# ssh-console generate host-keypair | view  Generate a 2048-bit RSA host key pair. If you believe the key's security was compromised, you can generate a new SSH key pair.
(config)# ssh-console hmacs add | demote | promote | remove | reset | set | view  Add, remove, or change the order of Hash-based Message Authentication Codes (HMAC).
```
Management Center - 3.0

**Examples**

```plaintext
(config)# ssh-console inline
Import an SSH object, for example, a client key.

(config)# ssh-console key-exchange-algorithms add | demote | promote | remove | reset | set | view
Add, remove, or change the order of key exchange algorithms.

(config)# ssh-console public-key-authentication enable | disable
Enable or disable public key authentication.
```

```plaintext
Examples

(config) # ssh-console generate host-keypair
Are you sure you want to regenerate the keypair? [yes,no] y
SSH host key successfully regenerated

(config-ssh-console) # ciphers view
Ciphers: aes128-ctr,aes192-ctr,aes256-ctr
```

### ssl

Enable or disable Cipher Block Chaining (CBC) ciphers. By default, CBC ciphers are enabled.

**Syntax**

```plaintext
(config)# ssl ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>create [keyring</td>
<td>ccl</td>
</tr>
<tr>
<td>delete [ca-certificate certificate</td>
<td>keyring</td>
</tr>
<tr>
<td>edit [ca-certificate certificate</td>
<td>keyring</td>
</tr>
<tr>
<td>inline [ca-certificate</td>
<td>ccl</td>
</tr>
<tr>
<td>regenerate certificate &lt;keyring-id&gt; subject &lt;subject&gt; [alternative-names] [force]</td>
<td>Regenerate an existing CA certificate and provide new subject and alternative name data. Force is optional, and will overwrite an existing certificate without confirmation.</td>
</tr>
<tr>
<td>trust-package [auto-update</td>
<td>download-now</td>
</tr>
<tr>
<td>view [ca-certificate</td>
<td>ccl</td>
</tr>
</tbody>
</table>
Management Center - 3.0

Notes

• The sub-commands that previously listed can either be entered in SSL configuration mode (at the `config-ssl` prompt) or in configuration mode (at the `config` prompt).

• Use the `show full-configuration ssl` command in configure mode to display basic SSL settings. Use the `(config-ssl-view)# ?` command to view specific keyrings, CA Certificate Lists, Certificates, and Certificate Signing Requests.

Examples

Add a certificate from a Certificate Authority; the certificate name in this example is `ca1`.

```
(config)# ssl
(config-ssl) inline ca-certificate ca1 content
-----BEGIN CERTIFICATE-----
MIIiEdTCCAvWgAwIBAgIJAIk7y/gggzO8MA0GCSqGSIb3DQEBBQUAMIGcMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJU3Vubnl2YWxl
MRIwEAYDVQQDA1CHV1lEMEExMDExNTQ2LWIwMTUtMjI0Ny0xMDY2LTIwMDUtMTI1
MQswCQYDVQQGEwJQQ0EwJwYDVQQDEBoUI3Vubnl2YWxlMB4XDTI0MDQ0MjA1MMY1
Fg0wEAYDVQQIEwNQQ0EwDwYDVQQHEDAUaGEwDQYJKoZIhvcNAQcBFgEBMA0GA1UE
CgwKU29vdGltZSMBMGA1UdJQQEBGQIwCYhZDVQQGEwJQQ0EwJwYDVQQDEBoUaGEw
-----END CERTIFICATE-----
<Ctrl-D>
```

CA certificate `ca1` is added successfully.

To view the certificate details for the `ca1` certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer:     /C=US/ST=California/L=Sunnyvale/O=Blue Coat/CN=ca.bluecoat/  
emailAddress=eric.chi@bluecoat.com
Subject:    /C=US/ST=California/L=Sunnyvale/O=Blue Coat/CN=ca.bluecoat/  
emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
```

ssl create

Create SSL keyrings, CA Certificate Lists (CCLs), Certificate Revocation Lists (CRLs), signing requests, self-signed certificates, and ssl-contexts.
### Syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssl create ?</code></td>
<td>Create a CA Certificate List (CCL).</td>
</tr>
<tr>
<td>`ssl create keyring &lt;keyring id&gt; algorithm rsa length &lt;key_length&gt; showable [yes</td>
<td>no</td>
</tr>
<tr>
<td><code>ssl create certificate &lt;keyring id&gt;</code></td>
<td>Create a self-signed certificate associated with the specified keyring. You will be prompted to define values for each of the certificate fields (country, state, and so forth).</td>
</tr>
<tr>
<td><code>ssl create ssl-context &lt;context_id&gt; [keyring &lt;keyring_id&gt;] [ccl &lt;ccl_name&gt;] [protocol [ &lt;protocol&gt; ... ]] [cipher-suite [ &lt;cipher-suite&gt; ... ]]</code></td>
<td>Creates an SSL context with the specified name and (optional) keyring, CCL, protocols and cipher suites.</td>
</tr>
<tr>
<td><code>ssl create signing-request &lt;keyring id&gt;</code></td>
<td>Create a request for a signed certificate associated with the specified keyring. You must specify all parameters when prompted for 'Value for subject'</td>
</tr>
<tr>
<td><code>ssl delete ?</code></td>
<td>Delete CA certificate.</td>
</tr>
<tr>
<td><code>ssl delete ca-certificate &lt;certificate name&gt;</code></td>
<td>Delete a CA Certificate List (CCL).</td>
</tr>
<tr>
<td><code>ssl delete ccl</code></td>
<td>Delete a Certificate Revocation List (CRL).</td>
</tr>
<tr>
<td><code>ssl delete certificate &lt;keyring id&gt;</code></td>
<td>Delete the certificate that's in the specified keyring.</td>
</tr>
<tr>
<td><code>ssl delete keyring &lt;keyring id&gt;</code></td>
<td>Delete the specified keyring.</td>
</tr>
<tr>
<td><code>ssl delete signing-request &lt;keyring id&gt;</code></td>
<td>Delete the certificate request for the specified keyring.</td>
</tr>
<tr>
<td><code>ssl delete ssl context &lt;context_id&gt;</code></td>
<td>Delete the specified SSL context.</td>
</tr>
</tbody>
</table>

#### Examples

```text
(config)# ssl create keyring sslkey algorithm rsa length 3072 showable no

(config)# ssl create signing-request sslkey subject "C=US,ST=CA,O=Symantec,CN=mc" alternative-names "198.51.100.20, altname2.companyname.com"
```

### ssl delete

Delete SSL certificates, Certificate Revocation Lists (CRLs), keyrings, and signing requests.

#### Syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssl delete ?</code></td>
<td>Delete CA certificate.</td>
</tr>
<tr>
<td><code>ssl delete ca-certificate &lt;certificate name&gt;</code></td>
<td>Delete a CA Certificate List (CCL).</td>
</tr>
<tr>
<td><code>ssl delete ccl</code></td>
<td>Delete a Certificate Revocation List (CRL).</td>
</tr>
<tr>
<td><code>ssl delete certificate &lt;keyring id&gt;</code></td>
<td>Delete the certificate that's in the specified keyring.</td>
</tr>
<tr>
<td><code>ssl delete keyring &lt;keyring id&gt;</code></td>
<td>Delete the specified keyring.</td>
</tr>
<tr>
<td><code>ssl delete signing-request &lt;keyring id&gt;</code></td>
<td>Delete the certificate request for the specified keyring.</td>
</tr>
<tr>
<td><code>ssl delete ssl context &lt;context_id&gt;</code></td>
<td>Delete the specified SSL context.</td>
</tr>
</tbody>
</table>

#### Example

```text
(config-ssl)# delete signing-request sslkey
```
ssl edit

Edit CA certificate lists (CCLs), Certificate Revocation Lists (CRLs), or SSL contexts.

Syntax

```
(config)# ssl edit ccl [action] ?
```

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add a certificate by name to the selected CA certificate list.</td>
</tr>
<tr>
<td>remove</td>
<td>Remove a certificate from the selected CA certificate list.</td>
</tr>
<tr>
<td>reset</td>
<td>Empty the CA certificate list for this CA certificate list.</td>
</tr>
<tr>
<td>set</td>
<td>Set CA certificate list for this CA certificate list.</td>
</tr>
<tr>
<td>view</td>
<td>View the certificates in the selected CA certificate list.</td>
</tr>
</tbody>
</table>

```
(config)# ssl edit crl [action] ?
```

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>download</td>
<td>Download a certificate revocation list.</td>
</tr>
<tr>
<td>path</td>
<td>Set the download URL of the CRL. When you enter a URL, the system periodically checks the URL to update the contents of the CRL. The refresh interval is set using the <code>refresh-interval</code> command.</td>
</tr>
<tr>
<td>refresh-interval</td>
<td>Set the amount of time to elapse before revalidating the CRL information specified in <code>path</code>. The value must be as follows: `&lt;auto</td>
</tr>
<tr>
<td>view</td>
<td>View CRL configuration.</td>
</tr>
</tbody>
</table>

```
(config)# ssl edit ssl-context [action] ?
```

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccl</td>
<td>Set the CCL for the SSL context.</td>
</tr>
<tr>
<td>cipher-suites</td>
<td>SSL context cipher suite configuration.</td>
</tr>
<tr>
<td>keyring</td>
<td>Set the keyring for the SSL context.</td>
</tr>
<tr>
<td>protocols</td>
<td>Set SSL context protocols.</td>
</tr>
<tr>
<td>view</td>
<td>View the SSL context configuration.</td>
</tr>
</tbody>
</table>

Examples

Add CRL URL path.

```
(config-ssl)# create crl crl_name
(config-ssl)# edit crl crl_name
(config-ssl-crl_name)# path http_or_https_url_of_crl
(config-ssl-crl_name)# refresh-interval 2.5h
```

(config)# ssl
(config-ssl)# edit ccl browser-trusted

(config-ccl-browser-trusted)# add esignit.org
ok
(config-ccl-browser-trusted)# view
Name: browser-trusted
FIPS compliant: no
Certificates:
1st_Data_Digital
A-Trust-Qual-02
A-Trust-Root-05
A-Trust-nQual-03
AC1_Raiz_Mtin
ACA_ROOT
ACCV_ACCVRAIZ1
ACEDICOM_Root
..

ssl inline
Import SSL keyrings, Certificate Revocation Lists (CRLs), signing requests, and certificates.

Syntax
(config)# ssl inline ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca-certificate</td>
<td>Import a Certificate Authority (CA) certificate from terminal input (typically by pasting the certificate content with a right-click). Press Ctrl-D after pasting the certificate content.</td>
</tr>
<tr>
<td>certificate</td>
<td>Import a certificate into the specified keyring. You will be prompted to paste the certificate content and press Ctrl-D when finished.</td>
</tr>
<tr>
<td>crl</td>
<td>Import certificate revocation list (CRL). You will be prompted to paste the CRL content and press Ctrl-D when finished.</td>
</tr>
<tr>
<td>keyring</td>
<td>Install a keyring. Keyrings are containers for SSL certificates on the appliance, and can be used to manage self-signed or CA-signed certificates. You will be prompted to paste the keyring content and press Ctrl-D when finished.</td>
</tr>
<tr>
<td>signing-request</td>
<td>Install a request for a signed certificate associated with the specified keyring. You will be prompted to paste the signing request content and press Ctrl-D when finished.</td>
</tr>
</tbody>
</table>

Examples
Add a certificate from a Certificate Authority; the certificate name in this example is ca1.

(config)# ssl
Enter the certificate below and end it with a Ctrl-D

-----BEGIN CERTIFICATE-----
MIIDcTCCAvWgAwIBAgIJAIk7y/gggz0MA0GCsqGSIb3DQEBCwUAMIGcMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJUEwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEoIAQAwHgYDVR0PAQH/MB8GA1UdDwEB/wQEAw
eMBoIAfKdCCAgAwggMiMBAGA1UEBhMCR0KVMRMwEQYDVQQKDAcMRA8wDgYDVR0T
BBAdBgNVHQ8BAf8EAwIGBgNAQgIBDQIBDQIBDgIBDgIBDgIBDgIBDgIBDgIBDg
-----END CERTIFICATE-----

<Ctrl-D>

CA certificate ca1 is added successfully.

To view the certificate details for the ca1 certificate:

```bash
(config-ssl)# view ca-certificate ca1
```

Issuer:   /C=US/ST=California/L=Sunnyvale/O=Blue Coat/OU=Development/CN=ca.bluecoat/
emailAddress=eric.chi@bluecoat.com
Subject:  /C=US/ST=California/L=Sunnyvale/O=Blue Coat/OU=Development/CN=ca.bluecoat/
emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT

```bash
ssl view
```

View CA Certificate List (CCL), Certificate Revocation List (CRL), certificate, keyring details, and signing request confirmations.
**Syntax**

```
(config)# ssl view ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ca-certificate &lt;certificate name&gt; [verbose]</code></td>
<td>Show CA certificate and content.</td>
</tr>
<tr>
<td><code>ccl &lt;ca certificate list name&gt;</code></td>
<td>View the details for a specific CA Certificate List.</td>
</tr>
<tr>
<td><code>crl &lt; certificate revocation list name&gt;</code></td>
<td>View the details for a specific Certificate Revocation List (CRL).</td>
</tr>
<tr>
<td><code>certificate &lt;keyring id&gt;</code></td>
<td>Show the certificate that’s in the specified keyring.</td>
</tr>
<tr>
<td><code>keypair &lt;keyring id&gt;</code></td>
<td>Show the RSA private key for the specified keyring. If the keyring was created with the &quot;showable no&quot; option, the key will not be displayed.</td>
</tr>
<tr>
<td><code>keyring &lt;keyring id&gt;</code></td>
<td>Show details about the specified keyring, including its certificate and any signing requests.</td>
</tr>
<tr>
<td><code>signing-request &lt;keyring id&gt;</code></td>
<td>View certificate request for the specified keyring.</td>
</tr>
<tr>
<td><code>ssl-context &lt;context id&gt;</code></td>
<td>View SSL context configuration.</td>
</tr>
</tbody>
</table>

**Examples**

To view the certificate details for the ca1 certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue Coat/OU=Development/CN=ca.bluecoat/
emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue Coat/OU=Development/CN=ca.bluecoat/
emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
```

To show information about a keyring, in this case called sslkey:

```
(config-ssl)# view keyring sslkey
Keyring ID: sslkey
Private key showability: no-show
Signing request: absent
Certificate: present
Certificate subject: /C=us/ST=ca/L=pa/O=symantec/OU=marketing/CN=symantec.com/
emailAddress=test@test.com
Certificate issuer: /C=us/ST=ca/L=pa/O=symantec/OU=marketing/CN=symantec.com/
emailAddress=test@test.com
Certificate valid from: Jul 21 05:17:51 2017 GMT
Certificate valid to: Jul 21 05:17:51 2017 GMT
```

To view the CA certificates contained in the CA certificate list, bluecoat-licensing:
BC_Engineering_CA

To view the default SSL context:

```bash
(config-ssl)# view ssl-context default
Name: default
Keyring: default
CCL: browser-trusted
Protocols: tlsv1.2 tlsv1.1 tlsv1
```

**statistics-monitoring**

The statistics-monitoring command can be used view the parameters for the storage of device statistics for managed devices and to set thresholds for how long Management Center will retain that data. The thresholds set here control the data used for reports in Management Center's management console, under Reports > Statistics Monitoring. These reports contain data from devices that have been configured to report statistics, and their associated hardware statistics such as CPU and memory utilization, and traffic flow. This command is available in both enable # mode and (config)# modes, however only the view subcommand is available in enable mode.

**Syntax**

```
# statistics-monitoring [subcommands]
```

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maintenance</td>
<td>Enable or disable database maintenance for gathered statistics. Database maintenance initiates constant analysis of the stored data with the goal of optimizing query performance for reports that use this data. The default value is enable.</td>
</tr>
<tr>
<td>set-per-hour-lifetime</td>
<td>Set a lifetime for how long the appliance will retain per-hour trend data. Must be entered in number of days between 1 and 732. The default value is 366 days.</td>
</tr>
<tr>
<td>set-per-minute-lifetime</td>
<td>Set a lifetime for how long the appliance will retain per-minute trend data. Must be entered in number of days between 1 and 30. The default value is 7 days.</td>
</tr>
<tr>
<td>view</td>
<td>View current statistics monitoring lifetime settings, record statistics, and disk usage data.</td>
</tr>
</tbody>
</table>

**Example**

```
# statistics-monitoring view
Total devices: 2
Reporting devices: 1
```
Maintenance: enabled

<table>
<thead>
<tr>
<th>Data Characteristics:</th>
<th>Lifetime</th>
<th>Records</th>
<th>Disk Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>minute</td>
<td>7 days</td>
<td>140439</td>
<td>91 MB</td>
</tr>
<tr>
<td>hour</td>
<td>366 days</td>
<td>142380</td>
<td>52 MB</td>
</tr>
</tbody>
</table>

**timezone**

Set the time zone where the appliance is located or choose the Coordinated Universal Time (UTC) time standard.

**Syntax**

```
(config)# timezone [area]/location | UTC | GMT
```

**Supporting Commands**

- `show timezone current` Display the currently configured timezone
- `show timezone` Display the available timezone areas.
- `show timezone <area>` Display the full list of timezones in a specific area.
- `show timezone <value>` Display the current time to see the local time in a specific timezone.

**Examples**

To select UTC as the time standard (instead of setting a time zone):

```
(config)# timezone UTC
```

To set an Antarctica time zone:

```
(config)# show timezone
Africa
America
Antarctica
Arctic
Asia
Atlantic
Australia
Europe
Indian
Pacific
UTC
GMT
all
current
```

```
(config)# show timezone Antarctica
Antarctica/McMurdo
```
upload
Upload the third-party attributions zip file to an FTP site.

Syntax
# upload ATTRIBUTIONS <full-url/filename> <username> <password>

NOTE
ATTRIBUTIONS must be in uppercase.

Example
upload ATTRIBUTIONS ftp://exampleftp.com/attributions.zip mary ********

virtual-ip
Add a virtual IP address to one of the interfaces on Management Center. The virtual IP address can be used with Management Center failover.

Syntax
(config)# virtual-ip address | view

<table>
<thead>
<tr>
<th>address</th>
<th>Assign a virtual IP address to the current interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
<td>View the current virtual IP address.</td>
</tr>
</tbody>
</table>

Example
(config)# virtual-ip address 198.51.100.15
localhost(config)# virtual-ip view
Virtual-ip:
  Status: starting up...
  Address: 198.51.100.15
  Interface: 0:0
  Peer: not defined
Enable Mode Commands

The following commands are available in enable mode. Enable is a privileged mode that requires its own password.

To enter enable mode, type `enable` at the standard command prompt (`>` ) and enter the password. The prompt will change to `#`. To see a list of commands available in enable mode, type `help` or `?` at the `#` prompt.

**authentication**

Define authentication realms, local users, and security settings for administrative logins to Management Center.

**Syntax**

```
(config)# authentication ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable-password</td>
<td>Change the password for entering enable (privileged) mode.</td>
</tr>
<tr>
<td>management max-concurrent-logins</td>
<td>Set the maximum number of concurrent logins per user. By default, the number of concurrent administrative logins is unlimited.</td>
</tr>
<tr>
<td>management inactivity-timeout</td>
<td>Specify the number of seconds a session can be inactive before it is terminated. By default, this is 1800 seconds.</td>
</tr>
<tr>
<td>password</td>
<td>Specify a new password for the default admin account.</td>
</tr>
</tbody>
</table>

**Notes**

- The sub-commands listed above can either be entered in authentication configuration mode (at the `config-authentication` prompt or in configuration mode (at the `config` prompt).
- Use the `show full-configuration` command in authentication configuration mode to display the authentication settings.

**Examples**

```
(config)# authentication password
Enter current password: *****
Enter new password: *****
Confirm new password: *****
ok
```

**backup**

Back up the Management Center configuration, and view, export, and restore existing backups.

**Syntax**

```
(config)# backup [subcommands]
```

**NOTE**

While you may also run this command from the enable prompt, Symantec recommends running this command at the `(config)` prompt.

**Subcommands**

```
(config)# backup create [description] [statistics-monitoring-trend-data]
```
Management Center - 3.0

(config)# backup create

Create a full system backup.

(config)# backup create description

Create a Management Center backup and provide a description of that backup.

(config)# backup create statistics-monitoring-trend-data[include|exclude]

Define whether to include Statistics data when creating backups. By default, this data is excluded.

(config)# backup delete <index_number>

Delete the specified configuration backup.

Use the backup view command to determine the index number to use.

(config)# backup export <index_number> <URL> [passphrase] [password] [username]

Export the specified backup to a destination FTP/FTPS, HTTP/HTTPS, or SCP/SFTP server. When exporting configuration backups, the CLI requires that you enter a passphrase to encrypt the backup file before sending it to the specified server. Password and Username entries are optional, and dependant on the destination server's requirements.

Use the backup view command to determine the index number to use. <URL> is the URL of the destination server and path. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP. Verify the filename on the server, and include that in the path as in the following example: ftp://192.0.200.68/bcmc_backup_20180402_191517.tgz.gpg.

(config)# backup import <URL> [passphrase] [password] [username]

Import a backup from a specified server. To import the backup, you must enter the passphrase that was used to encrypt the backup during the initial backup export.

<URL> is the URL of the external server and path. Supported protocols are FTP, FTPS, HTTP, HTTPS, and SCP.

(config)# backup restore <index_number>

Restore a Management Center backup, specified by the index number. This command is only available when the backup command is entered from a (config) prompt.

Use the backup view command to determine the index number to use.

(config)# backup view

View existing configuration backups.

Transfer Configuration and Data to Another Appliance

To transfer configuration and data from one Management Center appliance to another:

1. On the first Management Center: use the backup create command to back up the configuration.
2. Use the backup export command to upload the backup to a Web, FTP, SCP, or SFTP server.
3. Log in to the second Management Center appliance, and use the `backup import` command to download the backup from the server specified in step 2.
4. Restore the backup using the `backup restore` command.

**WARNING**
Configuration backups are not human-readable, and can only be restored to Management Center appliances running the same version as the original appliance was running at the time the backup was recorded.

**Example**

```
(config)#
    backup create description "before upgrade to 2.0" statistics-monitoring-trend-data exclude
ok

(config)# backup view

1. Version : 2.1.0.0 (196304-Debug), Creation Time : 2017-01-09 21:05:27 UTC,
   Statistic Monitoring Trend Data : false, Size : 4.6 MB,
   Description : none
2. Version : 2.0.0.0 (214174-Debug), Creation Time : 2018-02-23 19:03:00 UTC,
   Statistic Monitoring Trend Data : false, Size : 2.7 MB,
   Description : before upgrade to 2.0
(config)# backup export 2 ftp://192.0.200.55/appliance_backups/ passphrase "this is a test passphrase"

Securing backup archive ... Exporting backup archive ... ok

(config)# backup import ftp://192.0.200.55/appliance_backups/bcmc_backup_20180402_200649.tgz.gpg
Value for 'passphrase' (<string>): *****************
Importing backup archive bcmc_backup_20180402_200649.tgz.gpg ...
Downloading backup archive ...
Verifying backup archive ...
Securing backup archive ...
Backup archive successfully imported.
ok
```

clock

Manually set the time and date of the appliance in Coordinate Universal Time (UTC).

**Syntax**

```
# clock day <value>|hour <value>|minute <value>|month <value>|second <value>|year <value>
```

Each value must be entered as a separate command.

**Examples**

To set the date to September 2, 2016:

```
# clock day 2
# clock month 9
# clock year 2016
```
NOTE
If you are using an NTP server, you do not need to manually set the clock.

configure
A command to enter a mode in which CLI commands are available for changing the configuration of the software and appliance.

Syntax
# configure

Notes
• When in configure mode, the command prompt changes to: (config)#
• Type ? to see a list of CLI commands available in configure mode.
• Type exit to disable configure mode. The command prompt changes to: #

diagnostic-systems
Manage diagnostic images installed on the system. Up to six images can be installed on the system. If your system already has six images installed and you add another image, the oldest unlocked image will be replaced with the new image, unless you have designated a particular image to be replaced.

Syntax
(config) # diagnostic-systems ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Cancel the download process of an image that is currently downloading</td>
</tr>
<tr>
<td>delete &lt;image#&gt;</td>
<td>Delete an image from the system. Use the diagnostic-systems view command to identify the image number to delete.</td>
</tr>
<tr>
<td>load &lt;URL&gt;</td>
<td>Download and install a diagnostic image on the system. &lt;URL&gt; is the path to an image on a web server that the appliance has access to. Example: <a href="http://webserver.mycompany.com/images/diag.bcs">http://webserver.mycompany.com/images/diag.bcs</a></td>
</tr>
<tr>
<td>lock &lt;image#&gt;</td>
<td>Lock a diagnostic image to protect it from accidental deletion.</td>
</tr>
<tr>
<td>replace &lt;image#&gt;</td>
<td>Designate which image will be replaced next (if the system already has six installed images and you load another image). If you do not specify an image to be replaced, the oldest unlocked image on the system will be replaced.</td>
</tr>
<tr>
<td>unlock &lt;image#&gt;</td>
<td>Unlock a diagnostic image that you no longer want to protect from deletion. You have to unlock a locked image before you can remove it.</td>
</tr>
<tr>
<td>unset-replace</td>
<td>Unset image to be replaced next. When a replacement image is not designated, the oldest image will be replaced when you load a seventh image.</td>
</tr>
</tbody>
</table>
### view

Show a list of installed diagnostic images along with their image numbers, software versions, release IDs, whether the image is locked or unlocked, whether it has ever been booted, creation date/time, and boot date/time. The summary at the bottom of the list indicates which image number is the current running system, the default system to run the next time the appliance is restarted, and the image number that will be replaced next.

**Example**

```
(config) # diagnostic-systems load http://webserver.mycompany.com/images/diag.bcs
```

### diagnostics

Provide access to the appliance or submit troubleshooting information to Support to help diagnose hardware or software issues.

**Syntax**

```
# diagnostics ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activate-remote-access</td>
<td>Activate remote diagnostics access so that Symantec Support can help troubleshoot an issue on your appliance.</td>
</tr>
<tr>
<td>heartbeat view</td>
<td>send</td>
</tr>
<tr>
<td>service-info send</td>
<td>Generate and upload the service diagnostics information to Symantec. Enter the case number if you have opened a support case.</td>
</tr>
<tr>
<td></td>
<td>[service request number]</td>
</tr>
</tbody>
</table>

**Examples**

```
# diagnostics heartbeat send

# diagnostics service-info send 123456789
```

### disable

Return to standard mode.

**Syntax**

```
# disable
```

When enable mode is turned off, the prompt changes from `#` to `>`,

### display-level

Set the depth of the configuration that is shown by the show full-configuration and show running-configuration commands. For example, if the display-level is set to 1, only top-level configuration nodes and their values are shown. If it is set to 2, then top-level nodes and their child nodes are shown, and so on. By default, the entire configuration is shown.
Syntax

# display-level {level<n>}

Examples

# display-level 1

**event-log**

Manage syslog settings. The syslog feature gives administrators a way to centrally log and analyze events on the system.

**NOTE**
Management Center releases before 2.0 used the `rsyslog-output` command to define settings to configure syslog event output to remote servers.

**Syntax**

(config)# event-log

**NOTE**
You can add multiple syslog servers.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **level <value>**              | Set the level to specify which messages to suppress to the syslog server. Releases of Management Center prior to 2.0.x used service enable-verbose-logging to set the log level. If no event-log level is defined, the log detail mirrors what was available in Management Center 1.x with verbose logging disabled. For example, setting the level to 3 allows messages with levels 0 - 3 and suppresses messages with levels 4 - 7. *<value>* can be one of the following:
| 0 Emergency: system is unusable |
| 1 Alert: action must be taken immediately |
| 2 Critical: critical conditions |
| 3 Error: error conditions |
| 4 Warning: warning conditions |
| 5 Notice: normal but significant condition |
| 6 Informational: informational messages |
| 7 Debug: debug-level messages |
| **syslog add host <host> port <port>** | Configure a syslog server where *<host>* is the host name or IP address of the syslog server. Optionally, you can also specify a custom port, where *<port>* is the port number. |
| **syslog add udp host <host> port <port>** | Configure a syslog server using UDP where *<host>* is the host name or IP address of the syslog server. Optionally, you can also specify a custom port, where *<port>* is the port number. |
| **syslog add tls host <host> port <port>** | Configure a syslog server using tls where *<host>* is the host name or IP address of the syslog server. Optionally, you can also specify a custom port, where *<port>* is the port number. |
| **syslog remove host <host>** | Remove a configured syslog server by specifying the *<host>*. |
| **syslog clear** | Removes all configured syslog servers. |
| **view** | View syslog settings |
TIP
TCP syslog communication is not supported in the initial release of MC 2.0.x. Look for updates to this feature in future releases.

NOTE
The sub-commands listed above can either be entered in the enable prompt, event-log configuration mode (at the config-event-log prompt, or in configuration mode (at the config prompt).

Examples
(config)# event-log

(config-event-log)# syslog add udp host 203.0.113.17
Added syslog server host 203.0.113.17:514.
(config-event-log)# view
Log level: 5 (notice)
Remote syslog servers:
203.0.113.17:514

exit
Exit from current mode. For example, if you are in configuration mode, exit returns you to enable mode. If you are in health-monitoring mode, exit returns you to configure mode.

Syntax
exit

NOTE
If you type exit when you are in standard or enable mode, the management session is closed.

Example
(config-authentication)# exit
(config) # exit

#

failover
Configures Management Center failover. Management Center supports failover using two appliances. One appliance is delegated as the primary partner and the other as the secondary partner. During continuous replication, users can perform all normal operations on the primary appliance. Users cannot access the secondary appliance—its sole purpose is to replicate actions occurring on the primary node so that it can take over if something happens to primary node. See Configure Management Center Failover for more information.

NOTE
Management Center 2.0.x supports multiple network interfaces. Symantec recommends that failover partners are configured to communicate over a separate channel. This communication takes place on TCP port 2025. Ensure that this port is open between the two appliances in your security infrastructure.
Syntax
This command is available from an enable mode prompt (#) or the (config)# mode prompt. Running failover in enable mode provides only the view option, while (config)# mode provides all of the options detailed below.

# failover [subcommands]

Subcommands

#failover view

Display current failover settings.

#failover make-primary

Configures the appliance to be the primary partner in the failover group and creates an authentication token for the secondary node that is valid for twenty-four hours.

WARNING
Make note of this token, as it is required for failover make-secondary.

#failover make-secondary [interface|primary-ip|token]

Configures the appliance to be the standby partner in the failover group. Use the optional interface parameter to configure an IP address used by the primary failover host to connect to the secondary node. To force the outgoing communications for failover, define routes in the routing table to force the device-name. See #unique_463/unique_463_Connect_42_ for syntax and additional details.

NOTE
To avoid conflicts with the primary appliance, the secondary appliance cannot run the following CLI commands: installed-systems, diagnostic-systems, licensing, db-maintenance, service purge-vpm-cache, snmp, and statistics-monitoring.

#failover replicate
[authentication-configuration|acl-configuration|diagnostics-configuration]
[false|true]

This command is only available on the secondary failover partner. The command allows you to optionally replicate the authentication, logging and alert, and access control list (ACL) configuration of the primary failover partner.

#failover disable

Disables all failover settings.

Example

#failover view
Failover:
Status: Healthy (0 second replication delay)
Primary*: 198.51.100.20
Secondary: 198.51.100.24

The failover view command output is different on the secondary failover partner:

```
# failover view
Status: Healthy (1 second replication delay)
Primary: 198.51.100.20
Secondary*: 198.51.100.24
Replicating:
ACL Configuration: false
Authentication Configuration: false
Diagnostics Configuration: true
Last status update 11 second(s) ago
(*) this Management Center

#failover make-primary
One-time initial authentication token for secondary node: 58f1ddaa6f878f96
Failover:
Status: Healthy (0 second replication delay)
Primary*: 192.0.100.20
Secondary: 192.0.100.21
Token Expires: Mar 28, 2018
Last status update 1 second(s) ago
(*) this Management Center
Please record authentication token for setup with primary and press Enter.

# failover make-secondary
Value for 'primary-ip' (<IP address>): 192.0.100.20 Value for 'token' (<string, min: 12 chars, max: 36 chars>): ***********
Warning: Initial failover data transfer may take a long time to complete. To complete the failover setup, allow for transfer to finish and do not disable failover on 192.0.100.20 (primary) or 192.0.100.21 (secondary) during this operation. Services on 192.0.100.20 (primary) will not be available while initial failover setup is performed.
Are you sure you want to continue? y
Please authenticate to primary server...
admin@192.0.100.20's password:
Shelving operational data on secondary...done.
Stopping services on secondary...done.
Stopping services on primary...done.
Retrieving snapshot of primary's data...

# failover replicate diagnostics-configuration true
This command, available only on the secondary failover partner, replicates the logging and alert configuration of the primary failover partner.

fips-mode

Enables or disables Federal Information Processing Standards (FIPS) mode. When you enter FIPS mode, the appliance is restored to factory defaults and all previous configurations are destroyed. When you exit FIPS mode, all FIPS configurations are destroyed.

NOTE
Refer to the failover documentation for more information about running Management Center in FIPS mode.

Syntax
```
# fips-mode {subcommands}
```

Subcommands
```
# fips-mode enable
Enables FIPS mode.

# fips-mode disable
Disables FIPS mode
```

halt

Halts the operating system and stops all CPUs. Once the system is cleanly halted, the user may safely press the power switch to turn off the appliance.

Syntax
```
# halt
```

NOTE
The halt and shutdown commands are similar; the only difference is that shutdown disconnects the power via the CLI command.

health-monitoring

View Health Monitoring (HM) events and status, and view and change HM settings.

Syntax
```
(config-health-monitoring)# ?
```
clear-history

Clear the entire event history

```
product1234-10414124(config-health-monitoring)#
clear-history
Event history has been cleared for all metrics.
```

history-duration

Sets the number of days that the HM framework is to store its history of events.
- It takes one argument, an integer representing the number of days.
- Default value is 30.
- Once per day, the HM framework clears the event history of all events older than the specified number of days.

```
product1234-10414124(config-health-monitoring)#
history-duration
(<int>) (30): 60
```

view

Show health status and metric settings. Get detailed information.

history

Specify how far back in the command history previously-entered commands can be retrieved. For example, with a history size of 5, the previous five commands can be retrieved. Each time you press the up arrow, a previously-entered command is displayed.

**NOTE**
When using the up arrow to retrieve previously-entered commands that use passwords, password values are obscured with asterisks.

**Syntax**

```
# history <size>
```

logout

Log out the current user. The management session is ended.

**Syntax**

```
# logout
```

pcap

Capture packets that are sent to and/or from the appliance. The captured data can be imported into a packet analysis tool such as Wireshark.

**NOTE**
Unlike in version 1.x, Management Center 2.0.x does not support packet capture filters for host or port. Rather, all traffic is captured based on the direction and interface defined.
### Syntax

```bash
# pcap ?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>start</strong></td>
<td>Start capturing packets.</td>
</tr>
<tr>
<td><strong>stop</strong></td>
<td>Stop capturing packets.</td>
</tr>
<tr>
<td><strong>transfer &lt;full-url/filename&gt; &lt;username&gt; &lt;password&gt;</strong></td>
<td>Copy captured data to an FTP site. While not necessary, Symantec recommends that you use <code>pcap stop</code> before using this command.</td>
</tr>
<tr>
<td>**filter direction [both</td>
<td>in</td>
</tr>
<tr>
<td>**filter expression [host</td>
<td>port]**</td>
</tr>
<tr>
<td><strong>filter interface &lt;nic&gt;</strong></td>
<td>Filter packets by interface number (0:0, 1:0, 1:1).</td>
</tr>
<tr>
<td>**limit [capsize</td>
<td>count</td>
</tr>
</tbody>
</table>

**NOTE**
Before enabling packet capture, you can optionally restrict the packets that are captured by filtering by direction (in, out, host, port) or interface (for example, just packets sent out of the 1.0 NIC.

After capture is turned on, the system will create a `.dmp` file in TCPDump format and start capturing packets into this file. Packets are captured until capturing is disabled with the `pcap stop` command, or after 30 minutes, whichever comes first.

### Examples

```
(config)# pcap filter direction in

(config)# pcap filter expression host 198.51.100.26 port 22
(config)# pcap limit snapshot-length 65535
(config)# pcap start
(config)# pcap stop

(config)# pcap transfer ftp://example.com/john_files/test.dmp john.smith *****
```

### ping

Generate pings to test connectivity with another device on the network. If the device answers the pings from Management Center, a message displays such as 5 packets transmitted, 5 received, 0% packet loss, time 3007ms. If Management Center is unable to connect with the device, the system displays a message such as 5 packets transmitted, 0 received, 100% packet loss, time 13999ms.

**NOTE**
Previous releases of Management Center supported disabling how the appliance responds to ping from other sources on your network. This functionality is not supported in Management Center 2.0.x; the appliance will always respond to ICMP requests received on configured and connected interfaces. Syntax
**Syntax**

```
# ping ipv4|ipv6 source <source ip address> dont-fragment repeat <ping count> size <packet size> <ip address>|<hostname> ?
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>ipv6</td>
</tr>
<tr>
<td>source &lt;source ip address&gt;</td>
<td>The source IP address to put in the ping packet</td>
</tr>
<tr>
<td>repeat &lt;ping count&gt;</td>
<td>The number of ping packets to send. The default is 5.</td>
</tr>
<tr>
<td>size &lt;packet size&gt;</td>
<td>The size of the ping packets (in bytes). The default is 100 bytes.</td>
</tr>
<tr>
<td>dont-fragment</td>
<td>Set the dont-fragment flag on the ping packets.</td>
</tr>
<tr>
<td>&lt;ip address&gt;</td>
<td>&lt;hostname&gt;</td>
</tr>
</tbody>
</table>

**Examples**

```
# ping repeat 3 size 50 cnn.com

PING cnn.com (157.166.226.25) 50(78) bytes of data.
58 bytes from www.cnn.com (157.166.226.25): icmp_seq=1 ttl=115 time=63.2 ms
58 bytes from www.cnn.com (157.166.226.25): icmp_seq=3 ttl=115 time=62.9 ms
--- cnn.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 62.880/63.022/63.268/0.338 ms
# ping 10.10.10.10

PING 10.10.10.10 (10.10.10.10) 100(128) bytes of data.
--- 10.10.10.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 13999ms
```

**restart**

Reboots the system and restarts services such as image, licensing, subscription, SNMP, and health monitoring. You will need to restart the system after upgrading to a new image or changing the running image on the appliance.

**Syntax**

```
# restart
```

**restore-defaults**

Restore system to factory default settings. This process deletes all data on the appliance.

**Syntax**

```
# restore-defaults factory-defaults [halt|shutdown] [force]
```
### halt
After the system is restored to factory defaults, the operating system is halted and CPUs are stopped.

### shutdown
After the system is restored to factory defaults, the operating system is halted, CPUs are stopped, and the appliance is powered off.

### force
The user is not prompted to confirm the action.

#### Examples

```bash
# restore-defaults factory-defaults
Restoring box to factory state. This will delete all customer data and shutdown the system. Do you want to proceed (yes/no):
```

If the user responds with y (for yes), the system will be restored to factory defaults and all customer data will be wiped from the drives.

```bash
# restore-defaults factory-defaults shutdown force
The user is not asked to confirm the action; the system is restored to factory defaults and then powered down.
```

#### send
Send one or all users a message to their terminal. The message will be shown in the CLI session of any logged-in user.

**Syntax**

```bash
# send <user>|all <message>
```

**NOTE**

The user must be logged on to receive the message.

**Examples**

```bash
# send all "This is an important message."
```

```bash
# Message from admin@ManagementCenterMain at 2016-09-22 15:09:36...
This is an important message.
```

#### shutdown

**Syntax**

```bash
# shutdown
```

#### subscription
View and download subscriptions for which your appliance has licenses. Examples include anti-virus (Kaspersky, McAfee, Sophos) and allowlisting services. When you request a download of an anti-virus subscription, the system will check
to see if updates are available for the license, engine, and patterns; if so, it will download the components that require updating.

Syntax

```
# subscription allowlisting | anti-virus {kaspersky|mcafee|sophos} view | download get-now [background]
```

If you specify the optional background parameter, the download happens in the background; the command prompt returns right away, allowing you to proceed with other operations. Without the background parameter, the download occurs in the foreground and you cannot use the CLI until the download is complete.

Examples

```
# subscription anti-virus mcafee view

Subscription detail for mcafee:

Last Update                          Expire Date    Validity
----------                            -----------     --------
2016-09-13T17:26.642+0000           2019-12-31      VALID
2016-09-13T17:14:29.855+0000         2019-12-31      VALID
2016-09-13T17:14:50.095+0000         2019-12-31      VALID

# subscription anti-virus kaspersky download get-now background

License download started for the vendor kaspersky
Engine download started for the vendor kaspersky
Patterns download started for the vendor kaspersky
ok

# subscription allowlisting download

License download status for the vendor allowlisting:

   Complete
ok

# subscription allowlisting view

Subscription detail for allowlisting:

Last Update                          Expire Date    Validity
----------                            -----------     --------
2016-09-13T17:54.007+0000            2016-12-31      VALID
```

Syntax

```
# subscription allowlisting | anti-virus {kaspersky|mcafee|sophos} view | download get-now [background]
```

If you specify the optional background parameter, the download happens in the background; the command prompt returns right away, allowing you to proceed with other operations. Without the background parameter, the download occurs in the foreground and you cannot use the CLI until the download is complete.

Examples

```
# subscription anti-virus mcafee view

Subscription detail for mcafee:

Last Update                          Expire Date    Validity
----------                            -----------     --------
2016-09-13T17:14:26.642+0000         2019-12-31      VALID
2016-09-13T17:14:29.855+0000         2019-12-31      VALID
2016-09-13T17:15:42.095+0000         2019-12-31      VALID
```
License download started for the vendor kaspersky
Engine download started for the vendor kaspersky
Patterns download started for the vendor kaspersky
ok

# subscription allowlisting download

License download status for the vendor allowlisting:
   Complete
ok

# subscription allowlisting view

Subscription detail for allowlisting:

<table>
<thead>
<tr>
<th>Last Update</th>
<th>Expire Date</th>
<th>Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-09-13T17:54.007+0000</td>
<td>2016-12-31</td>
<td>VALID</td>
</tr>
</tbody>
</table>

---

**system-services**

This command is provided as a troubleshooting tool, to be used at the direction of support, the system-services command allows you restart specific running services without restarting the appliance.

**NOTE**

Previous versions of Management Center provided these commands under the #service command.

**Start or Stop Management Center Services**

# system-services list

Lists the status of all running services.

# system-services restart [management-center | report-generator | statistics-monitoring]

Restarts the specified running service.

# system-services status [management-center | report-generator | statistics-monitoring]

Show the current status of the specified service.

# system-services stop [management-center | report-generator | statistics-monitoring]

Stops the specified service.

# service start [management-center | report-generator | statistics-monitoring]

Starts the specified service.

**Examples**

Use the system-services list command to view the current status of the services.
Management Center# system-services list

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>management-center</td>
<td>Running</td>
</tr>
<tr>
<td>report-generator</td>
<td>Running</td>
</tr>
<tr>
<td>statistics-monitoring</td>
<td>Running</td>
</tr>
</tbody>
</table>

Management Center# system-services restart management-center
management-center was successfully restarted.
Management Center# system-services status management-center
management-center is Running.

**Standard Mode Commands**

The following commands are available in standard mode, the mode after logging in to the CLI. The > prompt indicates standard mode.

To see a list of commands available in standard mode, type `help` or `?` at the > prompt.

### show

Display information about the system and settings.

**Syntax**

```
(config)# show
?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>classification-banner message</td>
<td>Show the currently defined classification banner message and feature status</td>
</tr>
<tr>
<td>status</td>
<td>(enabled vs. disabled). See <code>classification-banner</code>.</td>
</tr>
<tr>
<td>cli</td>
<td>Display CLI-related settings, such as complete-on-space, idle-timeout, and</td>
</tr>
<tr>
<td></td>
<td>history.</td>
</tr>
<tr>
<td>clock</td>
<td>Display current date and time (local and UTC) and timezone.</td>
</tr>
<tr>
<td>full-configuration</td>
<td>Display current configuration. This displays the same output as the <code>show</code></td>
</tr>
<tr>
<td></td>
<td>running-configuration command in standard/enable mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When in a configuration mode, such as authentication or SSL mode,</td>
</tr>
<tr>
<td></td>
<td>the show full-configuration command shows just the settings applicable to</td>
</tr>
<tr>
<td></td>
<td>the mode.</td>
</tr>
<tr>
<td>hardware-configuration</td>
<td>Display system hardware configuration details, such as amount of RAM,</td>
</tr>
<tr>
<td></td>
<td>number of CPUs, and NIC speed.</td>
</tr>
<tr>
<td>history</td>
<td>Display a list of previously-entered CLI commands.</td>
</tr>
<tr>
<td>licenses</td>
<td>Show license components, including subscription services. For each component,</td>
</tr>
<tr>
<td></td>
<td>the activation and expiration dates are listed.</td>
</tr>
<tr>
<td>login-banner message</td>
<td>status</td>
</tr>
<tr>
<td></td>
<td>(enabled vs. disabled). See <code>login-banner</code>.</td>
</tr>
<tr>
<td>notification</td>
<td>Display notifications.</td>
</tr>
<tr>
<td>password-policy-configuration</td>
<td>Display current settings for password policy, such as minimum password</td>
</tr>
<tr>
<td></td>
<td>length. See <code>password-policy</code>.</td>
</tr>
<tr>
<td>raid</td>
<td>Display RAID configuration information. See <code>show raid</code>.</td>
</tr>
</tbody>
</table>
reboot_reason
Show the reason the appliance was last rebooted. Possible reasons include:
- Reboot_requested
- Shutdown_requested
- Halt_requested
If an unexpected reboot occurs (for example, when the system reboots on its own or the plug is pulled), the reason is listed as Unknown.

running-config
Display current configuration.

ssl ca-certificate | certificate | keypair | keyring | signing-request
Display certificate details.

statistics
Display system statistics.

timezone
List supported timezones.

version
List the software version and release ID, appliance serial number, and the MAC address.

**NOTE**
These commands are available in standard and enable modes.

**Examples**

```
! Created by: admin
! Date: 2016-10-13 22:19:51
! Client: cli
!
splunkforwarder
  host idxl.mycompany.com
!
(config)# show version

CAS release 2.1.1.1
Serial number: 0000000000
NIC 0 MAC: 000000000000
```

**Syntax**

```
(config)# show
?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appliance-csr</td>
<td>Show appliance certificate signing requests (CSR).</td>
</tr>
<tr>
<td>banner-message</td>
<td>Display pre-authentication consent banner message</td>
</tr>
<tr>
<td>banner-status</td>
<td>Display pre-authentication consent banner status (enabled vs. disabled).</td>
</tr>
<tr>
<td>classification-banner</td>
<td>Show the currently defined classification banner message and</td>
</tr>
<tr>
<td>message</td>
<td>status</td>
</tr>
<tr>
<td>cli</td>
<td>Display CLI-related settings, such as complete-on-space, idle-timeout, and</td>
</tr>
<tr>
<td></td>
<td>history.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>clock</td>
<td>Display current date and time (local and UTC) and timezone.</td>
</tr>
<tr>
<td>configuration commit changes</td>
<td>Display committed configuration changes.</td>
</tr>
<tr>
<td>configuration rollback changes</td>
<td>Display configuration changes that were rolled back.</td>
</tr>
<tr>
<td>full-configuration</td>
<td>Display current configuration. This displays the same output as the <code>show running-configuration</code> command in standard/enable mode. <strong>Note</strong>: When in a configuration mode, such as authentication or SSL mode, the <code>show full-configuration</code> command shows just the settings applicable to the mode.</td>
</tr>
<tr>
<td>hardware-configuration</td>
<td>Display system hardware configuration details, such as amount of RAM, number of CPUs, and NIC speed.</td>
</tr>
<tr>
<td>history</td>
<td>Display a list of previously-entered CLI commands.</td>
</tr>
<tr>
<td>licenses</td>
<td>Show license components, including subscription services. For each component, the activation and expiration dates are listed.</td>
</tr>
<tr>
<td>login-banner message</td>
<td>status</td>
</tr>
<tr>
<td>notification</td>
<td>Display notifications.</td>
</tr>
<tr>
<td>password-policy-configuration</td>
<td>Display current settings for password policy, such as minimum password length. See <code>password-policy</code>.</td>
</tr>
<tr>
<td>raid</td>
<td>Display RAID configuration information. See <code>show raid</code>.</td>
</tr>
<tr>
<td>reboot_reason</td>
<td>Show the reason the appliance was last rebooted. Possible reasons include:</td>
</tr>
<tr>
<td></td>
<td>Reboot_requested</td>
</tr>
<tr>
<td></td>
<td>Shutdown_requested</td>
</tr>
<tr>
<td></td>
<td>Halt_requested</td>
</tr>
<tr>
<td></td>
<td>If an unexpected reboot occurs (for example, when the system reboots on its own or the plug is pulled), the reason is listed as <strong>Unknown</strong>.</td>
</tr>
<tr>
<td>running-config</td>
<td>Display current configuration.</td>
</tr>
<tr>
<td>ssl ca-certificate</td>
<td>certificate</td>
</tr>
<tr>
<td>statistics</td>
<td>Display system statistics.</td>
</tr>
<tr>
<td>timezone</td>
<td>List supported timezones.</td>
</tr>
<tr>
<td>version</td>
<td>List the software version and release ID, appliance serial number, and the MAC address.</td>
</tr>
</tbody>
</table>

**NOTE**
These commands are available in standard and enable modes.

**show raid**
Display RAID configuration information.

**Syntax**
> show raid
array [<raid_name>]  Display the state of the RAID array <raid_name>, or state of all RAID arrays if a raid name is not specified.

members [<raid_name>]  Display hard disk drives that are part of the RAID <raid_name>, or all hard drives in the system if a raid name is not specified.

spares  Display all spare hard disk drives available in the system.

**Examples**

# show raid array

```
+-------------+-------------+----------------------------+-------------------+
| RAID name   | RAID level  | RAID size(used/total)       | RAID state        |
|-------------|-------------+----------------------------+-------------------+
| casma_raid  | raid10      | (1000.07 GB / 3000.21 GB)   | active            |
|             |             | 100% completed              |                   |
|-------------|-------------+----------------------------+-------------------+
```

# show raid members

```
RAID name: casma_raid
Location     State
slot6         active sync set-A
slot1         active sync set-B
slot2         active sync set-A
slot3         active sync set-B
slot4         active sync set-A
slot5         active sync set-B
```

**help**

Display a list of all commands and a brief description of each. Alternatively, use ? to display the list. This command is also available in privileged mode.

**Syntax**

```
> help
```

or

```
> ?
```

**Example**
enable
Enter the elevated privilege mode, known as enable mode. You will be prompted to enter the enable password.

Syntax
> enable

Notes
• When enable mode is turned on, the prompt changes from > to #,
• To return to standard mode, use the disable command.

quit
Exit the management session.

Syntax
> quit