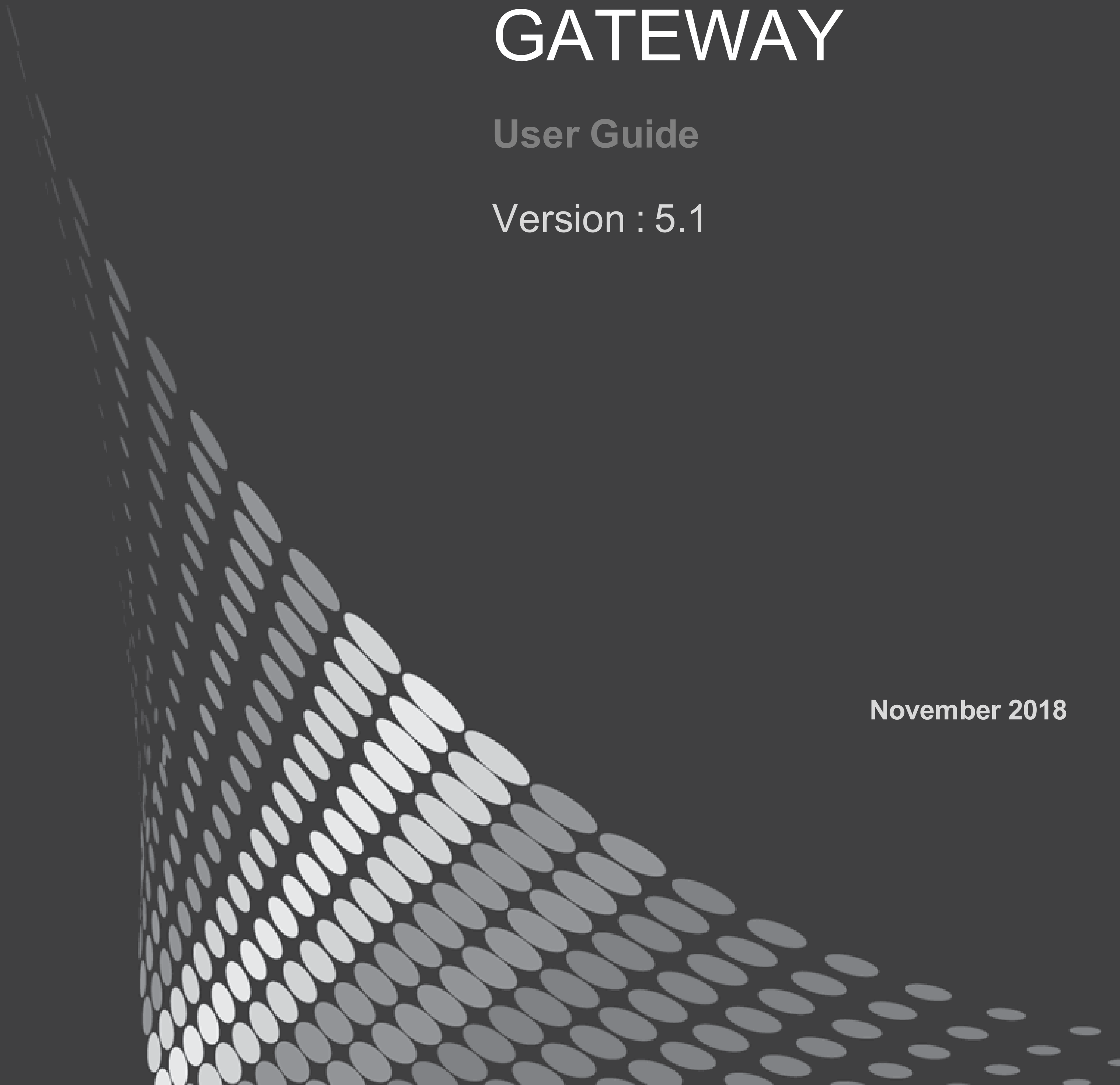
APTEAN

SERVICE GATEWAY

User Guide

Version : 5.1



November 2018

4325 Alexander Drive, Suite 100 • Alpharetta, GA 30022-3740 • www.aptean.com • info@aptean.com

Contents

About the Guide

The Service Gateway User Guide helps telecommunications and digital service providers to optimally use the software to manage the large-scale network of hardware components used by the consumers of their services.

This guide is intended for network engineers and customer support representatives who use Service Gateway to provision and manage customer implementations.

This guide focuses on the features of Service Gateway that are available using the web-based user interface.

Using this Guide

The major sections of the guide are based on the broad categories of functional areas that match the top-level menu. For details on each area, see the following topics:

- Overview
- Getting started
- Using Session menu commands
- Administering Service Gateway
- Configuring inventory features
- Managing configuration features
- Configuring policies
- Configuring reports
- Using the CSR User Interface
- Condition Editor
- Velocity Scripting

1

Overview

Service Gateway overview

Service Gateway allows you to configure, manage and support multiple broadband devices and services. It uses a centralized Auto Configuration Server (ACS) to identify, configure, and query virtually all types of current or legacy CPE devices, including those with standards-based or proprietary interfaces.

Service Gateway has the following main features:

- Supports multiple devices, including home gateways, VoIP ATAs, IPTV STBs, and both fixed and mobile wireless terminals
- Hardware vendor independent platform
- Supports TR-069 and other applicable Broadband Forum standards
- Minimal bespoke integration
- CSR analytics
- Alarm processing
- Instrumentation for fault management
- Integration with northbound web services and southbound protocol abstraction for operations support systems (OSSs)
- Integration with Consona Subscriber desktop and self-care capabilities

Additionally, Aptean provides an interoperability test lab service to existing and potential customers to verify that their CPEs can be managed by Service Gateway.

Platform support

Following is a list of third-party platform component considerations:

- For WebLogic installations, WebLogic 11gR1 (10.3.5) is required. WebLogic 9.2 MP3 is no longer supported.
- For JBoss installations, JBoss 6.1 is required. JBoss 4.0.4 is no longer supported.
- For the CWMP Servers, Tomcat 7.0.27 is required. Tomcat 5.0.25 is no longer supported.
- Java 6 is required for all components. Java 5 is no longer supported.
- For browser clients, Flash Player 10 is required. Flash Player 9 is no longer supported.
- For deployments on Windows, Windows Server 2008 is required. Windows Server 2003 is no longer supported.

The following Operating Systems are supported:

- RedHat Enterprise Linux 6.2, when used with JBoss.
- Solaris 10 x86, when used with WebLogic.

2

Getting Started

Access restrictions

Service Gateway provides different levels of access restrictions for different types of users based on assigned permissions. The user types which are assigned by groups include administrators, realm users, and enterprise users. Access restrictions based on assigned permissions are used to control the subscribers, devices, and service configurations that a user can access.

Administrators

A system administrator has no access restrictions and can access all areas of Service Gateway.

Realms

If a user is restricted by realm, they can only access the items that belong to the realms with which they are associated from the following list.

Realms provide access restrictions on the following items within Service Gateway:

- File Management (File Servers, Files, and Vendor Templates)
- Inventory Management (Devices, Hardware, and Firmware)
- Subscriber Management (Subscribers)
- Service Configuration (Service Levels and Service Associations; Services, Templates, Attributes, Domains, Parameter Mappings, Software, and Modules)
- Policy Management
- Platform Configuration (Users, Groups, User Preferences, Administrative Domains, and Network Associations)

Enterprises

Enterprises can span multiple realms, and are not associated with or restricted by realms. Enterprises provide users with access to a specific list of subscribers and devices, regardless of the realm with which those subscribers and devices are associated. Enterprise users do not have permissions to log into the Service Gateway GUI; rather, they are created to interact with user portals and custom interfaces.

Enterprises are used to provide access restrictions to an explicit list of subscribers and devices within Service Gateway and are limited to the following:

- Inventory Management (Devices)
- Subscriber Management (Subscribers)
- Platform Configuration (Users, Groups, and User Preferences)

Enterprise subscribers

An enterprise subscriber is a subscriber that is not associated with any specific realm. As such, they can be associated with any unassigned devices in the system, regardless of the realm with which the device is associated. Normal subscribers, on the other hand, can only be associated with devices within that subscriber's realm(s).

Logging into Service Gateway

To access Service Gateway:

1. Using the Web browser, go to the URL provided by your system administrator.

   For example, **http://hostname:9090/** where **hostname** is the name of the server hosting the Service Gateway application. The URL is case–sensitive and must be entered exactly as shown.

   Note: Your system may be configured to use a different URL to access Service Gateway. If you need assistance, contact your system administrator.

2. On the login page, enter your username and password. The password is case sensitive and must be entered exactly as it was assigned to you.
3. Click **Login**.

   Once you log in, you will see the Home Page of Service Gateway.

If	Then
The password has expired or an administrator has set the account to "User Must Change Password on next login"	A pop-up appears prompting you to change your password, with the following instruction: "To change your password, enter your existing password and your new password twice." Enter the new password as instructed and you will be directed to the Home Page.
If the administrator has set a Password Expiry notification period and a user whose account will expire soon logs in	A message similar to the following is displayed: "Password Expiry notice. Your password will expire in 1 day and 23 hours."

Filtering search results

Most windows and sections of Service Gateway provide a filter feature, indicated by a magnifying glass (🔍) icon, to allow you to search through a list and display only those results that match the search criteria. To activate the filter, click the **magnifying glass** and enter the filter parameters. The filter is dynamic and the results display is updated as soon as you start providing your search criteria.

Refresh button

A refresh button is available on each screen. This button can be used to refresh the data that is being displayed, so that any recent changes made by another user can be viewed.

Using Editors

Service Gateway provides the following Editors to build conditions and to edit and validate scripts:

Condition Editor. Used to define a set of conditions or filters which must be met to match an entity to a device. Conditions can be specified for a number of entities such as real-time probes, templates, services, policies, and policy actions. When you select an option from the **Insert Expression** drop-down list, an expression is inserted in the **Condition Editor** text box.

Velocity Script Editor. Supports the use of Velocity scripting, in a number of places within the application, to generate dynamic content. The Velocity script editor can be opened by clicking on the edit icon ( ) located at the upper right corner of the script text box.

Accessing context-sensitive help

Service Gateway provides context sensitive help ,which can be accessed as follows:

- Select Dynamic Help from the Help menu - this displays the main help page for the type of item your are currently viewing.
- Click the question mark icon on each screen - this displays the tab-specific help for the tab that you are currently viewing.

IP Addresses

Service Gateway supports both IPv4 and IPv6 addresses. All IP addresses are stored in the database as IPv6 addresses, but any IPv4 addresses are displayed using the IPv4 format in the user interface.

3

Using Session Menu Commands

The session menu contains the **Home Screen** and session related items, which include **Session Information**, **Toggle Diagnostics Panel**, **Lock**, and **Logout** features.

Home Screen

The Home Screen provides shortcuts to features that are also available through the menu. It can be used as a starting place to access most Service Gateway features, as well as recently viewed reports. The **Home Screen** is displayed when you log into the system. It can also be accessed by selecting **Session > Home Screen**.

Session Information

The **Session Information** page deals with the current logged in user's login session details, as well as user preferences and password modification. To access the **Session Information** page, select **Session > Session Information**. It contains the following tabs:

- Status
- Preferences
- Password

Status tab

The **Status** tab shows the status for the current user in the current login session. This includes the following information:

- **Session State**. Indicates if a user is logged in, and which user is logged in.
- **Current Language**. Displays the Locale ID code of the currently active locale.
- **Server URL**. Displays the URL of the server that the interface is currently connected to.

Preferences tab

The **Preferences** tab allows the user to modify settings from the default settings to preferred settings. To modify any of the settings, you must first select the **Override?** check box for the appropriate preference setting. You can modify the following preferences:

- **Language**. The current language the UI is displayed in. Only languages that have been translated and set up on the server will appear in the **Language** drop-down list. By default, English is the only option available.
- **Session Timeout**. The number of seconds that a session is idle before it is automatically locked, requiring the user to enter their password to resume using the interface.
- **Show Hidden Reports**. Some reports that are only used as a drill-down from another report, or only relevant in the context of a specific interface action (such as deleting an object that has other objects referencing it) will be hidden by default. Selecting this check box will show all such reports.
- **Default Device Search Type**. Sets the default search type that is to be used when searching for a device.
- **User Interface Layout Direction**. Selecting **Right to Left** will display the UI in a mirror image, which is more natural for some countries and languages.

Password tab

The **Password** tab allows the currently logged in user to change their password.

To change the password:

1. Enter your existing password in the **Current Password** field.
2. Enter the new password in the New Password and Verify New Password fields.
3. Click **Save**

Toggle Diagnostics Panel

The Diagnostic Information panel provides additional information or settings that help in diagnosing issues with Service Gateway. Only users with the ***Diagnostics Panel*** permission can access this panel.

Selecting **Session > Toggle Diagnostics Panel** opens the **Diagnostic Information** panel on the right of the screen. It contains the following tabs:

- SOAP Log
- Local UI Memory Usage
- Application Object Cache
- Logging
- Distributed Data

Clicking **Toggle Diagnostics Panel** while the **Diagnostic Information** panel is open hides the panel.

SOAP Log tab

The SOAP Log tab is used to debug the SOAP/XML that is used for communication between the UI and the application server. If the UI is not displaying the data that must be displayed, or the application server is not performing the action that is being requested, the SOAP log can be used to view the SOAP messages that are being exchanged with the application server to help diagnose the problem.

By default, SOAP messages are not logged. To enable SOAP logging, do the following:

1. On the **Diagnostic Information** panel, select the **SOAP Log** tab.
2. Select the **Web Service Logging Enabled** check box at the bottom of the panel and then start using the UI.

   All SOAP messages are logged to this panel.

By default, the displayed text uses line wrapping. If you do not want each line to be wrapped, clear the **Wrap** check box at the bottom of the panel.

To clear the text that is currently displayed in the **SOAP Log** tab, click **Clear**.

Local UI Memory Usage tab

The **Local UI Memory Usage** tab displays the memory in use by the UI. The UI is a Flash application, and it can store a lot of information in memory.

This tab can be used to view the Service Gateway UI memory usage. The memory usage display is a rolling graph that is constantly being updated. It shows the memory usage for the past 5 minutes.

Application Object Cache tab

Service Gateway incorporates Ehcache, a caching engine, to store a lot of frequently read information to reduce database queries and to help improve system performance. The **Application Object Cache** tab provides information about cache usage.

If cache statistics are not visible when you open this tab, click the **Refresh Cache Statistics** button. All the caches that have been initialized in the application server that the user is currently accessing are listed in the following columns of the **Cache Statistics** table:

- The **Cache Name** column displays the name of the cache. Cache names are descriptive enough to give an idea of the information that is contained in each cache.
- The **Objects** column displays the total number of items that are currently in that cache.
- The **Hits** column shows the total number of times that the information that was requested from the cache was available in the cache, thereby avoiding a database query.
- The **Misses** column shows the number of times that the information that was requested from the cache was not present in the cache. As a result, a database query was required to retrieve the data to populate the cache and return the value to the user.

If you want to clear all the objects from the cache, click the **Clear Object Cache** button. Use this action with caution, and only clear the cache when you are absolutely certain you need to do so.

Typically, objects are cleared from the cache if a user manipulates the data in the database directly, without using the application to do so. This action is strongly discouraged.

Note: This button only clears the cache on the application server that the web browser is currently communicating with. This is important in a clustered environment, as it will not clear the cache on the other cluster members.

If you want to view how much memory is being used by each cache, select the **Get Memory Stats** check box. An additional column called **Memory**, showing the memory usage (in bytes) for each cache, is displayed in the **Cache Statistics** table, .

Note: All columns in this table can be sorted.

Logging tab

The **encore.properties** file defines all the modules in Service Gateway that log to the **Encore.log** file. The logging level for each module can be changed in this file. However, changing the logging level for each module requires restarting the application server, a task that is not often desirable in a live production system.

Due to the high amount of data that can be logged, many customers often define each module to only log errors or warnings, not informational or debug information. When a problem does occur, often the error or warning log levels are not sufficient to help diagnose the exact nature of the problem and information or debug logs are often requested.

The **Logging** tab allows users to programmatically change the logging levels for each module without requiring a system restart. This is very helpful as it allows users and customer support to change the log levels to obtain more detailed logs while an error is being diagnosed. Once the additional logs have been obtained, the log levels can be switched to their original levels, also without requiring a system restart.

To view the current log levels, click the **Get Loggers** button. All the loggers defined by Service Gateway are displayed in the **Loggers** table, along with their current log levels.

To change a log level, select it from the drop-down list in the **Log Level** column. Once you have set the new log levels, click the **Set Loggers** button. The log level for the application server that the web browser is currently communicating with is changed. In a cluster set-up, the log level is changed across the entire cluster.

Note: All columns in this table can be sorted.

Distributed Data tab

Service Gateway now uses distributed data engines to share runtime state information across all cluster members. The **Distributed Data** tab allows a user to view the cluster members that are sharing data, as well as the distributed data structures that have been initialized.

To view or refresh the current statistics, click the **Get Statistics** button. The current runtime state information is displayed in three tables as follows:

The table at the top of this pane lists all the nodes that are sharing distributed data. It has the following columns:

- **IP Address**. The IP address of the node.
- **Port**. The port that the node is using to share data with other nodes.

Note: The current node is highlighted in bold.

The middle table lists all the distributed maps that have been initialized and are in use. It has the following columns:

- **Name**. Displays the name of the map.
- **Total Objects**. Displays the total number of objects in each map that are shared across all cluster members.
- **Local Objects**. Displays the number of objects that are being held by the current cluster member.

If you click an entry in the middle table, the bottom table in the following tabs is populated as follows:

- **Total Objects**. Displays the map key as well as the objects that are stored in the map for all objects that are shared across all the cluster members.
- **Local Objects**. Displays the map key as well as the objects that are being held by the current cluster member.

Lock and Logout

Selecting **Session > Lock** locks the current login session, requiring the current user's password to be entered to resume the session. The session will also be automatically locked when a user's session expires.

Logging out exits the session and logs off the currently logged in user from that web browser.

4

Administration

Administer Service Gateway

This topic introduces the various administration features of Service Gateway that are available from the Administration menu. To display the Administration menu, click **Administration** on the main menu bar.

The **Administration** menu allows you to perform the following functions:

- Monitor the performance and health of the Service Gateway system
- Configure security features
- Manage external servers
- Configure the Service Gateway environment

Monitoring the performance and health of the Service Gateway system

Performance management allows you to monitor the performance and health of the Service Gateway system. It has the following features:

- **Dashboard** - provides a configurable real-time display of current Key Performance Indicator (KPI) values.
- **Monitoring** - opens a monitoring screen with one or more historical charts of KPIs over time.

Using Performance Dashboard

Service Gateway's **Performance Dashboard** is a configurable dashboard that displays a summary of all application servers and CWMP protocol servers in the deployment. The dashboard is updated in real-time and allows health thresholds to be configured. Performance indicators are color-coded for an at-a-glance indication of potential problems.

To access the Performance Dashboard screen, go to **Administration > Performance > Dashboard**.

Configuring health thresholds

On the **Performance Dashboard** screen, click the ☰ icon. The **Dashboard Configuration** screen with a list of Key Performance Indicators (KPIs) opens.

The list of KPIs can be filtered by Server Type and KPI Name.

The **Dashboard Configuration** screen allows you to set the **Refresh Interval** and **Disable Session Timeout** parameters.

Adding a KPI

1. Click **New** on the **Dashboard Configuration** screen. The **Viewing New KPI** pane opens on the bottom of the screen.
2. On the **General** tab, click within the **KPI** field or click the 🗗 icon. The **Select KPI** page opens.
3. Perform the following steps in the **Select KPI** page:
   a. Select the server type from the **Server Type** drop-down list.
   b. Select the KPI from the **KPI** pane. The list of KPIs are displayed in a tree view. Click the right arrow (▶) to expand the list. When you select a KPI, its description is displayed in the **Description** pane.
   c. Click **Ok**.
4. On the **Thresholds** tab:
   a. Set the thresholds for the following parameters if required:
      - **High Critical**
      - **High Warning**
      - **Low Critical**
      - **Low Warning**

   These thresholds are used to determine the colors of the status icons that appear next to the KPIs on the **Performance Dashboard**. For details, see Threshold options.

b. Choose an **Escalation** mode from the drop-down list. Available options are **None** and **Server**.

   If the **Escalation** mode is set to **Server**, then the worst KPI status (Normal, Warning, or Critical) is reflected on the server icon on the Performance Dashboard. For details, see Escalation options.

5. Click **Save**. The new KPI is visible in the KPI list pane.

Deleting an existing KPI

1. Click the desired KPI in the **KPI** list at the top of the **Dashboard Configuration** screen. Its details are displayed in the **Viewing KPI** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Modifying an existing KPI

Click the desired KPI in the **KPI** list at the top of the **Dashboard Configuration** screen. Its details are displayed on the following tabs of the **Viewing KPI** pane.

- General
- Threshold

General

The **General** tab contains the following fields:

- **KPI**. The KPI that must be displayed on the **Performance Dashboard**. Clicking within the field or on the 🗐 icon opens the **Select KPI** dialog box.
- **Row**. The row within the **Server Type** pane on the **Performance Dashboard** that the KPI must appear in.
- **Column**. The column within the **Server Type** pane on the **Performance Dashboard** that the KPI must appear in.

Threshold

The **Thresholds** tab is used to configure thresholds that will be used to determine the colors of the status icons that appear next to the KPIs on the **Performance Dashboard**. It also allows you to specify the **Escalation** mode that must be reflected on the server icon.

Threshold options

The following threshold options can be configured on this tab:

- **High Critical**
- **High Warning**
- **Low Critical**
- **Low Warning**

These thresholds are used to determine the colors of the status icons that appear next to the KPIs on the Dashboard as follows:

Threshold	Status icon color
Between **Low Warning** and **High Warning**	Green
Between **High Warning** and **High Critical** or Between **Low Warning** and **Low Critical**	Yellow
Above **High Critical** or below **Low Critical**	Red

Escalation modes

Available **Escalation** modes are **None** and **Server**.

If the **Escalation** mode is set to **Server**, then the worst KPI status (Normal, Warning, or Critical) is reflected on the server icon on the Dashboard:

If	Then
All KPIs are green	A green check mark appears on the server icon.
The worst KPI status is yellow (warning)	A yellow warning icon symbol appears on the server icon.
The worst KPI is red (critical)	A red X appears on the server icon.

Viewing performance trends

The **Performance Monitoring** screen provides a configurable chart view, showing recent trends in key performance indicators over time. Each graph can contain multiple key performance indicators, and multiple graphs can be displayed at a time.

The application performance monitoring interfaces provide better insight into the load being placed on the system and how the system is handling that load. These views are useful during troubleshooting and as a constant display in a network operations center (NOC).

To access the **Performance Monitoring** screen, go to **Administration > Performance > Monitoring**.

The drop-down list below the **Search** button at the top right of the screen provides the following options:

- **New Tab**. Allows to add a new monitoring tab.
- **Rename Current Tab**. Allows to rename an existing monitoring tab.
- **New Monitor**. Allows to configure the **Monitoring Chart** view. For details, see Configuring the Monitoring Chart view.
- **Save Layout**. Allows to save a configured layout.
- **Load Layout**. Allows to load a configured layout.

Configuring the Monitoring Chart view

To configure the Monitoring Chart view:

1. From the drop-down list at the top right of the **Performance Monitoring** screen, select **New Monitor**. The **Monitor Configuration** dialog box opens.
2. Perform the following steps to configure the monitoring parameters:

   a. Enter a title for the new monitoring tab in the **Title** field.

   b. Select the appropriate values for the following settings:

      - **Module Width**
      - **Module Height**
      - **Update Frequency**
      - **Maximum Duration**

   c. Associate a performance indicator with the chart view by dragging it from the **Available Performance Indicators** table to the **Current Performance Indicators** table.

      To delete a performance indicator for the **Current Performance Indicators** table, select it and click **Delete.**

d. Edit the following columns in the **Current Performance Indicators** table if required:

   - **Servers**
   - **Colour**
   - **Width**

e. Click **Add**. The monitoring chart is displayed in the selected tab on the **Performance Monitoring** screen.

Modifying the monitoring configurations

To modify the monitoring configurations:

1. Click the ☰ icon on the top right of the monitoring chart. The **Monitor Configuration** dialog opens.
2. Make changes as required.
3. Click **Ok**.

Configuring security features

The **Security** menu allows you to configure groups, realms, and users within the Service Gateway environment. It also allows you to view audit logs.

To access the Security menu, go to **Administration > Security**.

The Security menu provides the following features:

- Audit Logs
- Groups
- Realms
- Users

Audit Logs

Audit logging keeps track of every action performed by any logged in user that results in a change to a database record, including the addition, modification and deletion of objects. Logs may be searched and reviewed by any user with the *View Audit Logs* permission.

Note: Audit logging must be enabled via the system-wide preference **Audit Logging Enabled**.

Viewing a list of Audit Logs

To view the audit logs:

1. Go to **Administration > Security > Audit Logs**.
2. Click the magnifying glass to open the **Search** tab.
3. Provide the following details:
   a. Specify a **Start Time** and **End Time** using the calendar tool.
   b. Select the desired parameters from the **User**, **Operation**, and **Object Type** drop-down lists.
4. Click **Submit**. Audit Logs matching the selected criteria are displayed in the **Audit Logs** search results pane.

Deleting Audit Logs

Audit logs are automatically deleted after the period of time specified by the system-wide preference **Audit Log Expiration Age (seconds)**.

Tip: Audit logging must be turned on to keep a log of the activity, but if logging is turned off, you can still view logs for a previous time period during which the logging was enabled assuming that they have not been purged.

Viewing Audit Log record details

To view an audit log record, click the record in the **Audit Logs** search results pane. Its details are displayed in the General tab of Audit Log details display pane at the bottom of the screen.

Note: An audit log record cannot be modified.

General tab

The **General** tab contains details about the audit log record.

This tab has the following fields:

- **Time Logged**. Displays the date and time that the activity occurred.
- **Remote IP Address**. If the activity was performed using the user interface, displays the IP address of the remote host.
- **Operation**. Indicates the type of activity that was carried out against the record. It displays one of the following values: Add, Update, Delete, Add Association, or Delete Association.
- **Description**. Displays detail about changes, if any, during an Update operation. Many object types will display the old and new values of fields that have been modified during the Update operation.
- **Primary Object**. Displays the type of object and the name of the object that was modified. If the object still exists, the name is a hyperlink to the edit screen for the object. Otherwise, the message, "(This object no longer exists)" appears after the name.
- **Associated Object**. For **Add Association** and **Delete Association** operations, this field displays the type and name of the object that was associated with or disassociated from the primary object.

Configuring and managing groups

Groups are used to simplify the association of users with function-level permissions. Groups may be created based on typical user roles within an organization, such as an administrator, manager, analysts, and so on. All users within the system are assigned to one or more groups. The groups are assigned to specific permissions that determine which Service Gateway features a logged in user can access.

To access the **Groups** management page, go to **Administration > Security > Groups**. This page can only be viewed by users with the ***Manage/View User Accounts*** permission.

Groups can be filtered by Name, Description, and Realm.

Any custom group that is created can be deleted. However, the following default groups, included with the system, cannot be deleted.

- **AdminGroup**. This group represents the highest level of permission available.
- **EnterpriseAdminGroup**. This group is associated with all of the permissions that are assigned to Enterprise users.
- **RealmAdminGroup**. This group is associated with all of the permissions that are assigned to Realm users.

Adding a group

1. Click **New** on the **Groups** management screen. The **Viewing New Group** pane opens on the bottom of the screen.
2. On the **General** tab, enter information in the following fields:
   - **Name**. Short name of the group. It cannot contain spaces or any of the following characters: (,), ', ", ;, \, -, {, or }
   - **Description**. Description of the purpose of the group. This is an optional field.
3. On the **Permissions** tab, associate permissions with a group by selecting them from the **Available** pane and dragging them to the **Current** pane. To remove a permission from a group, select it from the **Current** pane and drag it back to the **Available** pane.
   - To select multiple items, hold down the CTRL key and click each item or hold down the Shift key and click the first and last items in a range of consecutive items.
4. On the **Realms** tab, associate realms with a group by selecting them from the **Available** pane and dragging them to the **Current** pane. If no realms are associated with a group, then the group is available to all realms
   - To remove a realm from a group, select it from the **Current** pane and drag it back to the **Available** pane.

- To select multiple items, hold down the CTRL key and click each item or hold down the Shift key and click the first and last items in a range of consecutive items.

Note: If a group has been associated with a realm, and users within that realm are assigned to the group, then that realm association cannot be removed from the group.

5. Click **Save**. The new group is visible in the **Groups** list pane.

Deleting an existing group

1. Click group in the **Groups** list pane. Its details are displayed in the **Viewing Group** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying group properties

To view or modify the details for a specific group, select the desired group from the **Groups** list pane. Its details are displayed in the following tabs of **Viewing Group** pane at the bottom of the screen:

- General
- Permissions
- Realms

General tab

The General tab contains the following editable fields:

- **Name**. The short name of the group. It cannot contain spaces or any of the following characters: (,), ', ", ;, \, -, {, or }
- **Description**. A description of the purpose of the group. This is an optional field.

Permissions tab

The Permissions tab is used to associate permissions with a group.

- To associate a permission with a group, select it from the **Available** pane and drag it to the **Current** pane.
- To remove a permission from a group, select it from the **Current** pane and drag it back to the **Available** pane.

To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

Note: The permissions assigned to a group will be assigned to all users that belong to the group.

Realms tab

The Realms tab is used to associate realms with a group. If no realms are associated with a group, then the group is available to all realms.

- To associate the group with one or more realms, select the realms from **Available** pane and drag them to the **Current** pane.
- To remove a realm association, select the realm from the **Current** pane and drag it back to the **Available** pane.

To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

Note: If a group has been associated with a realm and users within that realm are assigned to the group, then that realm association cannot be removed from the group.

Configuring and managing realms

Realms provide a mechanism to segregate much of the content that is managed by Service Gateway to support geographic separation or multi-tenancy. For details on some of the aspects that are segregated by realm, see Realms under Access Restrictions.

To open the Realms management screen, go to **Administration > Security > Realms**. The list of realms can be filtered by Name and Description.

Adding a realm

1. Click **New** on the **Realms** management screen. The **Viewing New Realm** pane opens on the bottom of the screen.
2. On the **General** tab, provide the following information:

   - **Name**. Short name of the realm.
   - **Description**. A description of the purpose of the realm. The is an optional field.
   - **Default?**. Sets the default realm for the system. Select this check box to make this realm the new default realm.

     The default realm is automatically selected in all **Realm** drop-down boxes when creating a new realm-constrained object (such as devices, hardware, firmware, services, and policies). This makes it easier when creating new objects in the system, as only the **Realm** option is required to be changed when creating an object for items other than the default realm.

   Note: Only one realm can be set as the default realm.

3. Click **Save**. The new realm is visible in the **Realms** list pane.

Deleting an existing realm

1. Click realm in the **Realms** list pane. Its details are displayed in the **Viewing Realm** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: If a realm is associated with another object, it cannot be deleted and the "This realm is referenced by other objects" message appears. Click the **Details** button to open the Realms Reference Summary page in a new browser window.

Viewing and modifying realm properties

Click realm in the **Realms** list pane. Its details are displayed on the General tab of the **Viewing Realm** pane at the bottom of the screen.

General tab

The General tab contains the following editable fields:

- **Name**. Short name of the realm.
- **Description**. The description or purpose of the realm. This is an optional field.
- **Default?**. Sets the default realm for the system. Select this check box to make this realm the new default realm.

Note: Only one realm can be set as the default realm.

Configuring and managing users

Users are accounts that are authorized to access the system. They can be given access to only specific functions by assigning appropriate groups and to a subset of the content by assigning one or more realms or subscribers. Additionally, an administrator may manage the user's password policy, user preferences, and policy access.

This page can only be viewed by users with the *Manage/View User Accounts* permission.

To open the **Users** management screen, go to **Administration > Security > Users**. The list of users can be filtered by Username, First or Last Name, and Realm.

Adding a user

1. Click **New** on the **Users** management screen. The **Viewing New User** pane opens on the bottom of the screen.
2. On the **User Information** tab,
   a. Enter the appropriate values in the following mandatory fields:
      - **User Name**
      - **Password**
      - **Password Verify**

   b. Enter values in the other fields if required

   c. If this user account is for a limited period, select the **Account Expires?** check box and provide the account expiration time and date.
3. Click **Save**.

Deleting a user

1. Click user in the **Users** list pane. The user's details are displayed in the **Viewing User** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying user properties

To view the details for a specific user, select the desired user from the **Users** list pane. Its details are displayed in the following tabs of **Viewing User** pane at the bottom of the screen:

- User Information
- Password Policy
- Access Control
- User Preferences
- Policy Restrictions
- Tab Permissions
- Report Restrictions
- Template/Service Restrictions

User Information tab

The User Information tab allows basic information about a user account to be viewed and changed. The tab contains the following fields:

- **User Name**. The user name that is used to log in to the system.
- **First Name**. The given name of the user. This is an optional field.
- **Last Name**. The surname of the user. This is an optional field.
- **Email Address**. The email address of the user. This is an optional field.
- **Password**. The password to be associated with this user name. This field also allows the password of a user to be reset. The current password of an account cannot be recovered.
- **Password Verify**. When setting the password of a user, this field must contain the same value as the **Password** field.
- **Account Expires?**. If this option is selected, the following two fields are activated and allow an account expiry date and time to be set. After the specified period, the user cannot log in.
  - **Account Expiration Date**. Specifies the date when a user account expires.
  - **Account Expiration Time**. Specifies the time on the date set in the **Account Expiration Date** field when a user account expires.

⚠ **Caution:** When logged in, user accounts that have Account Expiry dates set are only permitted to manage other users that have an Expiry Date that is equal to or less than their own.

Password Policy tab

The **Password Policy** tab allows an administrator to control aspects of a user password. The defaults for each of the settings on this page are configured within the system-wide preferences (**Default Password Policy** settings under **Administration > Settings > Preferences > User Settings**), but may be altered independently for each user if desired.

This tab allows the definition of the following password settings:

- **Maximum Password Age (days)**. Specifies the maximum number of days that a password is allowed to remain unchanged. After the specified number of days is reached, the user is required to change the password when logging in. A value of 0 disables this feature.
- **Expiry Warning Period (days)**. Specifies the number of days before the password expires that a warning message is displayed. When the user logs in within the specified period, a pop-up message appears notifying them of the time left before the expiration of their password. A value of 0 disables this feature.
- **Minimum Password Age (minutes)**. Specifies the length of time (in minutes) that must pass before the user can change their password. This option is used to make it difficult for a user to reuse a password by defeating the Passwords to Remember option. If a user attempts to change a password twice within the specified time, they will be denied. Administrators are not subject to the minimum password age restriction.

Note: The minimum password age setting does not apply if the user is forced to change the password after an administrator has set a temporary password that must be changed at the next log in.

- **Number of Passwords to Remember**. When set to a value greater than zero, prohibits users from creating a new password that is the same as a recently used password. To specify the number of passwords that must be remembered, provide a value greater than 0. Regardless of this setting, a user is never allowed to create a new password that is the same as their current password.
- **Force Password Change on Next Login**. Selecting this check box prompts a user to change the password at the time of the next log in. Once the password is changed, this check box is cleared automatically.

Access Control tab

The **Access Control** tab of the **Viewing User** pane allows an administrator to configure access restrictions for a user. Access to product features is granted by assigning one or more groups to the users. Access to content can also be restricted using one of two models: **Realm** or **Enterprise**.

The following options are available for **Content Restriction**:

- **None**. This option does not restrict the user based on content, only by function via groups.
- **Realm**. This option allows one or more realms to be associated with the user. The user can only see the content within those realms. It is highly encouraged that only permissions belonging to the built-in *RealmAdmin* group be granted to such users. Additional permissions may grant users access to content from other realms, or affect changes that will impact other realms.

- **Enterprise**. This options allows one or more subscribers to be associated with a user and with zero or more other enterprise users. This model may be used to provide a technical representative of a corporate subscriber access to a group of related subscribers and to allow them to manage sub-accounts with the same or limited access.

The following four sub-tabs are available depending on the **Content Restriction** and current state of the record:

- **Realms**. This tab is only available for realm users.
  - To assign a realm to a user, select it from the **Available** pane and drag it to the **Current** pane.
  - To unassign a realm from a user, select it from the **Current** pane and drag it back to the **Available** pane.
- **Groups**. This tab is available for all user types.
  - To assign a group to a user, select it from the **Available** pane and drag it to the **Current** pane.
  - To unassign an enterprise user from a user, select it from the **Current** pane and drag it back to the **Available** pane.
- **Enterprise Users**. This tab is only available when editing an existing enterprise user. An enterprise user with the necessary permissions can manage other user accounts that are associated with it.
  - To assign an enterprise user to a user, select it from the **Available** pane and drag it to the **Current** pane.
  - To unassign an enterprise user from a user, select it from the **Current** pane and drag it back to the **Available** pane.
- **Subscribers**. This tab is only available when editing an existing enterprise user.
  - To specify the list of subscriber accounts that an enterprise user can view, select the subscriber record from the **Available Subscribers** pane and drag it to the **Current Subscribers** pane.
  - To remove visibility of a subscriber to an enterprise user, select the subscriber in the **Current Subscribers** pane and click **Delete**.

User Preferences tab

The **User Preferences** tab manages the user specific preferences available to a user, as well as any preferences (that the users themselves cannot set), which may be specified for each user by an administrator.

You can modify the following preferences:

- **Language**. The current language the UI is displayed in. Only languages that have been translated and set up on the server will appear in the **Language** drop-down list. By default, English is the only option available.
- **Session Timeout (seconds)**. The number of seconds that a session is idle before it is automatically locked, requiring the user to enter their password to resume using the interface.
- **ACS-Server API Timeout (milliseconds)**. The number of milliseconds to wait before the communication session times out if no response is received. This timeout is used when Service Gateway interacts with the CWMP servers to communicate with a device for actions that do not involve file transfers.
- **ACS-Server API File Transfer Timeout (milliseconds)**. This timeout is similar to the **ACS-Server API Timeout**, except that it applies to actions that involve transferring a file to or from the device. For example, to apply a firmware upgrade to the device or to deliver a vendor-specific configuration file to the device.
- **Show Hidden Reports**. Some reports that are only used as a drill-down from another report or are only relevant in the context of a specific interface action (such as deleting an object that has other objects referencing it) will be hidden by default. Selecting this check box will show all such reports.
- **Default Device Search Type**. Sets the default search type that is to be used when searching for a device.
- **ACS-Server CPE Timeout (milliseconds)**. This timeout is similar to the **ACS-Server API Timeout**, except that it covers the communication between the CWMP server and the device. This timeout is for actions that do not involve file transfers.

  Note: This value should be less than the value set for **ACS-Server API Timeout**, as the communication between the device and the CWMP server needs to complete before the CWMP server can respond to Service Gateway

- **ACS-Server CPE File Transfer Timeout (milliseconds)**. This timeout is similar to the **ACS-Server CPE Timeout**, except that it applies to actions that involve transferring a file to or from the device.

  Note: This value should be less than the **ACS-Server API File Transfer Timeout**.

- **User Interface Layout Direction**. Selecting **Right to Left** will display the UI in a mirror image, which is more natural for some countries and languages.

> **Note:** If a specific user creates a policy, the global preference values are used for **ACS-Server API Timeout**, **ACS-Server API File TRansfer Timeout**, **ACS-Server CPE Timeout**, and **ACS-Server CPE File Transfer Timeout** instead of the user-specific settings. The user preferences for these values are used for CSR, Object Browser, and web services.

Each user preference has an **Override?** check box after the name of the preference and before the value field.

If	Then
The **Override?** check box is selected	The specified value is considered for this user.
The **Override?** check box is cleared	The value of the system-wide preference of the same name is considered for this user.

Policy Restrictions tab

The Policy Restrictions tab has the following sub-tabs to allow restricted access to policies based on **Policy Actions** , **Event Hooks** and/or **Policy Device List**:

- **Policy Actions**. Users with permissions to manage policies have access to all policy actions by default. Selecting the **Policy Action Restrictions Enabled** check box restricts a user to a subset of actions. Users that are restricted in this way can only create a policy that contains these actions in the workflow and only edit a policy if the workflow contains only actions that the user has access to.
    - To assign one or more actions to a user, select them from the **Available** pane and drag them to the **Current** pane.
    - To remove an action from a user, select it from the **Current** pane and drag it back to the **Available** pane.
    - To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

- **Event Hooks**. Users with permissions to manage policies have access to all event hooks by default. Selecting the **Event Hook Restrictions Enabled** check box restricts a user to a subset of hooks. Users that are restricted in this can only create an event or hybrid policy which uses one of the specified hooks. Also, they can only edit event/hybrid policies which reference one of the hooks that the user has access to.
    - To assign one or more hooks to a user, select them from the **Available** pane and drag them to the **Current** pane.
    - To remove a hook from a user, select it from the **Current** pane and drag it back to the **Available** pane.
    - To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.
- **Policy Device List**. The Policy Device List tab can grant access control to the method that can be used to define a policy device list. The available options are: CSV, Conditions, Device List Query, and Policy History. Selecting the '**Policy Device List Restrictions Enabled**' checkbox allows you to specify which methods of specifying a device list are available to a user. By default all options are available.

Tab Permissions

The **Tab Permissions** tab allows access controls to be defined for each tab in the Device View screens. Access controls can be set to either Read/Write or Read-Only. The default is Read/Write. Selecting the **Enable Tab Permissions** checkbox displays the list of tabs whose permission can be specified.

Report Restrictions

The **Report Restrictions** tab can be used to limit the reports that a user can access. By default a user has access to all reports. Selecting the **Report Restrictions Enabled** checkbox allows you to specify the nodes in the Report structure that the user can access. The user can access all reports that belong to that node.

Template/ Service Restrictions

The **Template/Service Restrictions** tab can be used to specify that users can only modify services and templates that they themselves have created. Selecting the **Template/Service List Restrictions Enabled** checkbox will restrict the user to only be able to modify templates or services that they have created. They can still view templates and services created by other users, but they cannot modify them.

Managing external servers

The **Administration > Servers** menu allows you to manage the various external servers that are used by Service Gateway. Following is the list of servers that are currently being used by Service Gateway:

- CWMP Servers
- Diagnostic Servers
- Email Servers
- File Servers
- STUN Servers
- XMPP Servers

Configuring and managing CWMP servers

CPE WAN Management Protocol (CWMP) servers are responsible for communicating with devices that implement the TR-069 management specification.

To view the list of CWMP servers that have established a connection to the Service Gateway instance, go to **Administration > Servers > CWMP**. The list of servers is displayed in the top pane of the **CWMP Servers** management screen with the following details: server Name, Hostname, IP Address, Status, and the Last Status Update time and date.

The list of CWMP servers can be filtered by Name.

Note: A user cannot add a CWMP Server. They are added to the database automatically when they are first installed/started and register with the system.

Deleting a CWMP server

To delete a server:

1. Click server in the **Servers** list pane. Its details are displayed in the **Viewing Server** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: A selected server can be deleted only if its **Status** is **Shutdown** or **Unknown**.

Viewing and modifying CWMP server properties

To view or modify the details for a specific CWMP server, select the desired server from the **Servers** list pane. Its details are displayed in the following tabs of the **Viewing Server** pane at the bottom of the screen:

- General
- Runtime Data
- Configuration
- Preprocessing
- Event Management

General tab

The **General** tab contains the following read-only fields:

- **Name**. The name reported by the server.
- **Hostname**. The hostname of the server.
- **IP Address**. The IP Address of the server.
- **Status**. The current status of the server. Status can be one of the following: Startup, Running, Shutdown, or Unknown.
- **Last Status Update**. The date and time of the last status update received from the server.

In addition, the **CWMP Data Collection** check box can be set or cleared to enable or disable data collection for the server. When this is option enabled, the system collects performance statistics from the server, as well as details about each session with a device. By default, this option is disabled as it puts significant extra load on the system.

Renaming an ACS

The **ACS_NAME** and **ACSAPI_NAME** properties defined in the ACS.properties file for each CWMP server uniquely identifies the server and links it to the configuration and statistics in the database. If you rename the ACS to another name that already exists in the database, then the server will get that configuration. If the name does not already exist in the database, a new entry will be added. In this case, the default configuration will be delivered to the ACS.

To rename a CWMP server while keeping its configuration and statistics, perform the following steps:

1. Shut down the CWMP server and change the **ACS_NAME** and/or **ACSAPI_NAME** in ACS.properties.
2. Log into the UI, view the list of CWMP servers, and ensure that the **Status** is **SHUTDOWN** before proceeding.
3. Change the name of the servers to the same values as specified in **ACS.properties** and save the records.
4. Restart the CWMP server.

Runtime Data tab

The **Runtime Data** tab provides insight into the current load on the CWMP server. The sections and fields on this tab are as follows:

- **Overall**. This section provides information about the overall metrics.
  - **Server Load (%)**. Provides an overall indication of the load on the CWMP server. This load number is used by the event prioritization features to determine if events should be discarded. For details, see Event Prioritization.
  - **Uptime**. Indicates the amount of time that has elapsed since the CWMP server was started.

- **Processors**. This section provides information about the processors on the server.
  - **Available Processors**. The number of processors detected by the server.
  - **Load Average Threshold**. The configured load average threshold at which processor utilization is calculated as 100%.
  - **Load Average**. The current load average.
  - **CPU Load (%)**. The calculated percentage which contributes to the overall server load.
- **Threads**. This section provides information about the threads available to handle incoming connections.
  - **Maximum Threads Available**. The number of threads that are available to handle incoming connections.
  - **Thread Count**. The current number of threads in use.
  - **Thread Load (%)**. The calculated percentage of threads is use, which contributes to the overall server load.
- **Memory**. This section provides information about the memory usage of the server.
  - **Maximum Memory Available**. The maximum amount of memory that the server will attempt to use.
  - **Total Memory Allocated**. The current amount of memory allocated from the operating system by the server process.
  - **Free Memory**. The amount of total memory that is currently unused within the JVM.
  - **Memory Load (%)**. The calculated percentage of memory in use, which contributed to the overall server load.

Configuration tab

The **Configuration** tab allows you to view and change the configuration options for CWMP servers.

Note: Most ACS configuration options can now be managed via the central UI without the need to edit a properties file on each front-end server. In addition, the changes take effect without a restart of the Tomcat server. Defaults are specified for all options, which may be overridden per server.

Configuration options are listed in a table that can be sorted by option name. The table contains the following columns:

- **Option Name**. The name of the option. Pausing on the name displays a tooltip with the underlying property name that may be used in the ACS.properties file. For a list of options available in this tab, see Configuration options.

- **Option Value**. This column allows you to set the value of an option by either entering the value in the text field or selecting a value from a drop-down list. When configuring values for a specific server, select the **Override?** check box to override the default values set for the option.
- **Option Disposition**. This column displays the status of the option. The following values are available:
  - **Configurable Default**. The option is a default for all ACSs.
  - **Locally Configured**. The option has been set in the ACS.properties file, and it cannot be modified remotely.
  - **Overridable**. The option can be specified per ACS.
  - **Not Overridable**. The option cannot be specified per ACS; only the default may be modified.
  - **Read Only**. The option cannot be modified, except via the **ACS.properties** file.

Configuration options

The following table lists the options available under the **Option Name** column.

Option Name	Description
ACS Name	The name of this ACS instance, it must clearly identify the ACS to the end user. The ACS name identifies this ACS for heartbeat and reporting purposes. The name is also used to retrieve the ACS configuration from the database using the **Overridable** options.
ACS API Name	The name of this ACS API instance. This name is currently used only for display in the UI.
API Port	The port that the application server uses for communicating with the CWMP server, to instruct it on what to do with the device.
Application Server Connect Retries	The number of retries to attempt if the ACS is unable to contact the application server and **Standalone Mode** is disabled. This option is used to initiate the connection to the application server. It cannot be remotely configured. **Note:** This setting represents the number of retries, not the initial attempt, so the maximum total number of attempts will be this setting plus 1. Setting this value to 0 (zero) means that no retries will be attempted if the initial attempt fails.
Application Server Connect Retry Timeout (seconds)	The number of seconds to delay before attempting the next retry for connecting to the application server. The minimum delay is 1 second. This option is used to initiate the connection to the application server. It cannot be remotely configured.
Application Server Connect URL	The location of the JNDI server used by the CWMP server. This option is used to initiate the connection to the application server. It cannot be remotely configured. Further information can be found in the CWMP

Option Name	Description
	server's **ACS.properties** file.
Application Server Connect Username	The security username that is required for authenticating the Tomcat Servlet to the J2EE server. This option is used to initiate the connection to the application server. It cannot be remotely configured.
Authentication Mode	The HTTP-based authentication mode used to authorize the CPEs that contact the ACS. The following options are available: • **Basic**. Basic authentication is used. • **Digest**. Digest authentication is used. • **Digest-Session**. Digest authentication is used. The 'algorithm' directive in the authorization challenge is 'MD5-sess'. • **None**. CPEs are not normally authenticated. Authentication of individual devices can be enabled with CPE level authentication overrides. • **None-NoOverride**. CPEs are not authenticated. CPE level authentication overrides are not checked.
Connection Request Retry Timeout (ms)	The timeout, in milliseconds, that the ACS uses when reattempting a CONNECTION REQUEST to a device after an unsuccessful initial attempt. A reattempt is not made if this value is less than or equal to zero.
Connection Request Timeout (ms)	The HTTP timeout, in milliseconds, that the ACS uses when issuing a CONNECTION REQUEST to a device ConnectionRequestUrl to initiate a transaction with a device.
CWMP Data Chunk Size	When CWMP Data Collection has been enabled, this option specifiies the maximum size of CWMP, TICKLE, or ERROR data elements sent in a single message to the application server.
Deferred CR Timeout (ms)	The timeout, in milliseconds, that the ACS uses when checking if a queued RPC is in the server waiting queue. If the RPC is still in the server waiting queue after this timeout, the ACS issues a new connection request to the device.
Device IP Source	A comma-delimited list, of up to three potential sources of the IP address, that is is used to populate the device record in the inventory. The sources are examined in the order provided. If a source does not provide an IP address, the next source will be attempted. The three sources are as follows: • EXTERNAL_IP_ADDRESS - Use the IP address selected from the list of ExternalIPAddress parameters in the INFORM, selected according to the **External IP Address Priority** and **External IP Blacklist** options. This source does not select an IP address if all IP addresses match the IP Address Blacklist.

Option Name	Description
	• CONNECTION_REQUEST_URL - Use the IP address present in the ConnectionRequestURL parameter within the INFORM. This source does not select an IP address if an IP address is not present in the host portion of the URL - such as when a hostname is present instead. Hostnames will not be resolved to IP addresses. • REMOTE_ADDR - Use the IP address that is the source IP address of the HTTP connection that was used to send the INFORM to the ACS. This source always returns an IP address. In the following example, the IP address from the ConnectionRequestURL is used. If the ConnectionRequestURL is not present or empty or contains a hostname instead of an IP address, the remoteAddr of the HTTP/TCP connection is used: CONNECTION_REQUEST_URL,REMOTE_ADDR
Event Prioritization	Enables or disables the event prioritization feature of the CWMP protocol server.
Expand Empty XML Elements	Specifies that empty XML elements in a SOAP request that is sent to a device be formatted as <Command></Command> instead of <Command/>.
External IP Address Priority	This setting defines the parameter values used if more than one ExternalIPAddress parameter is present in an Inform message. Parameter values are: FIRST, FIRST_WANIP, FIRST_WANPPP, LAST, LAST_ WANIP, and LAST_WANPPP. The _WANIP and _WANPPP suffixes specify that the IP address associated with the WANIP or WANPPP interface is preferred. If a valid IP address of the preferred type is not present, the other is used.
External IP Blacklist	A comma-delimited list of IP addresses that are not considered valid for the ExternalIPAddress parameter in an Inform message. Any matching IP addresses are ignored when determining the IP address of the device as per the **External IP Address Priority** option. Trailing wild cards are valid. An example of a valid list is: 0.0.0.0,192.168.*
File Server URL	The base HTTP URL of the Tomcat ACS server. This option is used when doing a configuration backup or saving a file from a device to the database. It is also used as the 'realm' parameter in the authentication challenge header when the ACS challenges a device for Digest authentication.
Heartbeat Interval (seconds)	The time interval, in seconds, that the ACS waits between sending heartbeat reports to the application server. Setting this value to zero or negative turns off sending ACS heartbeats to the application server. The ACS always sends a status report on startup and shutdown regardless of the heartbeat interval.

Option Name	Description
Initial Context Factory	The class name of the initial context factory. This option is used to initiate the connection to the application server. It cannot be remotely configured. Further information can be found in the servers **ACS.properties** file.
Load Average Threshold	This threshold is used to transform the CPU load reported by the operating system into a percentage that can be used for event prioritization, along with other load metrics. The reported CPU load is scaled such that a load value equal to the threshold is reported as 100%. This allows the operator to adjust the reported system load based on individual server performance and workload.
Local ACS API URL	The ACS API URL for this specific ACS instance. This is used to post the RPC response from a device back to the ACS API.
Local ACS URL	The ACS URL for this specific ACS instance. This is used to notify the ACS servlet that there is a new RPC to deliver to a device.
Log HTTP Headers	Specifies whether any HTTP headers sent by the CPE should be logged in ACS-server.log
Map MAC Address Parameter	Setting this property to Enabled automatically parses the MAC Address from the ParameterList in an Inform message message from the device (if present) and associates its value with the device. . If present, the MAC Address is stored in the MAC Address field on the device record. The value for the last parameter in the ParameterList in the Inform message from the device that matches the following regular expression is retained: .*MACAddress\Z
Map PPP Username Parameter	Setting this property to Enabled automatically parses the PPP Username from the ParameterList in an Inform message from the device (if present) and associates its value with the device. If present, the PPP Username is stored in an attribute called DEVICE_PPP_USERNAME, and is associated with the device. The value for the last parameter in the ParameterList in the Inform message from the device that matches the following regular expression is retained: `InternetGatewayDevice\.WANDevice\.\d+\.WAN ConnectionDevice\.\d+\.WANPPPConnection\.\d+\.Username`
PPP Connection IP Blacklist	A comma-delimited list of IP addresses that are not considered valid for the detection of a PPP connection. Trailing wild cards, such as the following, are valid: 10.*,192.168.*,172.16.23.17
Provision CR Credentials	Specifies whether to automatically provision connection request credentials for CPEs.
Provision CWMP Credentials	Specifies whether to automatically provision authorization credentials for CPEs.
Provision STUN Credentials	Specifies whether to automatically provision STUN credentials for CPEs.

Option Name	Description
Provision XMPP Credentials	Specifies whether to automatically provision XMPP credentials for CPEs.
Record Discard Statistics	When enabled, statistics about events discarded by the event prioritization feature is stored in the database for reporting purposes.
Reprovision Auth after Firmware Upgrade	When enabled, causes the CPE authentication credentials to be reprovisioned on a CPE after a firmware upgrade completes.
Reprovision Connection Request after Firmware Upgrade	When enabled, causes the connection request credentials to be reprovisioned on a CPE after a firmware upgrade completes.
Reprovision CR Credentials on Failure	Specifies whether to automatically reprovision connection request credentials for a device if the device challenges for authentication creds and the device rejects them with a '401 Unauthorized' status code. This property is only valid if Provision CR Credentials is also set to Enabled.
RPC Response Wait Time (ms)	The timeout, in milliseconds, the ACS uses when checking for new RPC calls for a device after the device has responded to a previous ACS RPC call and no RPCs are queued for the device. This wait interval is also used when a device sends the ACS an empty POST. The purpose of this parameter is to hold a CWMP session open long enough for Service Gateway or another application to make a sequence of RPC calls to a device within the same CWMP session. This parameter must only be modified in consultation with Consona tech support.
Send Intermediate Result Data	Controls whether specific device interaction data must be collected in intermediate steps to allow for a more detailed view when communication timeouts occur. The collected data is sent to the ACS API URL of the RPC initiator. Thus, bandwidth and thread usage must be considered when enabling this feature.
Send RPC ParameterKey	Specifies whether to include the RPC ParameterKey element in a SOAP request sent to a device.
Server Port	Specifies the port that this server is listening on for incoming connections.
Session Throttling	Enables or disables the session throttling feature of the CWMP protocol server.
Shutdown ACS on Error	When enabled, this option will cause the Apache Tomcat server to shutdown if there is an error trying to contact the application server or to load the configuration during startup.
Standalone Mode	Indicates whether the ACS operates in a stand-alone mode and responds to requests from devices without contacting the application server using pre-defined responses. When Disabled, the ACS interacts with the application server normally. This option cannot be remotely configured.
Transfer Delay (seconds)	The value, in seconds, of the DelaySeconds parameter used by the ACS when it calls the Upload or Download RPC on a device.

Option Name	Description
Upload Path	Path portion of the URL that is provided to devices for uploading files to Service Gateway. This is concatenated with the FileServerURL parameter to form the Upload path when backing up a file to the database. This must correspond to the paths defined in ACS web.xml.
Vendors requiring 200 Empty Post	A comma-separated list of manufacturers for which the ACS uses HTTP 200 instead of HTTP 204 when it sends an empty POST to the device. The manufacturer is determined from the DeviceId.Manufacturer field in the device Inform message. The ACS check is case insensitive. While TR-069 specifies that the ACS use HTTP 204 for an empty POST to a device, in practice some devices do not handle HTTP 204 correctly and HTTP 200 must be used instead.

Preprocessing tab

Preprocessing is used to apply transformations to incoming messages from a device. It provides a flexible way to alter any incoming content before it is processed. This might be necessary if, for example, a particular firmware revision on a device was sending malformed content (for example: a badly formed Inform message). In such a situation, preprocessing can be used to modify the content so that it can be properly processed by the ACS.

Message preprocessing is based on programmatic modules. It currently has a simple but flexible search and replace module. If this particular module does not meet a provider's needs, new modules can be written to perform the required text preprocessing.

Search and Replace module

The search-and-replace module can be used to alter incoming content using configurable search-and-replace regular expression-based queries. The regular expressions must adhere to the rules defined at http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html#sum.

The search-and-replace configuration is done via an XML document. Specific definitions are contained within elements. A search element has two required attributes:

- pattern - used to specify the search regex.
- replace - used to specify the replace value.

Following is an example of a search-and-replace configuration:

```
<config>

<search pattern="ParameterLisst" replace="ParameterList"/>

</config>
```

This definition looks for substrings of 'ParameterLisst' (presumably from a bad Inform message) and replaces them with 'ParameterList' (1 s instead of 2). The pattern and replace attribute content can also take advantage of regular expression capture groups. For example:

```
<config>

<search pattern="ParameterLisst (\S+)" replace="ParameterList $1"/>

</config>
```

Following is an example of a more complicated configuration that contains multiple definitions:

```
<config>

 <search pattern="foo" replace="bar"/>

 <search pattern="bar" replace="foo"/>

</config>
```

In the above example, all instances of 'foo' in an incoming message would be replaced with 'bar'. The resulting content is then be fed into the second definition, causing all instances of 'bar' to be replaced with 'foo'.

The preprocessing mechanism is always run if module configuration has been specified. As a result, the only way to disable this mechanism is to remove the configuration.

Adding or deleting a preprocessing module

To add a preprocessing module, click **Add**. The following columns are activated and allow you to perform the required text preprocessing:

- In the **Description** column, enter a description of the purpose for this preprocessor.
- In the **Preprocessor** column, select the preprocessor to use from the drop-down list.
- In the **Configuration** column, enter the configuration for this preprocessor.
    - If the specified configuration spans multiple lines, the **Configuration** text field is grayed out. Click within the text field or on the 🗐 icon to open the **Script Editor** dialog box. The **Edit Script** text box is either blank (in the case of a new preprocessor definition) or displays the already defined configuration.
    - You can modify the configuration and click **Ok**. The updated configuration is populated in the **Configuration** text box. To discard the changes made, click **Cancel**.
- To remove a preprocessing module, select it and click **Delete**.

Event Management tab

The **Event Management** tab allows you to configure the event prioritization and session throttling mechanisms.

The event prioritization and session throttling mechanisms are configured via an XML document. This document can be manipulated via the user interface or exported to an XML editor of your choice, and then re-imported. The UI manages the document via a tree structure, starting with the **eventManagementConfig** root node.

Event Prioritization

Event prioritization looks at the content of incoming Inform messages, calculates an event priority based on that content, and then figures out if that event can be processed based on the current system load level. If the event priority is too low for the current system load, the event is discarded without being processed.

To configure event prioritization, right-click the **eventManagementConfig** root node and select **Add Event Priority**. **eventPriority** is added as a child of the **eventManagementConfig** node.

Event prioritization consists of three different components.

Component	Description	Configuring
Priority definitions	Defines a priority level and a set of conditions that an incoming event must satisfy to be given the specified priority level.	Right-click the **eventPriority** node and select **Add Priority Defs**. For more information, see Priority Definitions.
Handler definitions	Configures how the ACS responds to an event that is abandoned because it is not of a sufficient priority level.	Right-click the **eventPriority** node and select **Add Handler Defs**. For more information, see Handler Definitions.
Load/priority mappings	Specifies which event priorities are allowed to be processed by the ACS at certain system load levels.	Right-click the **eventPriority** node and select **Add Load Priority Mappings**. For more information, see Load/priority mappings.

Priority Definitions

The **priorityDefs** node consists of a set of priority definitions. A priority definition consists of a numeric priority level and an optional set of evaluation conditions:

- A particular priority level can only appear in a configuration once.
- One priority definition may be flagged as being the default priority level.

When determining the priority level of an event, the ACS sorts the priority definitions in priority level order, from highest (smaller numbers) to lowest (higher numbers). This allows for priority definitions to be added to the configuration in any order.

The ACS checks each priority definition until a match is found:

If	Then
A match is found	The incoming event is assigned the priority level for which the conditions match. **Note:** If no conditions are defined, then the **priorityDef** is not matched to any event unless the **priorityDef** is defined as the default.
No direct match is found and one of the priority definitions has been flagged as the default priority level	The event is assigned the default priority level.
No default priority has been defined	Any event that does not match the conditions for any **priorityDef** is automatically assigned the highest priority level in the system (smallest number), and it is processed.

Evaluation conditions consist of the following:

- A set of basic string comparators (manufacturer, oui, product class, serial number, event, and remote address).
- A numeric comparator (retry count).
- A set of binary operators (and, or, not).

String comparators can take advantage of regular expressions to do a variety of string matching. The regular expressions must adhere to the rules specified by the Java Pattern class at http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html#sum. All string comparisons are case insensitive. These operations can be combined and nested in any way allowed by standard binary operators.

Adding Priority Definitions

1. Right-click the **priorityDefs** node and select **Add Priority**. The **Add Priority** dialog box opens.
2. Enter a value in the **Priority Level** field.

Note: Priority level must be an integer value and is required. To make a Priority definition the default, select the **Default Priority?** check box.

3. Click **Save**.

Configuring event conditions for the priority definition

1. Right-click the priority node and select **Add Conditions**.
2. Right-click the **conditions** node and select **Add Condition**. The Add Condition dialog box opens.
3. Select the **Condition Type** from the drop-down list.
4. Click **Save**.

Handler Definitions

The **handlerDefs** node consists of a set of handler definitions. A handler definition consists of a response type and an optional set of evaluation conditions. As with priority definitions, one of the handler definitions may be flagged as the default handler.

The possible response types are:

- **Default**. This option tells the ACS to use the value returned by Tomcat to a client if no response code was specified (this is typically HTTP code 200).
- **HTTP Error Code**. This option allows you to specify a particular HTTP error/response code that the device recognizes. The code is a required value and must be an integer.
- **SOAP Fault**. This option results in a CWMP SOAP fault being returned to the client. The fault code is a required value and must be an integer that the device recognizes. Fault string is optional.
- **Inform Response**. This option results in an InformResponse being returned to the client, with no indication that the event is otherwise being ignored.

⚠ **Caution:** It is important to note that once an event has been abandoned, all further processing of that session is ignored by the ACS. This response is particularly important when sending back an InformResponse, since a CWMP client interprets that message as an indication that the session was properly established.

Adding Handler Definitions

1. Right-click the **handlerDefs** node and select **Add Handler**. The Edit Handler dialog box opens.
2. Select the **Response Type** from the drop-down list.

Note: To make a Handler definition the default, click the **Default Handler?** check box.

3. Click **Save**.

Configuring event conditions for the handler definition

1. Right-click the **handler** node and select **Add Conditions**.
2. Right-click the **conditions** node and select **Add Condition**. The **Add Condition** dialog box opens.
3. Select the **Condition Type** from the drop-down list.
4. Click **Save**.

Note: Handler conditions look and behave exactly the same as priority conditions.

Load/priority mappings

The **loadPriorityMappings** node consists of a set of load/priority definitions.

A load/priority definition consists of two values:

- A base load level
- A minimum priority level

The base load level specifies the system load level at which the specified minimum priority level is allowed to be processed. For example, a base load level of 85 and a minimum priority level of 5 means that once the system load hits 85%, only those events prioritized as level 5 or higher (4, 3, 2, 1, and 0) will be processed. Any events with a value lower than 5 will be abandoned. Base load level can be a floating point number, while minimum priority level must be an integer. Both values are required.

Adding Load Priority

1. Right-click the **loadPriorityMappings** node and select **Add Load Priority**. The **Add Load priority** dialog box opens.
2. Enter the appropriate values in the **Base Load Level** and **Lowest Priority** fields.
3. Click **Save**.

Session Throttling

A throttle definition can consist of multiple unique ID strings and/or multiple remote address values (both of which can be regular expressions, as defined in the Java Pattern class). At least one unique ID or remote address must be specified.

The session throttling mechanism keeps track of the number of events coming in from a device based on its CWMP-based unique ID as well as its remote IP address. Throttle definitions can be defined that check to see if the number of events from a particular device (based on ID or IP address) exceed some sort of threshold (for example, 10 events within the last minute).

To configure session throttling, right-click the **eventManagementConfig** root node and select **Add Session Throttling**.

Adding a throttle definition

To create a throttle definition:

1. Right-click the **sessionThrottling** node and select **Add Throttle**. The **Add Throttle** window containing all the configuration parameters opens.

2. Enter a value in the **Unique ID** field and click **Add**. The value is added to the list of Current Unique IDs. and/or
3. Enter a value in the **Remote Address** field and click **Add**. The value is added to the list of Current Remote Addresses.

Note: To delete an item, click it in the appropriate current window and then click **Delete**.

4. Enter a value (integer) in at least one of the optional thresholds fields.
5. Select the response type from the drop-down list.

If you select	Then
HTTP Error Code	Specify the **HTTP Code**.
SOAP Fault	Specify the **Fault Code** (the **Fault String** field is optional).

6. Click **Save**.

Editing Nodes

In general, an existing node can be edited by right-clicking on the desired node and selecting **Edit <component>** , where **<component>** is the node that is being edited. For example, if Priority Level is being modified, the menu item will display **Edit Priority**.

Some nodes that are actually managed via configuration of a parent level node (such as a **uniqueId** node within a throttle definition) offer no direct edit option and can only be manipulated by editing the parent node.

Deleting Nodes

Deleting a node works in a similar manner as editing a node - some nodes can only be deleted by deleting or editing the parent node.

Caution: The **Reset** button deletes the entire configuration tree. This action cannot be undone, so use this button with caution.

Importing or Exporting Event Management Configurations

If a configuration exists in an external XML document, it can be imported into the system. To import an external XML configuration document:

1. Click the **Import** button at the botton left of the tab. The **Event Management Configuration Import** dialog box opens.
2. Click **Browse**, navigate to the file you want to import, and click **Open**.
3. Click **Import**.

Once the file is imported, the contents are displayed and can be edited.

Whenever the configuration is saved, the contents are validated against an XML schema to ensure proper structure and content. If the validation encounters any errors, they are displayed on the screen, and the contents are NOT saved.

Once a configuration has been successfully validated and saved, it can be exported as a raw XML document by clicking the **Export** button.

Configuring and managing diagnostic servers

Diagnostic servers are used by the Upload and Download CSR diagnostic tests which measure file transfer speeds to and from devices that support TR-143 throughput diagnostic tests. Servers may be local hosts or remote hosts on the Internet. The servers configured in the **Diagnostic Servers** management screen appear as options for the CSR to use when initiating a diagnostic test.

To access the Diagnostics Servers management screen, select **Administration > Servers > Diagnostic**. The list of diagnostic servers is displayed in the top pane of the **Diagnostic Servers** management screen with the following details: Hostname, Description, and Realm.

The list of diagnostic servers can be filtered by Hostname, Description, and Realm.

Adding a Diagnostic server

1. Click **New** on the **Diagnostic Servers** management screen. The **Viewing New Diagnostic Server** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:

   a. Select the **Realm** and **Server Type** from the respective drop-down lists.

   b. Enter the name of the host in the **Hostname** field and the port number in the **Port** field.

   c. Specify if the server must support upload or download.

If	Then
The server must support upload	On the **Upload Files** tab, specify the filename including the full path in the **Upload File** field and click **Add**.
The server must support download	On the **Download Files** tab, specify the filename including the full path in the **Download File** field and click **Add**.

   d. Provide additional information if required.

3. Click **Save**.

Deleting a Diagnostic server

1. Click diagnostic server in the in the **Diagnostic Server** list pane. Its details are displayed in the **Viewing Diagnostic Server** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying a Diagnostic server

To view the details for a diagnostic server, select the desired server record from the **Diagnostic Server** list pane. Its details are displayed in the following tabs of the **Viewing Diagnostic Server** pane at the bottom of the screen:

- General
- Upload Files
- Download Files

General tab

The General tab contains the following fields:

- **Realm**. This diagnostic server will be available to devices within the specified realm.
- **Hostname**. The hostname of the diagnostic server that will be used to form the URL provided to the device.
- **Description**. A description of the server.
- **Server Type**. The protocol used by this server (HTTP or FTP). The selected protocol will be used to form the URL provided to the device.
- **Port**. The port on which the server listens for incoming connections. This value will be used to form the URL provided to the device.
- **Supports Upload**. Select this check box if the server is to be made available to CSRs as an option for upload tests.
- **Supports Download**. Select this check box if the server is to be made available to CSRs as an option for download tests.
- **Username**. The username that is required to connect to the server if the server requires authentication.
- **Password**.The password that is required to connect to the server if the server requires authentication.
- **Confirm Password**. Confirm the value entered in the **Password** field.

Tip: A CWMP server can be used as a Diagnostic server by specifying the external hostname and port for the CWMP server, and HTTP as the Server Type. Refer to Download Files and Upload Files for the filenames to specify when using this approach.

Upload Files tab

The Upload Files tab allows you to specify the pathnames and filenames of the files used for upload tests.

To add a new upload file to the list, specify the filename including the full path in the **Upload File** field and click **Add**.

To remove an existing file from a server, select the file from the **Current Upload Files** pane and click **Delete**.

If the Diagnostic server is also a CWMP Server, the following path and file can be used for a filename. The CWMP Server will accept and discard any file sent by the device.

/ACS-server/FileServlet/diagnostic

Download Files tab

The Download Files tab allows you to specify the pathnames and filenames of the files used for download tests. Multiple files may be placed on the same server to test the download speeds using various sizes or types of files.

To add a new download file to the list, specify the filename including the full path in the **Download File** field and click **Add**.

To remove an existing file from a server, select the file from the **Current Download Files** pane and click **Delete**.

If the Diagnostic server is also a CWMP server, the following format can be used for a filename to enable the device to access a file of a specific size with randomly generated content:

```
/ACS-server/FileServlet/diagnostic/<filesize>
```

where **<filesize>** is replaced with the desired size of the file in bytes. For example, a 1 MB test file of random bytes would be specified with a file size as follows:

```
/ACS-server/FileServlet/diagnostic/1000000
```

Note: The maximum filesize that can be specified is 10485760 bytes.

Configuring and managing Email servers

Email servers are used to send Email messages for features that provide email notification, such as the Reporting system. More than one email server may be configured to balance load and provide redundancy in case any server fails. SMTP Authentication may be enabled on a per server basis. Mechanisms supported are PLAIN, LOGIN, and DIGEST-MD5.

To view the list of email servers that have been configured, select **Administration > Servers > Email**. The list of servers is displayed in the top pane of the **Email Servers** management screen with the following details: SMTP Host, SMTP Port, and Priority. The list can be filtered on SMTP Host.

Adding an Email server

1. Click **New** on the **Email Servers** management screen. The **Viewing New Email Server** pane opens on the bottom of the screen.
2. On the **General** tab,
   a. Enter the hostname or IP address of the SMTP server in the **SMTP Host** field.
   b. Enter appropriate values in the other fields if required.
   c. If authentication is required to access this server, select the **Authentication Required** check box and enter the authentication user and password values in the respective fields.
3. Click **Save**.

Deleting an Email server

1. Click server in the **Email Servers** list pane. Its details are displayed in the **Viewing Email Servers** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying Email server properties

To view the details for a specific Email server, select the desired server from the **Email Servers** list pane. Its details are displayed in the following tabs of **Viewing Email Server** pane at the bottom of the screen:

- General
- Global Configuration

General tab

The General tab contains the following fields:

- **SMTP Host**. The hostname or IP address of the SMTP server.
- **SMTP Port**. The port on which the SMTP accepts incoming connections.
- **Priority**. When more than one server is configured, priority is used to define the order in which the servers are contacted (see Global Configuration for details).
- **Authentication Required**. Select this check box if authentication is required to access this server. When selected, a user name and password must be provided which will be used for all emails that are sent using this SMTP server.
- **Authentication User**. The user name to use during SMTP Authentication.
- **Authentication Password**. The password to use during SMTP Authentication.

! **Important:** If authentication is enabled and an authentication failure occurs while sending an email, the email is not sent even if the SMTP server does not strictly require authentication to send the email.

Global Configuration tab

The Global Configuration tab presents the same information regardless of the email server that is selected. It contains a single drop-down list with the following options that affect how multiple servers are contacted:

- **Random Order**. Each time an email message needs to be sent, one of the servers is chosen at random. If the email fails, another server in the list is chosen until the email is sent or all servers have failed.
- **Random One Only**. Each time an email message needs to be sent, one of the servers is chosen at random. If the email fails, no further attempts are carried out.
- **Prioritized List**. Each time an email message needs to be sent, the server with the highest priority (lowest number) is used. If the email fails, the next server in priority order is chosen until the email is sent or all servers have failed.
- **Prioritized One Only**. Each time an email message needs to be sent, the server with the highest priority (lowest number) is used. If the email fails, no further attempts are carried out.

Configuring and managing file servers

Service Gateway allows you to manage the file servers that are used in various operations. The file servers hold the configuration, web content, tone, ringer, application (apps), and firmware files that will be sent to devices. The file servers can be distributed regionally, closer to the end devices requesting the file transfers. Also, their usage can be segmented by domain. They can also be segmented by the WAN connection type that is being used by the device. For details, see File Servers per WAN Connection Type.

To view the list of file servers that have been configured, select **Administration > Servers > File**. The list of servers is displayed in the top pane of the **File Servers** management screen with the following details: Hostname, Description, Status, and Realm.

The list can be filtered by Hostname, Description, Status, and Realm.

Adding a file server

1. Click **New** on the **File Servers** management screen. The **Viewing New File Server** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:
   a. Select the **Realm** and **Protocol** values from the respective drop-down lists.
   b. Enter the appropriate values in the **External DNS or IP Address** and **Port** fields.
   c. Provide additional information as required.
3. On the **Domains** tab, associate one of more domains with the file server by selecting and dragging them from the **Available** pane to the **Current** pane.
   - To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.
4. Click **Save**.

Deleting a file server

1. Click server in the **File Servers** list pane. Its details are displayed in the **Viewing File Server** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying file server properties

To view the details for a specific file server, select the desired server from the **File Servers** list pane. Its details are displayed in the following tabs of **Viewing File Server** pane at the bottom of the screen:

- General
- Upload Settings
- Domains

General tab

The General tab contains the following fields:

- **Realm**. The realm to which the file server belongs. Only devices within this realm are able to access this file server.
- **External DNS or IP Address**. The hostname or IP address that is communicated to a device when instructing it to download a file from the file server. This hostname or IP address must be visible to the devices.
- **Description**. A description for the file server.
- **Protocol**. The protocol supported by this file server. Choose from: HTTP, FTP, TFTP, or HTTPS.
- **Port**. The port on which the file server listens for new connections from devices.
- **Document Root**. The path on the server from where devices can download files. All files downloaded from this server will be located at the specified path.
- **Status**. Indicates whether the server should be enabled or disabled. Select **Active** from the drop-down list to enable this server for use. To disable the server, select **Inactive**.
- **Username**. If devices are required to be authenticated before downloading a file, specify the username here.
- **Password**. If devices are required to be authenticated before downloading a file, specify the password here.
- **Confirm Password**. Confirm the value entered in the **Password** field.
- **Associated WAN Connection Type**. Specifies whether this file server is available for devices that are connected using a PPP WAN connection or an IP WAN connection, or either. See File Servers per WAN Connection Type for additional details on the use of this option.

File Servers per WAN Connection Type

Selection of a file server to instruct a device to use can be based on the WAN Connection type of the device. This parameter allows two sets of distinct files servers to be defined based on the type of network connection being used by a device.

The WAN connection type of a device is determined and updated while processing each Inform message from the device. A PPP WAN Connection type is deemed to be in use if ALL of the following conditions are met:

- the parameter *InternetGatewayDevice. WANDevice.{i}. WANConnectionDevice.{i}. WANPPPConnection.{i}. ExternalIPAddress* is found within the Inform message.
- the value of the parameter is a valid IP address.
- the IP address is NOT within the configurable blacklist of IP addresses.

If multiple *WANPPPConnection.{i}. ExternalIPAddress* are present in the Inform message, only one of them must meet the preceding criteria. In all other cases, the WAN connection type of the device is deemed to be IP.

When selecting a file server, the WAN connection type is included in the criteria that is used to determine which file server to use. The blacklist of IP addresses mentioned previously is specified via the ACS.properties file using the **PPPConnectionBlackList** property. For details on how to use this property, refer to the ACS.properties file.

Upload Settings tab

The Upload Settings tab contains the following fields:

Note: These fields are optional and only need to be provided if the file server supports uploads from Service Gateway over the SSH protocol.

- **Upload DNS or IP Address**. The internal hostname or IP address used to establish an SSH session from the Service Gateway application server.
- **Upload Authentication Type**. The type of SSH authentication enforced by the SSH server, either **Password** or **Public Key**. To use **Public Key**, a PEM file containing a DSA or RSA private key in OpenSSH key format must be specified in the system properties file (encore.properties) by an administrator.
- **Upload Path**. The path name to the document root of the file server.
- **Upload Username**. The user name that is required for SSH authentication.
- **Upload Password**. The password that is required for SSH authentication. If using Public Key authentication and the PEM file is encrypted on the local filesystem, this is the password required to decrypt the PEM file. If the PEM file is not encrypted, the password field may be left blank.
- **Confirm Upload Password**. Confirm the value entered in the **Upload Password** field.

Domains tab

The Domains tab is used to associate one or more domains with a file server. When instructing a device to download a file, the system selects a file server from those that are associated with the same realm as the device and then lists the domain (or a parent domain) of the device. At least one domain must be associated with the file server. When you associate a file server with an administrative domain, the file server is automatically associated with all of that domain's child domains, so you do not have to explicitly choose each child domain.

- To associate a domain with the file server, select the domain from the **Available** pane and drag it to the **Current** pane.
- To remove the association between a domain and a file server, select the domain from the **Current** pane and drag it back to the **Available** pane.

  To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

Configuring and managing STUN servers

STUN servers assist the CWMP servers when establishing a connection to a device behind a NAT device or firewall. To view a list of STUN servers that have established a connection to the Service Gateway instance, select **Administration > Servers > STUN**.

The **STUN Servers** list in the top pane displays the server Name, Description, Hostname, Port, and Status. The list can be filtered by Name, Description, Hostname, and Status.

Adding a STUN server

1. Click **New** on the **STUN Servers** management screen. The **Viewing New STUN Server** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:
    a. Enter the name reported by the server in the **Name** field.
    b. Enter the hostname of the server in the **Hostname** field.
    c. Enter the appropriate values in the other fields if required.
3. Click **Save**.

Deleting a STUN server

1. Click server in the **STUN Servers** list pane. Its details are displayed in the **Viewing STUN Server** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying STUN server properties

To view the details for a specific STUN server, select the desired server from the **STUN Servers** list pane. Its details are displayed in the following tabs of **Viewing STUN Server** pane at the bottom of the screen:

- General
- Runtime Data

General tab

The General tab contains the following fields:

- **Name**. The name reported by the server.
- **Description**. A description of the server.
- **Hostname**. The hostname of the server.
- **Port**. The port that the server is listening on.
- **Status**. The current status of the server. Status can be one of the following: Startup, Running, Shutdown, or Unknown.
- **Last Status Update**. The date and time of the last status update received from the server.

Runtime Data tab

The Runtime Data tab displays the most recently reported runtime data for the STUN server. The read-only fields on this tab are:

- **Available Processors**. The number of processors detected by the server.
- **Thread Count**. The current number of threads running on the server.
- **Total Memory**. The amount of memory currently allocated from the operating system by the server process.
- **Max Memory**. The maximum amount of memory that the server will attempt to use.
- **Free Memory**. The amount of total memory that is currently unused within the JVM.
- **Uptime**. The amount of time that has elapsed since the STUN server was started.

Configuring and managing XMPP servers

XMPP servers assist the CWMP servers when establishing a connection to a device behind a NAT device or firewall. Conceptually XMPP servers are similar to STUN servers, except that they use a different protocol for communicating with the devices behind the NAT devices or firewalls. To view a list of the XMPP servers that have established a connection to the Service Gateway instance, select **Administration > Servers > XMPP**.

The XMPP Servers list in the top pane displays the Server Address, Server Port, and Realm. The list can be filtered by Server Address.

Adding an XMPP server

1. Click **New** on the XMPP Servers management screen. The **Viewing New XMPP Server** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:
   - Select **Realm** from the drop-down list.
   - Enter the IP address or hostname of the server in the **Server Address** field.
   - Enter the port of the server in the **Server Port** field.
   - Select the **Active** checkbox to mark the server as active.
3. On the **Domains** tab, associate one or more domains with the file server by selecting and dragging them from the **Available pane** to the **Current** pane.
   - To select multiple items, hold down the CTRL key and click on each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.
4. Click **Save**.

Deleting an XMPP server

1. Click a server in the XMPP Servers list pane. Its details are displayed in the Viewing XMPP Server pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **OK**.

Viewing and modifying XMPP server properties

To view the details for a specific XMPP server, select the desired server from the XMPP Servers list pane. Its details are displayed in the following tabs of Viewing XMPP Server pane at the bottom of the screen:

- General
- Domain

General tab

The General tab contains the following fields:

- **Realm**. The realm to which the XMPP server belongs. Only devices within this realm are able to access this XMPP server.
- **Server Address**. The hostname or IP address of the server.
- **Server Port**. The port that the server is listening on.
- **Active**. A flag indicating whether the server is active

Domains tab

The Domains tab is used to associate one or more domains with an XMPP server. When provisioning a device to communicate with an XMPP server, the system selects an XMPP server from those that are associated with the same realm as the device and then lists the domain (or a parent domain) of the device. When you associate an XMPP server with a domain, the XMPP server is automatically associated with all of that domain’s child domains, so you do not have to explicitly choose each child domain.

- To associate a domain with the XMPP server, select the domain from the **Available** pane and drag it to the **Current** pane.
- To remove the association between a domain and an XMPP server, select the domain from the **Current** pane and drag it back to the **Available** pane.
- To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

Configuring the Service Gateway environment

The **Administration > Settings** menu provides access to the various configurable aspects of Service Gateway. Following is the list of features that can be configured to tailor the Service Gateway environment to your needs:

- Custom Menu Options
- File Types
- Load Metrics
- Plugins
- Preferences
- Real-time Probes
- Record Purging
- System Keys

Managing Custom Menu Options

Custom Menu Options allows options to be added to the Service Gateway menu bar which link to the URL of an external web site or web-based application. The new option can be added to any of the existing top-level menus and can be specified to only appear to users of a specific realm or those that have a specific role.

Custom Menu Options in a menu are indicated by the ↗ icon. Clicking on a custom menu option will open up a new browser window, directed towards the configured URL.

Custom Menu Options can only be managed by users that have the ***Manage/View Custom Menu Options*** permission.

To view the list of Custom Menu options, select **Administration > Settings > Custom Menu Options**. A list of menu options with Name, URL, Required Role, and Required Realm is displayed in the top pane. The list of menu options can be filtered by Name.

Adding a menu option

1. Click **New** on the **Custom Menu Options** management screen. The **Viewing New Menu Option** pane opens on the bottom of the screen.
2. On the **General** tab of the **Viewing New Menu Options** pane:

   a. Enter the name of the option to appear on the menu in the **Name** field.

   b. Enter the URL that the new browser window must be directed to in the **URL** field.

   c. Select the appropriate values from the following drop-down lists:

      - **Required Realm**
      - **Top-Level Menu**
      - **Required Role**

      Name and **URL** are mandatory fields, while the other selections are optional.

3. Click **Save**.

Deleting a menu option

1. Click menu option in the **Custom Menu Options** list pane. Its details are displayed in the **Viewing Custom Menu Option** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying a menu option

To view the details for a menu option, select it from the **Custom Menu Options** list pane. Its details are displayed in the General tab of the **Viewing Custom Menu Option** pane at the bottom of the screen.

General tab

The General tab contains the following fields:

- **Required Realm**. If set to **Any**, the option is available to a user from any realm. Otherwise, the option is only be visible to a user that is associated with the selected realm.
- **Name**. The name of the option as it must appear in the menu.
- **URL**. The URL that a new browser window is directed towards when the menu option is clicked.
- **Top-Level Menu**. The top-level menu under which this option must appear. Apart from the top-level menu options that are normally available in this drop-down list, it also includes an option called **Tools**.

Note: When a custom menu option is added and associated with the Tools top-level menu, the Tools menu will appear on the menu bar if the logged in user has the realm and role defined for this custom menu option. When visible, the Tools menu appears between the Report and Help top-level menus.

- **Required Role**. If set to **Any**, the option is available to a user regardless of their assigned permissions. Otherwise, the option is only visible to a user that is associated with the selected permission via group membership.

Categorizing file types

Service Gateway categorizes device files into groups called file types. To view a list of existing file types, go to **Administration > Settings > File Types**. The following default file types are available:

- **Configuration**. Files used for updating the configuration on a device.
- **Content**. Files that contain only Web content for a device's Web-based interface.
- **Firmware**. Files used for upgrading a device's firmware.
- **Ringer**. Files used for ringer definitions in devices that support voice service.
- **Software Module**. Files used to install applications to a device using the Software Modules feature.
- **Tone**. Files used for tone generations in devices that support voice service.

Adding a file type

Device files can be further categorized by adding additional file types. To add a file type:

1. Click **New** on the **File Types** management screen. The **Viewing New File Type** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:
   a. Enter the name for the file type in the **Name** field.
   b. Select a category for the file type from the **Category** drop-down list.
   c. Enter the text string to send to the device with the Download or Upload RPC commands in the **CWMP FileType** field.
3. Click **Save**.

Deleting a file type

1. Click file type in the **File Types** list pane. Its details are displayed in the **Viewing File Type** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: Only user-defined file types may be modified or deleted.

Viewing and modifying a file type

To view the details for a file type, select it from the **File Types** list pane. Its details are displayed in the General tab of **Viewing File Type** pane at the bottom of the screen.

General tab

The General tab contains the following fields:

- **Name**. The name of the file type.
- **Category**. This drop-down lists allows you to define how files of this type will be used by the system. For example, if you select **Firmware**, files with this file type will be used by the firmware features of Service Gateway.
- **CWMP FileType**. This field allows you to enter the text string that gets sent to the device with the Download or Upload RPC commands.

Managing Load Metrics

Load Metrics allows the performance indicators that are used to determine an aggregate application server load to be specified. These performance indicators are used by the Event Prioritization feature.

Load Metrics can only be viewed by users that have the ***View Servers*** permission, and can only be modified by users that have the ***Manage/View Servers*** permission.

To display the list of Key Performance Indicators (KPI) that are defined for use as Load Metrics, select **Administration > Settings > Load Metrics**. A list of KPIs with threshold details is displayed in the top pane. The list of menu options can be filtered by KPI Name.

Adding a KPI

1. Click **New** on the **Load Metrics** management screen. The **Viewing New Load Metric** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:

   a. Click within the KPI field or on the ▤ icon. The Select KPI dialog opens with the KPIs listed in a tree view.

      - On the **Select KPI** dialog, expand the node and select the required KPI.
      - Click **Ok**.

   b. Enter the appropriate content in the **Threshold** field if required.

3. Click **Save**.

Deleting a KPI

1. Click KPI in the **Load Metrics** list pane. Its details are displayed in the **Viewing Load Metric** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying a KPI

To view the details for a KPI, select it from the **Load Metrics** list pane. Its details are displayed in the General tab of **Viewing Load Metric** pane at the bottom of the screen.

General tab

The General tab contains the following fields:

- **KPI**. The KPI to use as a load metric. Clicking on the field opens the Select KPI dialog.
- **Description**. The description of the load metric. This is a read-only field.
- **Threshold**. An optional field, it is used to express the KPI value as a percentage. If the KPI is already a percentage (as is the case with connection pool usage and memory usage), then a threshold is not required. For other KPIs, such as ***Threads In Use*** or ***updateServiceGateway*** times, a threshold can be specified. The value specified in this field is considered as 100% when it is converted to a percentage.

! **Important:** Thresholds are evaluated individually for each application server. For example, when using the ***Threads In Use*** KPI and specifying a threshold of 500, the threshold is 500 for each server and not for the system as a whole.

Viewing plugins

Plugins are one way that the functionality of Service Gateway is extended. Many plugins are provided out-of-the-box.

To view the list of installed plugins, select **Administration > Settings > Plugins**. A list of plugins with the Name, Type, and Status is displayed in the the **Plugins** list pane at the top of the **Plugins** screen. The list of plugins can be filtered by Name and Type, which can be one of the following: **ACS Preprocessor**, **Action**, or **Templates**.

Note: Plugins cannot be added or deleted from the UI. Installing or uninstalling a plugin is performed only by a system administrator.

To view the details of a plugin, select it from the **Plugins** list pane. Its details are displayed in the General tab of the **Viewing Plugins** pane at the bottom of the screen.

General tab

The General tab contains the following fields:

- **Name**. The name given to this action.
- **Type**. The type of action. It is one of the following:
  - **ACS Preprocessor**. These plugins are used to pre-process incoming INFORM Events from TR-069 capable devices.
  - **Action**. These plugins are used in the workflow of a policy.
  - **Templates**. These plugins are used by the configuration management and synchronization module to push configuration to devices.
- **Enable**. This check box can be used to enable or disable a plugin.

Caution: Disabled actions cannot be used by other Service Gateway modules.

Setting preferences

The Preferences interface allows you to configure several system-wide preferences for Service Gateway. To access the **Preferences** management screen, select **Administration > Settings > Preferences**.

Viewing and modifying preferences

A list of **Preferences** is displayed on the left pane, as follows:

- General
- Session
- CWMP
- Record Purging
- User Settings
  - Default Password Policy
  - Password strength

Click preference to view or modify its properties in the right pane.

General page

The General page allows you to configure several system-wide preferences for Service Gateway. The following table lists the preferences available within this page.

Preference	Description
Application Server Status Update Lock Timeout (seconds)	The amount of time that must elapse before the Application Server Status Update Lock is deemed as stale and released.
Audit Logging Enabled	Determines whether audit logs are maintained by the system.
Configuration Backups Maintained Per Device	Specifies the maximum number of configuration backups that are to be retained for a device. Whenever a new configuration backup is stored for a device, the system will delete the oldest ones to ensure that no more than the number specified by this preference is kept.
Default Device Search Type	Sets the default search type that is to be used when searching for a device.
Device URL Path	When viewing a device in the Device Summary module of the CSR UI, the IP Address may appear as a hyperlink that is used to connect to the management web interface on the device, provided neither the Device URL Protocol preference nor the Device Protocol setting for the firmware (Inventory >

Preference	Description
	Firmware) is set to **Disabled**. When enabled, this preference specifies the path that is included when the URL is constructed. For example, if you specify a path of “/web”, then the URL may appear as http://<ipAddress>/web.
Device URL Protocol	Specifies the default protocol to use when constructing the URL to access the management web interface on a device (via the IP Address hyperlink) when viewing the device in the Device Summary module of the CSR UI. This value can be overridden by the Device Protocol property on the firmware record. Valid values: Disabled, HTTP, or HTTPS. If disabled is selected, no URL is constructed, unless overridden by the setting on the firmware record.
Disable Database Storage of Inventory Device Files	When checked, any files that are uploaded to the system via the **Inventory > Device Files** screen will be transferred to any defined File Servers without being stored in the database. This improves system performance when uploading large device files.
Maximum Inventory Firmware Upgrade Attempts	Sometimes a bad firmware image can result in the device reporting an incorrect software version, which may result in automated inventory-based firmware upgrades being re-attempted each time a device reboots. This preference puts a limit to such an infinite loop by imposing a limit on the number of firmware upgrade attempts to the same firmware revision.
Active Policy Device List Generation Timeout (seconds)	Specifies the amount of time that must elapse before an attempt to generate a device list for a policy is deemed to have stalled. This check occurs each time a policy runs, and occurs more frequently than the **Passive Policy Device List Generation Timeout**.
Passive Policy Device List Generation Timeout (seconds)	Specifies the amount of time that must elapse before an attempt to generate a device list for a policy is deemed to have stalled. This check occurs when a timer-based job runs to check for such stalled attempts, and is meant to be a safeguard to catch any occurrences that are not dealt with by the **Active Policy Device List Generation Timeout** preference.
Maximum Number of Rows in a Report	Specifies the maximum number of rows that will be shown in a report.
Performance Monitoring Remote Server Communication Protocol	Specifies the protocol to use when interrogating other cluster members for their load metrics.

Preference	Description
	Valid values: HTTP and HTTPS.
Performance Monitoring Remote Server Timeout (seconds)	Indicates the amount of time to specify as the HTTP connection and socket timeouts when interrogating other cluster members for their load metrics.
Policy Action Timeout (seconds)	Specifies the amount of time that must elapse before an executing policy action is deemed as stale and must be forcibly failed.
Policy Execution History Minimum Update Interval (seconds)	To reduce database updates during policy execution, summary counts of successful, skipped, and failed devices are kept in memory and only written to the database periodically. This preference controls how frequently that data is written to the database.
Policy Timer Execution Timeout (seconds)	Specifies the amount of time that must elapse before the Policy Timer Execution Lock is deemed as stale and released.
Policy Timer Retry Lock Timeout (seconds)	Specifies the amount of time that must elapse before the Policy Timer Retry Lock is deemed as stale and released.
Purge Partitions Execution Timeout (seconds)	The amount of time that must elapse before the Purge Partitions Execution Lock is deemed as stale and released.
Real-Time Probe Timeout (seconds)	Specifies the amount of time that must elapse before an SNMP request to a device times out.
Date Format for Reports	Specifies the date format to use in reports. Unless specified otherwise, dates are displayed as “yyyy-MM-dd HH:mm:ss”. If the default value provided by Service Gateway is not used, any date specified must be a valid **Datejs** format, as specified at http://code.google.com/p/datejs/wiki/FormatSpecifiers
Base URL for links in e-mailed reports	Specifies the base URL to use in emailed reports. This URL is used to access the report.
Scheduled Jobs Execution Timeout (seconds)	Specifies the amount of time that must elapse before the Scheduled Jobs Execution Lock is deemed as stale and released.
Load Metrics Time Window (seconds)	Specifies the time window from which to take data points when retrieving loads metrics for display in the dashboard and monitor graphs.
Start of Fiscal Year	Defines the start of the fiscal year. This value is used in reports when defining an SqlVariable of the following types: ‘datelist’, ‘datetimelist’, ‘datelistlow’, or ‘datelisthigh’.
Sticky Search Results	When selected, device and subscriber search results are

Preference	Description
	retained when you navigate away from and return to those screens where the search was performed. When cleared, the search results are cleared each time you navigate back to those screens.
Subscriber Last Name Required	By default, Service Gateway requires that you specify a last name for a subscriber. Since not all cultures use last names, this setting can be used to make the last name optional for a subscriber.
Server Status Treated as SHUTDOWN (seconds)	The CWMP, STUN, and Application Servers that are part of Service Gateway send regular heartbeat messages to update their current status. This is used to help determine server load, as well as which servers are currently online. This setting specifies the amount of time that must elapse since the last heartbeat message is received from a server before that server is considered to be shutdown.
Unlock Devices	The Synchronize Configuration policy action locks the device’s configuration whenever a failure is detected. When this setting is selected, the system automatically unlocks those devices once the amount of time specified by the “Device Unlocking Age” preference has elapsed.

Session page

The Session page allows you to configure system-wide session preferences for Service Gateway. The following table lists the preferences available within this page.

Preference	Description
Auto-Invoke Real-Time Probes	Determines whether or not to execute CSR real-time probes on a device refresh or tab change.
Exclude Unrestricted Firmware in Upgrade Path Options	When associating firmware with hardware, this preference specifies whether any firmware without a product class association is shown.
Language	Specifies the current language that the UI is displayed in. Only languages that have been translated and set up on the server appear in the **Language** drop-down list. By default, English is the only option available.
Maximum CWMP Device Event Results Allowed	Specifies the maximum number of device events to display when viewing a device.
Maximum Policy Device Results Allowed	Specifies the maximum number of devices to list in the lower pane of the **Policy Logging** screen.
Maximum Search Results Allowed	Specifies the maximum number of results to display when

Preference	Description
	searching for devices and subscribers.
Session Timeout (seconds)	Specifies the number of seconds that a session is idle before it is automatically locked, requiring the user to enter their password to resume using the interface.
Show Hidden Reports	By default, some reports that are only used as a drill-down from another report or only relevant in the context of a specific interface action (such as deleting an object that has other objects referencing it) will be hidden. Selecting this check box will show all such reports.
User Interface Layout Direction	Selecting **Right to Left** displays the UI in a mirror image, which is more natural for some countries and languages. This preference can be set system wide and per user.

CWMP page

The CWMP page allows you to configure system-wide preferences for CWMP servers on Service Gateway. The following table lists the preferences available within this page.

Preference	Description
ACS-Server API File Transfer Timeout (milliseconds)	When communicating with a CWMP device, Service Gateway communicates with the CWMP server, which in turn communicates with the device. To ensure that these connections do not stay open indefinitely, timeouts must be defined for each of these connections. Although not enforced, it is recommended that the connection between the CWMP server and the device is ended before the connection between Service Gateway and the CWMP server. This setting specifies the timeout for the connection between Service Gateway and the CWMP server for any RPCs that involve transferring a file to or from the device.
ACS-Server API Timeout (milliseconds)	This setting represents the timeout for the connection between Service Gateway and the CWMP server for any RPCs that do NOT involve transferring a file to or from the device.
ACS-Server API URL	Specifies the URL that is used by Service Gateway to communicate with the CWMP servers. This can be a comma-delimited list of all the CWMP servers that are deployed. Service Gateway will balance the load between all the CWMP servers that are listed.
ACS-Server CPE File Transfer Timeout (milliseconds)	This setting represents the timeout for the connection between the CWMP server and the device for any RPCs that involve transferring a file to or from the device. This value should be less than the **ACS-Server API File**

Preference	Description
	Transfer Timeout.
ACS-Server CPE Timeout (milliseconds)	This setting represents the timeout for the connection between the CWMP server and the device for any RPCs that do NOT involve transferring a file to or from the device. **Note:** This value should be less than the value set for **ACS-Server API Timeout**, as the communication between the device and the CWMP server needs to complete before the CWMP server can respond to Service Gateway.
ACS-Server Kicked Handler JNDI Name	Specifies the JNDI name to use for accessing the handler for the Kicked RPC from a device. Service Gateway includes a default handler that returns the **nextUrl** property specified in a device attribute called **KICKED_NEXTURL**. If this attribute is not present on the device, this handler returns the **nextUrl** that the device has sent. If a different behavior is required, a custom handler can be provided, and this property must be updated to be the JNDI name for that new handler.
ACS Workflow to check for Next Queued Inform Event	If enabled, the ACS workflow will check to see if there is another event queued for this device. If there is, it will process that event.
ACS Workflow to check for Queued Policy Devices	If enabled, the ACS workflow will check to see if the same device is already queued to be processed by an Event-driven policy. If it is, then the policy will be invoked to process that queued device.
Configuration Sync Results Tracking JMS Queue	The JMS Queue that is used for posting tracking records when **External Tracking of Configuration Sync Results** is enabled.
External Tracking of Configuration Sync Results	If enabled, tracking records of Configuration Sync RPCs are generated and posted to the **Configuration Sync Results Tracking JMS Queue**.
External Tracking of Get Parameter Action RPCs	If enabled, tracking records of Get Parameter Action RPCs are generated and posted to the **Get Parameter Action RPCs Tracking JMS Queue**.
Get Parameter Action RPCs Tracking JMS Queue	The JMS Queue that is used for posting tracking records when **External Tracking of Get Parameter Action RPCs** is enabled.
Maximum BOOT Events to Queue	A device can send an event while a policy is still processing that device, or it is doing other tasks that are yet to be completed. In either of these cases, the device is considered to be busy and any incoming events from the device are queued. To prevent this queue from growing too large, this preference can be used. This preference allows you to specify the maximum number of

Preference	Description
	BOOT events that can be queued for a device.
Maximum BOOTSTRAP Events to Queue	Specifies the maximum number of BOOTSTRAP events that can be queued for a device.
Maximum CONNECTION REQUEST Events to Queue	Specifies the maximum number of CONNECTION REQUEST events that can be queued for a device.
Maximum DIAGNOSTICS COMPLETE Events to Queue	Specifies the maximum number of DIAGNOSTICS COMPLETE events that can be queued for a device.
Maximum KICKED Events to Queue	Specifies the maximum number of KICKED events that can be queued for a device.
Maximum PERIODIC Events to Queue	Specifies the maximum number of PERIODIC events that can be queued for a device.
Maximum SCHEDULED Events to Queue	Specifies the maximum number of SCHEDULED events that can be queued for a device.
Maximum TRANSFER COMPLETE Events to Queue	Specifies the maximum number of TRANSFER COMPLETE events that can be queued for a device.
Maximum VALUE CHANGE Events to Queue	Specifies the maximum number of VALUE CHANGE events that can be queued for a device.
Policy to check for Next Queued Device	If enabled, the policy will check for a queued device and process it immediately, rather than waiting for the timer job to check for the next device to process. Enabling this preference can improve policy throughput.
Promote Periodic Informs from Unknown Devices to Bootstrap	Devices only get properly registered with the system when they send a BOOT or a BOOTSTRAP Inform. If a device is accidentally deleted from Service Gateway, the only way to get it back into the system automatically is if it sends one of those two events. Selecting this preference forces Service Gateway to treat an incoming PERIODIC Inform as if it were a BOOTSTRAP Inform if the device does not exist in the database.
Upload Diagnostic Test File Lengths (bytes)	A comma-delimited list that specifies the sizes (in bytes) that can be used when specifying a test file to use for upload diagnostics.

Record Purging page

The Record Purging page allows you to configure several system-wide record purging preferences for Service Gateway. The following table lists the preferences available within this page.

Preference	Description
Age Devices	When this option is selected, Service Gateway will automatically delete any devices that have not been in communication with the system beyond the time specified by

Preference	Description
	the **Inactive Device Expiration Age** preference.
Partition Purging DDL Error Retry Count	Specifies the number of times a partition option will be retried if an error occurred while performing the DDL. The value has a range of 0 to 1000, inclusive of both.
Partition Purging DDL Error Retry Wait (ms)	Specifies the amount of time (in milliseconds) to wait before retrying a failed DDL operation. The value has a range of 10 ms to 10000 ms, inclusive.
ACS Statistics Expiration Age (seconds)	Specifies the amount of time that must elapse before ACS statistics are purged from the database.
Audit Log Expiration Age (seconds)	Specifies the amount of time that must elapse before audit logs are purged from the database.
CWMP Discarded Events Expiration Age (seconds)	Specifies the amount of time that must elapse before events that are discarded by the either the event prioritization or the session throttling features are purged from the database.
Inactive Device Expiration Age (seconds)	Specifies the amount of time that must elapse since the last time a device has been in communication with the system before it is purged from the database. Inactive devices are only purged if the **Age Devices** preference is selected.
Job Status History Expiration Age (seconds)	Specifies the amount of time that must elapse before the job status history is purged from the database.
Policy History Expiration Age (seconds)	Specifies the amount of time that must elapse before the policy history is purged from the database.
Report Log Expiration Age (seconds)	Specifies the amount of time that must elapse before report logs are purged from the database.
Saved Report Expiration Age (seconds)	Specifies the amount of time that must elapse before saved reports are purged from the database. Only saved reports that show **Yes** in the **Expires?** column will be purged.
Server Statistics Expiration Age (seconds)	Specifies the amount of time that must elapse before server runtime statistics are purged from the database.
Maximum Temporary File Age (seconds)	Specifies the amount of time that must elapse before temporary files used by Service Gateway are purged.
Firmware Upgrade Log Expiration Age (seconds)	If **Purge Firmware Upgrade Log** is enabled, only records older than this value will be purged.
Maximum Records to Expire at a Time	Specifies the maximum number of records that can be purged from the database at a time. This is used on a per record type basis. So, if this value is set to 1000 and both policy history records and server statistics are being purged, a maximum of 1000 policy history records and a maximum or 1000 server statistic records will be purged.

Preference	Description
	Note: This preference only applies to records that are purged using a delete query. It does not apply to partition-based purging.
Device Unlocking Age (seconds)	When the **Unlock Devices** preference is selected, this value specifies the amount of time that must elapse before the device's configuration is automatically unlocked by the system.
Purge Firmware Upgrade Log	Determines whether or not firmware upgrade records will be purged.
Partition Purging Maintenance Window Start Time (hh:mm)	This preference, along with the following preference, can be used to define a maintenance window during which partition-based purging can occur. It specifies the local time when this maintenance window starts.
Partition Purging Maintenance Window Duration (minutes)	Specifies the length of the maintenance window, in minutes. Partition-based purging will only occur within the window defined by this and the preceding preference.

Default Password Policy page

The Default Password Policy page allows you to configure system-wide password preferences for Service Gateway. The following table lists the preferences available within this page.

Preference	Description
Force Password Change on Next Login	Selecting this check box prompts a user to change the password at the time of the next log in. Once the password is changed, this check box is cleared automatically.
Number of Passwords to Remember	When set to a value greater than zero, prohibits users from creating a new password that is the same as a recently used password. To specify the number of passwords that must be remembered, provide a value greater than 0. Regardless of this setting, a user is never allowed to create a new password that is the same as their current password.
Maximum Password Age (days)	Specifies the maximum number of days that a password is allowed to remain unchanged. After the specified number of days is reached, the user is required to change the password when logging in. A value of 0 disables this feature.
Minimum Password Age (minutes)	Specifies the length of time (in minutes) that must pass before the user can change their password. This option is used to make it difficult for a user to reuse a password by defeating the Passwords to Remember option. If a user attempts to change a password twice within the specified time, they will be denied. Administrators are not subject to the minimum password age restriction.
Expiry Warning Period (days)	Specifies the number of days before the password expires that a warning message is displayed. When the user logs in within the specified period, a pop-up message appears notifying them of the time left before the expiration of their password. A value of 0 disables this feature.

Password Strength page

The Password Strength page allows you to configure password strength settings for Service Gateway. The following table lists the preferences available within this page.

Preference	Description
Maximum Password Length	Specifies the maximum number of characters that the password may contain.
Minimum Digit Count in Password	Specifies the minimum number of digits that the password must contain.
Minimum Lowercase Character	Specifies the minimum number of lowercase characters that the

Preference	Description
Count in Password	password must contain.
Minimum Password Length	Specifies the minimum number of characters that the password must contain.
Minimum Punctuation Count in Password	Specifies the minimum number of punctuation characters that the password must contain. Valid punctuation for a password are: • Commas (,) • Exclamation points (!) • Semi-colons (;) • Colons (:) • Hyphens (-) • Periods (.) • Backslashes (\)
Minimum Uppercase Character Count in Password	Specifies the minimum number of uppercase characters that the password must contain.

Managing Real-time Probes

A Real-time Probe is used by the CSR features to interact with a device in real-time to retrieve or set information. A Real-time Probe definition includes a list of parameters.

To access the **Real-time Probes** management screen, go to **Administration > Settings > Real-time Probes**. The list of Real-time Probe Parameter Groups is displayed in the top pane of the screen.

This list can be filtered by Name, Description, Probe Type, and Realm.

Adding a Real-time Probe Parameter Group

1. Click **New** on the **Real-time Probe Parameter Groups** management screen. The **Viewing New Parameter Group** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:
   a. Select a **Realm** from the drop-down list.
   b. Enter the name of the probe in the **Name** field.
   c. Specify the following options (for details, see the General tab):
      - **Capability Match**
      - **Probe Type**
      - **View Type**
3. On the **Parameters** tab, assign at least one parameter to the probe as follows:
   a. Click the **Choose Data Model** drop-down list and select a data model. Its parameters are displayed in a tree structure in the **Data Models** pane.
   b. Expand the tree nodes, select the desired parameters, and drag them into the **Current Parameters** table.
4. Click **Save**.

Deleting a Real-time Probe Parameter Group

1. Click Real-time Probe Parameter Group in the **Real-time Probe Parameter Groups** list pane. Its details are displayed in the **Viewing Real-time Probe Parameter Group** pane at the bottom of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying a Real-time Probe Parameter Group

To view the details for a Real-time Probe Parameter Group, select it from the **Real-time Probe Parameter Groups** list pane. Its details are displayed in the following tabs of the **Viewing Real-time Probe Parameter Group** pane at the bottom of the screen:

- General
- Parameters
- Capabilities
- Groups
- Conditions

General tab

The General tab contains the following fields:

- **Realm**. The realm to which a real-time probe is to be associated. The devices in the selected realm will have access to this real-time probe.
- **Name**. The name of the probe, as it appears to the CSR user.
- **Description**. The description of the real-time probe.
- **Capability Match**. Determines how the list of capabilities on the Capabilities tab is used. It has the following options:
  - **Match Any**. Specifies that the probe is available to a device that has any of the defined capabilities.
  - **Match All**. Specifies that the probe is available to a device that has all of the defined capabilities.
- **Probe Type**. Determines whether or not the CSR is given the option to update values that are retrieved. It has the following options:
  - **Read Only**. These parameter values are retrieved for display only and cannot be updated.
  - **Read/Write**. Any parameter values that are deemed writable, according to the data model definition, can be updated.
- **View Type**. Determines the presentation layout of the retrieved parameters. It has the following options:
  - **Record**. This layout is recommended for displaying non-indexed parameters. Groups of indexed parameters can be navigated by selecting the desired indexes from a drop-down list.
  - **Table**. This layout is recommended for displaying indexed parameters. Each group of parameters that share the same rightmost index value will be presented in a tabular format, allowing all "records" to be viewed at once.

- **Walk Parameter Tree**. Determines how parameter values of indexes are retrieved from the device.
  - When this check box is selected, multiple calls are made to the device, iterating through each branch of the parameter tree. This results in more round-trips to the device, but may reduce the overall bandwidth and device CPU requirements.
  - When the check box is cleared, an entire section of the device's parameter tree is retrieved in a single operation.

Parameters tab

The Parameters tab allows you to assign parameters to the probe.

! **Important:** When selecting multiple parameters for a probe, they must all have the same base object. If any index placeholders (denoted by {i}) are present, they must all share the same hierarchy up to the rightmost index placeholder.

To assign parameters to a probe:

1. On the **Data Models** pane, click the **Choose Data Model** drop-down list. The list of available parameters for the specific data model are displayed in a tree structure.
2. Expand the tree nodes, select the desired parameters, and drag them into the **Current Parameters** table.
3. Click **Save**.

The **Current Parameters** table contains all parameters that are assigned to the probe. Each entry in the **Current Parameters** table has a configurable name that appears on the CSR screen.

Parameters can be reordered within the **Current Parameters** table by using a drag-and-drop operation.

For Read/Write probes, two additional columns are present in the **Current Parameters** table: **Validation Type** and **Validation Value**. If you select a **Validation Type** other than **None**, any updated values must match the criteria specified in the **Validation Value** column before they are sent to the device.

To unassign a parameter from a probe, select it from the **Current Parameters** table and click **Delete**.

Capabilities tab

The Capabilities tab allows capabilities to be assigned to the probe. It allows you to define which capabilities a device must have to be eligible for this probe.

To assign capabilities

1. Browse and select the desired capability from the **Capabilities** pane. The list of capabilities can be filtered by Name.

2. Drag it into the **Current Capabilities** table in the bottom right pane.

The **Current Capabilities** table contains all the capabilities that are assigned to the probe. To remove a capability from this table, select it and click **Delete**.

Groups tab

Associating groups with a Real-time Probe restricts the visibility of the probe to users that are associated with at least one of the associated groups. If a real-time probe is not associated with any groups, all users will be able to use it.

To associate a group with a Real-time Probe, select it from the **Groups** table and drag it to the **Current Groups** table. The list of groups can be filtered by Name, Description, and Realm.

To disassociate a group with a Real-time Probe, select it from the **Current Groups** table and click **Delete**.

Conditions tab

Conditions are used to control which devices the real-time probe is applicable to. The real-time probe will only appear as an option for a device if the device matches the given conditions. A real-time probe that does not have any conditions defined will apply to all devices.

For details on defining a set of conditions that match a device, see Condition Editor.

⚠ **Caution:** Since capabilities can also be specified in conditions, ensure that conditions that contradict any capabilities specified in the Capabilities tab are not defined. If there is a contradiction, then the real-time probe will never match any device, and can never be selected as an option in the Real-time Probe CSR module. For example, if this tab specifies that the device must have the CWMP capability, while the conditions specify that the device must NOT have the CWMP capability, then the real-time probe will not be available for any device.

Managing record purging

The Record Purging screen provides insight into the record purging mechanism. It also allows you to configure some aspects of its operation.

Service Gateway makes use of two methods to purge records from the database: delete queries and date range partitioning, which takes advantage of the table partitioning feature of Oracle Enterprise Edition. Date range partitioning can be enabled on many of the tables that experience rapid growth, and for which the current method of record purging proves computationally expensive and difficult to tune. Dropping a partition is significantly faster and cheaper than executing a delete statement, allowing historical data to be kept for much longer periods of time if desired.

Service Gateway creates a partition to be used for each calendar day, based on UTC time. Partitions are created several days in advance, and dropped once they reach a configurable age in days. The time of day this activity occurs can be confined to a configurable window of time within the day. If, for any reason, a partition does not exist for the current day when a record is added, the record is placed into a default partition and is automatically moved to the proper partition when the partition is created.

To access the record purging screen, go to **Administration > Settings > Record Purging**. A list of entries with each entry representing a database table that may be included in partition-based purging or delete query purging is displayed in the **Record Purging Entries** list pane. The list of Record Purging Entries can be filtered by Table Name.

By default, partition-based purging is not enabled. The database administrator is responsible for partitioning the tables and enabling each to participate in partition-based purging.

Record Purging settings can only be viewed by a user with the *View Global Preferences* permission, and can only be changed by a user with the *Manage/View Global Preferences* permission.

Note: Record purging tables cannot be added or removed using the UI.

Viewing and modifying a record purging table

To view or modify a record purging table, select it from the **Record Purging Entries** list pane at the top of the **Record Purging** management screen. Its details appear in the following tabs of the Viewing Record Purging details pane at the bottom of the screen.

- General
- Partitions

General tab

The General tab contains the following fields:

- **Table Name**. The name of the database table.
- **Parent Table**. The name of the parent table if this table has a relationship with another table.
- **Purge Type**. The type of purging that is active for this table. It has the following options:
    - **Date Range Partitioning**. When a table with this Purge Type is enabled, the table is partitioned and purging is carried out by dropping the oldest partition(s).
    - **Delete Query**. When a table with this Purge Type is enabled, the table is not partitioned and purging is carried out by using a delete query. This Purge Type is used for tables that do not typically store historical data or store a relatively small number or records.
- **Record Expiry (days)**. The number of days to keep records in this table. This field is only editable for tables with a purge type of **Date Range Partitioning**.
- **Tablespace Name**. The name of the Oracle tablespace to be used when creating a new partition. This input box can be used in three ways:
    - Left blank – The new partitions are created using the Oracle schema's default tablespace.
    - Standard text – The new partitions are created in the tablespace specified by this text.
    - Velocity script – The new partitions are created in the tablespace specified by the evaluated velocity script. This allows for partitions to be created in different tablespaces (for example, per day of week, per week of month, or round-robin).

      Service Gateway does not create the tablespaces that are defined in the script, they already need to exist. The velocity script is used to determine which tablespace is to be used by the partition.

      In this case,while the Velocity Script editor can be used to define the script, none of the options in Insert <*script element*> are applicable.
- **Status**. Indicates whether the purging rule for this table is enabled.

Partitions tab

The Partitions tab displays the list of partitions that currently exist for a table, the tablespace that each occupies, and the number of rows that exist in each partition.

Caution: The **Rows** column is based on information from the database metadata, which is typically only updated periodically (perhaps daily) and is not a live record count.

Managing system keys

System keys are extensible fields that can be used for storing additional information about devices and for performing inventory searches in the system. While many of the system keys are built-in, the system keys can also include custom keys that are defined for each instance of the application.

Tip: For information on creating custom system keys during the installation process, refer to the ***Service Gateway Installation Guide***.

Custom system keys can be used in conditions through the application to refine the use of policies, actions, and templates based on the value of a system key. Wildcard characters (*) may be used when specifying the required value.

Custom system keys can be populated by manually providing values, by parameter mappings, or through customized integration with other systems. These systems can include Web services integration with other systems such as CRM systems or through the use of customized device registration modules.

System Keys can only be managed by users that have the *Manage/View System Keys* permission.

To access the list of defined system keys, go to **Administration > Settings > System Keys**. A list of system keys is displayed in the **System Keys** list pane at the top of the **System Keys** management screen. This list can be filtered by Name.

Note: System keys cannot be added or removed using the UI.

Viewing and modifying system keys

To view or modify a system key, select it from the **System Keys** list pane. Its details appear in the following tabs of the **Viewing System Key** pane at the bottom of the screen:

General

Transformation Script

General tab

The General tab contains the following fields:

- **Display Name**. The name that is used as the field name for this system key on forms, when a Localization Key is not available. This field is read-only.
- **Table Name**. The name of the database table that this system key extends. This field is read-only.
- **Field Name**. The name of the database field used to store the values of this system key. This field is read-only.

- **Localization Key**. The name of a UI localization key that is used to display the name of the field in different languages. This field is read-only for system-defined system keys.
- **Format**. An optional regular expression that is used to restrict the values of a system key during a record update. This field is read-only for system-defined system keys.
- **Enabled?**. If this check box is selected, the system key will be available for use within the application. This field is read-only and is always selected for system-defined system keys.
- **Display in Search Results?**. If this check box is selected, the field will be displayed in search results when searching for a device. This field is read-only and is always selected for the *Unique ID String* system key.
- **Searchable?**. If this check box is selected, the field will be available as a search option for device searches. This field is read-only and is always selected for the *Unique ID String* system key.
- **System Defined?**. A read-only check box. If selected, the system key is system-defined.
- **Unique?**. A read-only check box. If selected, the system key has been specified as unique during creation.
- **Clear Duplicates?**. This is a read-only check box that is specified when the system key is initially created and used when the **Unique?** check box is selected. If selected, when the system key is updated by an automatic process (such as parameter mapping), any other devices with the same value for the system key will have their value set to NULL. Attempts to set a duplicate value using the UI will still result in an error indicating that one of the system keys is not unique.
- **Editable?**. If this check box is selected, the value of this system key for a device may be modified using the device edit screen. This field is read-only and is always selected for system-defined system keys.

Transformation Script tab

The Transformation Script tab allows you to provide an optional script to transform a system key value before displaying it in the UI, and then transform that display value back to the database format when saving it.

This tab has the following fields:

- **Example Storage Value**. A storage value that must be provided before you save the script. It serves the following purposes:
  - Helps to check for syntax errors.

    If any syntax errors are present in the script, they will be reported at this time, and you will not be able to save the script until all errors in the script have been resolved.

  - Validates that the two functions do the inverse of each other, as follows:

    The underlying code calls transformForDisplay() on the **Example Storage Value** and then passes the result to the transformForStorage() function. If that function returns the same value as the **Example Storage Value**, then the two functions are doing the inverse of each other.

- **Script**. A JavaScript function that can be used to transform a system key value before displaying it in the UI, and then transform that display value back to the database format when saving it.

Transformation script for system keys

The transformation script for system keys is a JavaScript function that can be used to transform a system key value before displaying it in the UI and then transform that display value back to the database format when saving it.

To define a JavaScript function, either click in the **Script** text box (which is read-only), or on the icon located at the upper right of the **Script** text box. This **Script Editor** opens.

When editing the transformation script for a system key, you must provide the following two functions:

- transformForStorage() - this function is used to take the value that is displayed in the UI and transform it before it gets stored in the database.
- transformForDisplay() - this function is used to take the database value, and transform it before it is displayed in the UI.

// Auto-generated script content

```
function transformForStorage(value) {

   return value;

}

function transformForDisplay(value) {

    return value;

}
```

Following is an example of how the transformation script can be used with MAC Addresses:

Assume that Service Gateway has stored MAC addresses in the database in lowercase with all delimiters removed, such as “aabbccddeeff”. Now, with the built-in MAC address field on the device, that gets displayed as “aa:bb:cc:dd:ee:ff” in the UI. If a customer using a custom system key to store MAC addresses wants to have the same behavior for the storage as the display that exists for the built-in MAC address field, it can be done using the transformation script.

Example Scripts

The following script can be used to return an error instead of a value:

// Auto-generated script content

```
function transformForStorage(value) {
   if (value.length != 12) {
    error.setErrorString("Invalid MAC Address");
     return;
   }
   return value;
}
```

In the preceding case, an error is returned if the input value is not exactly 12 characters in length. The error message is displayed in an error dialog box when trying to save the device changes. The changes are not saved when this error occurs.

Testing the transformation script

You can test your transformation script, to make sure it is returning the required value, by entering a sample value in the **Test Value** field and clicking **Evaluate**.

The Script Editor has two radio buttons that allow you to specify the function that is to be tested as follows:

- **For Storage**. Select this option to test the transformForStorage() function.
- **For Display**. Select this option to test the transformForDisplay() function.

The transformed value is displayed on the bottom pane. If you set the error string, a pop-up dialog box opens with the returned error message.

After evaluating the script, you can click **Ok** to accept the script or **Cancel** to discard the changes.

5

Configuring Inventory Features

Configure inventory features

The Inventory menu allows you manage the following features of Service Gateway:

- Devices
- Device Files
- Firmware
- Hardware
- Subscribers

Inventory features are available from the **Inventory** menu in the Service Gateway User Interface.

Managing devices

Each device within the Service Gateway system is represented by a device record. The individual devices are assigned to a specific realm and a specific domain within that realm. The domain and realm parameters are used to help determine which system users can see the device and which services and configuration templates can be applied to the device.

Devices within the system can be registered either manually or automatically. Manual registration is done by using the inventory API or by adding a device via the UI. Automatic registration occurs, for example, when a device sends an Inform message to the ACS. The ACS checks to see if a device matching the derived unique ID exists within the system. If it does not, it is automatically entered.

When registering a device automatically, the system fills in as many details as it can, based on the information available at the time. Such information includes realm and domain associations, the unique ID, IP address, MAC address, serial number, hardware association, and firmware association. CWMP, for example, provides mechanisms for retrieving almost all of this information.

To access the **Device** management screen, select **Inventory > Devices**. The **Device Search Results** list is displayed on the top pane. However, no devices will be listed when you first go to the **Device** screen. You must enter some search criteria in the **Search** tab before you can retrieve a list of devices.

Performing a search operation

By default, the **Search** tab is displayed on the top left when you open the **Device** screen. If the **Search** tab is not displayed, you can access it by clicking on the magnifying glass on the **Device Search Results** pane.

Note: The magnifying glass icon on the **Device Search Results** pane does not work in the same way as it does in most other places in Service Gateway. In this instance, it is used to provide search criteria to determine which records are retrieved from the database and displayed in the user interface.

The **Search By** drop-down list allows you to search by IP address, MAC address, unique ID string, and, if the device is attached to a subscriber, account number, last name, and phone number. Any System Keys defined and specified as Searchable will also be available in this drop-down list. The default option is specified by the **Default Device Search Type** system preference.

After selecting an option from the drop-down menu, you can enter a search **Keyword**. The format of the search string depends on the search mode.

- For IP address, the string must be a full or partial IPv4 or IPv6 address. A partial address is a text string with a trailing wildcard, such as 192.168.*
- For unique ID or any subscriber information, it is a basic text string with or without wildcards.

You can further limit results using one or more of the following filters:

- **Realm**. Only realms for which you are a member are available.
- **Domain**. If a realm is chosen, you can narrow the results to those devices in a specific domain. If the **Include Children** check box is selected, then devices in child domains of the selected domain are also shown.
- **Device Status**. You can limit the search results based on the device status: Online, Offline, or Locked.
    - A device is deemed to be online if its last successful communication time is more recent than the last unsuccessful communication time.
    - A device is deemed to be offline if its last unsuccessful communication time is more recent than the last successful communication time.
    - A device is locked if the **Lock Configuration** check box has been selected. See General tab for details on the **Lock Configuration** check box.
- **Hardware**. You can limit results to only those devices with a specific hardware.
- **Firmware**. You can limit results to only those devices with a specific firmware.

Once you have specified your search criteria, click **Submit**. A list of devices matching the search criteria is displayed in the **Device Search Results** pane. You can select a device from this list and then perform actions on it.

If too many devices meet the search criteria, a pop-up message will request that you narrow the search criteria. The maximum number of search results that can be displayed is specified by an administrator, using the **Maximum Search Results Allowed** system preference.

By default, search results will be retained until you perform a new search, even if you navigate to other screens and return. This behavior can be disabled by an administrator by clearing the **Sticky Search Results** system preference.

Adding device records

To add a device record to the system:

1. Click **New** on the Device management screen. The **Viewing New Device** pane opens on the bottom of the screen.
2. On the **General** tab, select a **Realm** and **Domain** and enter the **Unique ID**. All other fields are optional.
3. Optionally, perform the following steps:
    a. On the **Services** tab, associate services with a device by selecting and dragging them from the **Services** table to the **Current Services** pane.
    b. On the **SNMP** tab, set the SNMP information.

c. On the **Attributes** tab, associate attributes with a device by selecting and dragging them from the **Attributes** pane to the **Current Attributes** table.

4. Click **Save**.

Deleting device records

To delete a device record from the system:

1. Select one or more device records from the **Device Search Results** list pane.

    - To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

    Note: If a selected device cannot be deleted for any reason, such as when it is in use by a policy, that does not prevent the other devices that are not in use from being deleted.

2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

    Note: A device record cannot be deleted if it is currently being executed upon by a policy.

Viewing and modifying device records

To view the details for a specific device record, select the desired device record from the **Device Search Results** list in the top pane. Its details are displayed in the following tabs of the Viewing Device pane at the bottom of the screen.

Tip: For those users with permission to access the CSR view, clicking on the unique ID in the header of the view/edit form will take you directly to the CSR view for the selected device.

- General
- Services
- SNMP
- Attributes
- Status
- Object Cache
- Database of Record
- Backups
- Manual Overrides

- Events
- Object Browser
- Device/Gateway Association
- Gateway Device List

General tab

The General tab allows the basic details about the device record to be viewed and modified.

The fields on this tab are as follows:

- **Realm**. Required field. Only realms that are visible to the user appear in this drop-down list. The realm may only be altered if the device is not associated with any other records in the database. This allows the realm to be changed if an error was made upon initial data entry. The associations that inhibit a change to realm include (but may not be limited to) services, attributes, hardware, firmware, DBoR entries, and configuration. This drop-down list is disabled if the realm cannot be changed.
- **Domain**. Required field. Clicking on this field opens the Select Domain dialog. Within this dialog, a domain can be found by using the filter functionality or by navigating the hierarchy. When the desired domain is found, click **Ok** to close the dialog and return to the form.
- **Unique ID**. Required field. A unique identifier for a device. For TR-069 compliant devices, this must match the Unique ID String that the device uses to identify itself. The recommended format for the Unique ID String for TR-069 devices is **OUI-ProductClass-SerialNumbe**r. If product class is not available, it is omitted.
- **IP Address**. The reference IP address for the device. This may be an IPv4 or IPv6 formatted address. This is an optional field.
- **MAC Address**. An optional field which can be used for searching and device identification.
- **Serial Number**. An optional field which can be used for searching and device identification.
- **Hardware**. The hardware currently associated with the device. This is an optional field.
- **Firmware**. The firmware currently associated with the device. This is an optional field.
- **Scheduled Activation Date**. An optional field which can be used for generating reports comparing when a device was scheduled to register with the system to when it actually did register. Activation may be scheduled if the devices were being pre-provisioned (perhaps via the web services API), before being delivered to customers and activated.
- **Lock Configuration**. If this check box is enabled, the configuration synchronization action does not engage for the device, regardless of any changes made to service definitions or configuration templates. Configuration changes can still be made manually.

Note: The Configuration Synchronization policy action automatically locks the configuration if it fails to properly update the device.

Any **System Keys** that are defined to be **Editable** are also available on this tab.

⚠ **Caution:** Changing some of these values, such as domain, hardware, and firmware can have large impacts on the services and configuration templates that are available to the device.

Services Tab

The Services tab displays the list of services that may be associated with the device.

All available services are listed in the **Services** table on the left. This list is generated from the list of all services within the same realm as the device. The list can be filtered by Name, Code, and Realm. Services that are associated with a device are listed in the **Current Services** pane on the right.

- To associate a service with a device, select the desired service from the **Services** table and drag it to the **Current Services** pane.
- To remove a permission from a group, select it from the **Current Services** pane and click **Delete**.

Note: Adding and removing services are likely to cause device configuration changes the next time the device triggers a configuration synchronization action.

SNMP tab

If the device supports SNMP, the **SNMP** tab can be used to manage basic SNMP information.

This tab allows you to specify the version of SNMP that a device supports and to define the read-only and read-write community strings.

Attributes tab

The Attributes tab shows details about any custom attributes that can be set for the device. Only attributes that have been defined for the **Device** object will be available (see Using Attributes for more information).

All attributes that have been defined for the **Device** object are displayed in the Attributes pane on the left of the screen. The list of available attributes can be filtered by Name. Currently defined attributes are displayed in the **Current Attributes** table.

You can associate attributes with a device by selecting and dragging them from the **Attributes** pane to the **Current Attributes** table.

Status tab

The Status tab contains information about the status of communication attempts with the device.

- The **First Registered Date** is the date and time that the device first initiated a registration action with the system.
- The **Last Registered Date** is the date and time of the most recent initiated registration action that the device triggered.
- The **Last Successful Communication Date** is the date and time of the most recent communication with the device.
- The **Last Unsuccessful Communicate Date** is the date and time of the most recent attempt that the system made to contact the device (such as via a CWMP connection request), but failed to hear from it.
- **Obsolete Firmware Upgrade Attempts** is a count of failed automatic firmware upgrades. Once this count reaches the maximum value specified by the system preference **Maximum Inventory Firmware Upgrade Attempts**, no more attempts will be made to upgrade the firmware. To resume attempts, the count can be reset to zero (0) by clicking **Reset**.

Note: Reset is immediate and cannot be undone.

Object Cache tab

The Object Cache tab displays information about cached data model parameters. Any data model parameters that are flagged as Cache Values will be cached when that parameter is written via the CSR UI or EAI web services.

It can also be populated by the **Update CWMP Cache on Value Change** policy action.

Database of Record tab

The Database of Record tab shows details about the configuration templates that are currently associated with a device; whether they have been applied or whether they are pending application or removal. The following information is displayed for each configuration template:

- **Template Name**. The name of the configuration template.
- **Service Name**. The name of the service to which the template is to be applied. For manual overrides, this field will be empty.

- **Status**. One of the following:
  - **ACTIVE**. The template has been delivered to the device.
  - **APPLY_PENDING** or **UNDO_PENDING**. The template is scheduled to be applied or removed.
  - **APPLY_IN_PROGRESS** or **UNDO_IN_PROGRESS**. The template is currently being applied or removed.
  - **APPLY_FAILED** or **UNDO_FAILED**. An attempt to apply or remove the template failed, resulting in the configuration of the device being locked.
  - **APPLY_DEFERRED** or **UNDO_DEFERRED**. The template has been processed and is being combined with subsequent templates for delivery as a single batch update.
- **Order**. The relative order in which the templates were applied to the device.
- **Reason**. The reason that the template was applied. It can one of the following:
  - **SERVICE**. The template is indirectly associated with the device via a service.
  - **DEVICE**. The template is directly associated with the device via a manual override.
  - **OTHER**. Some other mechanism associated the template with the device (such as custom logic).
- **Delivery Date**. The date and time when the template was delivered to the device.

Deleting Entries

Database of record entries can be deleted. To delete an entry, click the desired entry and then click **Delete**.

⚠ **Caution:** Unlike other changes to the device information (template associations, attribute definitions, and so on), which can be undone by clicking the main device edit **Cancel** button, deleting an entry from the database of record occurs immediately and is permanent.

Backups tab

The Backups tab lists the stored configuration backups for the device. The information shown about each backup is as follows:

- **Backup Date**. The date and time when the backup was stored.
- **Filename**. The filename of the backup content, as provided by the device.
- **Reason**. The reason specified for the backup.
- **Last Known Good**. Whether or not this is the last known good configuration file for this device.

Note: Only one backup per device may have this check box selected.

To change the last known good configuration for a device, select the check box in the right-most column for the desired backup and save the device record.

To download the content of a backup to the local computer, select a backup and click **Download**.

To delete a backup, select a backup and click **Delete**.

For more detail on how these backups are managed, see the Configuration Backup and Configuration Restore policy actions.

Manual Override tab

The Manual Override tab is used to manage any manual configuration overrides for a device. Manual overrides can be used to modify an existing service configuration or to provide configuration in lieu of any service associations.

Available configuration templates that can be assigned to a device are listed in the **Available** table while currently assigned templates are listed in the **Current** table. To add a configuration template to a device, select and drag it from the **Available** to the **Current** table. To remove a template from a device, select it from the **Current** table and click **Delete**.

Once a template has been placed in the **Current** table, the following three configuration options must be defined:

- **Delivery Rule**. The possibilities are:
  - **Always**. The template will be unconditionally delivered every time the device configuration is synchronized. This is useful if a device does not persist configuration across a reboot.
  - **On Change**. The template will only be redelivered during configuration synchronization if the template has not yet been delivered, or the content of the configuration differs from the previous content that was delivered.
  - **Once**. The template will only be delivered if it does not yet exist in the Database of Record for the device.
- **Override Type**. The possibilities are:
  - **Append**. This template will be delivered after templates associated with services.
  - **Prepend**. This template will be delivered before templates associated with services.
  - **Replace**. This template will be delivered in place of another template if a service associated with the device would have delivered it.
- **Replacement Template**. This option is only required and used for replace overrides. If an override is specified for replacement, this drop-down list is used to select the template to be replaced.

When the configuration synchronization action runs, it starts to determine the configuration for a device in the following order:

1. It obtains all of the **Prepend** overrides, in the order that they are specified in the **Current** table.
2. It processes all of the templates associated with any services associated with the device, again in order of services and templates within the service.
3. It looks for any **Replace** overrides. If any of these overrides match a template (via the replacement template option) that will be applied to a configuration, those template configurations will be replaced with the new configuration.
4. It looks for any **Append** overrides, again in the order that they are specified in the **Current** table and processes those.

Events tab

The Events tab lists the events that have been logged for the device, with the most recent event listed first. Selecting an event will cause the parameters and values for that event to be displayed.

The number of events that are returned and displayed can be limited by using the **Maximum CWMP Device Event Results Allowed** system preference.

Note: Device events are only logged when CWMP event logging has been enabled for the ACS.

Object Browser tab

The Object Browser tab is used to allow a system user to browse through the data models supported by a device in real time.

Click **Start** to activate the object browser. The system will contact the device, grab the first level of objects and parameters, and display them in the **Current Parameter Tree** pane. Click parameter to view its full name and current value on the right of the screen.

Note: If you click an object node, the system will grab the first level of objects and parameters under the selected object.

The object browser allows you to modify parameter values. To modify a parameter value,

1. Click the parameter in the **Current Parameter Tree** pane.
2. Enter a new value in the **Value** field.
3. Click **Save**.

The system will attempt to set the new parameter value on the device.

Device/Gateway Association tab

The Device/Gateway Association tab is only available if the device has the Annex F Device capability. This tab lists the parent device (or gateway) that this device sits behind, as well as status information about the association with that parent device.

Gateway Device List tab

The Gateway Device List tab is only available if the device has the Annex F Gateway capability. This tab lists any child devices that sit behind the gateway and that are listed in the ManageableDevice table in the gateway data model. The list includes the three components that uniquely identify a device: the OUI, the Product Class, and the Serial Number.

Managing device files

Device files are files that can be delivered to a device. Examples of device files include firmware images, ring tones, and configuration files. These files contain static content and are hosted by the file servers on the network.

To access the **Device Files** management screen, select **Inventory > Device Files**. A list of currently defined device files are displayed in the top pane. The list can be filtered by Filename, Description, Realm, and Type. The filter is dynamic and the results display is updated as soon as you start entering in a filename or description or select a realm or file type.

Adding device files

You can add a device file to the system as follows: by manually entering the file information or by uploading an existing file.

- When adding a file manually, the user must ensure that the file is uploaded to each file server that can possibly be selected to deliver that file to a device.
- When uploading an existing file, Service Gateway will try to transfer the file to all file servers that have their **Upload Settings** defined. For any servers that do not have their **Upload Settings** defined, the user is required to transfer the file.

To upload an existing file:

1. Click **New** on the **Device Files** management screen. The **Viewing New File** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:
   a. Select a **Realm** (if the **Default** realm is not appropriate).
   b. Select the **Upload existing file to server** check box.
   c. Browse and select the file to upload and click **Open**. The name of the file is displayed in the **Filename** field.
   d. Enter a description in the **Description** text box.
   e. Select a **File Type** from the drop-down list
3. Click **Save**.

Tip: You do not have to enter the file size when uploading the file content. It is calculated automatically.

To add a file manually:

1. Click **New** on the **Device Files** management screen. The **Viewing New File** pane opens on the bottom of the screen.
2. On the **General** tab, do the following:
    a. Select a **Realm** (if the **Default** realm is not appropriate).
    b. Enter a name for the file in the **Filename** field.
    c. Enter a description in the **Description** text box.
    d. Enter the file size (in bytes) in the **Size** field.
    e. Select a **File Type** from the drop-down list.
3. Click **Save**.

Deleting device files

To delete a device file from the system:

1. Select the desired device file from the **Device Files** list.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

A device file can only be deleted from the system if the file has no active associations. For instance, if a firmware file is currently associated with a hardware and/or firmware record, the file cannot be deleted until the association is removed. If the device file cannot be deleted because of existing associations, click **Details** button to view a report that lists the associations.

Viewing device files

To view the details for an existing device file, select it from the **Device Files** list in the top pane. Its details are displayed in the following tabs of the **Viewing Device File** pane at the bottom of the screen:

- General
- Upload Status

General tab

The General tab allows you to view and modify the basic details about a device file. All the fields on this tab can be modified when adding a new device file. However, when modifying an existing device file, only the description can be altered.

The fields on this tab are as follows:

- **Realm**. The realm within which this device file is available to be used.
- **Upload existing file to server**. If this check box is selected, then a file from the local computer can be selected to be uploaded to all available file servers over SSH. Otherwise, it is assumed that the file is to be placed on the files servers using some other mechanism.
- **Filename**. The name of the file.
- **Description**. A description for the file. This is an optional field.
- **Size**. The size, in bytes, of the file. This value only needs to be specified for a new file if **Upload existing file to file server** is not selected.
- **File Type**. The type of file. This selection affects the features in Service Gateway that this file will be available for use within.

Upload Status tab

For files that have been uploaded using the UI, the Upload Status tab is enabled and displays the status of the files that are uploaded to each file server defined in the same realm as the device file.

For each file server, the **Uploaded** column displays **Yes** if the file has been transferred to the file server, and **No** if it has not.

Managing firmware

Firmware records represent a specific version of firmware that is running (or can be run) on a device in a specific realm. They are typically associated with hardware records, since a specific firmware will usually only run on a specific hardware.

Firmware records are comprised of a manufacturer, a version, and a realm. This means that there can be multiple entries for the same manufacturer/version if the realms are different.

Firmware records can be created manually or registered automatically by the system. Firmware records are registered automatically when the system identifies a firmware record from a device that has not yet been recorded in the database. When this happens, it will be assigned to the realm to which the device belongs. Firmware records discovered automatically will also be automatically associated with an appropriate hardware record (either an existing one or a newly-discovered one).

Firmware records may also have firmware image file associations. This association can be done directly or as part of a hardware association, but not both. The associations are made with firmware files that are managed via the Device Files module. Files would normally be associated with a firmware version directly, but there may be some devices that, while running the same firmware version, require different firmware image files because of different hardware architecture.

When creating a firmware/hardware association, you can also specify a firmware status. For details on the possible status values, see Status.

To access the **Firmware** management screen, select **Inventory > Firmware**. A list of currently defined firmware records are displayed in the top pane. The list can be filtered by Manufacturer, Version, and Realm.

Adding firmware records

To manually add a firmware record to the system:

1. Click **New** on the **Firmware** management screen. The **Viewing New Firmware** pane opens on the bottom of the screen.
2. On the **Genera**l tab, do the following:

    a. Select a **Realm** from the drop-down list.

    b. Enter the manufacturer's name and the version number of the firmware in the **Manufacturer** and **Version** fields respectively.

    Note: The name and version number must be the same as reported by the firmware image.

    c. Optionally, select a firmware file and the protocol from the **File** and **Device Protocol** drop-down lists respectively.

3. On the **Hardware Filters** tab, optionally enter the product class of the hardware that the firmware is permitted to be associated with in the **Product Class** field and click **Add**. The new Product Class filters are displayed in the **Current Product Class Filters** pane. To delete a filter, select it and click **Delete**.
4. On the **Hardware** tab, select and drag the desired hardware from the **Available** table to the **Current** table. If required, make changes in the following columns:
    - **File**
    - **Status**
    - **Upgrade Path**

    To delete a hardware from the **Current** table, select it and click **Delete**.
5. On the **Attribute** tab, associate attributes with the firmware as follows:
    a. Select and drag the desired attributes from the **Attributes** pane to the **Current Attributes** table.
    b. Click **Value** column and enter a value as appropriate.

    To delete an attribute from the **Current Attributes** table, select it and click **Delete**.
6. Click **Save**.

Deleting firmware records

To delete firmware records from the system:

1. Select one or more firmware records from the **Firmware** list in the top pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

    When deleting more than one firmware, any firmware that has currently active associations, except associations with a device, is not deleted. All selected firmware that have no active associations will be deleted.

! **Important:** If you delete a firmware record that is associated with any device records in the system, the firmware record association for those devices is set to None (that is, the associations are deleted).

Viewing and modifying firmware records

To view the details for a specific firmware record, select the desired firmware record from the **Firmware** list in the top pane. Its details are displayed in the following tabs of the **Viewing Firmware** pane at the bottom of the screen:

- General
- Hardware Filters
- Hardware
- Attributes

General tab

The General tab allows you to view and modify basic information about the firmware. It has the following fields:

- **Realm**. Required field. Only realms that are visible to the user appear in this drop-down list. The realm of an existing firmware cannot be modified.
- **Manufacturer**. Required field. The manufacturer's name as reported by the firmware image.
- **Version**. Required field. The version number as reported by the firmware image.
- **File**. This is the firmware image, defined in Device Files. A file may only be specified if no files are specified for the specific hardware associations on the **Hardware** tab. The files in this drop-down list are limited to the files in the realm specified for this firmware.
- **Device Protocol**. This field specifies the protocol that should be used to construct the URL to the device's console UI, which is used by the link on the CSR Device Summary module. It has the following options:
  - **Inherit Global**. Specifies the use of the value specified by the **Device URL Protocol** system preference.
  - **http**. Specifies that the HTTP protocol will be used when constructing the URL to the console UI of the device.
  - **https**. Specifies that the HTTPS protocol will be used when constructing the URL to the console UI of the device.
  - **Disabled**. Disables the link for any devices using this firmware.

Hardware Filters tab

Hardware filters can be used to restrict the list of hardware visible in the Hardware tab, to reduce association errors and make it easy to find the intended record. By specifying a list of product classes, only hardware of one of the specified product classes will be available to be associated with the firmware.

Caution: The product class string needs to match the product class of the hardware exactly, including spacing and case.

Hardware tab

The Hardware tab shows details about any hardware associations for the firmware record. The **Available** table shows a list of potential hardware records to which the firmware can be associated. The **Current** table shows all of the current firmware/hardware associations.

To add a new association, select and drag a hardware entry from the **Available** table to the **Current** table. To remove an association from the **Current** table, select it and click **Delete**.

Tip: The same hardware-firmware associations that can be set from this tab can also be viewed and managed from the point of view of a specific hardware. See Firmware tab.

File

If a device file association has not been made (on the General tab), you can specify a firmware file to use by clicking on the **File** drop-down list and selecting an appropriate option. The drop-down list contains any files that are in the same realm as the firmware, and are of type Firmware (see General tab).

Note: If a file association has been made on the General tab, the **File** drop-down option will be grayed out on the Hardware tab.

Status

The status of the association determines how many features of Service Gateway use the firmware when presented with a device of the given hardware. This status is used to determine if the firmware on the device needs to be upgraded. The possible status values are:

- **Deprecated**. Indicates that it is acceptable for the firmware to exist on this hardware, and it does not strictly require an upgrade. However, this firmware should not be applied to any further devices.
- **Obsolete**. Indicates that this firmware should not be used for this hardware and that an upgrade is required. If a device is seen on the network with this hardware and firmware, the system will attempt to upgrade it if a valid upgrade path is available.

- **Recommended**. May only be applied to one of the associations for any given hardware/firmware combination. It indicates the ideal firmware that should be applied to the hardware. During a manual upgrade, where a CSR is presented with a drop-down of firmware images to choose from, the recommended firmware will be the default option if an upgrade path is not specified.

Note: There can only be a single recommended firmware for a given hardware.

- **Unqualified**. This is the default value when a new association is discovered on the network. It operates similarly to **Deprecated**, in that it does not force an upgrade but should not be propagated to other devices either. If differs in that it visually indicates that the status needs to be reviewed and explicitly set.
- **Valid**. Indicates that this is one of a set of valid firmware versions for this hardware, and that it may be propagated to devices. These will appear as options to the CSR.

Upgrade Path

The **Upgrade Path** indicates the new firmware that should be used during an upgrade for a device of the given hardware that is currently using this firmware version. Selecting "(Use Recommended)" will cause the recommended firmware that is associated with the hardware to be used. Otherwise, it may be a specific firmware if the hardware requires multiple or stepwise upgrade paths.

Note: The contents of the **Upgrade Path** drop-down list are affected by the Hardware Filters configured for the firmware. They are limited to those with the same product class associations as the hardware. Additionally, a system preference called **Exclude Unrestricted Firmware In Upgrade Path Options** controls whether or not firmware without product class associations are included in the drop-down list.

Attributes tab

The Attributes tab shows details about any system attributes that are associated with the firmware record. Only attributes that have been defined for the **Firmware** object will be available (see Using Attributes for more information).

Available attributes are displayed in the **Attributes** pane on the lower left of the screen while currently defined attributes are displayed in the **Current Attributes** table on the lower right of the screen.

To add an attribute, select and drag it from the **Attributes** pane to the **Current Attributes** table. The list of available attributes can be filtered by Name.

To remove an association from the **Current Attributes** table, select it and click **Delete**.

Managing hardware

Hardware records represent a specific hardware platform that a device is built on. They are typically associated with firmware records, since a specific firmware will usually only run on a specific hardware.

Hardware records are comprised of a manufacturer, revision, OUI, device type, product class, and a realm.

Hardware records can be created manually or registered automatically by the system. Hardware records are registered automatically when the system identfies a hardware record from a device that has not yet been recorded in the database. When this happens, it will be assigned to the realm to which the device belongs. Hardware records discovered automatically will also be automatically associated with an appropriate firmware record (either an existing one or a newly-discovered one).

To access the **Hardware** management screen, select **Inventory > Hardware**. A list of currently defined hardware records are displayed in the top pane. The list can be filtered by Manufacturer, Revision, and Realm.

Adding hardware records

To manually add a hardware record to the system:

1. Click **New** on the **Hardware** management screen. The **Viewing New Hardware** pane opens on the bottom of the screen.
2. On the **General** tab, select the **Realm** and enter the appropriate details in the text fields. **Manufacturer** and **Revision** are required fields, while the rest are optional fields.
3. On the **Firmware** tab, associate a firmware with the hardware record by selecting and dragging it from the **Available** table to the **Current** table. You can specify a firmware file association for each hardware record. If required, make changes in the following columns:

   - **File**
   - **Status**
   - **Upgrade Path**

   To remove an association from the **Current** table, select it and click **Delete**.

4. On the **Attributes** tab, associate attributes with the hardware record as follows:

   a. Select and drag the desired attributes from the **Attributes** pane to the **Current Attributes** table.

   b. Click **Value** column and enter a value as appropriate.

   To delete an attribute from the **Current Attributes** table, select it and click **Delete**.

5. Click **Save**.

Deleting hardware records

To delete a hardware record from the system:

1. Select one or more hardware records from the **Hardware** list in the top pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

   When deleting more than one hardware, any hardware that has currently active associations, except associations with a device, is not deleted. All selected hardware that have no active associations will be deleted.

! **Important:** If you delete a hardware record that is associated with any device records in the system, the hardware record associations for those devices are set to None (that is, the associations are deleted).

Viewing and modifying hardware records

To view the details for a specific hardware record, simply select the desired hardware record from the **Hardware** list in the top pane. Its details are displayed in the following tabs of the **Viewing Hardware** pane at the bottom of the screen:

- General
- Firmware
- Attributes

General tab

The General tab contains basic information about the hardware, including the name of the manufacturer (or vendor), product class, revision, OUI, device type, and realm. Except for the manufacturer, revision, and realm, all the other values can be modified.

The **Communication Grace Period** specifies an additional number of seconds to be applied to timeouts when communicating with devices of this hardware, to accommodate hardware with slower response times.

Firmware tab

The Firmware tab shows details about any firmware associations for the hardware record. The **Available** table shows a list of potential firmware records to which the hardware can be associated. The **Current** table shows all of the current firmware/hardware associations.

To add a new association, select and drag a firmware entry from the **Available** table to the **Current** table. To remove an association from the **Current** table, select it and click **Delete**.

Tip: The hardware-firmware associations that can be set in this tab can be viewed and managed from the point of view of a specific firmware. See Hardware tab.

File

If a firmware is not associated directly with a device file, you can specify a firmware file to use by clicking on the **File** drop-down list and selecting an appropriate option. The drop-down list contains any files that are in the same realm as the hardware, and are of type Firmware (see General tab).

Note: If a file association has been made on the General tab of the firmware record, the **File** drop-down option will be grayed out.

Status

The Status of the association affects how many of the features make use of the firmware, when presented with a device of the given hardware. The possible status values are:

- **Deprecated**. Indicates that it is acceptable for the firmware to exist on this hardware, and it does not strictly require an upgrade. However, this firmware should not be applied to any further devices.
- **Obsolete**. Indicates that this firmware should not be used for this hardware and that an upgrade is required. If a device is seen on the network with this hardware and firmware, the system will attempt to upgrade it, if a valid upgrade path is available.
- **Recommended**. May only be applied to one of the associations for any given hardware/firmware combination. It indicates the ideal firmware that should be applied to the hardware. During a manual upgrade, where a CSR is presented with a drop-down of firmware images to choose from, the recommended firmware will be the default option if an upgrade path is not specified.
- **Unqualified**. This is the default value when a new association is discovered on the network. It operates similarly to **Deprecated**, in that it does not force an upgrade but should not be propagated to other devices either. If differs in that it visually indicates that the status needs to be reviewed and explicitly set.
- **Valid**. Indicates that this is one of a set of valid firmware versions for this hardware, and that it may be propagated to devices. These will appear as options to the CSR.

Upgrade Path

The **Upgrade Path** indicates the new firmware that should be used during an upgrade for a device of the given firmware that is currently using this firmware version. Selecting "(Use Recommended)" will cause the recommended firmware that is associated with the hardware to be used. Otherwise, it may be a specific firmware if the hardware requires multiple or stepwise upgrade paths.

Note: The contents of the **Upgrade Path** drop-down list are affected by the Hardware Filters configured for the firmware. They are limited to those with the same product class associations as the hardware. Additionally, a system preference called **Exclude Unrestricted Firmware In Upgrade Path Options** controls whether or not firmware without product class associations are included in the drop-down list.

Attributes tab

The Attributes tab shows details about any system attributes that are associated with the hardware record. Only attributes that have been defined for the Hardware object will be available (see Using Attributes for more information).

Available attributes are displayed in the **Attributes** pane on the lower left of the screen while currently defined attributes are displayed in the **Current Attributes** table on the lower right of the screen.

To add an attribute, select and drag it from the **Attributes** pane to the **Current Attributes** table. The list of available attributes can be filtered by Name.

To remove an association from the Current Attributes table, select it and click **Delete**.

Managing subscribers

Subscriber records typically contain information about customers that are subscribers to one or more services. The main purpose of subscriber records is to provide a way to group devices together by who is currently using them. Services may also be assigned to subscribers, which will be inherited by all of the devices associated with the subscriber.

Subscribers are of two types:

- **Normal**. Comprises subscribers that are associated with only a single realm. Normal subscribers typically represent regular consumers that may have one or more devices and/or services and are likely to be present in a single location.
- **Enterprise**. Comprises subscribers that do not have realm restrictions. Enterprise subscribers typically represent the users of a large corporate subscriber that may have hundreds of devices spread over large areas for its individual locations or users.

Subscriber records consist of name information (first, last), address, contact information (phone numbers, email address), billing/account numbers (typically managed by a third-party system), and company details.

Note: Company name is an optional field for normal subscribers, but a mandatory field for enterprise subscribers.

Another important aspect of enterprise subscribers is that because they have no realm restrictions, these subscriber records need to be managed by system user accounts with appropriate access to all of the necessary realms. Administrative users have this ability, but in order to help protect the system, special enterprise system users can be created for the sole purpose of managing enterprise subscribers. More details can be found in the Users section.

To access the **Subscribers** management screen, select **Inventory > Subscribers**.

Performing a search operation

You must enter some search criteria in the **Search** tab before you can perform any action on a subscriber. The **Search** tab can be accessed by clicking on the magnifying glass on the **Subscriber** management screen. Enter as much information as necessary to find the record(s) that you are looking for.

Note: The magnifying glass icon on the **Subscriber** management screen does not work in the same way as it does in most other places in Service Gateway. In this instance, it is used to provide search criteria to determine which records are retrieved from the database and displayed in the user interface.

Once you have specified your search criteria, click **Submit**. The search results will be shown on the **Subscriber Search Results** pane on the top of the screen.

If too many devices meet the search criteria, a pop-up message will request that you narrow the search criteria. The maximum number of search results that can be displayed is specified by an administrator, using the **Maximum Search Results Allowed** system preference.

By default, search results will be retained until you perform a new search, even if you navigate to other screens and return. This behavior can be disabled by an administrator by clearing the **Sticky Search Results** system preference.

Search results can also be filtered by Realm.

Adding subscriber records

To add a subscriber record to the system:

1. Click **New** on the **Subscriber** management screen. The **Viewing New Subscriber** pane opens on the bottom of the screen.
2. On the **General** tab,

   a. Select the **Account Type** - **Normal** or **Enterprise**.

   b. Enter the appropriate details in the text fields.

      - The **First Name** and **Last Name** are required fields while the rest are optional fields.
      - For **Normal** subscribers, you must select a **Realm** while for **Enterprise** subscribers, **Company Name** is a required field.

3. On the **Devices** tab, search for a device (for details on the search box and results pane, see Devices). From the **Device Search Results** pane, select and drag the desired device to the Current Devices table. To remove a device, select it in the **Current Devices** table and click **Delete**.
4. On the **Attributes** tab,

   a. Select and drag the desired attributes from the **Attributes** pane to the **Current Attributes** table.

   b. Click **Value** column and enter a value as appropriate.

   To delete an attribute from the **Current Attributes** table, select it and click **Delete**.

   Note: Attributes are associated with realms. So, enterprise subscribers that have no realm associations will not be able to select any attributes.

5. Click **Save**.

Deleting subscriber records

To delete a subscriber record from the system:

1. Select the desired subscriber record from the **Subscriber Search Results** list.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: A subscriber record cannot be deleted if any devices are associated with it.

Viewing and modifying subscriber records

To view the details for a specific subscriber record, select the desired subscriber record from **Subscriber Search Results** list in the top pane. Its details are displayed in the following tabs of the **Viewing Subscriber** pane at the bottom of the screen:

- General
- Services
- Devices
- Attributes

General tab

The General tab contains basic information about the subscriber, including the account type, realm, name details (first, middle, last), company details, contact information (phone, e-mail), address, and billing/account number. All of these values can be modified.

- The **First Name** and **Last Name** are required fields while the rest are optional fields.
- For **Normal** subscribers, you must select a **Realm** while for **Enterprise** subscribers, **Company Name** is a required field.

While there are no issues associated with changing the account type from **Normal** to **Enterprise**, some restrictions do exist when changing the account type from **Enterprise** to **Normal**.

To change the account type from **Enterprise** to **Normal**, the subscriber must either have no devices associated with it or if it has devices associated, all the devices must be within the same realm.

- If devices are associated with the subscriber and the account type is changed from **Enterprise** to **Normal**, then the realm is automatically set to the same realm as the devices.

- If no devices are associated with the subscriber, the **Realm** drop-down list is activated and you can select a realm as required.

Note: The **Last Name** may or may not be a required field, depending on administrator preferences. This is controlled by the **Subscriber Last Name Required** preference.

Services tab

The Services tab allows you to manage the services associated with a subscriber. All of the devices associated with the subscriber will inherit the services that are associated with the subscriber, in addition to any services that are associated directly with the device. When evaluating conditions or the Velocity script that reference services, the full list of services that applies to both the device and the subscriber will be used.

To associate a service with a subscriber, drag the service from the **Services** table to the **Current Services** table.

To dissociate a service from a subscriber, select it from the **Current Services** table and click **Delete**.

Caution: Enterprise subscribers do not have any realm associations, so there are no services available to associate with the subscriber.

Devices tab

The Devices tab comprises the **Device Search Results** table and **Current Devices** table. The **Device Search Results** table works exactly the same as the **Device Search Results** table on the main **Devices** management screen (for more information, see Devices).

To associate a device with the subscriber, select and drag the device record from the **Device Search Results** table to the **Current Devices** table.

To remove an association, select the device from the **Current Devices** table and click **Delete**.

Attributes tab

The Attributes tab shows details about any system attributes that are associated with the subscriber record. Only attributes that have been defined for the **Subscriber** object will be available (see Using Attributes for more information).

Available attributes are displayed in the **Attributes** pane on the lower left of the screen while currently defined attributes are displayed in the **Current Attributes** table on the lower right of the screen.

To add an attribute, select and drag it from the **Attributes** pane to the **Current Attributes** table. The list of available attributes can be filtered by Name.

To remove an association from the **Current Attributes** table, select it and click **Delete**.

⚠ **Caution:** Enterprise subscribers do not have any realm associations, so there are no attributes available to associate with the subscriber.

6

Managing Configuration Features

Manage configuration features

The Configuration menu allows you manage the following features of Service Gateway:

- Attributes
- Capabilities
- Data Model Definitions
- Data Models
- Domains
- Parameter Mappings
- Services
- Software Modules
- Templates

You can access the configuration features from the**Configuration** menu in the Service Gateway User Interface.

Managing attributes

Attributes can be used to add additional fields to the following types of records: devices, domains, hardware, firmware, services, and subscribers. These fields may hold additional data that is used within configuration templates, or to make decisions about how to communicate with a device. Each realm has its own set of attributes.

There are two types of attributes: simple and complex. Simple attributes are single elements with a name and a value. Complex attributes can be grouped to represent a structured multi-field set of related data. Whereas a particular object (device, subscriber, hardware, and so on) can only contain a single instance of a simple attribute, multiple complex attributes can be associated, essentially creating an array of multi-variable attributes.

Attributes can be associated with specific types of objects. When this is done, only instances of the specified objects can use those attributes. For example, if an attribute is configured as being accessible only to hardware and firmware objects, that attribute can only be selected when editing hardware or firmware records.

To access the main attribute management screen, select **Configuration > Attributes**. The **Attributes** management screen displays the **Attributes** tree in the left pane. From the **Choose Realm** drop-down list, select a realm. All the attributes defined for the selected realm are displayed in a hierarchical tree structure. Nodes with arrows next to them represent items that can be expanded or collapsed. The list of attributes can be filtered by Name.

Simple attributes are not expandable, while complex attributes are. Expanding a complex attribute will show all of the sub-attributes. Complex attributes cannot be nested.

Adding attributes

To add an attribute to the system:

1. Select a realm from the **Choose Realm** drop-down menu in the **Attributes** pane.
2. Click **New**.

3. In the **Viewing New Attribute** pane on the right of the screen, do the following:

   a. Enter a name for the attribute in the **Name** field. Attribute names are case-insensitive and must be unique. It is possible to have two attributes with the same name if they are in different groups (or if one instance is a simple attribute and the other instance is part of a complex attribute). Attribute names are unique per realm; that is, the same name can be used for different attributes in different realms.

   b. Select a **Value Type**

   c. Depending on the value type selected, you may be able to specify a validation pattern. If this field is active, you can alter the regular expression as necessary.

   d. Select an attribute type.

If you select	Then
Simple	The **Group** drop-down menu is deactivated (and any value currently selected is ignored).
Group	Enter in a name for the group (if you are creating a new group) or choose an existing group from the drop-down menu.

4. Associate a domain object with this attribute by selecting it from the **Available** pane and dragging it to the **Current** pane.

   To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

5. Click Save.

Note: To create a complex attribute with many sub-attributes, add the required attributes one at a time; setting the attribute type to Group and selecting the appropriate group name for each attribute.

Deleting attributes

To delete an attribute from the system:

1. Select the desired attribute from the **Attributes** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: Complex attributes cannot be deleted as a group. You must select and delete each sub-attribute one at a time. Attributes cannot be deleted if they are associated with an object (device, service, hardware, firmware, and so on).

Viewing and modifying attributes

To view the details for an attribute, select the appropriate attribute from the **Attributes** pane. Its details are displayed on the General tab of the **Viewing Attributes** pane.

General tab

The fields on the General tab are as follows:

- **Realm**. A read-only field that indicates the realm within which this attribute has been defined. To choose the realm for a new attribute, select the realm from the **Choose Realm** drop-down menu in the Attributes pane.
- **Name**. The name of the attribute. Attribute names must begin with a letter and must only contain letters, digits, underscores, and hyphens. It is a suggested convention to use uppercase names for attributes, to enhance readability within scripts and expressions; but, it is not required.
- **Value Type**. Determines the type of data that will be stored in the attribute. It has the following options:
  - **Password.** Password attributes are free-form text strings, but the text data is Base64-encoded before being stored in the database. This prevents passwords from being stored in clear text. When retrieving password attribute values from the database, the system automatically decodes the strings. Additionally, when viewing a password attribute, the value is replaced with a series of asterisks and editing requires that the entire value be retyped. The validation string for password attributes is fixed as being any string of characters.

⚠ **Caution:** Changing an existing attribute to or from the Password type will not automatically encode the existing values in the database. When these values are decoded, they typically would have nonsense characters as the values.

  - **Text.** Text attributes are free-form text strings. The default validation string for text attributes is '.*', but you can change it.
  - **Unsigned Integer.** Unsigned integer attributes contain unsigned integer values, represented as text strings. The validation string is fixed as being any string of digits.
  - **IP Address.** IP address attributes contain IP addresses in dotted-quad format. The validation string is fixed as being 4 sets of one to three digits separated by a dot ('.'). For IPv6 addresses, use the Text type and provide a regular expression to restrict the input as desired.
  - **Email Address.** Email address attributes contain email address strings (for example: john.smith@example.com). The validation string is fixed.
  - **MAC Address.** MAC address attributes contain MAC addresses in colon-delimited form (for example: 0a:bc:12:5c:34:5d). The validation string is fixed as being 6 pairs of hexadecimal digits separated by a colon (':').

- **Validation Pattern**. This field may only be edited if a **Value Type** of **Text** is chosen. It must contain a regular expression to be applied to any values assigned to an attribute via the GUI. There is an implicit match on the beginning and end of the value. If a validation pattern is changed, any existing values that no longer match that pattern will be permitted to persist during edits to the record, as long as the values themselves are not altered.
- **Attribute Type**. Either **Simple** or **Complex** must be chosen. Simple attributes are single elements with a name and a value. Complex attributes can be grouped to represent a structured multi-field set of related data.
- **Group**. This field is required only for complex attributes, and it becomes the prefix for the attribute. More than one attribute can use the same group name to construct a multi-field structure.
- **Objects**. Attributes can be associated with one or more types of object by dragging them from the **Available** to **Current** lists. Only instances of the specified objects will be able to attach and configure those particular attributes. For example, if an attribute is configured as being accessible only to hardware and firmware objects, that attribute can only be attached to hardware or firmware records.
- **Inherited by Child Domains**. This check box is available when **Domains** is chosen as one of the group associations. With this check box selected, when the attribute is added to a domain, all children of that domain will also inherit that attribute.

Note: When viewing the attribute details, the only parameters that can be changed are the value type, the validation pattern (if it is not a fixed pattern), and the object associations.

Using attributes

Once attributes have been defined, they can be added to appropriate database records (devices, hardware, firmware, and so on). Records that can have attributes have their own **Attributes** tabs (as discussed in many areas throughout this guide).

There are two attribute types: simple and complex. Objects can only have a single instance of a simple attribute and multiple instances of a complex attribute.

Consider an example where the following attributes are defined and associated with devices:

1. Simple attribute called DEVICE_PPP_USERNAME
2. Complex attribute called SIP_CONFIG, which contains the following sub-attributes:
   - USER_AGENT_DOMAIN
   - USER_AGENT_PORT

In this case, when you click **Attributes** tab for a device record, you can view details similar to the following:

All the available device attributes are displayed in the **Available Attributes** table. You can select and drag the attributes to the **Current Attributes** table.

In a scenario where **DEVICE_PPP_USERNAME** and two instances of **USER_AGENT_DOMAIN** are used, assigning simple and complex attributes works differently.

Simple attributes are just a name and a value, which may be left blank. If you try to drag a second instance of **DEVICE_PPP_USERNAME** to the **Current Attributes** table, an error message is displayed indicating that only one instance can be defined.

However in the case of the complex attributes, they are given a full name that includes an instance number. This allows entities, such as templates (for example), to then reference each instance of the **USER_AGENT_DOMAIN** attribute.

Managing capabilities

Capabilities are logical representations for abilities or functionality that can be configured on a device. Examples of capabilities include USB support, wireless Ethernet, VoIP, management protocol support (CWMP, SNMP, and so on), set-top box program guides, and firewall support.

Capabilities have the following features:

- **Hierarchy:** Capabilities can be arranged in a hierarchy. Child capabilities represent optional capabilities that may only be present if the parent capability is present. This eases user navigation of capabilities and helps with the optimization of automatic capabilities discovery.
- **Device Associations:** Capabilities can be manually associated to particular device hardware (that is, a particular hardware record and any firmware record), device firmware (that is, a particular firmware record and any hardware record), or a combination of hardware and firmware, provided that those hardware and firmware records have already been defined within the system.
- **Dynamic Discovery Support:** Capabilities can also be defined with dynamic discovery test cases. When the system detects a new hardware or firmware record, these discovery test cases are run to determine the capabilities that should automatically be attributed to the new hardware or firmware record.

Once defined, capabilities can be used as conditionals for configuration templates and policies, helping the system determine when specific configurations or policies must be run.

A capability must only be entered into the system if it has some significance to a business or technical process. For example, the ability for a wireless device to hook up to an external antenna may never be important to the system, and thus there is very little reason for the system to be aware of it. Capabilities must only be added to the system if they are deemed useful for providing a service.

Note: Capabilities do not represent consumable resources on the device. For instance, a capability would indicate that a particular device hardware and/or firmware supports USB functionality, but would not provide any details about the number of USB ports that exist or that are currently in use. This kind of information falls under the realm of resource management.

To access the **Capabilities Definition** management screen, select **Configuration > Capabilities > Definitions**. The **Capabilities Definitions** management screen displays the capabilities in a hierarchical tree structure in the **Capabilities** pane. Nodes with arrows next to them represent items that can be expanded or collapsed.

The list of capabilities can be filtered by Name and Realm.

Adding capabilities

Note: Capabilities can only be managed by users with the *Manage/View Capabilities* permission.

To add a capability definition, do the following:

1. Click **New** on the **Capabilities** pane. The **Viewing New Capability** pane opens on the right of the screen.
2. On the **General** tab:
    a. Select a **Realm** from the drop-down list.
    b. Select the **Parent Capability** from the drop-down list. This is optional. If a parent capability is not selected, the new capability appears as a new root node.
    c. Enter a name for the capability.
    d. Enter a description. This is an optional field.
3. Click **Save**.

Once the capability has been added, associations with hardware and firmware may be added manually if required. For information about how to configure these associations, see Viewing and modifying capabilities.

Deleting capabilities

To delete a capability from the system:

1. Select the desired item from the **Capabilities** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: Only user-defined capability entries can be deleted; clicking on a system-defined capability does not enable the Delete button.
A capability can only be deleted if it has no child elements.

Viewing and modifying capabilities

To view the details for an existing capability, click the desired capability in the **Capabilities** tree. Its details are displayed in the following tabs of the **Viewing Capabilities** pane on the right of the screen:

- General
- Associations

General tab

The General tab contains the following fields:

- **Realm**. The realm in which this capability is defined. Once defined, the realm cannot be changed. A capability is only available to the hardware, firmware, and test cases defined within the same realm. System-defined capabilities are not part of a realm and can be used by all realms.
- **Parent Capability**. The options in this drop-down list are only available once a realm is selected. It can be set to None to define a top-level capability. Alternatively, another existing capability can be selected, thereby defining a child capability. Child capabilities represent capabilities that may only be present on a device if the parent capability is present. This is an optional field.
- **Name**. A short descriptive name for this capability.
- **Description**. A description of this capability. This is an optional field.

Note: For system-defined capabilities, none of the fields in this tab can be modified. For user-defined capabilities, the name and description fields can be modified at any time.

Associations tab

Capabilities can be associated with a specific hardware, a specific firmware, or a combination of the two. The Associations tab is used to manage these associations.

The table at the top of the **Associations** tab provides a list of current associations.

To add an association, do the following:

1. Select the **Realm** from which the hardware and firmware are to be chosen. This option is only active for a system-defined capability. For a user-defined capability, this option is inactive and set to the realm in which the capability was defined.
2. Select an appropriate hardware record or **Any** from the Hardware drop-down list.
3. Select an appropriate firmware record or **Any** from the Firmware drop-down list.
4. Click **Add** (this button is only activated when you select either a hardware or firmware). The new hardware-firmware association appears in the table of current associations.

! **Important:** Additions and selections of associations are not permanently saved until the capabilities record is saved.

To delete an association:

1. Select a row in the table of current associations.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Managing data model discovery

Capabilities can be assigned to hardware and firmware combinations automatically when the system detects new combinations. When the system detects a new hardware and firmware combination, it will try running all of the defined capability test cases that are in the same realm as the device to see which capabilities can be associated with the new hardware and/or firmware.

The type of test case, described here, is based on the interrogation of the device data model. If the test cases pass, a chosen capability will be assigned to either the hardware, or the firmware, or a combination of both.

Tip: The system automatically associates the CWMP capability to any firmware that is communicating with Service Gateway via the ACSs using the CWMP protocol. Therefore, a test case is not required to assign this capability.

To access the **Data Model Discovery** management screen, select **Configuration > Capabilities > Data Model Discovery**. A list of currently defined test cases are displayed in the top pane. These test cases are identified by the **Capability** that is assigned if the test case passes. The list of definitions can be filtered by Capability.

A specific capability can appear in this list more than once if there are multiple test cases defined for it.

Adding data model test cases

To add a data model test case:

1. Click **New** on the **Data Model Discovery** management screen. The **Viewing New Test Case** pane opens at the bottom of the screen.
2. On the **General** tab:
   a. Select a **Realm** from the drop-down list.
   b. Select a capability mapping from the **Map Capability to** drop-down list. The available choices are **Hardware Only**, **Firmware Only**, and **Hardware and Firmware Combination**.
3. On the **Tests** tab, create all of the required parameter and/or object tests as follows:
   a. Select a data model from the **Data Models** pane. The list of data models can be filtered by Parameter Name.
   b. Expand the selected data model and select the desired object or parameter.
   c. Drag the selected object or parameter to the **Object or Parameter Name** column in the lower right pane.
   d. Change the **Test Type** if required.

e. Enter a test value (a string, range, regular expression, and so on) in the **Test Value** column if required.

Note: Test value is required only if the Test Type selected is: **Equals**, **Is Like**, **Is Between**, or **Is One Of**.

4. On the **Capability** tab,

   a. Select a capability from the **Capabilities** pane. The list of capabilities can be filtered by Name.

   b. Drag the selected capability to the **Selected Capability** table in the lower right pane.

   If you want to change the capability, you must first remove it from the **Selected Capability** table by selecting it and clicking **Delete**. Then, drag a new capability from the **Capabilities** tree.

5. Click **Save**.

Deleting data model test cases

To delete a data model test case from the system:

1. Select the desired test case from the list of currently defined test cases.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying data model test cases

To view the details for a specific data model test case, select the desired test case from the **Data Model Test Cases** list pane. Its details are displayed in the following tabs of **Viewing Existing Test Case** pane at the bottom of the screen:

- General
- Tests
- Capability

General tab

The General tab has the following fields:

- **Realm**. The realm of devices that this discovery test case will be executed against.
- **Map Capability to**. Specifies the objects that the capability will be associated with if the data model tests against a device pass. The options are **Hardware Only**, **Firmware Only**, and **Hardware and Firmware Combination**.

Tests tab

The Tests tab shows all of the parameter and object tests that have been defined. It has the following panes:

- **Data Models pane.** Displays the data models in a hierarchical tree structure. Click the data model drop-down menu to view the list of all data models registered with the system (for example, Device 1.0, InternetGatewayDevice 1.0, and STBService 1.0). Once you select a data model from the menu, you can navigate and select objects and parameters to associate with a test case.

  Data Models can be filtered by Parameter Name.

- **Test Definitions pane.** Displays a list of test definitions. To add a parameter or object to the test case, drag it to the **Test Definitions** pane on the right of the screen. Multiple parameters or objects can be specified, in which case ALL tests must pass in order for the test case to pass and the capability to be assigned. This pane has the following columns:
  - **Object or Parameter Name.** Contains the data model parameter or object against which the test will be run.
  - **Test Type.** Specifies the types of tests to run. The following types of tests are available:
    - **Exists.** Does a specific parameter or object exist?
    - **Does Not Exist.** Is a specific parameter or object absent?
    - **Is writable.** Is a specific parameter or object writable?
    - **Equals.** Does a parameter have a specific value?
    - **Is like.** Does a parameter value match a regular expression?
    - **Is between.** Is a parameter value between two values (for example, is the value between 1 and 10)?
    - **Is one of.** Is a parameter value within a set of possible values (an enumeration)? The list of possible values must be provided as a comma-delimited list.
  - **Test Value.** Contains the value to check the parameter for (a string value, range, regular expression, and so on) if appropriate. Objects cannot be checked for values.

Capability tab

The Capability tab is used to select the capability that is assigned to the test case.

Note: Only one capability can be associated with a test case at any time.

To add a capability:

a. Select a capability from the **Capabilities** pane. The list of capabilities can be filtered by Name.

b. Drag the selected capability to the **Selected Capability** table in the lower right pane.

If you want to change the capability, you must first remove it from the **Selected Capability** table by selecting it and clicking **Delete**. Then, drag a new capability from the **Capabilities** tree.

Managing RPC Method Discovery

Capabilities can be assigned to hardware and firmware combinations automatically when the system detects new combinations. When the system detects a new hardware and firmware combination, it will try running all of the defined capability test cases that are in the same realm as the device to see which capabilities can be associated with the new hardware and/or firmware.

The type of test case described here is based on the RPC methods supported by the device. If the test case passes, a chosen capability will be assigned to either the hardware, or the firmware, or a combination of both.

RPC method test cases are test cases that look for support for a specific set of RPCs on a specific hardware and/or firmware. For example, ScheduleInform is an optional RPC for CWMP-capable devices. An RPC method test case can then be created that would check if that method is supported by a specific hardware/firmware combination. If found, the capability is associated with that hardware/firmware combination.

To access the **RPC Method Discovery** management screen, select **Configuration > Capabilities > RPC Method Discovery**. A list of currently defined test cases are displayed in the top pane. These test cases are identified by the capability that is assigned if the test case passes. The list of definitions can be filtered by the RPC Method and Capability that is assigned if the test case passes.

Adding RPC Method test cases

To add an RPC method test case:

1. Click **New** on the **RPC Method Discovery** management screen. The **Viewing New Test Case** pane opens at the bottom of the screen.
2. On the **General** tab:

   a. Select a **Realm** from the drop-down list.

   b. Select a capability mapping from the **Map Capability to** drop-down list. The available choices are **Hardware Only**, **Firmware Only**, and **Hardware and Firmware Combination**.

3. On the **RPC Methods** tab, select the RPC method that the device must support from the **Available** pane and drag it to the **Current** pane.

   To select multiple items, hold down the CTRL key and click each item with your mouse, or hold down the Shift key and click the first and last items in a range of consecutive items.

4. On the **Capability** tab, associate a capability with the test case as follows:

   a. Select a capability from the **Capabilities** pane. The list of capabilities can be filtered by **Name**.

b. Drag the selected capability to the **Selected Capability** table in the lower right pane.

Note: To remove a capability, select it and click **Delete**.

5. Click **Save**.

Deleting RPC Method test cases

To delete an RPC method test case from the system:

1. Select the desired test case from list of currently defined test cases in the top pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying RPC Method test cases

To view the details for a specific RPC method test case, select the desired test case from the **RPC Method Test Cases** list pane. Its details are displayed in the following tabs of Viewing Existing Test Case pane at the bottom of the screen:

- General
- RPC Methods
- Capability

General tab

The General tab provides the following fields:

- **Realm**. The realm of devices that this discovery test case will be executed against.
- **Map Capability to**. Specifies the objects the capability will be associated with if the data model tests against a device pass. The options are **Hardware Only**, **Firmware Only**, and **Hardware and Firmware Combination**.

RPC Methods

The RPC Methods tab shows a list of all available RPC methods and which ones are currently assigned to the current test case. To change the RPC associations, select the RPC methods that the device must support from the **Available** pane and drag it to the **Current** pane. The test is deemed to pass if a device reports support for all of the selected RPC methods.

Capability tab

The Capability tab is used to select the capability that is assigned to the test case.

Note: Only one capability can be associated with a test case at any time.

To add a capability:

1. Select a capability from the **Capabilities** pane. The list of capabilities can be filtered by Name.
2. Drag the selected capability to the **Selected Capability** table in the lower right pane.

If you want to change the capability, you must first remove it from the **Selected Capability** table by selecting it and clicking **Delete.** Then, drag a new capability from the **Capabilities** tree.

Managing data model definitions

Data Model Definitions are XML documents that conform to the schema defined by the Broadband Forum. Versions 1.0 through 1.4 of the data model schema are supported. Once a definition file has been uploaded, the data models or components defined within it can be imported into the system and used by various features throughout the application.

To access the **Data Model Definitions** management screen, select Configuration > Data Model Definitions. A list of currently uploaded definitions are displayed in the upper right pane. The list of definitions can be filtered by name, description, and specification URI.

Adding definitions

To add a definition:

1. Click **New** on the **Data Model Definition** management screen. The **Viewing New Data Model Definition** pane opens on the bottom of the screen.
2. On the General tab,
   a. Enter a name in the **Name** field.
   b. Browse and upload the data model definition XML file from your file system.
   c. Enter a description. This is an optional field.
3. Click **Save**.

Tip: The Broadband Forum publishes data model definitions for its specifications at the following location: http://www.broadband-forum.org/cwmp.php

Deleting data model definitions

To delete a data model definition:

1. Select a definition from the **Data Model Definition** list.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: When a definition is deleted, any data models or components that have been imported from the template remain in the system and must be deleted separately if desired.

Viewing and modifying a data model definition

To view a definition, select the appropriate definition record from the **Data Model Definitions** list pane. Its details are displayed in the following tabs of **Viewing Data Model Definitions** pane at the bottom of the screen:

- General
- Import
- XML

General tab

The General tab contains the following fields:

- **Name**. A useful name for the definition, such as the name and version of the specification by which it is defined.
- **Specification**. A read-only field that is only visible for an existing definition. It displays the URI of the specification derived from the XML definition.
- **Definition file**. This field is used to upload a file to the definition record. It must be specified for a new definition record. When editing an existing definition, it will be blank. To overwrite the definition, a new file can be specified.
- **Description**. A description for the definition. This is an optional field.

Import tab

The Import tab allows data models and components defined within a definition to be imported into the system.

If	Then
Any data models are defined in the definition	A drop-down list of models is displayed. To import a model: ○ Select it and click **Import Model**. If the model has already been imported, a pop-up appears asking if the current model should be overwritten.
Any components are defined in the definition	A drop-down list of components is displayed. To import a component: ○ Select it and click **Import Component**. You will be prompted to choose an existing data model and branch within that data model to graft the component to. If the import would overwrite any objects or parameters, a pop-up appears asking for confirmation.

If	Then
No data model or components are defined in the definition	The following message is displayed: This definition does not include any models or components. Nothing to import.
The definition depends on other definition files, and these dependencies have not yet been uploaded	The following message is displayed, referencing the specification URI that is required: The referenced specification 'urn:broadband-forum-org:example' was not found. Please upload this specification to enable imports.

XML tab

The XML tab provides a preview of the XML definition file. Only the first 100 lines are displayed. To download the complete XML definition file, click the **Download** button on the upper right corner of the tab.

Managing data models

A data model is a description of a set of objects and parameters supported by a device. A data model is typically defined as part of a specification from the Broadband Forum or another standards body. A device vendor may also provide a proprietary data model to access their own value added features. Data models are typically imported from an XML document (see Data Model Definitions). They can then be altered by adding additional components or parameters to reflect the capabilities of the managed devices.

Data models serve two primary purposes within the application:

- First, they are the source of possible values wherever parameters need to be chosen, including template definitions, creation of real-time probes, definition of policy actions to retrieve parameters from devices, and data model test cases for capability discovery.
- Second, they are used to configure the data model parameters which are to be included in a device cache.

To access the **Data Model** management screen, select **Configuration > Data Models**. The **Data Models** pane is displayed on the left of the screen. Click the **Choose Data Model** drop-down menu to view the list of all data models registered with the system (for example, Device 1.0, InternetGatewayDevice 1.0, and STBService 1.0). Once you choose a data model from the menu, you can navigate and select its object or parameter. The details of the selected object or parameter are displayed on the **General** tab of the **Viewing Data Models** pane on the right of the screen.

Nodes may be added or deleted from the tree.

Adding a data model node

To add a new data model parameter or object:

1. From the **Data Models** pane, select a data model from the **Choose Data Model** drop-down list.
2. Click an object to make it the parent node for a new object or parameter.

Note: Only object nodes can contain parameters.

3. Click **New** on the **Data Models** pane.
4. On the **General** tab in the right pane,

   a. Enter the appropriate details in the following fields:

      - The fully-qualified name of the parameter in **Name** field.
      - A description of the object or parameter in the Description field.

b. Select the required options from the following drop-down lists:

- **Access**
- **Type**

Depending on the selected **Type**, you may need to enter additional details as required.

c. Select the **Cache Values** check box if the system must maintain the last known value for this parameter for each device.

5. Click **Save**.

Deleting a data model node

To delete a data model node:

1. Select a node from the **Data Models** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

⚠ **Caution:** Deleting a node will also delete its child nodes.

Deleting a data model

To delete an entire data model:

1. Select a data model from the **Choose Data Model** drop-down list.
2. Select the top-most (root) node of the tree.
3. Click **Delete**.
4. When asked for a confirmation, click **Ok**.

Viewing and modifying data model nodes

To view details about an object or parameter, navigate and select it from the **Data Models** pane. Its details are displayed on the General tab of the **Viewing Data Models** pane on the right of the screen.

General tab

The General tab contains the following fields:

- **Name**. The fully-qualified name of the parameter. The name of an existing node cannot be altered. When adding a new node, only the right-most component of the name may be specified. The prefix is that of the parent node.
- **Description**. A description of the object or parameter. This is an optional field.

- **Access**. The level of access a device provides for the node, either Read Only or Read/Write.
- **Type**. The parameter type specifying the class of value that the device supports for this node. It can be one of the following: Base64, Boolean, Date/Time, Integer, String, Unsigned Integer, Object, or Object Array.
- **Maximum Length**. This field is displayed for the Base64 and String types. It specifies the maximum number of characters permitted in the value.
- **Minimum Value**. This field is displayed for the Integer and Unsigned Integer types. It specifies the minimum value permitted as a numeric value. It is an optional field.
- **Maximum Value**. This field is displayed for the Integer and Unsigned Integer types. It specifies the maximum value permitted as a numeric value. It is an optional field.
- **Cache Values**. If this check box is selected, the system will maintain the last known value for this parameter for each device. This last known value can be updated when parameters are received from a device via a Value Change Inform, and is updated whenever the system sets the value on the device. The value cache is combined with a live snapshot of a device to create a configuration snapshot.

Managing domains

Domains can be used to logically divide devices into sub-groups. Domains are structured hierarchically and may be modeled in whatever manner suits the operator. A typical domain model is geography (for example, country, province, city, and grid area). However, because the domain names themselves are just free-form text strings, the list of modeling possibilities is endless.

Domains can be assigned to a device either manually or through an automated process based on IP network blocks. Automatic domain association will only occur if the device has not yet been registered in the system database.

When creating automatic domain associations, the system will check to see if a domain node has been defined that includes a network block definition that encompasses the IP address of the device that is being registered. If such a domain exists, the device will be registered with that domain. If the IP address does not fall within any defined network blocks, the device will be assigned to the default domain for the tree.

Devices will only have their domain automatically assigned (via the network blocks) if the device does not yet exist in inventory. That is, automatic domain association will not apply to devices added manually via the GUI or web services interface.

There can be only one default domain per realm. If a default domain has already been defined and you then specify a different domain node to be the default, the previous domain node will automatically have the default domain flag removed.

To access the **Domain** management screen, select **Configuration > Domains**. The **Domains** pane is displayed on the left of the screen. Available domains are displayed in a tree structure with available realms at the top level. Nodes with arrows next to them represent items that can be expanded or collapsed. Select a domain from the **Domains** pane to view its details in the **Viewing Domains** pane on the right of the screen. The list of domains can be filtered by Name.

Adding domains

To add a new domain node:

1. Click **New** on the **Domains** pane.
2. On the **General** tab in the right pane, do the following:

   a. Select a **Realm**.

   b. Click within the **Parent Domain** field or on the 📄 icon. In the **Select Domain** dialog box that opens, select a domain, and click **Ok**.

   c. Enter a name for the new domain in the **Name** field.

3. On the **Networks** tab, click **New** to define any network blocks that are to be used for automatic domain association if required.

   Note: A full network definition can only be defined once within the entire system and IP networks cannot overlap.

   To remove a network block from the **Current Networks** list, select it and click **Delete**.

4. On the **Attributes** tab, associate attributes with the domain as follows:

   a. Select and drag the desired attributes from the **Attributes** pane to the **Current Attributes** table.

   b. Click **Value** column and enter a value as appropriate.

5. Click **Save**.

Deleting domains

To delete a domain node:

1. Select a domain node from the **Domains** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

   Note: A domain node can only be deleted if it has no children.

Viewing and modifying domains

To view a domain, select the appropriate record from the tree in the **Domains** pane. Its details are displayed in the following tabs of the **Viewing Domain** pane on the right of the screen:

- General
- Networks
- Attributes

General tab

The General tab contains the following fields:

- **Realm**. The realm to which this domain belongs. This may only be specified when adding a new domain. The realm of existing domains may not be changed.
- **Parent Domain**. Domains may be defined hierarchically to as many levels deep as desired. To specify a top-level domain, select the root domain (/) as the parent. The parent domain of an existing domain may be changed, allowing an entire branch of the hierarchy to be moved.

- **Name**. The visible name of this domain. A short descriptive name is suggested. The name of a domain may be changed at any time.
- **Description**. A description of this domain. This is an optional field.
- **Realm Default**. If this check box is selected, this is the default domain for the realm. It determines the domain in which newly registering devices are placed, and affects many of the defaults throughout the user interface. Selecting this domain as the default domain automatically deselects the previous default domain.

Note: Only one domain per realm may be the default.

Networks tab

The Networks tab allows the domain to be associated with one or more IP networks. These mappings are used to assign a realm and domain to a new device that is registering for the first time.

When a new device registers, if its IP address falls within any of the defined networks across all realms/domains, the device is assigned to that realm and domain as it is added to the system.

Network mappings consist of the network number and the number of bits to be used for the subnet mask. It is not permitted to add overlapping networks to different domains within the system, even if the domains are in different realms.

To add a new network mapping:

1. Click **New** on the top right corner of the **Current Networks** table.
2. Modify the **Base IP Address** and **CIDR Bits** fields.
   - If the IP Address is specified in IPv4 dotted-quad notation, the CIDR Bits must between 0 and 32, inclusive.
   - If an IPv6 address is specified, CIDR Bits may be specified up to 128.

To modify an existing network mapping, click the appropriate row and column and change the value as required.

To delete an existing network mapping, click the mapping and then on the **Delete** button in the upper right corner of the **Current Networks** table.

Attributes tab

The Attributes tab shows details about any attributes that have been associated with the domain record. Only attributes that have been defined for the **Domain** object are available (for more information, see Using Attributes).

All available attributes are displayed in the **Attributes** pane on the left of the screen. The list of available attributes can be filtered by Name. Currently defined attributes are displayed in the **Current Attributes** table.

You can associate attributes with a domain by selecting and dragging them from the **Attributes** pane to the **Current Attributes** table.

Managing parameter mappings

The Parameter Mappings feature can be used to map the value of parameters contained within a device event (CWMP Inform message) to device attributes and system keys. Each time a device event is received, the parameters and values sent are compared against the mappings defined in Parameter Mappings. If a match is found, the specified field on the device is updated.

To access the **Parameter Mappings** management screen, select **Configuration > Parameter Mappings**. A list of currently defined mappings are displayed in the top pane. The list of Parameter Mappings records can be filtered by the data model Object Name.

Adding parameter mappings

To add a new parameter mapping:

1. Click **New** on the **Parameter Mappings** management screen. The **Viewing New Parameter Mapping** pane opens on the bottom of the screen.
2. On the **General** tab:
   a. Select the appropriate values from the following drop-down lists:
      - **Realm**
      - **Test Type**
      - **Map Type**
      - **System Key**
      - **Attribute**

   b. Enter values in the following fields:
      - **Object Name**. Click **Browse Data Models** to select an object from the **Data Models** pane.
      - **Values**
      - **Index**

   Note: **Realm** and **Object Name** are mandatory, as well as either **Attribute** or **System Key**, depending on the selected **Map Type**.

3. Click **Save**. The mapping comes into effect immediately.

Deleting parameter mappings

To delete a mapping:

1. Select a mapping from the **Parameter Mapping** list in the top pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying parameter mappings

To view a parameter mapping, select the appropriate record from the Parameter Mapping list in the top pane. Its details are displayed in the following tabs of the Viewing Parameter Mapping pane at the bottom of the screen:

- General
- Transformation Script

General tab

The General tab contains the following fields:

- **Realm**. The realm of devices that this mapping will apply to.
- **Object Name**. The name of the object or parameter contained within the Inform to map to a field on the device. You can either type in the name or select the name from a data model present in the system by clicking **Browse Data Model**.
- **Test Type**. The type of test to apply to the object and value. The mapping will only occur if the test passes. The test type can be one of the following:
    - **Existence**. The mere existence of the parameter will cause the value to be mapped.
    - **Equality**. The mapping will occur if the parameter value matches the value specified in the **Values** field.
    - **Range**. The mapping will occur if the parameter value is numeric and it falls within and is inclusive of the two values specified in the **Values** fields.
    - **Regular Expression**. The mapping will occur if the parameter value matches the regular expression provided in the **Values** field.
    - **List**. The mapping will occur if the parameter value is one present in the comma-delimited list provided in the **Values** field.
- **Map Type**. The type of device field to update, either **Attribute** or **System Key**.
- **Values**. This field is enabled for any **Test Type** other than **Existence**. Its usage depends on the selected **Test Type**.

- **Clear Mapping on Failed Match**. If this check box is selected, if a parameter is present in the Inform, but the test does not pass, the value will be cleared from the device.
  - If **Map Type** is **Attribute**, the attribute will be removed from the device.
  - If **Map Type** is **System Key**, the system key value will be set to an empty string.
- **System Key**. This drop-down list is enabled for a **Map Type** of **System Key**. It allows the target system key field to be selected. This drop-down list has the following options:
  - **MAC Address**
  - **IP Address**

    The preceding options are always present in this drop-down list as they are the built-in system keys.
  - Any defined custom system keys.
- **Attribute**. This drop-down is enabled for a **Map Type** of **Attribute**. It allows the target attribute to be selected.
- **Index**. If a complex attribute is selected as the target for an attribute mapping, the instance of the attribute must be specified.

Transformation Script tab

The Transformation Script tab allows you to provide an optional script that can be used to convert the parameter value into the required form before storing it in the database. For example, if all values are to be upper-cased before they are stored in the database.

This tab has the following fields:

- **Example Parameter Value**. A parameter value that is used to validate the script when you save it.
  - If you are defining a transformation script, this value must be provided before you save the parameter mapping.
  - If any syntax errors are present in the script, they will be reported at this time, and you will not be able to save the parameter mapping until all errors in the script have been resolved.
- **Script**. A JavaScript function that can be used to transform or change a value from the device before it is stored in the database.

Transformation script for parameter mapping

The transformation script for a parameter mapping is a JavaScript function that can be used to transform or change a value from the device before it is stored in the database. To define a JavaScript function, either click in the **Script** text box (which is read-only), or on the 🗎 icon located at the upper right of the **Script** text box. This **Script Editor** opens.

If a script is not yet defined for this parameter mapping, you will see the following auto-generated content:

// Auto-generated script content

```
function transformForStorage(value) {
    return value;
}
```

The script must contain the **transformForStorage** method, and it must return either a value or a specific error. Since the transformation script is a JavaScript, any JavaScript code is valid when writing this script.

Example Scripts

The following script can be used to convert a value to lower case:

// Auto-generated script content

```
function transformForStorage(value) {
  return value.toLowerCase();
}
```

The following script can be used to return an error instead of a value:

// Auto-generated script content

```
function transformForStorage(value) {
   if (value.length != 12) {
    error.setErrorString("Invalid MAC Address");
    return;
   }
  return value;
}
```

In the preceding case, an error is returned if the input value is not exactly 12 characters in length. The error message is written to Encore.log as a warning to be displayed if the situation occurs, and the parameter is not mapped.

Testing the transformation script

You can test your transformation script, to make sure it is returning the required value, by entering a sample value in the **Test Value** field and clicking **Evaluate**. The transformed value is displayed on the bottom pane. If you set the error string, a pop-up dialog box opens with the returned error message.

After evaluating the script, you can click **Ok** to accept the script or **Cancel** to discard the changes.

Configuring services

Customers purchase various services from a service provider. Services can include high-speed internet, VoIP, video on demand, and so on. Services can be further divided based on level of service, such as 5 MB Internet access versus 10 MB Internet access.

While service subscriptions are usually handled by a billing system of some sort, in many cases activation of a service will require configuration of some device. The services module takes care of the management of this service-related configuration.

Along with a name and an optional code (typically the service or billing code maintained in a billing system), service records can be assigned a priority, attributes, and configuration templates. As with most aspects of the system, services are associated with specific realms, enabling each realm to have their own service definitions.

If multiple services are assigned to a specific device, service priority values are used to determine the order in which available configurations are applied and delivered, with priority 1 occurring before priority 2, and so on.

If the service requires configuration templates, the Enable parameter must be checked. Once this is done, configuration templates can be added to the service definition. The order that templates are specified is important, since they are delivered in the order in which they are defined in the service.

As with the configuration templates themselves, when a template is added to a service you can configure a set of conditions that determine when the template will be applied. If you define a set of conditions in this manner, they will be combined with the existing template conditions in a boolean AND fashion. That is, any conditions defined for a template at the service level will further restrict when the configuration is applied.

To access the Services management screen, select **Configuration > Services**. A list of currently defined services are displayed in the top pane. The list of services can be filtered by Name, Code, and Realm.

Adding services

Services can be added in two ways:

- Using New
- Using Import

Using New

To add a service

1. Click **New** on the **Services** management screen. The **Editing New Service** pane opens on the bottom of the screen.
2. On the **General** tab,
    a. Select a **Realm** from the drop-down list.
    b. Enter the appropriate values in the **Name** and **Code** fields.
    c. Select the **Enable** check box if required. Selecting **Enable** activates the Priority and Templates tabs
3. On the **Priority** tab, select and drag the service definition entries to the correct priority positions. The service definition currently being viewed/modified is shown in bold text.
4. On the **Templates** tab,
    a. Select and drag configuration templates from the **Available** table to the **Current** table. The order in which you drag the templates is the order in which they will be applied, so drag them over in the correct order.
    b. Select a delivery rule for each template.
    c. Click **Conditions** to apply additional conditions (that is, in addition to any existing template conditions) if required.

    To delete a configuration template from the **Current** table, select it and click **Delete**.
5. On the **Attributes** tab,
    a. Select and drag the desired attributes from the **Attributes** pane to the **Current Attribute**s table.
    b. Click **Value** column and enter a value.

    To delete an attribute from the **Current Attributes** table, select it and click **Delete**.
6. Click **Save**.

Using Import

To import a service

1. Click **Import** on the **Services** management screen and select the file to be imported.

Note: Files with .xml extension can only be imported.

The **Editing New Service** pane is displayed at the bottom of the screen.

2. Modify the options on each tab of the **Editing New Service** if required.
3. Click **Save**.

The new service gets added and is displayed on the **Services** management screen.

Copying existing services

You can create a new service by copying an existing service and modifying it to suit your requirements. To copy an existing service to use as the basis for a new service:

1. Select the service that you want to copy from the **Services** management screen and click **Copy**.

Note: The **Copy** button is disabled if a new template is being created, or the existing template has already been copied.

The **Editing New Service** pane opens on the bottom of the screen.

2. On the **General** tab, enter a name for the new service.
3. Review all the options in each tab of the **Editing New Service** pane and modify as required. For details, see Viewing and modifying services.
4. Click **Save**.

Deleting services

To delete a service:

1. Select a service from the **Services** list in the top pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

! **Important:** When a service is deleted, any remove settings that have been configured for any configuration templates associated with the service will be executed the next time the configuration synchronization action is executed for the devices that were previously configured with the deleted service.

Viewing and modifying services

To view a service, select the appropriate record from the Services list in the top pane. Its details are displayed in the following tabs of the Viewing Service pane at the bottom of the screen:

- General
- Priority

- Templates
- Attributes

General tab

The General tab contains the following fields:

- **Realm**. The realm within which this service is defined, selected when the service is added. The realm of an existing service cannot be altered. A service is only available to devices, policies, and subscribers within the same realm.
- **Name**. A short descriptive name for the service.
- **Code**. A code for the service, to aid in integration with billing systems. This is an optional field.
- **Enable**. Selecting this check box indicates that configuration templates are associated with the server, thereby activating the **Priority** and **Templates** tabs.

Priority tab

The Priority tab shows the priority ranking for each service definition within the realm of the current service definition. This defines the order in which services will be sent to a device, when configuration for multiple services needs to be delivered. The service definition being viewed/modified is shown in bold text.

To change the priority of a particular service definition, select and drag the service definition into the appropriate position.

Templates tab

The **Templates** tab allows one or more configuration templates to be associated with the service. This tab is activated when the **Enable** check box has been selected on the **General** tab.

To associate a template with the service, select the desired template from the **Available** table and drag it to the **Current** table. To remove a template, select it from the **Current** table and click **Delete**. If you remove a template from a service that was previously applied to a device, any remove settings configured for the template will be executed during the next configuration synchronization.

For each template associated with the service, a delivery rule and conditions are specified. For details on how to configure the conditions, see Defining Conditions. The following delivery rules can be applied to a template:

- **Always**. The configuration template will always be delivered, whether the configuration content has changed or not.
- **On change**. The configuration template will be delivered only if the configuration content differs from that which was last delivered to the device.
- **Once**. The configuration will be delivered only if there is no record of the configuration having been delivered, even if the configuration content changes.

The order in which the templates are delivered can be changed by selecting and dragging the template items in the Current table to the appropriate positions.

Note: When editing templates associated with a service, the button used to edit conditions indicates when conditions are already set. The button is labeled **Specify Conditions** if conditions are not set and **Modify Conditions** if conditions are set. Also, pausing on the button displays the currently defined conditions as a tooltip, allowing them to be viewed without opening the condition editor.

Attributes tab

The Attributes tab provides details about any attributes that have been associated with the service record. Only attributes that have been defined for the **Service** object will be available (for more information, see Using Attributes).

All available attributes are displayed in the **Attributes** pane on the left of the screen. The list of available attributes can be filtered by **Name**. Currently defined attributes are displayed in the **Current Attributes** table.

You can associate attributes with a service by selecting and dragging them from the **AttributesCurrent Attributes**pane to the table.

Exporting Services

The services can be exported as .xml file.

To export a service

1. Select the service to be exported from the **Services** management screen.
2. Click **Export**.

The selected service gets exported as .xml file.

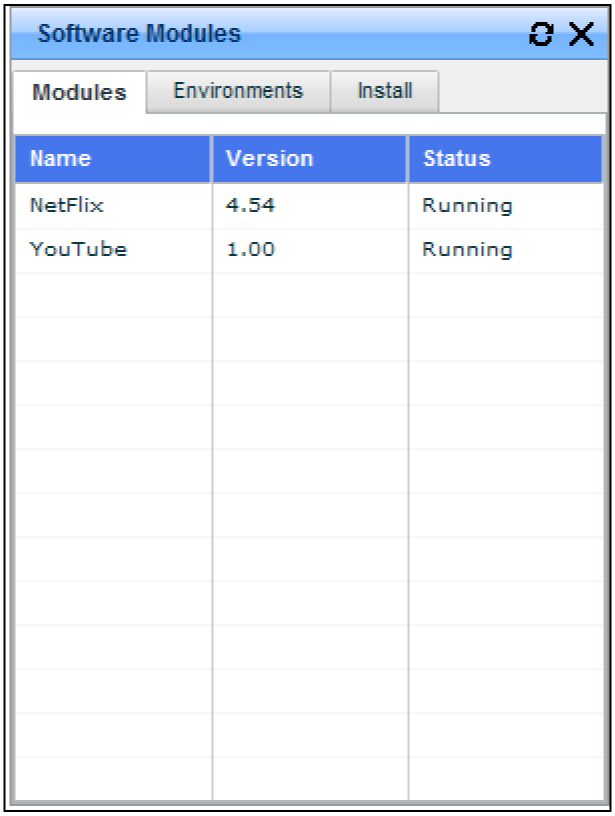
Managing software modules

Software modules are applications that run on end-user devices that support the Software Module Management portion of the CWMP 1.2 specification.

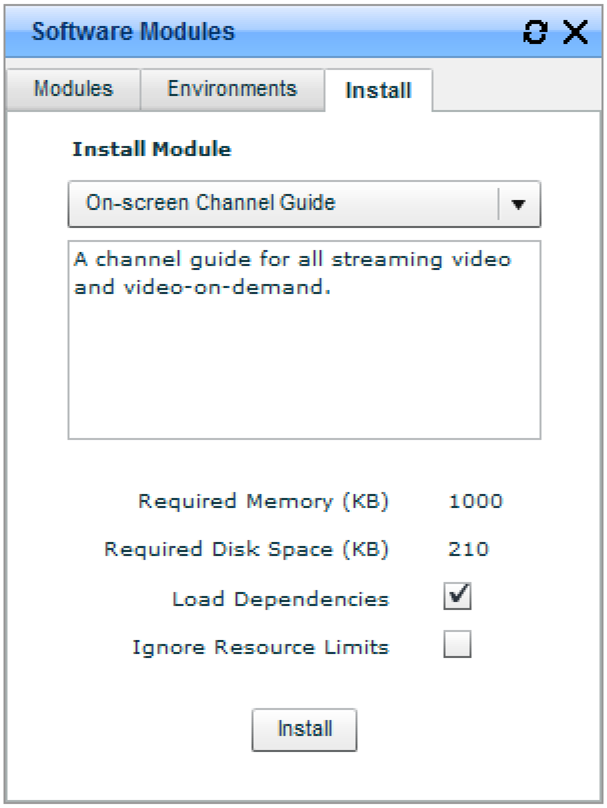
Software modules can be uploaded to the system and delivered to devices in several ways. Modules may be associated with a configuration template, allowing them to be part of configuration synchronization. They may be installed or uninstalled during scheduled maintenance using a policy action called Software Module Update, allowing new modules to be pushed to devices much like a firmware update. Lastly, a CSR module is available to view the modules currently installed on a device, as well as to install a new module, or uninstall an existing one.

All of these delivery mechanisms depend on a software module definition to describe the software module, which in turn depends on a device file which contains the actual binary content.

The anticipated resource footprint of software modules can be specified and a resource check performed before installing a new module, ensuring that the device has the storage capacity and available runtime memory to support the module. This check may be controlled in the same ways as the dependency check.



Name	Version	Status
NetFlix	4.54	Running
YouTube	1.00	Running



On-screen Channel Guide

A channel guide for all streaming video and video-on-demand.

Required Memory (KB) 1000

Required Disk Space (KB) 210

Load Dependencies ☑

Ignore Resource Limits □

To access the **Software Module** management screen, select **Configuration > Software Modules**. A list of currently defined software modules are displayed in the **Software Modules** list in the top pane. The list of software modules can be filtered by Name.

Adding software modules

To add a software module:

1. Ensure that the binary content of the software module has been uploaded to the inventory and file distribution subsystem using the Device Files management screen.
2. Click **New** on the **Software Modules** management screen. The **Viewing New Software Module** pane opens on the bottom of the screen.
3. On the **General** tab,
   a. Select a **Realm** from the drop-down list.
   b. Enter a **Name** for the new software module
   c. Enter values in the other fields if required.
   d. From the **File** drop-down list, select the previously uploaded file that contains the actual binary content of the module. This can be done later if it is not currently available
4. On the **Dependencies** tab, drag any existing software modules that this new module depends on from the **Available** pane to the **Current** pane.
5. Click **Save**.

Deleting software modules

To delete a software module:

1. Select a module from the **Software Module** list in the top pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying software modules

To view a software module, select the appropriate record from the Software Module list in the top pane. Its details are displayed in the following tabs of the Viewing Software Module pane at the bottom of the screen:

- General
- Dependencies

General tab

This General tab contains the following fields:

- **Realm**.The realm is chosen when the software module is initially defined. It cannot be modified.
- **Name**. A short name for this software module.

- **Description**. A description of this software module. It is an optional field.
- **Version**. The version of the software module.
- **Required Disk Space (kB)**. The estimated required disk space when the software module is installed on a device. This is used during the optional pre-check when determining if there is enough space on the device to install the module.
- **Required Runtime Memory (kB)**. The estimated required runtime memory when running the software module on the device. This is used during the optional pre-check when determining if there is enough runtime memory to install the module.
- **File**. The file that contains the actual binary content of the software module.

Dependencies tab

Software modules may have dependencies on other software modules. When a software module is installed, any dependencies may also be installed if they are not already present on the device. This behavior is optional, and can be enabled or disabled per template and per policy action. It is also an option when installing modules using the CSR module.

To indicate that the current software module depends on another software module that is already installed on the device, drag the other software module from the **Available** to the **Current** list.

Managing templates

Configuration templates contain configuration details that are used to enable and disable features and functionality contained in devices. Templates, once defined, can be associated with services and/or can be applied to individual devices.

A template consists primarily of configuration details that can be used to apply changes to a device, and optionally to remove those changes from a device. The exact content of a configuration detail depends on the configuration method chosen for the template. For details on the four configuration methods that are provided by default, see Configuration Methods.

Templates are processed whenever the configuration synchronization policy action is executed. All of the templates that apply to a specific device (via service associations and device overrides) are processed to determine the configuration details. Those details are then compared with the current known configuration of the device. Typically, if the new configuration differs from the previous configuration, the new details will be delivered (although this behavior may be altered by specifying a deliver rule when associating the template with a service or device). This may consist of the activation and/or deactivation of features, depending on the nature of the changes. Whenever configuration details are delivered to a device, those details are recorded in the *database of record* for that device.

⚠ **Caution:** When building templates, care should be taken to ensure that templates that are likely to be configured for on change delivery (configured from the Services menu item and Manual Override tab for devices) do not include values that will change frequently, such as some random value or a comment that has a timestamp for when the configuration content was generated. Having such values could have the unintended effect of the configuration always being delivered, although no material changes have occurred.

To access the **Template** management screen, select **Configuration > Templates**. A list of currently defined templates are displayed in the **Template** list in the top pane. The list of templates can be filtered by Name and Description.

Adding templates

Templates can be added in two ways:

- Using New
- Using Import

Using New

To add a template

1. Click **New** on the **Templates** management screen. The **Viewing New Template** pane opens on the bottom of the screen.
2. On the **General** tab,

   a. Select a **Realm** from the drop-down list.

   b. Enter a Name for the new template.

   c. Select the **Apply Method**.

   d. If required, select the **Remove Method**. **Remove Method** must be set to a value other than **None** to activate the **Remove Settings** tab.

> **Note:** **Realm**, **Name**, and **Apply Method** are mandatory, while the other fields in this tab are optional.

3. On the **Conditions** tab,

   a. Select the desired expressions from the **Insert Expression** drop-down list.

   b. In the **Expression** text box, click expression link to open the Edit Expression dialog box.

   c. In the **Edit Expression** dialog box, make the necessary changes and click **Ok**.

4. On the **Apply Settings** tab, fill the appropriate details in the form that is displayed for the method specified on the General tab. For details, see Configuration Methods.
5. On the **Remove Settings** tab, fill the appropriate details in the form that is displayed for the method specified on the General tab. For details, see Configuration Methods.
6. Click **Save**.

Using Import

To import a template

1. Click **Import** on the **Templates** management screen and select the file to be imported.

   Note: Files with .xml extension can only be imported.

   The **Editing New Template** pane is displayed at the bottom of the screen.

2. Modify the options on each tab of the **Editing New Template** if required.
3. Click **Save**.

   The new template gets added and is displayed on the **Template** management screen.

Copying existing templates

You can create a new template by copying an existing template and modifying it to suit your requirements. To copy an existing template to use as the basis for a new template:

1. Select the template that you want to copy from the **Templates** management screen and click **Copy**.

   Note: The **Copy** button is disabled if a new template is being created, or the existing template has already been copied.

   The **Viewing New Template** pane opens on the bottom of the screen.

2. On the **General** tab, enter a name for the new template.
3. Review all the options in each tab of the **Viewing New template** pane and modify as required. For details, see Viewing and modifying templates.
4. Click **Save**.

Deleting templates

To delete a template:

1. Select a template from the **Template** list in the top pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

When a template is deleted, any **Remove Settings** that have been configured for the template will be executed the next time the configuration synchronization action is executed for the devices that were previously configured with the deleted template.

Viewing and modifying templates

To view a template, select the appropriate template record from the **Template** list in the top pane. Its details are displayed in the following tabs of the **Viewing Template** pane at the bottom of the screen:

- General
- Conditions
- Apply Settings
- Remove Settings

General tab

The General tab contains the following fields:

- **Realm**. The realm is chosen when the template is created. It cannot be modified. This template will only be available to services and devices in the same realm.
- **Name**. A name for this template.
- **Description**. A description of the template. This is an optional field.
- **Apply Method**. This field specifies how the configuration details will be defined.
- **Reboot after Apply?** If this check box is selected, a reboot command will be sent to the device after this template is applied. Synchronization of configuration will continue to subsequent templates (if any) following the reboot.
- **Remote Method**. This drop-down list allows you to configure how the actions carried out by Apply Settings are reverted.
- **Remove before Reapply?** In some situations, it may be necessary to remove the old configuration before reapplying a template due to a change in the configuration content. This check box is used to enable this behavior. When selected, Remove Settings are executed before executing Apply Settings for a template that had previously been applied to a device.

Conditions tab

The Conditions tab is used to specify conditions that must be met to apply this template to a specific device. Conditions are used to ensure that the template is only applied to devices that are technically capable of receiving this configuration. For instance, if the configuration contains vendor specific parameters, then a condition should be used to limit its application to a certain set of hardware or firmware. A template that does not have any conditions defined can potentially be applied to all devices.

For details on defining a set of conditions that match a device, see Condition Editor.

Tip: Additional conditions may be specified when assigning a template to a service (see Templates tab), which are specific to the service.

Apply Settings tab

The Apply Settings tab contains the settings used to apply a configuration to a device. The fields available on this tab depend on the Apply Method selected on the General tab. For details, see Configuration Methods.

Remove Settings tab

The Remove Settings tab contains the settings that are used to remove configuration from a device, usually reversing the effects of the configuration defined in the Apply Settings tab. The fields available on this tab depend on the Remove Method selected on the General tab. For details, see Configuration Methods.

Exporting Templates

The templates can be exported as .xml file.

To export a template

1. Select the template to be exported from the **Templates** management screen.
2. Click **Export**.

The selected template gets exported as .xml file.

Configuration methods

A template consists primarily of configuration details that can be used to apply changes to a device, and optionally to remove those changes from a device. The exact content of a configuration detail depends on the configuration method chosen for the template. The following four configuration methods are provided by default:

- **Parameter Groups** contain changes that are to be made to one or more data models supported by the device. These changes can consist of parameter sets and unsets, notification enabling and disabling, and setting and removing access permissions. These changes can be performed using a parameter setting mechanism, such as the CWMP SetParameterValues or SetParameterAttributes requests. For details, see Template Method: Parameter Group.
- **Script Files** are text files that contain (typically) vendor-specific configuration information. In addition to device configuration details, these files may also contain a Velocity script, which will be processed by the template engine before being delivered to the device. This allows for some dynamic content within the files, including the use of attributes. These files are sent to devices via a file transfer mechanism, such as the CWMP Download request. For details, see Template Method: Script File.
- **Static Files** are proprietary files that contain vendor-specific configuration information, typically in a non-text format. The files that are available to templates are configuration files managed through the Device Files menu option. These files are sent to devices via a file transfer

mechanism, such as the CWMP Download request. For details, see Template Method: Static File.

- **Software Modules** are typically applications that can be installed onto end-user devices. This method allows a software module to be associated with a service. That is, the application is installed when the service is subscribed and uninstalled when the service is canceled. For details, see Template Method: Software Module.

Template Method: Parameter Group

The Parameter Group configuration method allows a set of commands to be configured to manipulate the data model of a device. The changes can consist of adding and deleting objects, setting parameters, enabling and disabling notifications, and setting access permissions.

- When **Parameter Group** is selected from the **Apply Method** drop-down list on the General tab, the Parameter Group screen is displayed on the Apply Settings tab.
- When **Parameter Group** is selected from the **Remove Method** drop-down list on the General tab, the Parameter Group screen is displayed on the Remove Settings tab.

The Parameter Group screen consists of the following:

- **Data Models** pane
- **Current Commands** table
- **Group similar set commands?** drop-down list box
- **Delete** and **Save** buttons

The **Data Models** pane displays a list of available data models in a drop-down list. Click data model to view its details. The details are displayed in a tree structure. The list can be filtered by Parameter Name.

The **Current Commands** table displays a list of commands associated with this template. To add a command to the list, select an object or a parameter from the **Data Models** pane and drag it to the **Current Commands** table.

By default, the **Operation** column is set to **Set Parameter** for parameters and **Add Object** for objects. However, you can change it as required. The available options are as follows:

- For Parameters: Set Parameter/Unset Parameter/Set Notification/Set Access List
- For Objects: Add Object/Delete Object/ Set Notification/Set Access List

If a value is required, an input box appears in the **Value** column. The value may contain Velocity scripting, providing access to the details of the device being configured.

If a data model object or parameter is chosen that contains one or more indexes, a drop-down box is provided for each index allowing you to specify the method of choosing the index. The available options are as follows:

- Create new index. This option will cause the device to choose a new index the first time the template is applied to the device.
- Prefer index. This option will attempt to use the specified index. If the index does not already exist on the device, you can create a new one the first time the template is applied. However, the device picks the actual index number. So, the actual index may not be the one that you specify in this field.
- Require index. This option will attempt to use the specified index. If the index does not exist, the template will fail to be applied.

Beside the drop-down list, there are two input fields.

- The first field is only applicable to Prefer index and Require index. It is either an explicit index number or a reference to a previously specified index by name.
- The second field is an optional name to associate with this index, so that it may be used in specifying the preferred or required index value in subsequent commands.

To remove a command, select it from the **Current Commands** table and then click **Delete**.

The **Group similar set commands?** drop-down list has the following options:

- **Use Individual RPCs**. This options causes each command in the template to be executed using an individual RPC to the device. This results in reduced performance due to the overhead incurred for each RPC call, but may be required for some devices and configuration settings.
- **Combine Adjacent RPCs within this configuration**. This option aggregates multiple commands into single RPC calls, within the confines of a single Parameter Group template, not across multiple Parameter Group templates that are associated with the same service or device.

The grouping logic works as follows: all AddObject commands and DeleteObject commands are sent as individual RPC calls to the device, as the underlying CWMP RPC call for those operations only accepts a single parameter. All consecutive Set Notification commands and Set Access List commands can be grouped together into a single SetParameterAttributes RPC call. This is because even with parameters that contain indexes, you must explicitly specify each index value.

The rules for grouping consecutive Set Parameter and Unset Parameter commands are slightly more complicated due to the business logic surrounding the rules for specifying indexes in parameters.

If the Set Parameter command includes either a CREATE NEW or a PREFER VALUE rule for the index, then that parameter will be handled separately the first time the template is applied to the device as follows:

- For CREATE NEW, an implicit AddObject operation is executed first, and then the value is set on the newly created parameter.
- For PREFER VALUE, the very first time the template is applied to the device, a GetParameterNames operation is executed first to determine if the preferred index value exists on the device. If it does not, an AddObject operation is applied then the SetParameterValues operation is used to set the parameter.

If the GetParameterNames operation determines that the index already exists on the device, a SetParameterValues operation can be used to set the value without having to issue an AddObject operation to the device. Once the template has been applied, Service Gateway records the index values that were used. Consequently, in further attempts to apply the template, the index values are known. As a result, Service Gateway does not have to issue either the GetParameterNames or AddObject operations as those Set Parameter commands are candidates to be grouped with other operations.

Any Set Parameter command where the parameter does not include any indexes or where the index rule is REQUIRE are candidates to be grouped with similar commands. All Unset Parameter commands require that you explicitly specify the index values, so they are also candidates to be grouped with other set value commands.

To summarize:

- AddObject and Delete Object commands cannot be grouped together.
- All consecutive Set Notification and Set Access List commands can be grouped together into a single SetParameterValues RPC call
- In general, all consecutive Set Parameter commands and Unset Parameter commands can be grouped together into a single SetParameterValues RPC call. The one exception to this is the first time the template is applied to the device. In that case, all Set Parameter commands that contain index rules of either CREATE NEW or PREFER VALUE cannot be grouped as additional RPC calls are required before the parameter value can be set.
- **Combine SetParameterValues across configurations**. This option follows the logic similar to the preceding option, but further minimizes the number of RPC calls when delivering mutiple

templates. When multiple templates to be delivered to a device have this option specified, the application of these templates is deferred until the last template with this option enabled has been executed. The last template will be combined with the previously deferred templates, and RPC aggregation will take place across all templates. The order will be maintained with the exception of SetParameterValues calls, which will be further deferred until all other RPCs have been carried out, then executed last as one RPC call.

⚠ **Caution:** This option will defer CWMP parameter configuration resulting in templates not being delivered in the explicit order defined within a service. For example, if a service uses three templates to configure a device, the first and third being parameter based with this option set, and the second being a file download, the file download will actually occur before any of the parameter sets, since the first parameter template is deferred and combined with the third. If this is not desirable behavior, do not use this option to aggregate across templates.

Template Method: Script File

The Script File configuration method allows the content of a text-based configuration file to be specified with optional script elements using the Velocity scripting language.

- When **Script File** is selected from the **Apply Method** drop-down list on the General tab, the Script File screen is displayed on the Apply Settings tab.
- When **Script File** is selected from the **Remove Method** drop-down list on the General tab, the Script File screen is displayed on the Remove Settings tab.

The fields on this screen are as follows:

- **Filename:** The filename value is used for any file delivery mechanism that requires it. For example, the CWMP Download request must include the name of a file, which the device will ask for when it goes to actually transfer the file. You only need to specify the filename; the full path to the file will be generated automatically by the system when required.
- **Template:** Text area containing the actual script text. The contents would typically be vendor-specific. You can enter the contents directly into the text box or you can click the 🗐 icon and use the Script Editor. Template scripts can be run through the Velocity Scripting engine, allowing the content to be dynamic and take advantage of a variety of attributes.
- **Contains Script Elements** : This check box is used to tell the system whether the content should be run through the Velocity template engine or not. If this option is not enabled, the engine will not run the text through the Velocity template engine. This may be important if the device script language contains elements similar to those found within a Velocity script, but are not intended to be processed by the Velocity template engine.

Template Method: Static File

This configuration method allows a static file of any format to be delivered to the device.

- When **Static File** is selected from the **Apply Method** drop-down list on the General tab, the Static File screen is displayed on the Apply Settings tab.
- When **Static File** is selected from the **Remove Method** drop-down list on the General tab, the Static File screen is displayed on the Remove Settings tab.

This screen consists of a single drop-down list showing all defined configuration files for the specified realm.

Template Method: Software Module

The Software Module configuration method allows a software module to be installed or uninstalled from a device, as part of configuration.

- When **Software Module** is selected from the **Apply Method** drop-down list on the General tab, the Software Module screen is displayed on the Apply Settings tab.
- When **Software Module** is selected from the **Remove Method** drop-down list on the General tab, the Software Module screen is displayed on the Remove Settings tab.

The fields on this screen are:

- **Software Module** A drop-down of available software modules that are defined within the same realm as the template.
- **Operation**. Choose whether to install or uninstall the selected software module.
- **Load Dependencies**. For the Install operation, if this check box is selected and the selected software module depends on other software modules that are not already present on the device, they will be installed prior to installing the selected module.
- **Ignore Resource Limits**. For the Install operation, if this check box is selected, the resource availability checks (disk and memory) will not be performed on the device prior to installation.

7

Policy

Configure policies

Policies are used to define how the system reacts to incoming events and also to define scheduled maintenance activities. A policy definition consists of triggers , failure thresholds, filters, and workflow.

Policy triggers allow you to specify the triggers (event-based, timer-based, or both) to be used for the policy, failure thresholds allow you to specify the deactivation thresholds, and workflow allows you to view and manage the actions (regular actions and a failure action) in a workflow. Filters allow you to specify which devices can be acted on by a policy. The list of devices can be built using either conditions, a static list (CSV file), the policy history, or device list queries.

Policy activity is captured in the database and may be viewed via the **Policy Logging** screen.

For more information on policies, see:

- Managing policy definitions
- Managing device list queries
- Viewing policy logs

Managing policy definitions

To access the policy configuration management screen, select **Policy > Definitions**. The **Policy Definitions** management screen displays the trigger types for which policies are defined in a hierarchical tree structure in the **Policy** pane on the left of the screen. Nodes with arrows next to them represent items that can be expanded or collapsed. The list of policies can be filtered by Name.

To view the list of policies for a specific trigger, click trigger name. The number in parenthesis after each policy definition indicates the precedence value assigned to the policy.

Adding policies

Policies can be added in two ways:

- Using New
- Using Import

Using New

To add a policy to the system

1. Click **New** on the **Policy** pane on the left of the screen. The **Viewing New Policy** pane opens on the right of the screen.
2. On the **General** tab,

   a. Enter a **Name** for the policy.

   b. Select a **Realm** from the drop-down list.

   c. Select the desired **Policy Trigger**

If	Then
Policy Trigger is set to **Event** or **Hybrid**	On the **Event** tab: i. Select the event that must trigger the policy from the **Hook** drop-down list. ii. Specify the **Active Days** when a policy is to be triggered by selecting the appropriate option(s).
Policy Trigger is set to **Schedule** or **Hybrid**	On the **Schedule** tab: • Specify the **Active Days** when a policy is to be triggered by selecting the appropriate option(s).
Policy Trigger is set to **Schedule**	On the **Filter** tab: • Select a **Device List Generation** method and enter the required parameters in the sub-tab that is enabled based on the selected method.

   d. Specify other settings as required.

3. On the **Workflow** tab, configure at least one action by selecting and dragging it from the **Available Actions** pane to the **Workflow Actions** table.
4. Review all the options in each tab of the **Viewing New Policy** pane and modify as required. For details, see Viewing and modifying policies.
5. Click **Save**.

Using Import

To import a policy

1. Click **Import** on the **Policy** management screen and select the file to be imported.

   Note: Files with .xml extension can only be imported.

   The **Editing New Policy** pane is displayed.

2. Modify the options on each tab of the **Editing New Policy** if required.
3. Click **Save**.

   The new policy gets added and is displayed on the **Policy** management screen.

Copying existing policies

You can create a new policy by copying an existing policy and modifying it to suit your requirements. To copy an existing policy to use as the basis for a new policy:

1. Select the policy that you want to copy from the **Policy** tree on the left of the screen and click **Copy**.

   Note: The **Copy** button is disabled if a new policy is being created, or the existing policy has already been copied.

   The **Viewing New Policy** pane opens on the right of the screen.

2. On the **General** tab, enter a name for the new policy.
3. Review all the options in each tab of the **Viewing New Policy** pane and modify as required. For details, see Viewing and modifying policies.
4. Click **Save**.

Deleting policies

To delete a policy from the system:

1. Select the policy from the **Policy** tree on the left of the screen.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying policies

To view the details for an existing policy, click the desired policy definition record on the **Policy** pane. Its details are displayed in the following tabs of the **Viewing Policy** pane on the right of the screen:

- General
- Event
- Schedule
- Thresholds
- Filter
- Workflow
- Status

General tab

The General tab allows you to view and modify basic information about a policy. It has the following fields:

- **Name**. A name for the policy. The policy name can be changed at any time.
- **Description**. A description of the policy. This is an optional field.
- **Realm**. The realm within which this policy will operate.
- **Enable**. This option indicates whether the policy is enabled. A policy must be enabled in order for it to process devices.
- **Precedence**. The workflow engine uses the value specified in this field to help determine which policy should be executed for a device. When multiple policies match all other conditions (event type, filters, time window, and so on), the policy with the highest precedence (that is, the lowest number) will be the only one that is executed.
- **Policy Trigger**. This drop-down list provides the following options to define the trigger type:
  - **Event**. Selecting this option enables the Event tab and allows to configure event-driven triggers.
  - **Schedule**. Selecting this option enables the Schedule tab and allows to configure timer-driven triggers.

- ○ **Hybrid**. Selecting this option enables both the Event and Schedule tabs and allows to configure both event-driven and timer-driven triggers.

- **Process Device**. Provides the following radio buttons that control how the policy executes multiple times against the same device.
  - ○ **On every event**. Indicates that the policy will run every time an event comes in, even if it has already run against the same device.
  - ○ **Once per period**. Indicates that irrespective of the number of events that are generated, a device will only have the policy executed once per defined time period. The possible period values are: hourly, daily, weekly, and monthly.

Note: The value drop-down list is only enabled if this option is selected.

- **Completion Action**. This drop-down list is enabled only if the **Once Per Period** option is selected as the mode for **Process Device**. This list may be used to specify an action to perform once the policy period has been completed. This action will be performed every time the period ends. When you select an action, any action configuration options that are available will appear at the bottom of the display. For example, you can specify the Send Email action and configure it to return details about how many devices were processed during the period.
- **Devices Per Launch.** This value, as well as **Launch Threads**, is used to tune how aggressively a list of queued devices is executed. While the policy is active and there is a queue of devices waiting to be executed, up to the number of devices specified in this field will be executed every minute by default. The frequency at which queued devices must be executed can be changed by modifying the following setting in the encore.properties file:\

  ENCORE_SYSTEM_TIMER.4=ejb/com.supportsoft.servicegateway.policy.Policy
  ExecutionManagerHome,executePolicies,60

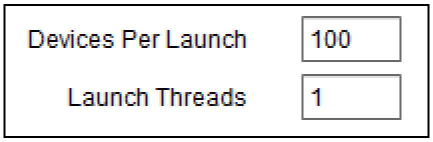
  The final value (60) is the number of seconds between each attempt, and that is the value that would need to be changed to alter the frequency with which devices are launched.

- **Launch Threads.** This field specifies the number of concurrent threads that are used to execute queued devices. This value can be increased if the number of executions for scheduled policies is not reaching its peak or not ramping up quickly enough.

Caution: While increasing launch threads can result in a faster ramp-up of devices being executed by a policy, it results in more threads, memory, and CPU being used on both the application server and database. Only increase this value if the database or application server resources are not already a bottleneck.

Parallel invocation of devices within a Schedule Policy

The **Launch Threads** option can be used to specify the number of parallel execution threads that are used to launch devices. By default, the value of **Launch Threads** is set to **1**. This indicates that each launch thread takes a list of one or more devices, and launches each of the devices serially. If **Launch Threads** is set to a value greater than **1**, the devices to be processed are divided evenly between the specified number of launch threads when the policy is run.



Devices Per Launch 100

Launch Threads 1

The **Devices per Launch** setting controls the maximum number of devices that can be initiated by a policy at any one time. However, the maximum number of devices that can be processed by a policy is determined by the **Event Concurrency Limit** for an event-driven policy and by the **Timer Concurrency Limit** for a scheduled or timer-driven policy.

Following is an example for an event-driven policy when the **Event Concurrency Limit** is set to 500 and **Devices per Launch** is set to 100. In this scenario:

- If 300 devices are currently in progress, then up to 100 devices can be launched the next time the policy tries to launch devices. While the event concurrency limit would allow Service Gateway to launch up to 200 more devices before the limit of 500 is reached, the **Devices per Launch** setting of 100 means that only 100 devices will be launched.
- If 450 devices are currently in progress, then only 50 more devices can be launched before the concurrency limit is met.

Event tab

The **Event** tab contains details about the event trigger to be used for the policy. This tab is enabled if the **Policy Trigger** is set to **Event** or **Hybrid**.

This tab contains the following fields:

- **Hook**. Specify the event that triggers the policy. For an explanation of the available events, see Policy Events.
- **Only Process Skipped Devices**. Typically, this flag only applies to hybrid policies. When flagged, the workflow will be run on the device only if the workflow engine attempted to run the policy against the device previously but the workflow was terminated because of a **STOP SKIP** operation.
  For a usage example, assume that a hybrid firmware upgrade policy has been defined and that a specific device is selected to be upgraded. However, the upgrade cannot proceed because the device is offline. The workflow action issues a **STOP SKIP** command when this is detected. Rather than wait until the next schedule window, you may want to trigger the upgrade as soon as you see the device again. For that, you may specify the **Boot** event and enable the **Only Process Skipped Devices** flag. The next time the device sends a **Boot** event, regardless of whether the timer portion is running or not, the policy will be executed.

- **Concurrency Limit**. This field specifies the maximum number of devices allowed to be active in the policy simultaneously.
- **Concurrency Limit Action**. This field specifies how an event is handled once the **Concurrency Limit** has been reached. It provides the following options:
  - **Ignore Event**. The event is discarded.
  - **Queue Indefinitely**. Events are queued and will be processed in the order that they were received when the concurrency limit drops back below the limit. However, new incoming events will still take precedence over queued events.
  - **Queue for X minutes**. As above, except that the event will only be queued for the specified number of minutes before it is discarded.
- **Concurrency Limit Action Workflow**. The action workflow type (**STOP PASS** or **STOP FAIL**) is returned when:
  - The event concurrency limit for the policy has been reached and the concurrency limit action is set to **Ignore**.
  - The **Concurrency Limit Action** is set to **Queue For** X **minutes**, and that time limit has been reached and the queued event is purged from the queue.
- **Active Days** and **Active Time**. Event-driven and hybrid policies can be configured only to be triggered by events on certain days and only during certain hours of the day. During days and/or times when the policy is not active, it will not be run even if the appropriate trigger comes in. These settings can be used to create maintenance windows, for example.

Note: The event hooks available to a user may be restricted on a per-user basis. See Policy Restrictions tab.

Schedule tab

The **Schedule** tab allows you to specify the timer trigger to be used for the policy. This tab is enabled if the **Policy Trigger** is set to **Schedule** or **Hybrid**.

This tab contains the following fields:

- **Active Days**. Timer-driven policies can be configured only to be active on certain days of the week. Select the days that the policy should be active.
- **Active Time**. Specifies the time window during each of the active days that the policy will be active.
- **Concurrency Limit**. Specifies the maximum number of devices that the policy will execute on simultaneously. For a hybrid policy,the maximum number of devices that the policy can process is the concurrency limit defined on the **Event** tab plus the concurrency limit defined in this field.

- **Filter Evaluation Period**. Specifies when the system should re-process device list filters. It has the following options:
  - **Once Per Period**. Indicates that filter evaluation occurs at the beginning of a new period and that the system will re-evaluate the filters once during the period length specified on the General tab (hourly, daily, or monthly).
  - **Once Per Active Window**. Indicates that filter evaluation occurs at the beginning of a new active window and that the system will re-evaluate the filters once during each active window, as defined by the **Active Days** and **Active Time** values.
  - **Never**. Indicates that the device filters will never be automatically re-evaluated; the list that is generated when the policy is approved is used for the lifetime of the policy or until it is manually regenerated.
- **Skipped Device Retry Time**. This specifies the minimum number of seconds since connectivity to a device was attempted and skipped before it will be attempted again. The default is 3600 seconds (1 hour).

Note: Skipped devices will not be processed or re-processed while there are Unattempted devices currently in the policy.

Thresholds tab

The **Thresholds** tab is used to configure a failure threshold for the policy.

A failure threshold can be used to disable a specific policy if too many devices are failing. For example, configuring a failure threshold for a firmware upgrade policy can prevent the system from damaging too many devices if there is a problem with the firmware image. Whenever a workflow for a device fails, the workflow engine will process the failure threshold (if one is defined). If it determines that the threshold has been crossed, it will disable the policy.

When a workflow terminates because an action generated a **STOP FAIL** operation, the workflow engine will apply that failure to the failure threshold if one has been configured. If the failure threshold (which is an absolute count of failures) is surpassed within a specific window, the failure action will be executed and the policy will be disabled. For example, if the failure count is set to 10 and the window is set to 20 minutes, the threshold will be triggered if more than 10 devices fail within 20 minutes.

- **Enable**. Used to enable or disable the threshold. When disabled, the other settings on this tab will also be disabled.
- **Failure Threshold**. Used to specify the total number of failures.
- **Failure Window**. Used to specify the time frame for failures, in minutes. The failure window is a moving window, so it applies to the past 'x' minutes. If the window is set to 20 minutes and the policy has been running for 30 minutes, the threshold is only applied to minutes 11-30.
- **Failure Action**. Used to specify the action to perform when the threshold has been reached.

Filter tab

The Filter tab is used to configure which devices will be acted upon by a policy. This tab provides four sub-tabs for specifying the devices that are permitted to be executed by the policy, as follows:

- **Conditions**. Allows devices to be specified using dynamically evaluated conditions.
- **CSV**. Allows devices to be specified using a static list (CSV file).
- **Device List Query**. Allows devices to be specified by selecting a query from the list of queries configured in the **Device List Query** management screen.
- **Policy History**. Allows devices to be specified by referencing the results of another policy.

The filter type to be used is specified via the **Device List Generation** drop-down list.

The **Generate Device List Upon Save** check box is used to initiate the device list generation process when the policy is saved.

Note: This is not applicable to event-driven policies.

Conditions

Selecting **Conditions** from the **Device List Generation** drop-down list enables the Conditions tab in the lower right pane. This tab allows an arbitrary boolean expression to be specified.

- For event-driven policies, this expression is evaluated against the current state of the database when the event arrives.
- For hybrid and scheduled policies, the conditions are used to determine the device list, whenever the device list is generated.

For details on how to configure conditions, see Defining Conditions.

CSV

Selecting **CSV** from the **Device List Generation** drop-down list enables the CSV tab in the lower right pane. If you have a list of devices stored in a text file, browse and select the file. Its contents will be loaded into the Device List text box where it can be edited as necessary. Alternatively, the CSV content can be pasted or typed into the text area.

Note: The CSV content should provide one device per line, with the first field of each line being an identifier for a device or subscriber.

When you specify CSV as the **Device List Generation** method, the **Device List Key** drop-down is enabled. A device list can contain a variety of information, such as a line consisting of several comma delimited values linked to the same record - address, phone number, billing number. So, this drop-down list is used to specify what data the first column represents so that the system can search for devices based on that value.

For example, the records you have may only consist of phone numbers. In that case, you enter (or load) in all of the data and then select **Phone Number** from the **Device List Key** menu. When the device list is generated, the system searches for all devices that are attached to subscriber records with each phone number in the list.

Device List Query

Selecting **Device List Query** from the **Device List Generation** drop-down list enables the Device List Query tab in the lower right pane. The **Device List Query** drop-down list allows you to select a query that can be used for building a policy device list.

Note: The queries that are available in the **Device List Query** drop-down list are defined in the **Device List Query** management screen (**Policy** > **Device List Queries**).

Policy History

Selecting **Policy History** from the **Device List Generation** drop-down list enables the Policy History tab in the lower right pane. This tab allows a different policy to be selected as the source of the device list for the current policy. The devices contained in the other policy may be further filtered by the status of the device in that policy, by selecting one or more of the **Device Status** check boxes as follows:

- **Select All**. This option will select or deselect all the other device status options, as described below.
- **Remaining**. This option will select all devices that have not yet been processed by the specified policy.
- **Succeeded**. This option will select all devices that have been successfully processed by the specified policy.
- **Failed**. This option will select all devices that were marked as failed when they were processed by the specified policy.
- **Skipped**. This option will select all devices that were marked as skipped when they were processed by the specified policy.

Workflow tab

The Workflow tab shows the actions that make up the workflow of the policy to be configured.

This tab displays a list of **Available Actions** on the left and a list of actions that make up the workflow and (optional) action to be used in case of failure on the right.

To add an action to the workflow, select and drag it from the **Available Actions** pane to the **Workflow Actions** table (or the **Workflow Failure Action** table in case of a failure action).

Note: The actions available to a user may be restricted on a per-user basis. See Policy Restrictions tab.

To change the order of the actions in the workflow, you can select and drag the actions to the correct row.

To delete an action from the workflow, select it and then click **Delete**. This is also applies to the failure workflow.

Clicking on an action in either the **Workflow Actions** or the **Workflow Failure Action** tables enables a set of tabs for configuring the action at the bottom of the display. The tabs for configuring an action are as follows:

- **Configuration**. This tab contains the configuration options specific to the policy action if any. For a list of the available actions and the configuration options for each, see Policy Actions.
- **Conditions**. This tab is used to specify conditions that must be met for this action to be executed. If the conditions are not met, the action is not executed. The workflow may or may not continue, depending on the setting of the **The policy action filters do not match the device.** result criteria on the Workflow Operations tab.
- **Workflow Operations**. This tab allows a workflow operation to be configured for every possible result of the action execution, which the workflow engine uses to decide how to proceed after the action is complete. There is also a check box to specify whether or not the result can trigger the action retry mechanism. The possible workflow operations are as follows:
    - **CONTINUE**. Continue with the next action if there is one.
    - **STOP FAIL**. Stop processing the workflow and treat the device as if it has failed. If a workflow failure action has been defined, it will be run. The failure also gets handled by any configured failure thresholds.
    - **STOP PASS**. Stop processing the workflow and treat the device as if it is completed successfully.
    - **STOP SKIP**. Stop processing the workflow and treat the device as if it was skipped (that is, it will be retried at a later time).

While most of the available results will be specific to the policy action, the following results are present for all actions:

  - **The policy action is not enabled**. This result is returned if the action has been administratively disabled.
  - **The policy action filters to not match the device**. This result is returned if the expression on the Conditions tab does not evaluate to **TRUE**.
  - **The policy action has timed out**. This result is returned if the workflow engine detects that an action has been in progress longer than the **Policy Action Timeout** value configured in system preferences.

- **Retries**. This tab configures the number of retries and the time between retries. Only those actions results that have the **Retry?** check box selected on the **Workflow Operations** tab will result in a retry.

Status tab

The Status tab displays the current status of an existing policy and provides a means to control the status.

This tab contains the following fields:

- **Policy Status**. The possible status values are as follows:
    - **CONFIGURED.** The policy has been defined with all the required settings, including device list criteria and workflow actions. However, the device list has not yet been generated.
    - **PENDING**. The same as **CONFIGURED**, except that the device list has been generated.
    - **APPROVED**. The same as **PENDING**, except that a system operator has clicked the **Approve** button. Once a policy has been approved, it can be executed.

  Once a policy has been approved, the status will reflect that. If you want to unapprove a policy, click the **Unapprove** button.

  Scheduled policies also provide the option to manually start the policy against the currently defined list of devices. This will run the policy regardless of the active window settings. There is also the option of stopping a running policy by clicking the **Stop** button.

- **Devices in Progress**. This displays the count of devices that are currently being executed by the policy.
- **Devices Queued in Backlog**. This displays a count of the devices currently queued due the event concurrency limit having been reached for an event-driven policy. When this count is greater than 0, a button to clear the current backlog will be available.

Exporting Policies

The policies can be exported as .xml file.

To export a policy

1. Select the service to be exported from the **Policy** management screen.
2. Click **Export**.

The selected policy gets exported as .xml file.

Policy events

A system can have two main sources of events as follows:

- CWMP Inform messages
- Internally-generated events

Inform messages typically contain an array of one or more CWMP events, such as **Bootstrap**, **Boot**, **Periodic**, and **Value Change**. These CWMP events are mapped to system events. Some events, such as activation, are generated by the system under specific conditions, usually while processing other events.

When an event is triggered, it is added to an event queue for the device that triggered it. If another event is triggered for a device while an event is already being processed, it will simply be added to the queue.

Following is a list of CWMP events:

- The **Bootstrap** event maps to the **CWMP BOOTSTRAP** event. A device will typically send this event under the following conditions:
  - The device is connecting to the network for the first time.
  - The CWMP ACS URL has been changed.
  - After a factory reset.

  This event triggers configuration synchronization for the device.
- The **Boot** event maps to the **CWMP BOOT** event, which is generated whenever the device boots up (power on, reboot command, and so on). An Inform message with a **Bootstrap** event may or may not also contain a BOOT event.
- The **download request** event is generated when the system receives a **CWMP REQUEST DOWNLOAD** request from the device.
- The **kicked** event is generated when the system receives a **CWMP KICKED** request from the device.
- The **periodic** event maps to the **CWMP PERIODIC** event. This event is generated by the device at a configured interval if periodic informs have been enabled.
- The **scheduled** event maps to the **CWMP SCHEDULED** event. If the device supports the **CWMP ScheduleInform** request, the device will generate this event at the time specified in the request.
- The **value change** event maps to the **CWMP VALUE CHANGE** event. This event is generated whenever certain parameter values flagged for notification (forced, passive, or active) have been modified by an entity other than the ACS. All of the parameters contained within the parameter list in the Inform will be passed along to the action for processing.

In situations where a CWMP Inform contains multiple events, they will be queued up and processed by the workflow engine in the following order:

1. Bootstrap
2. Boot
3. Value Change
4. Periodic
5. Scheduled

Following is a list of internally-generated events:

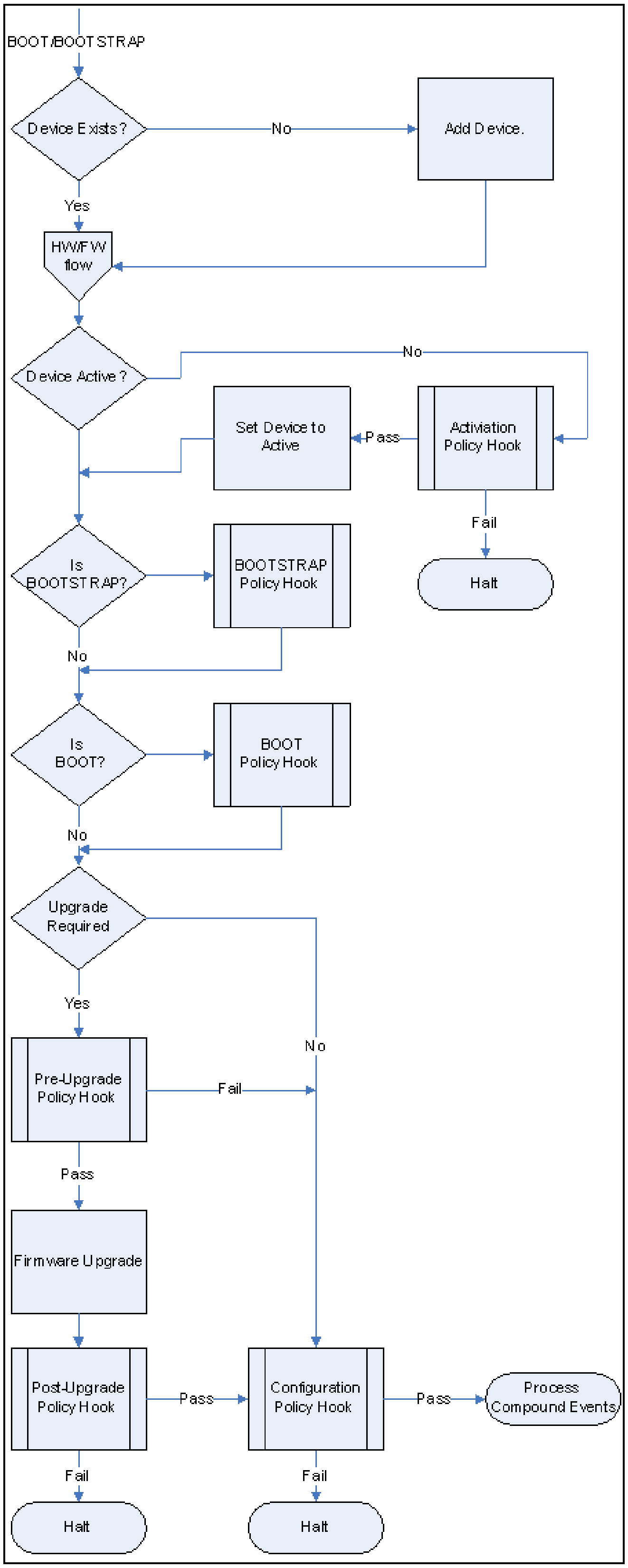
- The **activation** event is generated if the device is not flagged as being active when the workflow engine processes a **Bootstrap** or **Boot** event. The engine will then look for an appropriate activation policy and, if found, run it.

> **Note:** All devices added to the system, manually or through the ACS, are flagged as **Inactive**. Once the device has successfully been processed by an **Activation** policy, the device is marked as **Active**. Only an event from a device that has been successfully processed by an **Activation** policy can be processed by other policies.

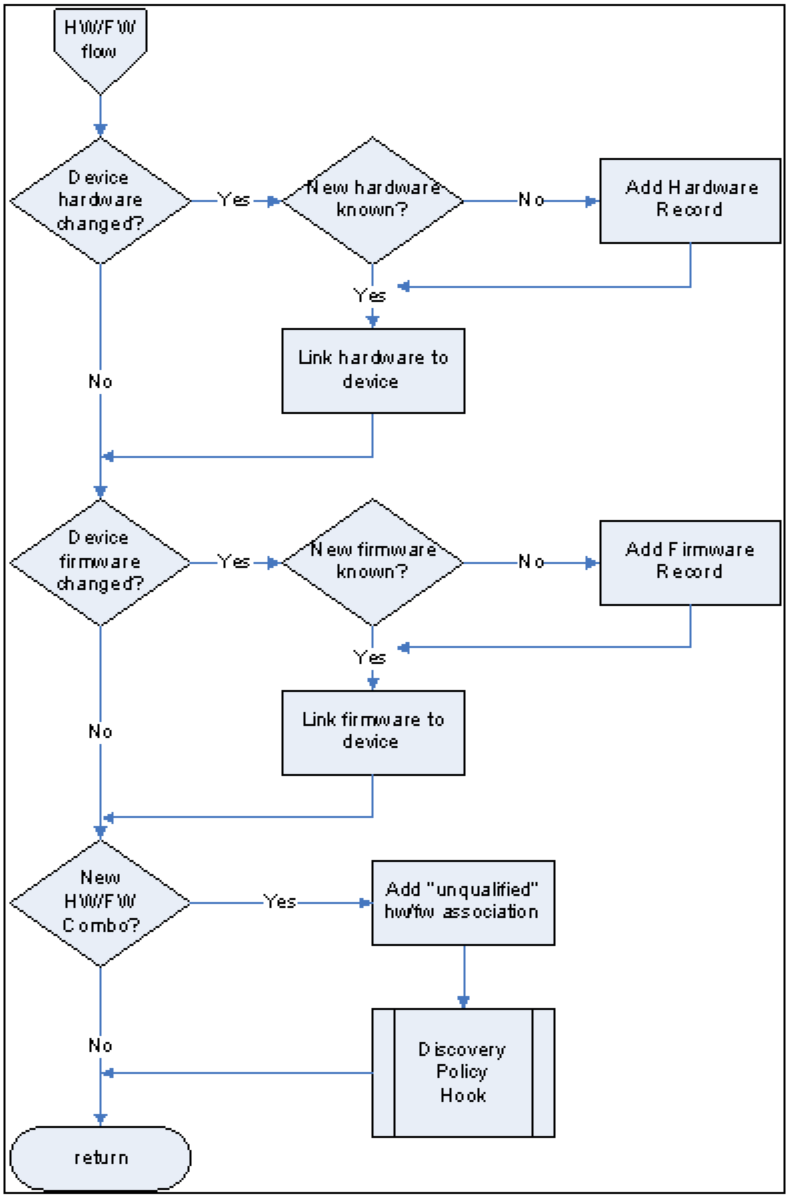
- The **configuration** event is generated when a **Boot** or **Bootstrap Inform** event is handled, but only if the device has been activated. For details, see the Boot and Bootstrap flow section.
- The **discovery** event is generated when the workflow engine processes a **Bootstrap** or **Boot** event. While processing, it will check to see if the hardware and firmware combination presented by the device is a known combination. If it is a new combination, the workflow engine will generate a discovery event. The engine will then look for an appropriate discovery policy and, if found, run it.
- The **pre-upgrade** event is generated as part of the built-in workflow for **Bootstrap** and **Boot** events. This internal workflow performs a check to see if a firmware upgrade is required for the device. If it is, the workflow engine will look for an appropriate pre-upgrade policy and run it before performing the actual upgrade.
- The **post-upgrade** event is generated as part of the built-in workflow for **Bootstrap** and **Boot** events. If the workflow performs an automated firmware upgrade, the workflow will look for an appropriate post upgrade policy and run it after performing the actual upgrade.
- The **timer-driven** event is generated if a policy is configured with a schedule. The system will generate this event when the date and time match the conditions configured in the schedule.

Boot and Bootstrap flow

Boot and **Bootstrap** events trigger a special workflow that may perform device registration, activation, and an automatic firmware upgrade (which is not the same as using the firmware upgrade action in a policy), along with the workflow that has been defined for the Bootstrap and/or Boot event. The following flowchart shows what the workflow engine will do when it receives a Bootstrap and/or Boot event:


BOOT/BOOTSTRAP
Device Exists?
No
Add Device.
Yes
HW/FW flow
Device Active?
No
Set Device to Active
Pass
Activation Policy Hook
Fail
Halt
Is BOOTSTRAP?
BOOTSTRAP Policy Hook
No
Is BOOT?
BOOT Policy Hook
No
Upgrade Required
Yes
No
Pre-Upgrade Policy Hook
Fail
Pass
Firmware Upgrade
Post-Upgrade Policy Hook
Pass
Configuration Policy Hook
Pass
Process Compound Events
Fail
Halt
Fail
Halt

The HW/FW Flow placeholder in the above diagram expands as follows:



Policy actions

Actions are plug-in modules that perform a specific task, such as probing a device, sending an e-mail, or executing a firmware upgrade.

For any specific action, there can be two sets of configuration details:

- The first set, which not all actions provide, is responsible for configuring how the action will work or the results that it will produce, such as the contents of an e-mail address or how to determine which firmware image to use for an upgrade.
- The second set, which is required, is used to map action-specific result codes (generated by the action when it runs) into workflow-specific operations (for example, mapping a device communication error into **STOP FAIL**).

CWMP Configuration Backup

This action retrieves the configuration file from a device using **Upload RPC**. You can perform the following on the **Configuration** tab:

- Provide a reason for the backup in the **Reason for backup** field. This reason is displayed in the list of files on the Devices: Backups tab.
- Flag the configuration file as the Last Known Good Configuration. If this option is selected, the backup is flagged as the **Last Known Good**. This backup configuration file will be used as the default file when restoring a configuration.

CWMP Configuration Restore

This action sends a previously backed up configuration file to a device using **Download RPC**. The backup flagged as **Last Known Good** is delivered. The Configuration tab for this action allows you to specify the following options:

- **Use most recent backup if Last Known Good configuration not found**. Select this check box to fall back to the most recent backup if a Last Known Good backup is not available for the device.
- **Lock device configuration upon restore**. Select this check box to lock the device configuration upon restore, so a subsequent configuration synchronization does not overwrite the restored configuration.

CWMP Configuration Snapshot

This action invokes the CWMP object cache capture and saves a snapshot of the current device configuration as determined by a merge of the live interrogation of the device and the current DBoR. This action can be used, for example, in a policy which periodically saves a last known good configuration snapshot of a device configuration if the device passes a diagnostic test.

The CWMP object cache capture involves determining which data models a device supports and then checking the data model definition in the system for those supported models for all parameters and objects that have the **cache values** flag enabled.

The Configuration tab for this action has a **Description** text box that allows you to enter a description that is saved with the snapshot

CWMP Data Model Capabilities Discovery

This action issues a set of CWMP requests to the device, as defined by the data model capability test cases, to determine specific conditions regarding the data model it supports. The test cases determine what objects and parameters to retrieve and what evaluations to perform on them. If the tests evaluate to true, the specified capability will be associated with the firmware and/or hardware (as defined by the test case) of the device. See the Data Model test case section for more information.

CWMP Factory Reset

This action sends a factory reset to a device.

CWMP Get Parameter Values (Attribute Storage)

This action retrieves one or more parameter values from a device and stores them in attributes on the device records.

The **Configuration** tab for this action has the following tabs:

- **General**. Allows you to specify the following:
  - **Overwrite Existing Values**. Determines if a value of an attribute must be overwritten with the value from the parameter.
    - If this check box is selected, it will overwrite the value of an attribute if that attribute is already associated with the device.
    - If this check box is cleared, then the attribute value is not overwritten.
  - **Walk Parameter Tree**. Determines how parameter values of indexes are retrieved from the device:
    - If this check box is selected, multiple calls are made to the device, iterating through each branch of the parameter tree. This results in more round-trips to the device, but may reduce the overall bandwidth and device CPU requirements.
    - If this check box is cleared, an entire section of the device's parameter tree is retrieved in a single operation.

- **Parameter Mappings**. Specifies the parameters to query on the device, and the database table columns those parameters will be stored in. These mappings are listed in the table displayed on this tab.

  To delete any existing mappings, select the mapping from the table and click the **Delete** button that is located at the upper right of the table.

  To add new mappings to the table, you must populate the **Parameter Name** and **Attribute Name** fields located below the table, and then click the **Add** button.

  - **Parameter Name**. The parameter name to query on the device. When you click this field, the **Data Model** tree is displayed, where you can then select the parameter to query. If the selected parameter includes any indexes, additional fields will be displayed so that the index values can be specified.
  - **Attribute Name**. The attribute that will be used to store the value queried from the specified parameter. When you click this field, the **Attributes** tree is displayed, where you can select the attribute that will be used to store the parameter value. If the selected attribute is a complex attribute, an additional field will be displayed so that the index value can be specified.

CWMP Get Parameter Values (Database Storage)

This action retrieves one or more parameter values from a device and stores them in a new database record, in a user defined table.

The **Configuration** tab for this action has the following tabs:

- **General**. Allows you to define the following values:
  - **Datasource**. The JNDI name of the datasource where the queried parameter values will be stored. This field defaults to **jdbc/com.supportsoft.encore.default_datasource**, which is the datasource used by Service Gateway. If you wish to store the parameter values in a different database, then the JNDI name for that datasource must be used instead.
  - **Table Name**. The name of the database table where the parameter values will be stored. While the intention is for operators to define their own tables to store this information, Service Gateway includes a generic table, SPRT_SG_ACT_CWMPGET_STATS, which can be used instead.
  - **Base Object**. The root object that contains the parameters that will be queried from the device. Only parameters that are immediate descendants of this base object can be queried. If the selected base object includes any indexes, additional fields will be displayed so that the index values can be specified.
  - **Walk Parameter Tree**. Determines how parameter values of indexes are retrieved from the device.

  - If this check box is selected, multiple calls are made to the device, iterating through each branch of the parameter tree. This results in more round-trips to the device, but may reduce the overall bandwidth and device CPU requirements.
  - If this check box is cleared, an entire section of the device's parameter tree is retrieved in a single operation.

- **Parameter Mappings**. Specifies the parameters to query from the device, and the attributes those parameters will be stored in. These mappings are listed in the table displayed on this tab. It also defines the fields (the columns from the table specified on the General tab) that will be used to store the parameter values. These mappings are listed in the table displayed on this tab.

  To delete any existing mappings, select the mapping from the table and click the **Delete** button that is located at the upper right of the table.

  To add new mappings to the table, select and drag a parameter from the **Data Models** tree to the **Current Parameters** table. After the parameter is added to the table, specify the field (column) name where the value will be stored by clicking in the **Field Name** cell for that row in the table, and typing in the column name.

- **Variables Mappings**. Allows you to map additional variables to columns in the database table. The variables that can be mapped appear in the **Available Variables** table, while the existing mappings appear in the **Current Variables** table.

  To delete any existing mappings, select the mapping from the **Current Variables** table and click the **Delete** button that is located at the upper right of the table.

  To add a new variable, select and drag the desired variable from the **Available Variables** table to the **Current Variables** table. After the variable is added to the **Current Variables** table, specify the field (column) name where the value will be stored by clicking in the **Field Name** cell for that row in the table, and typing in the column name.

  The following table lists the variables that can be selected.

Variable	Description
Timestamp	The current date and time, specified as a String. This allows the value to be stored in a database column defined as a character type, such as VARCHAR.
Timestamp as Date	The current date and time, specified as a Date object. This allows the value to be stored in a database column of type DATE.
Device Database ID	The primary key ID of the device.
Device MAC Address	The MAC address of the device.
Device IP Address	The IP address of the device.
Device Unique ID	The unique ID string of the device.
Base Object	The base object defined on the General tab.

Variable	Description
Object Index	The parameter that was queried.
Execution Group	The GUID that is generated when this information is stored in the database.
Policy Execution GUID	The GUID that identifies the current run (Period) of this policy.
Policy GUID	The GUID that identifies this policy that processed this device.

CWMP RPC Method Capabilities Discovery Action

This action issues a CWMP GetRPCMethods request to the device. The list of methods returned by the CPE will be checked with the existing RPC method capability test cases to see which capabilities will be associated with the firmware and/or hardware (as defined by the test case) of the device.

CWMP Reboot

This action sends a reboot command to a device.

Data Model Test

This action runs various tests against the data model supported by a device, such as testing for the existence of a particular parameter (or set of parameters) or specific parameter values.

The Configuration tab for this action has the following tabs:

- General.
    - **Description** . This text box allows you to enter a description of the workflow action.
    - **Walk Parameter Tree**: Determines how parameter values of indexes are retrieved from the device.
        - If this check box is selected, multiple calls are made to the device, iterating through each branch of the parameter tree. This results in more round-trips to the device, but may reduce the overall bandwidth and device CPU requirements.
        - If this check box is cleared, an entire section of the device’s parameter tree is retrieved in a single operation.
- Tests. Configuration for this action is exactly the same as for data model test cases for capabilities (see Data Model Discovery under Capabilities for more information).

Firmware Upgrade

This action will attempt to perform a firmware upgrade on the device.

For configuration, the **Firmware** drop-down menu contains a list of all firmware records for the realm and the **Use Recommended Firmware for Hardware** and **Use Upgrade Path for Firmware and Hardware** options.

- When configured to use the recommended firmware for the device hardware, the system will look for a recommended firmware version for the hardware. If there is a firmware file associated with that firmware/hardware combination, it will perform the upgrade. If such a firmware image file cannot be found, the action will return a result code of Firmware not available.

  When specifying a specific firmware from the drop-down menu, the system will attempt a firmware upgrade of the device provided that the hardware of the device is associated with the specified firmware record. In addition, the upgrade will only be performed if a firmware image file has been established for the firmware/hardware combination.

  Unlike the automated upgrade function, which will only automatically upgrade a device from an obsolete firmware to a recommended one, the firmware upgrade action will force the upgrade, regardless of which firmware is currently on the device and what the firmware/hardware association status might be.

- When configured to use the upgrade path for firmware or hardware, the system will follow the upgrade path that is defined for the hardware/firmware association in either the **Hardware** tab when viewing a firmware record (**Inventory > Firmware**) or on the **Firmware** tab when viewing a hardware record (**Inventory > Firmware**).

  If the device has firmware version x.y.z, and you have the associations defined on one of the specified tabs to upgrade that device to version x.y.w, then you can set the policy action to follow that path without having to select a specific firmware version in the action.

Forward Value Change to SNMP Manager

This action will parse the **VALUE CHANGE** events contained within a CWMP Inform message and pass the information to a third-party system via SNMP traps.

The **Configuration** tab for this action has the following tabs:

- **General**. Allows you to define the following values:
  - **Hostname**. Name of the SNMP destination host.
  - **Community String**. Community string for that host.
  - **Description**. An event description.
- **Parameter Filters**. Allows you to configure value change parameter filters.

If	Then
No filters are defined	All value change events are forwarded.
Filters are in place	Only those parameters matching the filters are forwarded.

To create a filter, select a data model object or parameter from the **Data Models** pane on the left and drag it to the **Current Parameters** table. Selecting an object will cause the filter to look for all parameters that are children to the object.

After specifying an object or parameter, you can then select a value test. The possible tests are as follows:

- **None**. No value tests will be performed. Using this option basically limits which value change events will be forwarded, without looking at the value itself.
- **Is Like**. Compares the value to a regular expression. If the value matches the regular expression, the filter passes.
- **Is Between**. Checks to see if the value falls between two specified values. If the parameter value is numeric and falls between the two values, the filter passes.
- **Is One Of**. Checks to see if the value matches an entry in an enumerated list of possible values. If the value matches an entry in the comma-separated list of values, the filter passes.

To remove a filter, select it from the **Current Parameters** table and click **Delete**.

Send Email

This action sends an email message to the specified recipient(s). The Configuration tab for this action contains the typical email fields to prepare and send a message: From, To, Subject, and Message.

Enter the appropriate values in these fields and click **Save** to associate an email message with this workflow action.

Full use of the Velocity template engine and tokens are available when configuring an email message. Unlike template parameter groups and script files, there is no option to pre-evaluate the email content using the Velocity engine.

Using Velocity Script in Send Email Action (for Policies)

Although the edit icon is not displayed to show the Velocity Script editor, velocity script can still be used in the **Send Email** policy action, in the **To**, **From**, **Subject**, and **Message** fields.

The **Send Email** action can be specified in several areas within a policy. Some velocity script tokens are applicable to all areas, while others are not. The following tokens are available in all places where the **Send Email** action can be specified in a policy.

Item	Property	Description
Policy	Name	The name of the policy.
	Description	The description of the policy.

Item	Property	Description
Policy Execution History	EndTime	The time that the policy ended.
	EndTrigger	The reason that the policy ended. Possible reasons are as follows: • there are no more devices to process • the policy period has ended • the policy was stopped by a user
	FailedCount	The total number of devices that have failed in this period.
	SkippedCount	The total number of devices that were skipped in this period.
	StartedBy	The user who started this policy.
	StartTime	The time when this policy period was started.
	StartTrigger	Specifies how the policy period was started. Possible values are as follows: • manually • by the timer • by an event
	StoppedBy	The user who stopped the policy.
	SuccessCount	The total number of devices that were processed successfully by the policy during this period.
	TotalCount	The total number of devices that were processed during this period. This value is the sum of the **FailedCount**, **SkippedCount**, and **SuccessCount**.

When the **Send Email** action is specified as either a **Workflow Action** or as the **Workflow Failure Action** on the **Workflow** tab, then all the tokens described in the Velocity Scripting section are also available.

Service Subscription

This action associates a specified service with the device. The **Configuration** tab for this action consists of the following elements:

- The **Action** radio buttons that can be used to add a service to a device or to remove a service from a device.
- The **Service** drop-down menu containing the list of available services within the realm.

As an example, this action can be used to set up a walled garden scenario for unknown devices. In this case, the service that is specified would be one that provides the configuration that is necessary to configure the device for a walled garden operation.

One or more services can be unsubscribed from a device by including the action multiple times in the policy workflow.

In addition to associating them with devices, services can also be associated with subscribers. All devices associated with a subscriber inherit any services that are associated with that subscriber, in addition to any services that are associated directly with the device. When evaluating conditions or Velocity scripts that reference services, the full list of services that apply to both the device and subscriber are used.

Software Module Update

This action allows a software module to be installed or removed from a device. The Configuration tab for this action has the following fields:

- **Software Module**. A drop-down of available software modules defined within the same realm as the template.
- **Operation**. Allows you to choose whether to install or uninstall the selected software module.
- **Load Dependencies**. For the Install operation: if this check box is selected and the selected software module depends on other software modules that are not already present on the device, they will be installed prior to the selected module.
- **Ignore Resource Limits**. For the Install operation: if this check box is selected, resource availability checks (disk and memory) will not be performed on the device prior to installation.

Synchronize Configuration

This action synchronizes the configuration for a device. It consults the service configuration and the DBoR for the device to determine if any new configuration needs to be sent down to the device. It will then instruct the system to perform whatever configuration changes are required.

Unconditional Result

This action returns a fixed result, which is configured via a drop-down menu on the Configuration tab. The possible results are:

- **Pass**
- **Skip**
- **Fail**

By default, these results are mapped to a similar workflow operation (that is, the Pass result code is mapped to the STOP PASS workflow operation). While it is possible to alter these mappings, it is not recommended to do so.

The **Delay (ms)** field allows you to specify the time (in milliseconds) that the policy action must wait before it sends the specified result.

Update CWMP Cache on Value Change

This action parses the **VALUE CHANGE** events contained within a CWMP Inform and uses the information to update the system's cache of CWMP parameter values for the device.

Update Database of Record on Bootstrap

This action clears the database of record (DBoR) for a device whenever it sends a CWMP Inform containing a BOOTSTRAP event. When a BOOTSTRAP is received, it is possible that none, some, or all its configuration has been cleared/reverted to factory defaults. By clearing the DBoR, the configuration synchronization action will attempt to redeliver all configuration details when it is next triggered.

The index cache is populated when the **Synchronize Configuration** policy action runs, and applies a **Parameter Group** template that includes indexes in the parameter names. This action clears the index cache for a device.

Managing device list queries

The **Device List Query** management feature provides a more flexible way to specify a device list for a policy. It allows you to define a query that meets your needs, while perhaps even involving custom database tables that are not part of the base product.

Device list queries are configured in the **Device List Query** management screen. These queries appear as options that can be used when defining a policy.

Note: The **Device List Query** management screen can only be accessed by administrators with ***Manage/View Policy Device List Queries*** and/or ***View Policy Device List Queries*** permissions.

! Important: The responsibility of writing efficient, high-performance queries lies with the administrator. If a query proves to be inefficient, it is up to the writer to ensure that any additional databases indexes are defined as necessary, and that the query is properly analyzed to ensure that it is high performing.

To access the **Device List Query** management screen, select **Policy > Device List Queries**. The list of queries is displayed in the top pane of the **Device List Query** management screen with the following details: Name, Description, and Realm.

The list of queries can be filtered by Name, Description, and Realm.

Adding queries

To add a query:

1. Click **New** on the **Device List Query** management screen. The **Viewing New Device List Query** pane opens at the bottom of the screen.
2. On the **General** tab, provide the following information:
   - **Realm**: Select the realm for the query from the drop-down list.
   - **Name**. Enter a name for the query.
   - **Description**. Enter a description of the query. This is an optional field
   - **Query**. Enter a query that can be used to build a policy device list. You can test if the query is valid by clicking the **Test** button. For details, see Testing the device list query.
3. Click **Save**.

Testing the device list query

You can test if your device list query is valid. That is, make sure that it returns the required value and that it is a SELECT query, as follows:

- Type the query in the **Query** text box and click **Test**.

If	Then
The query is valid	The **Test Device List Query** dialog opens with the result displayed in the **Test Results** text box. Click **Ok** to accept the query. ❗ **Important:** The query MUST return the UNIQUE_ID_STRING as the first column. The value returned in the first column of the query is used to select the device from SPRT_EC_DEVICE using the UNIQUE_ID_STRING column. **Note:** Up to 500 records are returned by a query (if the query returns more than 500 records, only the first 500 are shown in the **Test Results** text box.
The query is not valid	A pop-up dialog box opens with the returned error message. Click **Ok** to close the message.

Deleting queries

To delete a query:

1. Select one or more device list query records from the **Device List Query** pane.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Viewing and modifying queries

To view the details for a specific device list query record, select the desired record from the **Device List Query** pane. Its details are displayed in the General tab of the **Viewing <selected query>** pane at the bottom of the screen.

General tab

The General tab allows you to view and modify queries that can be used to build a policy device list. It has the following fields:

- **Realm**. The realm for the query. The query will be available to any policy that is in the same realm.
- **Name**. A name for the query.
- **Description**. A description of the query. This is an optional field.
- **Query**. A query that can be used to build a policy device list. You can test if the query is valid by clicking the **Test** button. For details, see Testing the device list query.

Viewing policy logs

The system logs a lot of information when policies execute. The log information includes a list of policies that were run, the time when the policies were run, the actions that were performed, and the results of those actions.

All the log information can be viewed on the logging screen. To access the **Policy Logging** screen, select **Policy > Logging**.

The **Policy Logging** screen consists of three sets of tables:

- The **Policy** display table appears at the top of the screen. It displays a list of all the policies in the system. The display consists of the policy name, the realm it is defined in, the trigger type, the current policy status, and the administrative status. The list can be filtered by Name. To view the details for a specific policy, select the desired policy from the table.
- The **Execution Log** table appears on the middle of the screen. Once you select a policy from the **Policy** display table, the execution log for that policy is shown in the **Execution Log** table. This table provides details for the policy each time it was run, including the start and end date and times (where appropriate) and how the policy was triggered. Statistics in this table include the number of devices that completed successfully, the number of times a device was skipped (including multiple skips of the same device), the number that failed, the number in progress, and the number that are remaining to be processed (including devices that have never been attempted and those that were attempted and skipped at least once). This is specifically useful information for timer-driven policies. Also included is information on how the policy might have ended if appropriate. For example, if a failure threshold was triggered, that information would be displayed in this table.
- The **Devices** table appears at the bottom of the screen. It displays details about the device and actions performed. Clicking a specific log entry displays the list of devices that were processed during that specific execution of the policy in the **Devices** tab. Information consists of the unique ID of the device, the IP address, start time, and the execution status. Clicking a specific device record in the **Devices** tab will show the actions that were executed, the action result code, and the workflow operation that was generated.

8

Configuring Reports

Configure reports

Reports are used to present data that is contained in the Service Gateway database or other relational databases. Reports can be run manually or according to a schedule that you specify. This section contains information on general report management techniques that can be applied to all reports. These techniques include running and modifying existing reports and creating new reports that meet your specific needs.

Reports generate times in IETF standard date format (that is, Mon, 25 Dec 1995 13:30:00 GMT+0430). Also, the HTML XSL transforms this date into the date format specified in the report definition if specified or the format specified in the global preferences. The output of this date is in the local time zone of the browser.

Note: The date format must meet the specifications of the **Datejs** open-source JavaScript Date Library.

Service Gateway comes with a set of default reports that can be used as they are, or modified to suit your needs, or used as a basis to create new reports. To see the complete set of default reports, go to **Report > Definitions** and expand the report group folders on the **Reports** pane on the left of the screen.

Contents

Managing report definitions

To access the **Reports** management screen, select **Report > Definitions**. The **Reports** management screen displays the reports in a tree structure in the **Reports** pane on the left. Reports can be organized into hierarchical groups. Nodes with arrows next to them represent items that can be expanded or collapsed. The list of reports can be filtered by Name.

Running a report

To run a report:

1. In the **Reports** pane, expand the category (folder) that contains the report that you want to run and select the report. Depending on the report that is selected, its details are displayed in the Viewing Report pane on the right.
2. Select the desired parameters. Each report contains a different set of selectable parameters. View the information on the right pane and make the selection depending upon what is presented on the screen.
3. Select the report format from the **view as** drop-down list. The list provides the following options: HTML, Graph, CSV, or XML. By default, the report format is HTML.
4. Click **Run Report**. The results are displayed in a new browser window.

Note: You can change the view for the report to any of the other acceptable formats from this browse window.

Adding reports

When creating a new report, it is recommended that you copy an existing report and modify it to suit your needs.

Use the following steps to copy and modify an existing report:

1. In the **Reports** pane, expand the category (folder) that contains the report that you want to run and select the report. Depending on the report that is selected, its details are displayed in the Viewing Report pane.
2. On the **XML** tab of the **Viewing Report** pane, select the XML code and then right-click and select **Copy**.
3. Click **New** on the **Reports** pane to create a new report.

4. On the **XML** tab of the **Viewing New Report** pane,

    a. Right-click and select **Paste** to paste the XML code that you copied previously into the current report.

    b. Replace the existing **Name** with the new report's name. This is the name that will appear in the Reporting menu. If you do not change this information, the new report will have the same name as the original report that you copied.

    c. Replace the existing **Description** and **Path**. The path information specifies the report's location in the **Reporting** menu. If you do not change the path information, the new report will be under the same heading/subheading in the menu as the report you copied.

    d. Modify the information in the **Query** section to specify the report parameters. Refer to the "Working with XML Reports" section for definitions and examples of XML report elements.

5. On the **Settings** tab, specify the **Realm Access**. The following options are available:

    - **None**. Specifies that this report will not be made available to any realm-constrained user.
    - **All**. Specifies that this report will be available to users associated with any realm in the system.
    - **Selected**. Makes this report available only to users in specific realms. Select this option and specify the realms that will have access to this report by dragging them from the **Available** list to the **Current** list.

6. Click **Save**.

To create a new report without copying an existing report as a starting point, follow the preceding instructions barring steps 2 and 4(a) (copying and pasting the XML code from an existing report).

Deleting reports

When you delete a report, the report is removed from the system and from the **Reporting** menu. To remove a report from the system:

1. In the **Reports** pane, select the report that you want to delete.
2. Click **Delete**
3. When asked for a confirmation, click **Ok**.

    The report is immediately removed from the **Reporting** menu.

⚠ **Caution:** Once you delete a report, you cannot recover it or any of its previously saved sets of results.

Viewing and modifying reports

To view a report, select the appropriate record from the **Reports** pane. Its details are displayed in the following tabs of the **Viewing Report** pane on the right of the screen:

- General
- XML
- Settings
- History
- Schedule

General tab

The **General** tab is not available when adding a report. It is only available for existing reports and allows a report to be executed in real-time.

This tab contains the description of the currently selected report, followed by any report parameters defined by the report. These parameters will vary from report to report. Any parameters required by a report will be indicated by a small arrow between the parameter name and the value.

To run a report, click **Run Report**. Once generated, the report is displayed in the selected format in a new browser window. The same report may be later viewed in a different format by accessing it on the **History** tab.

Note: When the report is run, Service Gateway will attempt to open it in a new window. If a pop-up blocker is used with the browser, enable it for the Service Gateway site to view the report results.

XML tab

The XML tab contains the actual XML-based definition of the report.

This section includes information about the elements that can or must be present in an XML report definition. For each element included here, you will find information about whether it is required or optional, as well as a list of acceptable attributes and elements.

<SPRTReport/> is the topmost element of the report XML definition and has the following required attributes.

<SPRTReport/>Attributes

Attribute	Description
id	A unique lowercase GUID without braces. A new identifier is created automatically when you click **New** or **Copy**.
version	A version string to indicate compatibility with the underlying database schema. At a

Attribute	Description
	minimum, the major version should be set to match the corresponding product version. Version strings should be in the **n.n.n.n** form and cannot exceed 20 characters.
standard	Indicates whether the report is a custom report or one shipped with the Platform software. Standard reports shipped with the product have standard="1". Reports with standard="1" are automatically replaced during software upgrades. Set standard="0" for all custom reports, so they will not be overwritten during software upgrades.
realtimeok	Indicates whether the report can be run interactively. Run interactively="1" and run via schedule only (not interactively)="0". By default, this value is "1", but if the report is known to take a long time to run or impacts production usage, set to "0".
hidden	Indicates whether the report is hidden and not shown to the user. By default, this attribute is **false**. If set to **true**, the report is not shown in the UI. This attribute is typically set to **true** for drill-down reports that should only be called by another report. To view reports that have this attribute set to **true**, the **Show Hidden Reports** preference (Administration > Settings > Preferences) must be selected.

<SPRTReport/> Elements

Element	Description
<Name/>	A short description suitable for display in the report tree. Name is limited to 200 characters. In practice, it is recommended that the name be kept even shorter for better usability.
<Description/>	A long description indicating the intent of the report, details on required parameters, and explanation of output. If the description includes XML reserved characters, it must be escaped using CDATA. There is no fixed limit to the description length.
<DateFormat/>	Customized date format for the report, overriding the **Date Format for Reports** preference. Format must adhere to the Datejs library format, as found at http://code.google.com/p/datejs/
<Path/>	A path indicating the default location of the report. Each folder element of the path should be separated by a slash, "/". The total path length is limited to 200 characters. In practice, avoid unnecessary levels of folders for better usability.
<Query/>	Contains the SQL query which will be run to generate the report. SQL variables from the <SqlVariable/> elements must be represented with the % sign around the name of the SQL Variable. This element must have at least one attribute set to true to indicate database vendor compatibility. For all but the simplest queries, this element should be escaped with CDATA tags. This element has the following attribute: • **oracle=**. Set to **true** if the query is compatible with Oracle.

Element	Description
	Note: Each database vendor attribute must be represented only once. One or more vendor attributes are required (**true**).
<SQLVariable/>	Represents a variable that will be substituted into the SQL query in the **<Query/>** element. Zero or more variables are required. This element has the following attributes: • **name**. The name of this variable. This parameter is not displayed to the user. This name should not have spaces or % symbols. A % symbol is automatically added to the start and end of the name and substituted in the query. For example, **SortOrder** will be substituted in the query where %SortOrder%is found. • **display**. A **display name** or **label** for the **<SQLVariable/>** that is being defined. Long explanations should be placed in <Description/> and not in this attribute. • **type**. One of the following values: ○ **edit**. A simple text field suitable for general data entry. ○ **datelist**. A selection list with pre-defined options, such as **Today**, **Yesterday**, or **Beginning of Q1**. The **Start of Fiscal Year** preference can be used to define what terms like **Beginning of Q1** actually mean ○ **dbselect**. A selection list with zero or more options based on the results of an SQL query defined in the **<SelectQuery/>** element. ○ **date**. A date entry field with a calendar control. ○ **datelow**. A date entry field with a calendar control that allows you to specify a date. It is used with the **datehigh** type (as a second SqlVariable) to specify a date range. It includes the time of day, which defaults to 00:00. ○ **datehigh**. A date entry field with a calendar control that allows you to specify a date. It is used with the **datelow** type (as a second SqlVariable) to specify a date range. It includes the time of day, which defaults to 23:59. ○ **datetime**. A date entry field that is similar to the **date** type, but includes a time as well as a date. ○ **dbedit**. A simple text field suitable for general data entry, but uses an SQL query (defined in **the <SelectQuery/>** element) to provide a default value. • **datacolumn**. This attribute is applicable when type is dbselect. Database column whose values are substituted in the query. • **displaycolumn**. This attribute is applicable when type is dbselect. Database column whose values are displayed as options descriptions.

Element	Description
	- **default**. The starting value for this variable when presented to the user or the value used when running the report automatically. Although not required, this attribute must always be present to avoid any missing variables. For date fields, defaults can be set to one of the following dynamic values. **Note:** The date parameter for the report will be an ANSI date (format of YYYY-MM-DD) without a time specification. ○ **Today**. The current date and time. ○ **Yesterday**. One day prior. ○ **Tomorrow**. One day in the future. ○ **Last Week**. Seven days prior. ○ **Week to Date**. The last Sunday, or start of the week as determined by the server. ○ **Last Month**. One month prior. In the event that the prior month has fewer days than the current day of the month, this value is the last day of the prior month. ○ **Month to Date**. The first day of the current month. ○ **Last Quarter**. One quarter prior. Like last month, the day of the month will be adjusted.
<**Column/**>	(Optional. Zero or one.) Use this element to hide columns and format the column headers. The text and any HTML formatting directives that you would like to display for the column headers must be enclosed between the <Column> and </Column> tags and should usually be escaped with CDATA tags. This element has the following attributes: - **name**. The column to hide or format the header. - **hidden**. If set to **true**, this column is not displayed in the HTML output.
<DSN/>	(Optional. Zero or more.) This element contains a DSN that points to a database where the report query is run. When the DSN element is absent, the report is run against the default database. Specifying a DSN element allows you to maintain your reports on one server and run them against databases on other servers. This element must have exactly one attribute set to **true** to indicate database vendor compatibility. The Reporting DSN priority is as follows (highest to lowest): 1. DSN element in the report itself. 2. **<DSN/> Attributes.** ○ **oracle**. Use "true" if the DSN is compatible with Oracle.

Element	Description
	○ **jndi**.The JNDI name for the datasource.
<DrillDown/>	(Optional. Zero or one.) Links a column in one report to a target report. Clicking on the link navigates the user to the target report. Parameters from the original parent report are passed to the target report according to the **<Parameter/>** element. This element has the following attributes: • **drillcol**. The database column name that is linked to the target report. • **report**. The GUID of the target report. • **display**. The text that is displayed when the user pauses over the **<DrillDown/>** link. • **<Parameter/>.** (Optional. Zero or more.) Specifies the parameters passed from the parent report to the target report. It has the following attributes: ○ **type**. The parameter type. Following are the valid values: ■ **column**. Column parameters are row values from the parent report. ■ **SqlVariable**. Parameters that were originally filled in for the parent report and are needed by the target report, for example, start and end dates ○ **name**. The name of the column or sqlVariable in the parent report. ○ **qsname**. The query string variable name that is used to pass this parameter to the target report. This name should match the SqlVariable name in the target report.
<Graph/>	Creates a view type of graph that uses a Microsoft Office Web Component to display a graph. **Note:** You must have Microsoft Excel installed for graphical output to function correctly.
<Total/>	Optional This element totals all the values of one column and displays the total in the last row of the report. This element has the following attributes: • **countcol**. The name of the column in the XML output to total. If the column is aliased, you must use the aliased column name. • **display**. The text that shows to the left of the total.
<SubTotal/>	Optional This element subtotals the values of the designated column. To effectively use this element, the data is sorted on the column defined in the groupcol attribute.

Element	Description
	This element has the following attributes: • **groupcol**. The column to break for subtotaling. If the column is aliased, you must use the aliased column name.The data is sorted on this column. When a new value is found in this column, a subtotal row is inserted. • **countcol**. The name of the column in the XML output to subtotal. If the column is aliased, you must use the aliased column name. • **<Break/>**. Optional. This element allows you to insert formatting between rows after a new value in a column.The data should be sorted on the column defined in the breakcol attribute. The data to insert should be enclosed between the **<break>** and **</break>** and should usually be escaped with CDATA tags. • **breakcol**. The column that you want to break for formatting.If the column is aliased,you must use the aliased column name.The data should be sorted on this column. When a new value is found in this column,the data for this element is inserted in the output.
<PostProcess/>	Allows a Velocity script to be specified to process the report results before they are presented to the user. The attributes that can be used for this element are: • **language**. Specifies the language used by the post processing script. Currently the only acceptable value is **velocity**. • **saveOutput**. Specifies whether the output of this script should be saved in the generated report XML. The default value is **false**. The following OOTB reports use of this feature to display the service names as a concatenation of the names of each service: • Devices with 2 service levels summary • Devices with 3 service levels summary

<SqlVariable/> Elements

Element	Description
<Option/>	Zero or more required. This element provides options for variables of select type and has the following attributes. • **value.** The variable value for this option. This is the value substituted, but it is not displayed to the user. • **display.** A user-friendly description of the value that is used in the select list.
<SelectQuery/>	Zero or more required. This element contains the SQL query that will be run to show the options when **<SqlVariable/>** is **dbselect**.

Element	Description
	This element should be within the **<SqlVariable></SqlVariable>** tags. This element must have at least one attribute set to **true** to indicate database vendor compatibility. For all but the simplest queries, this element should be escaped with CDATA tags. This element has the following attributes: • **mssql=**. Set to **True** if the query is compatible with Microsoft SQL Server. • **oracle=**. Set to **True** if the query is compatible with Oracle. • **db2=**. Set to **true** if the query is compatible with IBM DB2.

<Graph/> Elements

Element	Description
<ChartType/>	Required child element of <Graph/>. This element defines the chart type to display and has the following attributes: • **Name.** A user-friendly description of the name of the chart type (that is: bar, column, or line). • **Value.** A numeric value that defines the Excel chart type. ○ **1=Column** ○ **4=Bar** ○ **9=Line**
<Category/>	Required child element of <Graph/>. This element is the column to use as the category axis of the chart. It should look like <Category>ColumnName</Category>, where ColumnName is either the column name or the aliased column name that you want to use.
<Value/>	Required child element of <Graph/>. This element is the column to use as the value axis of the chart. It should look like <Value>ColumnName</Value>, where ColumnName is either the column name or the aliased column name that you want to use.
<Labels/>	Optional child element of <Graph/>. This element defines the chart labels to display and has the following attributes: • **chart.** A user-friendly description of the entire chart. • **catAxis.** A user-friendly description of the data in the category axis. • **valAxis.** A user-friendly description of the data in the value axis.

Settings tab

The Settings tab contains the following fields:

- **Style Sheet Group**. This drop-down list contains the style sheets that are defined under Reports > Style Sheets. The style sheets define the look of the resulting report, based on the selected presentation type (selected from the **view as** drop-down list on the **General** tab).
- **Realm Access**. Specifies which realms the report is available to.
  - **None**. Specifies that this report will not be made available to any realm-constrained user.
  - **All**. Specifies that this report will be available to users associated with any realm in the system.
  - **Selected**. Specifies that this report will only be available to users in specific realms.
- **Realms**. When **Selected** is chosen as the **Realm Access**, this field is used to choose the realms that can access the report. To allow a realm to access the report, select and drag the realm from the **Available** to the **Current** pane.

History tab

Every time a report is run, either manually or according to a schedule, the results are automatically saved so that you can review those results at a later time.

The **History** tab lists all recorded runs of a report which have not yet expired. The list will initially be displayed in reverse chronological order, but can be sorted by clicking on the column headers.

To view the results of a previous run of the report,

1. Select the desired result based on the time it was run and the user it was run by.
2. From the **View** drop-down list, select the format in which the results must be formatted. The results are formatted and displayed in a new browser window.

Note: The graph format is only available if the report definition includes the graphing tag.

Initially, all report results will expire after the period specified in the **Report Log Expiration Age** preference. This preference defaults to one day.To retain the report results for a longer period of time, select the results and click **Keep**. This will toggle the **Expires?** field for the result to switch from **Yes** to **No**. Once a report is flagged to be kept, it cannot be reverted back to expire. It can only be deleted.

! **Important:** Report results that are set not to expire will still be deleted after a long period of time, based on the **Saved Report Expiration Age** preference (the default is 90 days).

To delete a report result, select it and click **Delete**.

Editing Schedule tab

The **Schedule** tab allows one or more schedules to be set up for a report. The list of current schedules are displayed at the top of the tab.

To create a new schedule:

1. Click **New** on the **Schedule** tab of the **Viewing Report** screen. The **Editing New Schedule** pane opens on the bottom of the screen.
2. On the **Schedule** tab of the **Editing New Schedule** pane,

   a. Ensure that the **Schedule Enabled** check box is selected.

   b. Determine the **Schedule Type**, as follows:

If	Then
The report is to be run a single time	Select the **Once** radio button in the **Schedule Type** section, and then specify the **Next Start Date**.
The report is to be run at a recurring interval	Select the **Recurring** radio button in the **Schedule Type** section, specify the **Next Start Date**, and then specify the frequency using the options in the **Recurrence Type** section. The available options are as follows: • **Periodic Interval (days)** • **Weekly on**.

3. On the **Email** tab, select the **Send Email** check box and provide the required information if you want to automatically send an e-mail message of the report results.
4. On the **Parameters** tab, enter the required parameters.
5. Click **Save**.

To delete an existing schedule, select it from the **Schedules** list and click **Delete**.

To modify a schedule (for example, to change its timing or disable it):

1. Select it from the **Schedules** list. Its details are displayed in the **Editing Existing Schedule** pane at the bottom of the page.
2. Make the necessary changes.
3. Click **Save**.

Schedule tab

The Schedule tab of the of the **Editing Schedule** pane contains the following fields:

- **Schedule Enabled**. When this check box is selected, the schedule is enabled and the report will run at the specified time. To disable the schedule without deleting it entirely, clear this check box.
- **Next Start Date**. This field specifies the next day that the report will be run. For a recurring schedule, this field will automatically be updated each time the report runs.
- **Start Time**. This field specifies the time during the day that the report will run.
- **Schedule Type**. This field specifies whether or not the schedule is recurring.
- **Recurrence Type**. For recurring schedules, two modes of recurrence are available:
    - **Periodic Interval**. Specifies the number of days between runs.
    - **Weekly on**. Specifies the days of the week when the policy will run.

Email tab

The settings on the Email tab of the Editing Schedule pane can be used to automatically send an e-mail message containing the report results, each time the report is run by the schedule. The following fields are available:

- **Send Email**. Select this check box to enable the email option for this schedule.
- **To**. One or more recipient email addresses, separated by commas.
- **From**. A valid email address from which the email should appear to be sent.
- **Subject**. The subject line of the email message.
- **Format**. The format in which the report results must appear in the body of the email message. The options are HTML, CSV, and XML.

Parameters tab

If the report being scheduled requires any parameters to be specified, they must be set in the **Parameters** tab of the of the **Editing Schedule** pane. The parameters on this tab will vary from report to report.

Helpful tips

When using the report system, the following are helpful tips for creating and using reports effectively:

- Set the standard XML attribute to 0 when modifying a report, so the modified report is not overwritten during an upgrade of the application software.
- Set the realtimeok attribute to 0 to run a report only at a scheduled time to prevent time consuming reports from being generated interactively during peak hours of operation.
- Set the type attribute to date to use the calendar control to specify input fields for the date range for data over which to generate the report. The date value ensures valid dates are entered.
- Copy a report rather than starting from scratch to more easily see possible elements.
- Use full clauses in the <SqlVariable/> section especially with the select type. This allows more complex substitution.
- Outline extra information and instruction by putting more text in the <Description/> element rather than in the individual parameters.
- If the report could return many rows, provide a variable that allows selection of partial rows or all.

Some reports will display events or trends over time. In these cases, you will have to specify a reporting period by selecting a Start Time and End Time. Other reports may prompt you to specify other types of filters.

Managing report style sheets

Style sheets are used to control the look and feel of reports by modifying the underlying XSL used to transform the raw report results into a desired presentation format. There are four presentation types for which style sheets can be provided:

- **HTML**. Used to display a report in a browser window.
- **Email**. Used when including a report in an email message.
- **CSV**. Used to export a report to a machine readable format.
- **Graph**. Used to produce graphs that can be viewed in a browser window.

One or more of these types may be grouped together into a Style Sheet Group, which in turn can be specified by a report as the set of style sheets to use when that report is viewed. By default, there is only one Style Sheet Group defined, which contains a default style sheet for each of the four presentation types.

To access the **Report Style Sheets** management screen, select **Report > Style Sheets**. A list of existing XSL style sheets is displayed in the **Report Style Sheets** pane. This list includes the installed default group of style sheets, called System Default XSL. The list can be filtered on Group Name.

To remove an XSL scheme from a group, click that scheme's **Delete** button.

To remove an XSL group, select it and click **Delete**.

Adding a style sheet

To add a new style sheet

1. Click **New** on the **Report Style Sheets** management screen. The **Viewing New Report Style Sheet** pane opens on the bottom of the screen.
2. On the **General** tab,

    a. In the **Group** field, enter a name for the group.

    b. In the **Report Type** drop-down list, specify the output type for which this XSL formatting is to be applied.

Note: You can only create one scheme for each output type in a group. Also, a report will not run if there is no XSL scheme for the output type selected at runtime. For example, if a report is associated with a group that does not contain an XSL scheme for graph output, users cannot select the graph output type when they run the report.

3. On the **XSL** tab, enter the XSL markup in the text box.
4. Click **Save**.

Deleting a style sheet

To remove a style sheet

1. From the **Report Style Sheets** pane, select the style sheet that you want to delete.
2. Click **Delete**.
3. When asked for a confirmation, click **Ok**.

Note: The default group of style sheets cannot be deleted.

Viewing and modifying report style sheets

To view a style sheet, select the appropriate record from the **Report Style Sheets** pane. Its details are displayed in the following tabs of the **Viewing Style Sheet** pane at the bottom of the screen:

- General
- XSL

General tab

The General tab contains the following fields:

- **Group**. The name of the group to which the style sheet belongs. Each group may only contain one style sheet for any given report type.
- **Report Type**. The presentation type that this style sheet will be used for. It has the following options:
  - **HTML**. Used to display a report in a browser window.
  - **Email**. Used when including a report in an email message.
  - **CSV**. Used to export a report to a machine readable format.
  - **Graph**. Used to produce graphs that can be viewed in a browser window.

XSL tab

The XSL tab contains the XSL document that transforms the report output into the desired presentation format. Knowledge of XSL is required to construct the transformations. The XML operates on the raw XML report results, which leverage standard report schemas such as the Microsoft Rowset Schema.

9

Managing the CSR User Interface

Managing the CSR User Interface

This chapter describes the Customer Service Representative (CSR) Interface. This interface allows customer service representatives to search for a device and interact with it directly to assist in problem resolution.

Locating devices

CSRs can use the **Find Device By** search feature to locate specific devices and then access the CSR User Interface. This search feature is only available to users who have the ***CSR: View CSR*** permission.

The device search feature is always displayed at the top of the interface regardless of the section or menu selected. This accessibility allows users to search for a specific device or set of devices that match a specified search criteria from any page of Service Gateway.

Entering a search string in the **Find Device By** text field and clicking **Search** brings up the list of devices, which then allows the user to find and view the device details using the CSR Widgets user interface feature.

Tip: The default search option can be configured via the Default Device Search Type under Preferences. The global default can be overridden by a user's own preferences.

Working with search results

The **Search Results** tab is enabled when you enter a search string in the **Find Device By** text field and click **Search**. The **Search Results** tab displays a list of all devices that match the specified search criteria.

The columns displayed can be customized per user or group. Select **Display Columns** from the drop-down list on the top-right corner of the display. A list of all columns is displayed with check marks beside the currently enabled columns. Click column name to toggle it.

You can rearrange a column by selecting and dragging it to the desired location. Rearranging a column takes effect right away. Any changes are saved as part of the overall layout, see CSR UI Layouts.

Selecting a search result will automatically display the device in the first tab of the current layout (for instructions to create and save a layout, see CSR UI Layouts).

For details on the individual widgets found within the layout, see CSR UI Widgets.

CSR UI widgets

Widgets provide features to interact with a device and can be organized onto one or more tabs of the CSR User Interface. The same widget may be used multiple times on the same tab or on different tabs. The following widgets are available:

- Device Actions
- Device Local Log
- Device Status
- Device Summary
- Diagnostics
- Real-time Probe
- Software Modules

Device Actions

The Device Actions widget allows you to run actions directly on the device. To run an action, select an action from the drop-down list and then click **Execute**.

By default, the following actions are available:

- **Reboot**
- **Reset to Factory Defaults**
- **Configuration Snapshot**

After running an action, the results are displayed within the widget.

Device Local Log

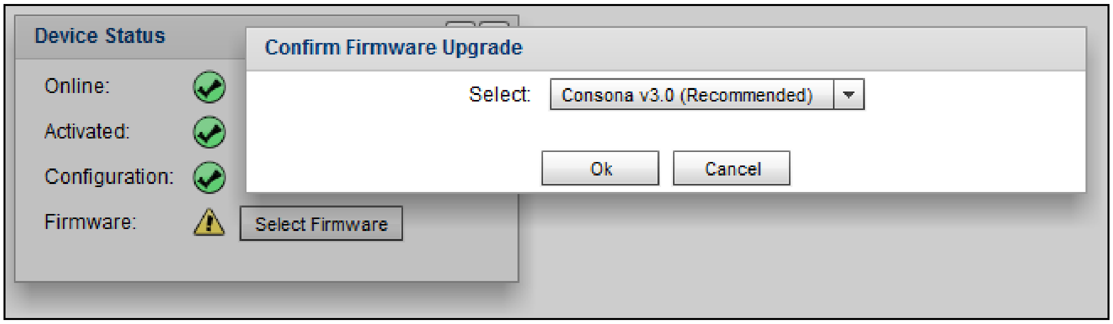
The Device Local Log widget displays the internal log maintained by the device. Often this log will only contain entries since it was last powered on.

Device Status

The Device Status widget displays the status of the following aspects of the device.

- **Online**. An attempt is made to establish contact with the device in real time. If the device responds to a connection request, the device is deemed as **Online** and a green check mark is displayed. The system displays a red X if the device is offline.
- **Activated**. This status indicates whether or not the device has successfully completed the defined activation policy that is executed against all newly registered devices.

- **Configuration**. This status indicates whether or not the device is up-to-date with the currently defined configuration for the device. In most provisioning scenarios, a device will synchronize its configuration every time it reboots. If the configuration is not up-to-date, a button is presented to trigger a configuration synchronization.
- **Firmware**. This status indicates whether or not the device is running a valid firmware , as indicated by a green check mark. If the device is not running a valid firmware, and one exists, an option to initialize a firmware upgrade is provided. A CSR with **CSR: Custom Firmware Selection** permission can choose the desired firmware from a drop-down list when performing the upgrade. Without this permission, the previous behavior of following the configured upgrade path is used.



Device Status

Online: ✓

Activated: ✓

Configuration: ✓

Firmware: ⚠

Confirm Firmware Upgrade

Select: Consona v3.0 (Recommended)

Tip: Pausing on the status icons may display a tool tip with additional details about the status if available.

Device Summary

The Device Summary widget provides a brief summary of the device.

You can configure the fields displayed in this widget as follows:

1. Click configuration icon (☰) in the title bar of the widget.
2. On the **Device Summary Settings** dialog box, do the following:
   a. Select the fields to display in the **Standard Fields** tab.
   b. Select the system keys to display in the **System Keys** tab.

      Up to eight custom system keys can be displayed.

   c. Click **Save**.

All changes made to the fields displayed are saved as part of the CSR Layout.

Diagnostics

The Diagnostics widget provides quick real-time diagnostics that can be run directly on the device to test whether it is responding to communication.

The CSR diagnostic module supports the TR-143 Download and Upload diagnostics, including management of Diagnostic Servers and associated upload and download paths.

You can select an available test from the drop-down list at the top of this widget, set the desired parameters in the Parameters tab, and initiate the test by clicking **Execute**. The Results tab will indicate that the test is running, then display the results once it has completed. The following tests are available:

- **Ping Test**. The device initiates an ICMP ping from itself to the specified host. The **Interface** drop-down list allows you to select one of the following options: **LAN IP**, **WAN IP**, **WAN PPP**, or **None** to be used as the origin of the test. The **Host** may be either a hostname or IP address. You can alter the repetitions, timeout, and payload size values before initiating the test.
- **ATM Loopback**. The device initiates an ATM loopback test. You can alter the repetitions and timeout values before initiating the test.
- **Download Test**. The device initiates a download test from the given host to itself to measure the speed of the downstream path to the device.The **Interface** drop-down list allows you to select one of the following options: **LAN IP**, **WAN IP**, **WAN PPP**, or **None** to be used as the origin of the test. You can also enter the URL of a file to download.
- **Upload Test**. The device initiates a upload test to the given host to measure the speed of the upstream path from the device. The **Interface** drop-down list allows you to select one of the following options: **LAN IP**, **WAN IP**, **WAN PPP**, or **None** to be used as the origin of the test. You can also enter the URL of a location to which the file is to be uploaded. Typically, a device will generate a file with random content of the size provided.

! **Important:** When initiating a ping or throughput test, the originating interface can be significant. Initiating a test from the LAN interface to a site on the Internet may be subject to the filters and parental controls of the device. Similarly, initiating a test from a WAN interface to an IP address within the LAN network may not succeed due to firewall or routing restrictions.

Real-time Probe

The Real-time Probe widget allows you to interrogate or modify the data model of a TR-069 compliant device. The available real-time probes are defined by an administrator (see Real-Time Probes).

To run a Real-time Probe, select a probe from the drop-down list and then click **Execute**. When the probe is complete, the real-time probe results are displayed within the widget in a tabular format, allowing a CSR to see all records in a table (such as Port Mappings or Firewall Rules) at once. This format also allows records to be added and removed from the table.

Software Modules

The Software Modules widget displays the software modules (sometimes called "apps") installed on a device and the current status of the operating environment. It also allows available modules to be installed or uninstalled.

Using CSR UI Layouts

The search results and tools presented to a customer service representative can be personalized and saved using Layouts. A Layout has a set of search result columns along with one or more tabs. Each tab contains one or more widgets. Additionally, some widgets support saving their state as part of a Layout.

Creating a new Layout

To create a new Layout, do the following:

1. Delete any tabs that are already defined.
2. From the drop-down list on the top right corner just below the Search button,
    a. Choose the columns that must be displayed in the **Search Results** tab by selecting or clearing the required columns under **Display Columns**.
    b. Select **Create New Tab**. The **New Tab** dialog box opens.
    c. Enter a name for the tab in the **Tab Name** field and click **Ok**.
3. On the new tab, select the right-arrow that appears on the left of the tab interface.
4. Select one of the available widgets from the list and then drag it into the open area of the tab.
5. Repeat step 4 until you have all of the widgets that you want displayed in the list.
6. Click the left-arrow on the right side of the widget selection list to close the list.
7. Optionally, from the drop-down menu on the top right of the page, save the layout for a single user by selecting **Save Layout** or for a group, by selecting **Save Layout for Group** and selecting the Group Name.

Modifying a Layout

Changing an existing layout is similar to creating a new layout. Tabs can be added or deleted, and widgets can be added, moved, or deleted.

The drop-down list at the top right of the screen provides the following options:

- **Create New Tab**. Allows to add a new tab.
- **Display Columns**. Allows to choose the columns that must be displayed in the Search Results tab.
- **Save Layout**. Allows to save a configured layout for a single user.
- **Load Layout**. Allows to load a configured layout for a single user.

- **Save Layout for Group**. Allows to save a configured layout for a group.
- **Load Layout for Group**. Allows to load a configured layout for a group.

Tip: Any changes that are made are not permanent until the Layout is saved. To revert changes, select **Load Layout** from the drop-down list.

Note: If a user is a member of a group, they are not automatically presented that group layout upon login. The user would have to load the layout for the group, and then save the layout as their personal layout.

10

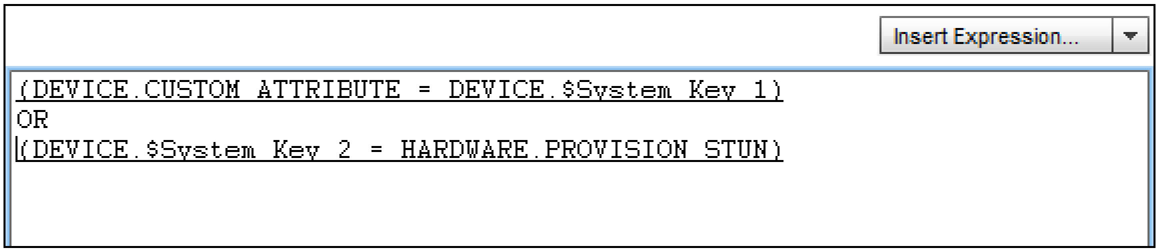
Condition Editor

The condition editor is used to define a set of conditions or filters, which must be met to match an entity to a device. Conditions can be specified for a number of entities such as real-time probes, templates, services, policies, and policy actions.

Conditions consist of one or more expressions, which are essentially properties of a device or are in some way associated with a device.

Expressions can be combined using the logical operators: AND, OR, and NOT. Standard operator precedence is used, with NOT being the highest priority, followed by AND, and lastly OR. As with mathematical operations, parentheses can be used to group operations together.

Also, the right side of an attribute or system key test within a condition can reference another system key of the device or an attribute of any object.



```
(DEVICE.CUSTOM ATTRIBUTE = DEVICE.$System Key 1)
OR
(DEVICE.$System Key 2 = HARDWARE.PROVISION STUN)
```

The following properties can be used when building conditions:

- Capabilities
- Device Attributes
- Device IP Address
- Device System Key
- Device MAC Address
- Domain
- Domain Attribute
- Firmware
- Firmware Attribute
- Hardware
- Hardware Attribute
- Service
- Service Attribute
- Subscriber Attribute

Note: Expressions involving these properties must be inserted using the Insert Expression drop-down list, as the expressions include hidden information that is necessary for saving and evaluating the condition. Attempting to manually type the expressions into the Condition Editor text box will not result in a valid condition.

When you select an option from the **Insert Expression** drop-down list, an expression is inserted in the **Condition Editor** text box where the cursor is located. Inserting a capability expression, for example, results in the following hyperlink being inserted:

(CAPABILITY = [Click to Select])

Clicking on the hyperlink displays a pop-up dialog box that allows you to select the capability that the device must have for this condition to match the device.

For example, if you want to match all devices with a specific capability, but that are not associated with a particular service, you can start by inserting the capability expression in the **Condition Editor** text box and then typing the logical operators *AND NOT* after that expression as follows.

(CAPABILITY = [Click to Select]) AND NOT

Making sure your cursor is placed after the word *NOT*, you can then insert a Service expression, resulting in the following entry in the **Condition Editor** text box:

(CAPABILITY = [Click to Select]) AND NOT (SERVICE = [Click to Select])

If you want to match all devices with a specific capability, but with one of two different firmware versions, then the entry in the **Condition Editor** text box is as follows:

(CAPABILITY = [Click to Select]) AND ((FIRMWARE = [Click to Select]) OR (FIRMWARE = [Click to Select]))

Note: The use of the parenthesis around the two firmware expressions ensures that the *OR* operation is completed before the *AND* operation.

When you click hyperlink, a pop-up dialog box is displayed. This dialog is used to replace the *[Click to Select]* text in the hyperlink with the actual property with which it is to be matched.

Most pop-up dialog boxes have a drop-down list that allows you to select the specific property. Once you have selected the desired property, click **Ok**.

For **Device IP Address** or **Device MAC Address**, you can enter the value in the provided text box. In both of these cases, you can use either the full value or a trailing wildcard (*) character.

For **System Keys** and **Attributes**, after you select the attribute name (for an attribute condition) or the system key (for a system key expression) from the provided drop-down list, you need to match the expression with a value (with or without a wildcard), a system key, or an object attribute by selecting the appropriate **Compare With** radio button.

If you select	Then
Value	Enter a value in the **Attribute Value** field. A trailing wildcard is also permitted. **Note:** By default, the Value radio button is selected.
System Key	Choose the desired system key from the **System Key** drop-down list.
Object Attribute	Choose the object type and the attribute name from the **Object Type** and **Attribute Name** drop-down lists respectively.

The **System Key** and **Object Attribute** options support the use of expressions similar to the following:

(DOMAIN.ATTRIBUTE_1 = DEVICE.$SYSTEM_KEY_1)

The preceding expression is requesting for a domain attribute called ATTRIBUTE_1 that has the same value as the device system key called SYSTEM_KEY_1.

After you build a condition, you can test it using the options available below the main text area as follows:

1. Specify a device against which to test it as follows:

   - Enter the unique ID for the device in the **Test Device with Unique ID** field or click the **Find** button.

     Clicking the **Find** button opens the **Find Device** dialog box, which works exactly like searching for a device on the Inventory > Devices screen. For details, see Performing a Search under Managing Devices. Selecting a device from the **Device Search Results** list closes the **Find Device** dialog box and populates the **Test Device with Unique ID** field with the unique ID of the device.

2. Click **Evaluate** to test the condition against this device. The **Evaluation Result** dialog box opens and displays one of the following messages:

   - *Expression evaluated as TRUE*. Indicates that the device matches the conditions.
   - *Expression evaluated as FALSE*. Indicates that the device does not match the conditions.

11

Velocity Scripting

There are certain input fields that along with accepting regular text strings for values will also accept Velocity scripts, allowing values to have a dynamic nature based on the object being processed.

Script Editor and Evaluator

Scripting elements that support Velocity scripting provide an **edit** icon beside the field:

Clicking the edit icon displays a new dialog window with two main components: an editor and a results display. The editor is a basic text editor, allowing you to create complex scripts more easily than in a single line input box. The pop-up also allows you to evaluate a script in real-time against a given device to test it before saving it and putting it into production.

Selecting an element from the **Insert Script Element** drop-down list on the **Edit Script** pane activates the **Insert Property Element** or the **Insert Attribute Element** dialog box that can be used to insert pre-formatted script for various elements that can be referenced. This helps to build the scripts without having to remember the syntax for accessing information that is available for the device.

To evaluate a script, you first need to find a device to run the script against. You can either enter the device's unique ID string manually or click the **Find** button to bring up an additional pop-up that contains the normal device search form. Clicking on a specific device record automatically places the device ID into the editor dialog window.

Once a valid device ID is filled in, the **Evaluate** button becomes active. Clicking on the **Evaluate** button will then process the script, using details from the device that you specified. Once the script content is complete, click **Save**, or click **Cancel** to undo any changes that were made.

Script Snippets

Useful snippets of the Velocity script can be selected from the drop-down list at the top of the pop-up windows. This provides snippets for commonly accessed information about the current device and related objects.

To insert a snippet, select the category from the drop-down list, then select or fill in any further information in the pop-up that appears and click **Ok**. The snippet is inserted at your cursor location.

The drop-down list includes access to the following information:

- Capabilities
- Device
- Device Attributes
- Domain
- Domain Attributes
- Firmware

- Firmware Attributes
- Hardware
- Hardware Attribute
- Services
- Service Attributes
- Subscriber Attributes

Depending on the item that you select from the drop-down list, you will be presented with one of the following dialog boxes:

- **Insert Property Element**. Displays when you select any item in the preceding list that includes the term Attribute.
- **Insert Attribute Element**. Displays when you select any of the other items in the preceding list.

Insert Property Element

The following table lists the properties that are available for each of the property items from the preceding list. In some cases extra drop-down lists or text boxes are displayed, depending on the property that is selected. These are explained in the Description column of the following tables, where applicable. In such cases, it may be possible to select items that are not associated with the device. For instance, if you are specifying the name for a specific capability, and that capability is not associated with the device, then the script will evaluate to an empty string for that element.

Item	Property	Description
Capability	**Count**	The number of capabilities that are associated with this device, via the hardware and/or firmware associated with the device.
	Description	The description for the specified capability. When selecting this property, an additional drop-down list is displayed allowing you to select a specific capability.
	Existence	Inserts a conditional statement into your script that only gets evaluated if the specified capability is associated with the device. When selecting this property, an additional drop-down list is displayed allowing you to select a specific capability.
	List	Lists all the capabilities associated with the device. This evaluates as a comma-delimited string, listing all the capabilities on one line.
	Loop	Inserts a loop statement into your script that lets the script loop over all the capabilities associated with the device. A comment block is also inserted that explains how to access various properties of the capability, as well as a loop counter. You are not limited to the information shown in the comment block; however, you can enter any other text or script in the loop.

Item	Property	Description
	Name	The name of the capability. When selecting this property, an additional drop-down list is displayed allowing you to select a specific capability
	System Defined	Specifies whether the capability is system-defined, or one that was added by a user via the UI. This will evaluate to either **true** or **false**. When selecting this property, an additional drop-down list is displayed allowing you to select a specific capability.
Device	Data Model Root	The data model root for the device. When TR-069 was initially released, the root node of the data model on the device was called InternetGatewayDevice. As the Broadband Forum continued to work on the specifications, a new root node was introduced, called Device. This property will display either **InternetGatewayDevice** or **Device**, depending on the data model root. If the data model root is not available for the specific device, this evaluates to an empty string.
	IP Address	The IP address of the device. If the IP address is an IPv4 address, it is displayed in the IPv4 format; otherwise, it is displayed in the IPv6 format.
	Is Active	Specifies whether a device has successfully been processed by an Activation policy. Possible values are **true** and **false**.
	MAC Address	The colon-delimited MAC address for the device, if one is present. An example of a colon-delimited MAC address is aa:bb:cc:dd:ee:ff.
	Object	Displays information about the device. Currently, this is only the unique ID of the device.
	Serial Number	Displays the serial number of the device, if any.
	System Key	Displays the value for the specified system key, if any. When selecting this property, an additional drop-down list is displayed allowing you to select a specific system key.
	Unformatted MAC Address	Displays the unformatted MAC address for the device, as it is stored in the database. This format is 12 lower case hexadecimal digits without any delimiters. An example of an unformatted MAC address is **aabbccddeeff**.
	Unique ID	Displays the unique ID of the device.

Item	Property	Description
Domain	Description	The description of the domain.
	Full Name	The full name of the domain, including all parent domains right up to the root domain. For example, **/ Child / Grandchild**.
	Object	The full name of the domain.
	Short Name	The name of the domain, without any parents in the chain. In the example used above, the short name would be **Grandchild**.
Firmware	Firmware Version	The version of the firmware.
	Manufacturer	The manufacturer of the firmware.
	Object	A string made up of the manufacturer and the version.
Hardware	Device Type	The device type of the hardware.
	Manufacturer	The manufacturer of the hardware.
	Object	A string made up of the manufacturer and the revision of the hardware.
	Product Class	The product class of the hardware.
	Revision	The revision of the hardware.
Services	Code	The code of the specified service. When selecting this property, an additional drop-down list is displayed allowing you to select a specific service.
	Count	The number of services that are associated with the device.
	Existence	Inserts a conditional statement into your script that only gets evaluated if the specified service is associated with the device. When selecting this property, an additional drop-down list is displayed allowing you to select a specific service.
	List	Lists all the services associated with the device. This evaluates as a comma-delimited string, listing all the services on one line.
	Loop	Inserts a loop statement into your script that lets the script loop over all the services associated with the device. A comment block is also inserted that explains how to access various properties of the service, as well as a loop counter. You are not limited to the information shown in the comment block. You can enter any other text or script in the loop.
	Name	The name of the service. When selecting this property, an additional drop-down list is displayed allowing you to select a specific service.
Subscriber	Account Type	The account type of the subscriber associated with the device, if any. Valid values are **NORMAL** or **ENTERPRISE**.

Item	Property	Description
	Address	The address of the subscriber.
	Address (Line 2)	The second address line of the subscriber.
	Billing Number	The billing number of the subscriber.
	City	The city of the subscriber.
	Company Name	The company name of the subscriber.
	Country	The country of the subscriber.
	Email Address	The email address of the subscriber.
	First Name	The first name of the subscriber.
	Last Name	The last name of the subscriber.
	Middle Name	The middle name of the subscriber.
	Object	A concatenation of the subscriber's first, middle, and last names.
	Phone Number	The phone number of the subscriber.
	Postal Code	The postal code of the subscriber.
	State	The province or state of the subscriber.

Insert Attribute Element

The following table lists the properties that are available for each of the attribute items from the preceding list. In some cases extra drop-downs or text boxes are displayed, depending on the element and attribute that are selected. These are explained in the Description column, where applicable. In such cases, it may be possible to select items that are not associated with the device. For instance, if you are specifying a specific attribute, and that attribute is not associated with the specific object type, then the script will evaluate to an empty string for that element.

The Insert Attribute Element dialog boxes are the same regardless of the attribute type (device, domain, hardware, firmware, service, or subscriber), so the following table applies to all attribute types.

Element	Description
Value	The value of the specified attribute. If selecting a complex attribute from the **Attributes** drop-down list, an additional text field called **Index** is displayed so that the index of the complex attribute can be specified.
Loop (All attributes)	Inserts a loop statement into your script that lets the script loop over all the attributes associated with the device, both simple and complex. A comment block is also inserted that explains how to access various properties of the attribute, as well as a loop counter. You are not limited to the information shown

Element	Description
	in the comment block, and can enter any other text or script in the loop
Loop (All group instances)	Inserts a loop statement into your script that lets the script loop over all the instances of a specific complex attribute that is associated with the device. A comment block is also inserted that explains how to access various properties of the group, as well as a loop counter. You are not limited to the information shown in the comment block, and can enter any other text or script in the loop.
Loop (Members of specific group)	Inserts a loop statement into your script that lets the script loop over all the attributes of a specific index of a complex attribute that is associated with the device. A comment block is also inserted that explains how to access various properties of the group, as well as a loop counter. You are not limited to the information shown in the comment block, and can enter any other text or script in the loop.
List (Members of specific group)	Displays a comma-delimited list of attribute names and their values for the specified index value for the specific group.
Repeat For Group	A special directive that is only applicable when defining a script for a parameter group template. Its purpose is to generate multiple entries in a SetParameterValues RPC call to a device using a single entry in the template, rather than having to define each entry in the template. The benefit is that the number of entries in the SetParameterValues RPC call will be controlled by the number of instances of the complex attribute, without requiring that the parameter group template be changed. So if one device (or the object it is associated with) has two instances of the complex attribute, that will result in two entries in the SetParameterValues RPC call. If another device (or the object it is associated with) has three instances of the complex attribute, that will result in three entries in the SetParameterValues RPC call. This is all done with a single parameter group template. Without this ability, two parameter group templates would have been required: one with two entries, and another with three entries.
List (All Attributes)	Displays a comma-delimited list of all the attribute names and their values, both simple and complex, which are associated with the device.
Existence	Inserts a conditional statement into your script that only gets evaluated if the specified attribute is associated with the device. When selecting this property, an additional drop-down list is displayed allowing you to select a specific attribute. If selecting a complex attribute from the Attributes drop-down list, an additional text field called Index is displayed, so that the index of the complex attribute can be specified.
Existence (Specific group)	Similar to the Existence element, except that it is for a specific index of a group, not the attribute within that group.
Existence (Any instance of group)	Similar to the Existence (Specific group) element, except that it is for any index of the specified group, not a specific index of that group.

Velocity Scripting Reference Guide

The Apache Group maintains documentation for the Velocity scripting language online, which can be found at:

http://velocity.apache.org/engine/1.5/user-guide.html