Dell Networking W-ClearPass Policy Manager 6.4

User Guide

Copyright Information

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg, et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Contents

Chapter 1
About Dell Networking W-ClearPass Policy Manager

The Dell Networking W-ClearPass Policy Manager platform provides role and device-based network access control across networks such as wired, wireless, and Virtual Private Network (VPN). Software modules for the Dell Networking W-ClearPass Policy Manager platform that includes Guest, Onboard, Profile, OnGuard, QuickConnect, and Insight simplify and automate the following tasks:

- Device configuration
- Provisioning
- Profiling
- Health checks
- Guest access

Dell Networking W-ClearPass Policy Manager provides device registration, device profiling, endpoint health assessments, and comprehensive reporting to automatically enforce user and endpoint access policies when devices connect to the network with the following built-in protocols:

- RADIUS
- SNMP
- TACACS+

Common Tasks in Policy Manager

When you use Dell Networking W-ClearPass Policy Manager, you may observe many common fields with similar functions in different locations. For example, importing or exporting from a list of items. This section explains how to perform the following common tasks:

- Importing on page 1
- Exporting on page 2

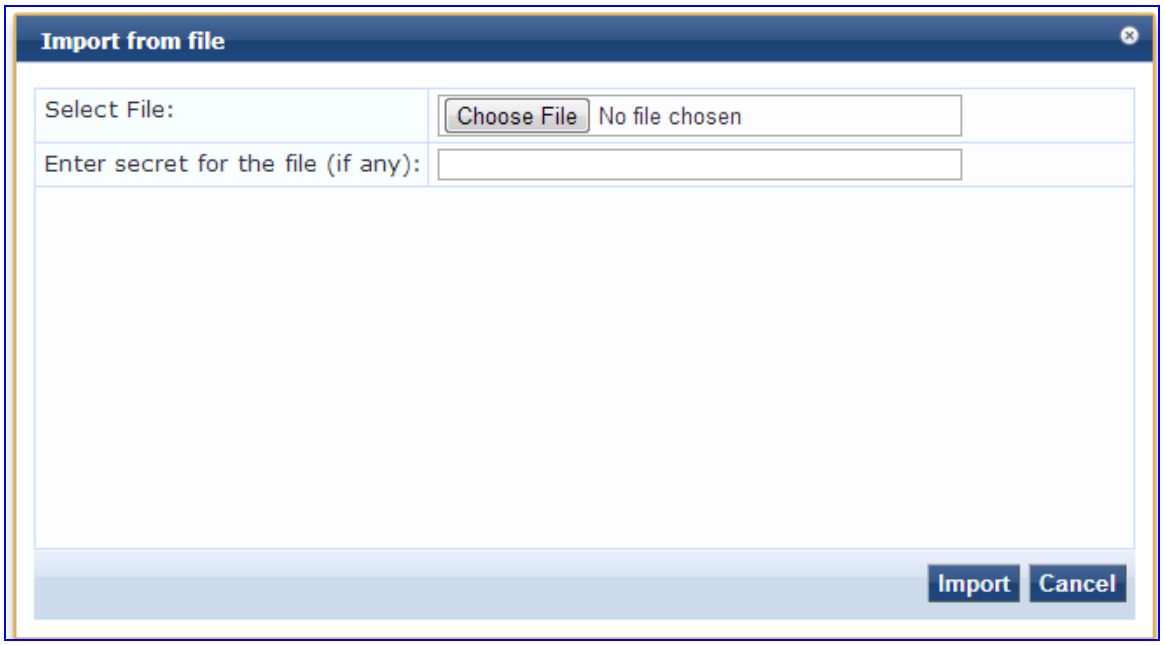
Importing

You can import the configuration and administration related information using most of the pages in Dell Networking W-ClearPass Policy Manager. This information is stored as an XML file which can be password protected. The tags and attributes in the XML file are described in the *Dell Networking W-ClearPass Policy Manager Configuration API Guide*.

In the popup, you can view the option that is similar to the following:

1. Click the **Import** link. The **Import from file** dialog box appears.

Figure 1: *Import from file example*



2. Click **Choose File**.
3. Select the file you want to import.

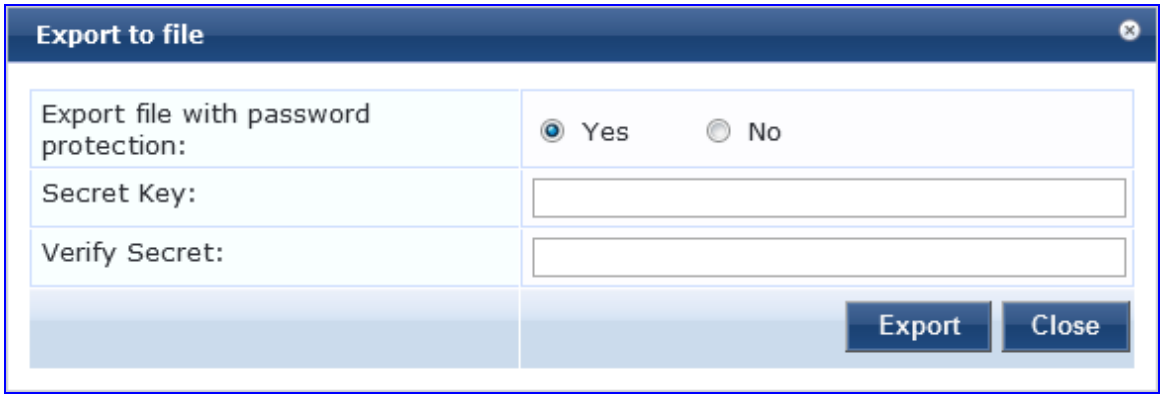
   You must select an XML file in the correct format. If you have exported files from different places from Policy Manager, ensure that you are selecting the correct file. See *Dell Networking W-ClearPass Policy Manager Configuration API Guide* for more information about the format and contents of XML files.
4. If the file is password protected, enter the password in the **Enter secret for the file (if any)** field.
5. Click **Import**.

Exporting

You can export the configuration and administration related information using most of the pages in Dell Networking W-ClearPass Policy Manager. You can export the information about one or more items. The configuration and administration information is exported as an XML file and this file can be password protected. The tags and attributes in the XML file are explained in the *Dell Networking W-ClearPass Policy Manager Configuration API Guide*.

1. Click the **Export** link. The **Export to File** dialog box appears.

Figure 2: *Export to File*



2. If you want the file password protected, select **Yes** and enter a password in the **Secret Key** and **Verify Secret** fields. If you do not want the file password protected, select **No**.
3. Click **Export**.

Depending on the browser you use, the file is either automatically saved to your hard drive, or you are prompted to save it in a specific location.

To export multiple items, select the check boxes in the rows of the specific items that you want to export.

This section provides an overview of the server ports. It also provides information on the initial Policy Manager setup using the Command Line Interface (CLI).

For more information, see:

Server Port Overview

The Dell Networking W-ClearPass Policy Manager server requires initial port configuration. The backplane of the Policy Manager contains three ports.

Figure 3: *Policy Manager Backplane*

The ports illustrated in the figure above are described in the following table:

Table 1: *Device Ports*

Key	Port	Description
A	Serial	Configures the Dell Networking W-ClearPass Policy Manager appliance initially using hardwired terminal.
B - eth0	Management (gigabit Ethernet)	Provides access for cluster administration and appliance maintenance using Web access, CLI, or internal cluster communication. This configuration is mandatory.
C - eth1	Data (gigabit Ethernet)	Provides point of contact for RADIUS, TACACS+, web authentication, and other data-plane requests. This configuration is optional. If this port is not configured, requests are redirected to the management port.

Server Port Configuration

Before starting the installation, collect the following information that you need, write it in the table below, and keep it for your records:

Table 2: *Required Information*

Requirement	Value for Your Installation
Hostname (Policy Manager server)	
Management Port IP Address	
Management Port Subnet Mask	
Management Port Gateway	
Data Port IP Address (optional)	**NOTE:** The Data Port IP Address must not be in the same subnet as the Management Port IP Address.
Data Port Gateway (optional)	
Data Port Subnet Mask (optional)	
Primary DNS	
Secondary DNS	
NTP Server (optional)	

Perform the following steps to set up the Policy Manager appliance:

1. **Connect and power on**

   Connect the serial port on the appliance to a terminal using the null modem cable provided and power on. The appliance is now available for configuration.

   Use the following parameters for the serial port connection:

   - Bit Rate: 9600
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None

2. **Login**

   You can create a unique appliance/cluster administration password later. For now, use the following preconfigured credentials:

   ```
   login: appadmin
   password: eTIPS123
   ```

   This initiates the Policy Manager Configuration Wizard.

3. **Configure the Appliance**

   Replace the **bolded** placeholder entries in the following illustration with your local information:

   ```
   Enter hostname: verne.xyzcompany.com
   Enter Management Port IP Address: 192.168.5.10
   ```

```
Enter Management Port Subnet Mask: 255.255.255.0
Enter Management Port Gateway: 192.168.5.1
Enter Data Port IP Address: 192.168.7.55
Enter Data Port Subnet Mask: 255.255.255.0
Enter Data Port Gateway: 192.168.7.1
Enter Primary DNS: 198.168.5.3
Enter Secondary DNS: 192.168.5.1
```

4. **Change your password**

   Use any string with a minimum of six characters:

```
New Password:************
Confirm Password: ************
```

   From now, you must use this new password for cluster administration and management of the appliance.

5. **Change the system date/time**

```
Do you want to configure system date time information [y|n]: y
Please select the date time configuration options.
1) Set date time manually
2) Set date time by configuring NTP servers
Enter the option or press any key to quit: 2
Enter Primary NTP Server: pool.ntp.org
Enter Secondary NTP Server: time.nist.gov
Do you want to configure the timezone? [y|n]: y
```

6. **Commit or restart the configuration**

   Follow the prompts:

```
Proceed with the configuration [y[Y]/n[N]/q[Q]
y[Y] to continue
n[N] to start over again
q[Q] to quit
Enter the choice:Y
Successfully configured Policy Manager appliance
************************************************************
* Initial configuration is complete.
* Use the new login password to login to the CLI.
* Exiting the CLI session in 2 minutes. Press any key to exit now.
```

When the Policy Manager system is up and running, navigate to the **Administration > Agents and Software Updates > Software Updates** page to view and download any available software updates. Refer to Updating the Policy Manager Software on page 471 for more information.

Powering Off the System

Perform the following steps to power off the system gracefully without logging in:

Connect to the CLI from the serial console using the front serial port and enter the following:

```
login: poweroff
password: poweroff
```

This procedure gracefully shuts down the appliance.

Resetting the Passwords to Factory Default

To reset the administrator password in Policy Manager to factory defaults, you can login to the CLI as the *apprecovery* user. The password to log in as the *apprecovery* user is dynamically generated.

Perform the following steps to generate the recovery password:

1. Connect to the Policy Manager appliance using the front serial port (using any terminal program). See Server Port Configuration on page 5 for details.
2. Reboot the system using the `restart` command.
3. After the system reboots, the following prompt is displayed for ten seconds:

   ```
   Generate support keys? [y/n]:
   ```

   Enter **y** at the prompt. The system prompts you with the following choices:

   ```
   Please select a support key generation option.
   1) Generate password recovery key
   2) Generate a support key
   3) Generate password recovery and support keys
Enter the option or press any key to quit.
   ```

4. To generate a password recovery key, select option 1.
5. After the password recovery key is generated, email the key to Dell technical support. A unique password will be generated from the recovery key and emailed back to you.
6. Enter the following command at the command prompt:

   ```
   [apprecovery] app reset-passwd
   ******************************************************
   * WARNING: This command will reset the system account *

   * passwords to factory default values                 *
   ******************************************************
   Are you sure you want to continue? [y/n]: y
   INFO - Password changed on local node
   INFO - System account passwords have been reset to factory default values
   ```

7. Now you can login with the new administrator password emailed to you by Dell technical support.

Generating a Support Key for Technical Support

To troubleshoot certain critical system level errors, Dell technical support might need to log into a *support shell*. Perform the following steps to generate a dynamic support password:

1. Log into the CLI and enter the following command:

   ```
   system gen-support-key
   ```

See gen-support-key on page 499 for details.

2. Connect to the Policy Manager appliance using the front serial port (using any terminal program). See Server Port Configuration on page 5 for details.
3. Reboot the system using the `restart` command.
4. When the system restarts, the following prompt appears for 10 seconds:

   ```
   Generate support keys? [y/n]:
   ```

   Enter **y** at the prompt. The system prompts with the following choices:

   ```
   Please select a support key generation option.
   ```

```
1) Generate password recovery key
2) Generate a support key
3) Generate password recovery and support keys
```

Enter the option or press any key to quit.

5. To generate the support key, select option 2. If you want to generate a support key and a password recovery key, select option 3.
6. After the password recovery key is generated, email the key to Dell technical support. A unique password can now be generated by Dell technical support to log into the support shell.

Policy Manager Dashboard organizes and presents the key information about various elements on Status, Performance, Summary, and so on. The **Dashboard** information is illustrated in interactive bar chart, graph, and table formats and you can click them to view the respective pages. Drag and drop elements from the left pane to customize the **Dashboard** layout as described in the following table:

Table 3: *Dashboard Layout Parameters*

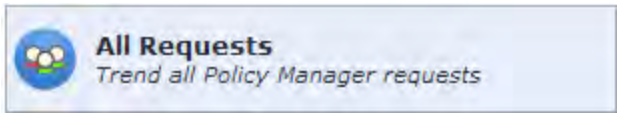
	Drag and drop the **All Requests** widget to **Dashboard** to view the graph that displays all requests processed by Policy Manager over the past week. Processed requests include RADIUS, TACACS+, and WebAuth requests. Clicking on each bar in the graph drills down into the **Access Tracker** page and shows the requests for the selected day.
	Drag and drop the **Health Status** widget to **Dashboard** to view the graph of the healthy and unhealthy requests over the past week. Healthy requests are the requests to which the health state was deemed to be healthy based on the posture data sent from the client. Unhealthy requests are the requests to which the health state was deemed to be quarantined (posture data received but health status is not compliant) or unknown (no posture data received). This includes RADIUS and WebAuth requests. The default data filters **Health Requests** and **Unhealthy Requests** are used to plot this graph. Clicking on each circle on the line graph drills down into the **Access Tracker** page and shows the healthy or unhealthy requests for the selected day.
	Drag and drop the **Authentication Status** to **Dashboard** to view a graph of the failed and successful requests over the past week. This graph includes RADIUS, WebAuth, and TACACS+ requests. The default data filters **Failed Requests** and **Successful Requests** are used to plot this graph. Clicking on each circle on the line graph drills down into the **Access Tracker** page and shows the failed or successful requests for the selected day.

Table 3: *Dashboard Layout Parameters (Continued)*

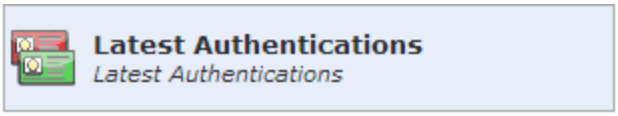
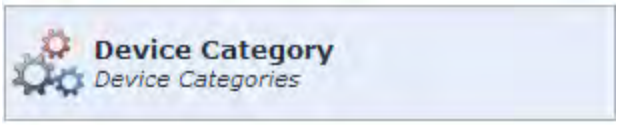
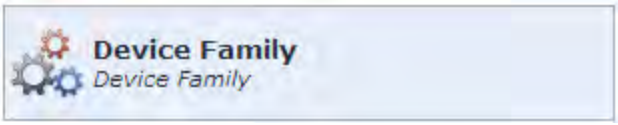
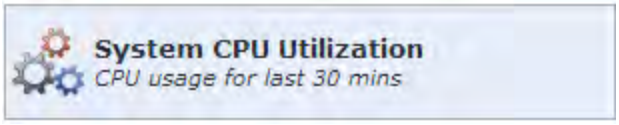
	Drag and drop the **Latest Authentications** widget to **Dashboard** to view the table with the latest authentications. Clicking on a row in the table drills down into the **Access Tracker** page and shows requests sorted by timestamp with the latest request displayed on the top.
	Drag and drop the **Device Category** widget to **Dashboard** to view the chart that shows the graph of all profiled devices categorized into the following built-in categories: • SmartDevices • Access Points • Computer • VOIP phone • Datacenter Appliance • Printer • Physical Security • Game Console • Routers • Unknown • Conflict **Unknown** devices are the devices that are not profiled by the profiler. **Conflict** indicates a conflict occurred in the categorization of the device. For example, if the device category derived from the HTTP User Agent string does not match with the category derived from DHCP fingerprinting, then a conflict is flagged and the device is marked as **Conflict**.
	Drag and drop the **Device Family** widget to **Dashboard** to view each of the built-in device categories. For example, selecting **SmartDevice** shows the different kinds of smart devices identified by **Profile**.
	Drag and drop the **System CPU Utilization** widget to **Dashboard** to view the CPU usage for the last 30 minutes. The utilization is presented in ten-minute increments. The widget displays the CPU utilization time in minutes and percentage for users, system, IO Wait time, and Idle time. For example, if you want to view the system CPU utilization for the period from 14:50 to 15:00, hover the mouse over the red line in the graph.

Table 3: *Dashboard Layout Parameters (Continued)*

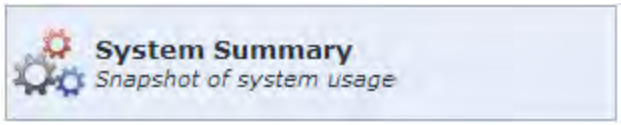
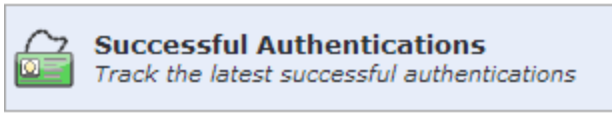
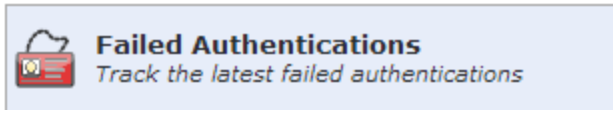
	Drag and drop the **Request Processing Time** widget to **Dashboard** to view the trend of total request processing time.
	Drag and drop the **System Summary** widget to **Dashboard** to view the **Percentage Used** statistics for the following: • Main Memory • Swap Memory • Disk • Swap Disk
	Drag and drop the **Successful Authentications** widget to **Dashboard** to view a table with the latest successful authentications. Clicking on a row in the table drills down into the **Access Tracker** page and shows successful requests sorted by timestamp with the latest request displayed on the top.
	Drag and drop the **Failed Authentications** widget to **Dashboard** to view the table with the latest failed authentications. Clicking on a row drills down into the **Access Tracker** and shows failed requests sorted by timestamp with the latest request displayed on the top.
	Drag and drop the **Service Categorization** widget to **Dashboard** to view the bar chart with each bar representing a Policy Manager service request that was categorized. Clicking on a bar drills down into the **Access Tracker** and shows the requests that were categorized into a specific service.
	Drag and drop the **Alerts** widget to **Dashboard** to view the table with latest system level events. Clicking on a row drills down into the **Event Viewer**.

Table 3: *Dashboard Layout Parameters (Continued)*

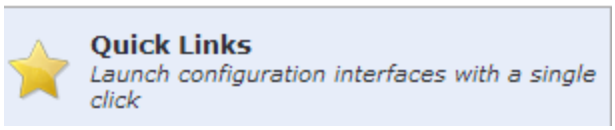
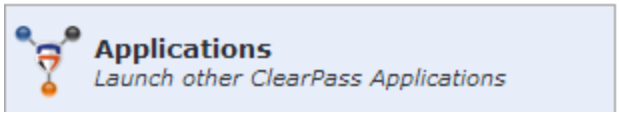
	Drag and drop the **Quick Links** widget to **Dashboard** to view the links to the following common configuration tasks: • **Start Configuring Policies** links to the **Start Here** page under the **Configuration** menu. You can start configuring Policy Manager services from here. • **Manage Services** links to the **Services** page under the **Configuration** menu. This page shows a list of configured services. • **Access Tracker** links to the **Access Tracker** screen in the **Monitoring** > **Live Monitoring** menu. • **Analysis & Trending** links to the **Analysis & Trending** screen in the **Monitoring** > **Live Monitoring** menu. • **Network Devices** links to the **Network Devices** screen in the **Configuration** > **Network** menu. You can configure network devices from here. • **Server Manager** links to the **Server Configuration** screen in the **Administration** menu. • **ClearPass Guest** links to the ClearPass Guest application. This application opens in a new tab. • **ClearPass Onboard** links to the ClearPass Onboard screen within the ClearPass Guest application. This application opens in a new tab.
	Drag and drop the **Applications** widget to **Dashboard** to view the links to the Dell Insight, Guest, and Onboard applications that are integrated with Policy Manager.
	Drag and drop the **Cluster Status** widget to **Dashboard** to view the status of all nodes in a cluster. The following fields are shown for each node: • **Status** - This shows the overall health status of the system. Green indicates healthy and red indicates connectivity problems or high CPU or memory utilization. The status also shows red when a node is out-of-sync with the rest of the cluster. • **Host Name** - Specifies the name of the host and IP address of the node.

Table 3: *Dashboard Layout Parameters (Continued)*

	• **CPU Util** - Specifies the snapshot of the CPU utilization in percentage. • **Mem Util** - Specifies the snapshot of the memory utilization in percentage. • **Server Role** - Specifies the name of the publisher or subscriber.

The **Monitoring** feature in Policy Manager provides access to live monitoring of components and other functions. For more information, see:

Live Monitoring

The **Live Monitoring** link provides access to six monitoring features. For more information, see:

Access Tracker

The **Access Tracker** page provides a real-time display of system activity. The following figure displays a sample **Access Tracker** page followed by parameter definition.

Figure 4: *Access Tracker Page*

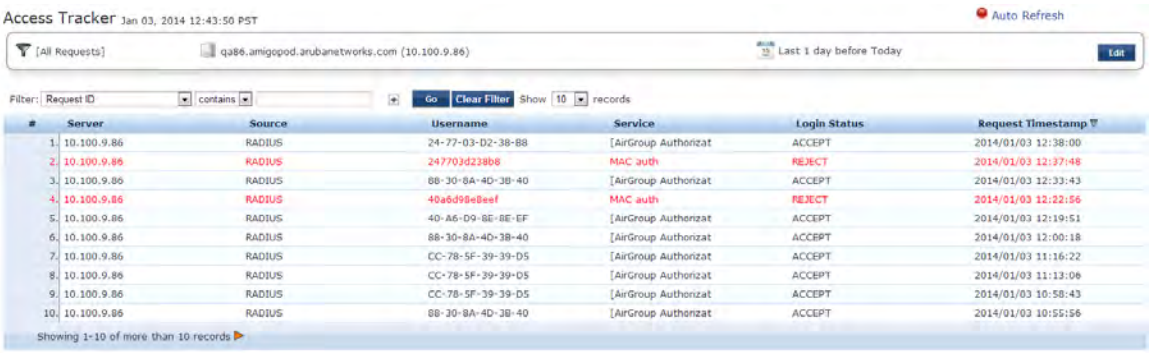


Table 4: *Access Tracker Page Parameters*

Parameter	Description
Server	Displays the IP address of the server.
Source	Displays the source of authentication. For example, TACACS or web authentication.
Username	Displays the MAC address of the user.
Service	Displays the name of the service. For example, Health Only, MAC authentication, or AirGroup Authorization.
Login Status	Displays the login status such as ACCEPT or REJECT.
Request Timestamp	Displays the data and time when the status was last updated.

For more information, see:

- Editing the Access Tracker on page 18
- Viewing Access Tracker Session Details on page 19

Editing the Access Tracker

You can change the **Access Tracker** parameters by clicking the **Edit** button.

Figure 5: *Access Tracker Page (edit mode)*

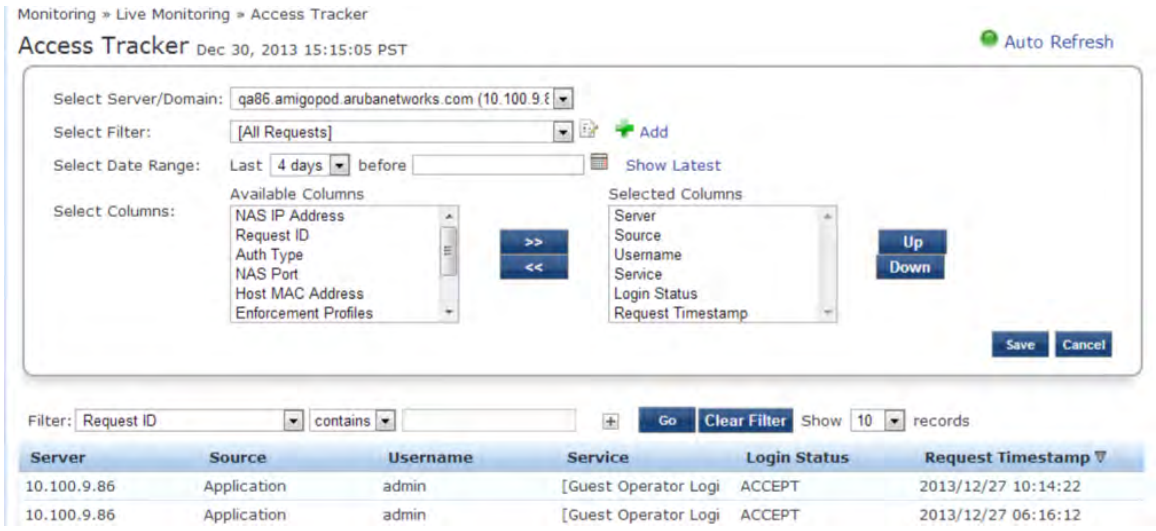


Table 5: *Access Tracker Edit Page (edit mode) Parameters*

Parameter	Description
Select Server/Domain	Select the server for which the dashboard data to be displayed. Select all the servers to display transactions from all nodes in the Policy Manager cluster.
Select Filter	Select a filter category to constrain data display. For a description of available filters, see Data Filters on page 58.
	Click to modify the current data filter. For more information, see Data Filters on page 58.
	Click to add a data filter. The **Data Filters** page opens. For more information, see Data Filters on page 58.
Select Date Range	Select the number of days prior to the configured date for which **Access Tracker** data to be displayed. Select 1-6 days or 1 week.
	Click to select a previous date.
Show Latest	Click to set the before date to Today.
Select Columns	**Available Columns**: Displays the column names that you can select and display in an **Access Tracker** report.
	Selected Columns: Displays the column names you selected to display in an **Access Tracker** report.

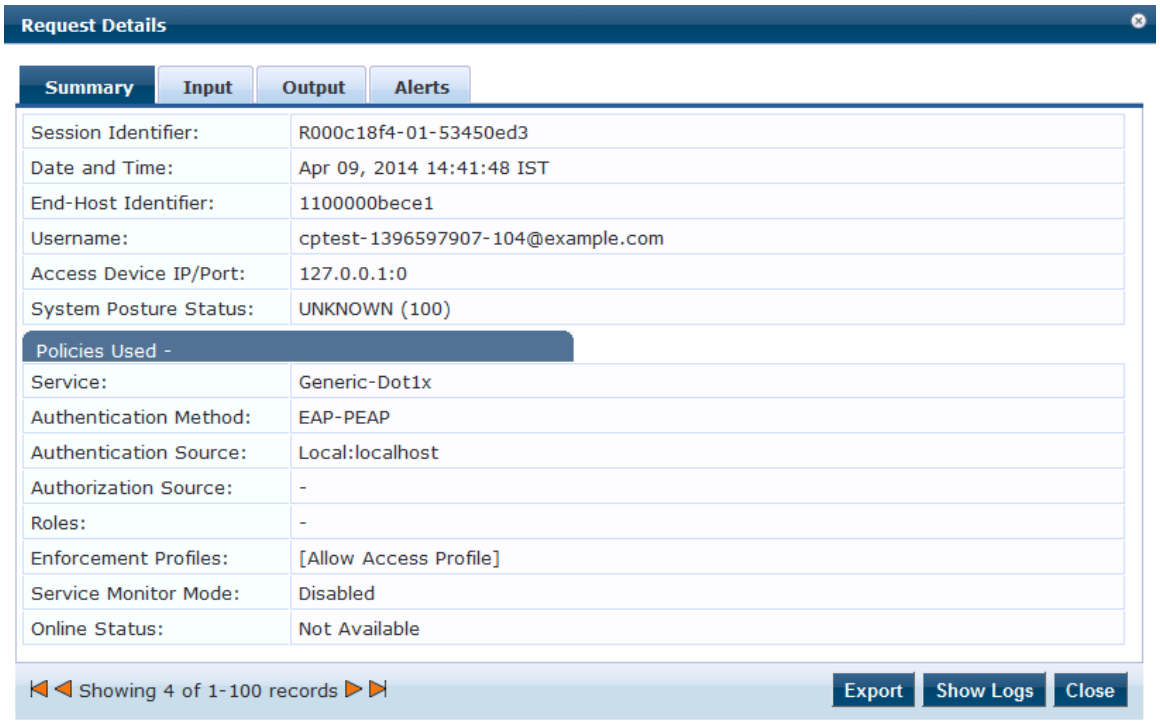
Viewing Access Tracker Session Details

This section includes examples of the tabs displayed on the **Request Details** page. To view details about a session, click a row in the table with any entry. The actions available depend on the type of device. The **Disconnect** or **Terminate Section** action is supported by all devices. Some devices support setting a session timeout, changing the VLAN for the session, applying an ACL, and so on.

Summary tab

This tab shows a summary view of the transaction including policies that are applied and protocol specific attributes. The following figure shows the example of the **Request Details - Summary** tab:

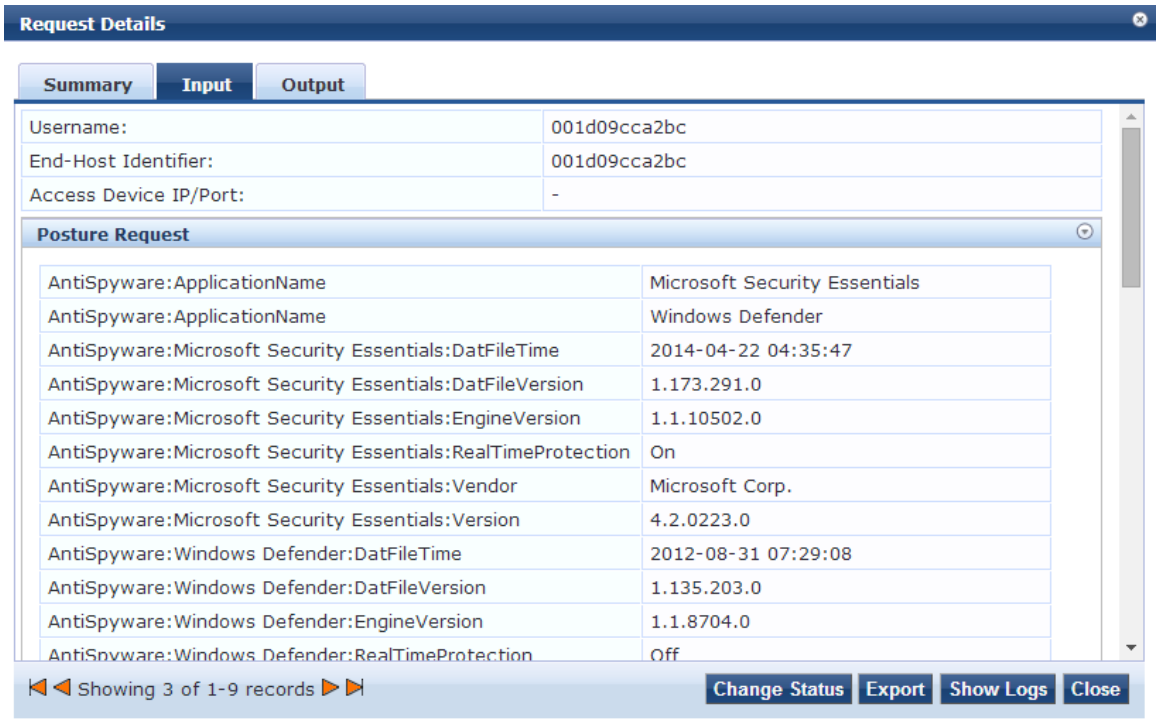
Figure 6: *Request Details - Summary tab*



Input tab

This tab shows protocol specific attributes that Policy Manager received in a transaction request; this includes authentication and posture details (if available). The **Input** tab also shows **Computed Attributes** that were derived from the request attributes. All of the attributes can be used in role mapping rules. The following figure shows an example of the **Request Details - Input** tab:

Figure 7: *Request Details - Input tab*



Output tab

This tab shows the attributes that were sent to the network device and the posture-capable endpoint. The following figure shows an example of the **Request Details - Output** tab:

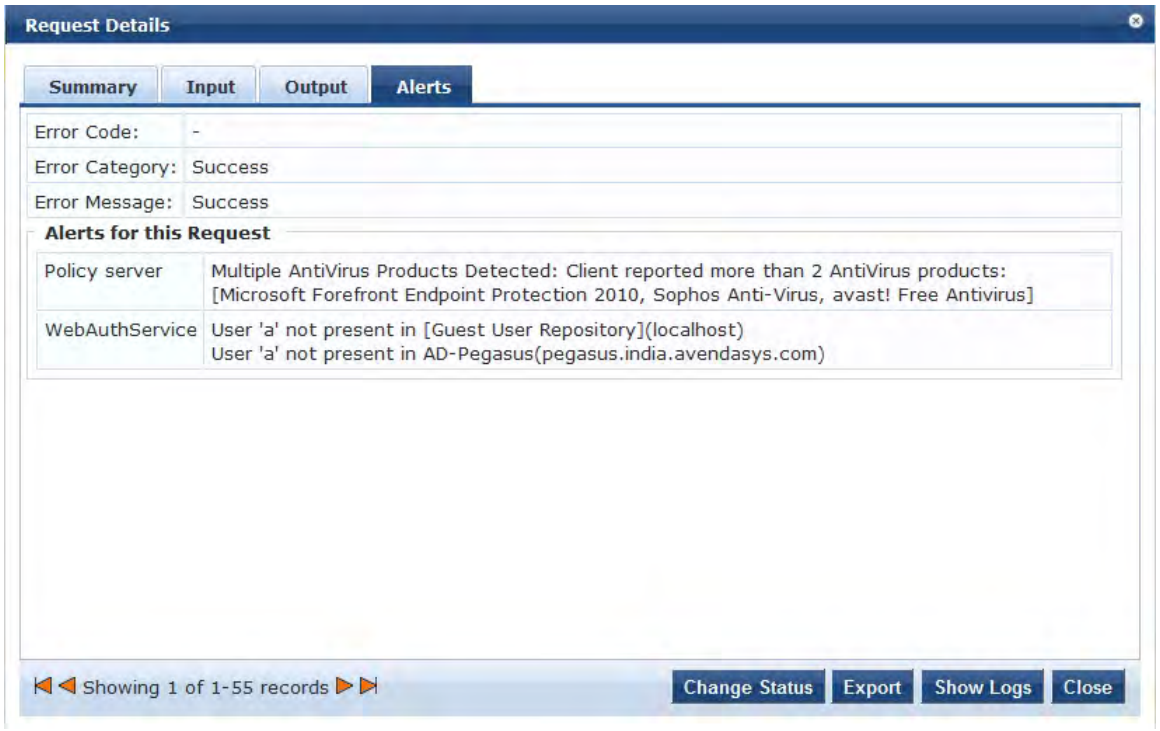
Figure 8: *Request Details - Output tab*

Administrators can view the posture response and posture evaluation with accurate results. For example, the administrator can view details such as missing registry keys and the reasons for a failed registry key check.

Alerts tab

This tab is displayed only when an error occurs. For example, if you select a row in a report where the **Login** status displays TIMEOUT or REJECT, an alert is triggered. The following figure shows an example of the **Request Details - Alerts** tab:

Figure 9: *Request Details - Alerts tab*



NOTE

Access tracker shows an alert if more than two anti-malware products are installed on a client.

Access Control Capabilities

You can use the **Access Control Capabilities** page to view or change the access control type. The **Access Control Capabilities** page is displayed if you click the **Change Status** button in the **Request Details** screen. The **Change Status** button is enabled only if you use the RADIUS and WebAuth authentication types.

Figure 10: *Access Control Capabilities*

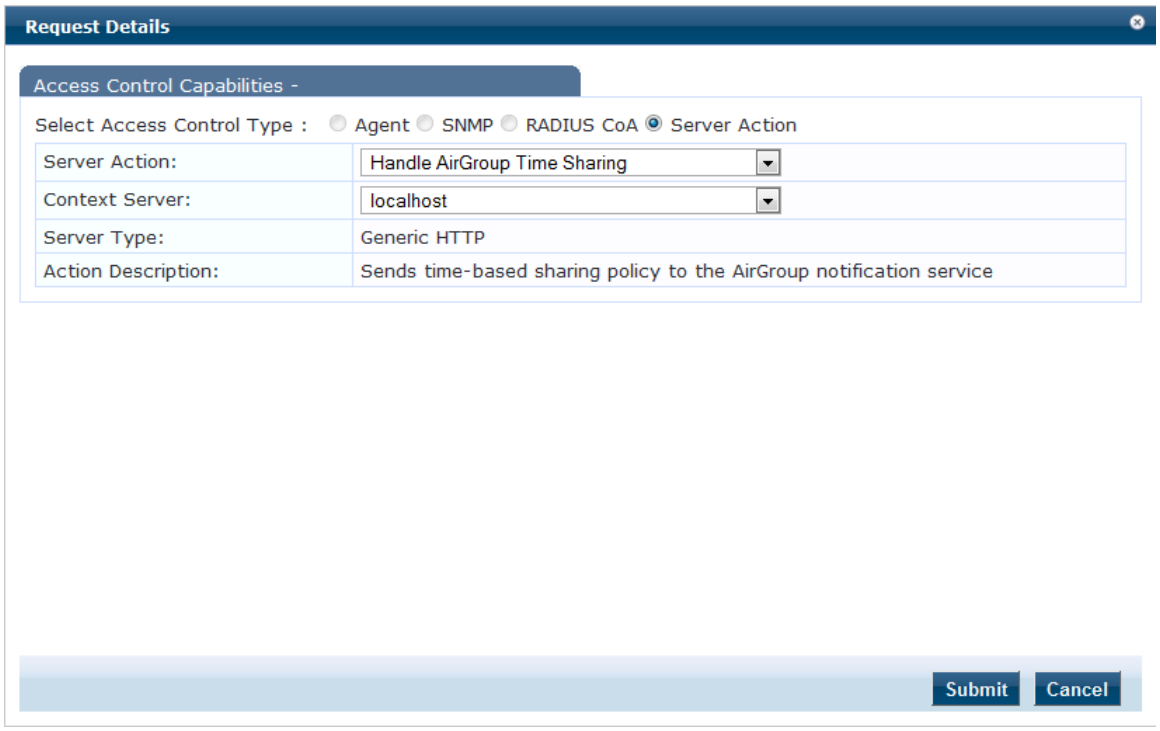


Table 6: *Request Details - Access Control Capabilities Page Parameters*

Parameter	Description

Change Status	You can view or change to any of the following access control types: .
	• **Agent -** This control is available for a session where the endpoint has the OnGuard Agent installed. The following actions are allowed:
	  ▪ Bouncing
	  ▪ Sending Messages
	  ▪ Tagging the status of the endpoint as **Disabled** or **Known**.
	• **SNMP -** This control is available for any session for which Policy Manager has the switch and port-level information associated with the MAC address of the endpoint. Policy Manager bounces the switch port to which the endpoint is associated using SNMP.
	NOTE: For this type of control, SNMP read and write community strings must be configured for the network device. You must configure the Policy Manager as an SNMP trap receiver to receive link up/down traps.
	• **RADIUS CoA -** This control is available for any session where access was previously controlled by a RADIUS transaction.
	NOTE: The network device must be RADIUS CoA capable and RADIUS CoA enabled, when you configure the network device in Policy Manager. The actions available depend on the type of device. The **Disconnect** or **Terminate Section** action is supported by all devices. Some devices support setting a session timeout, changing the VLAN for the session, and applying an ACL.

Server Action	Select the server action that is performed on endpoints. For example, Send message, Lock Device, Remote Wipe, and so on.
Context Server	Enter a valid server name. You can enter an IP address or domain name.
Server Type	Displays the server type configured when the server action was configured.
Action Description	Specifies the description of the action. For example, the description can be "Delete all information stored" if the configured action is **Remote Wipe**.

Accounting

The **Accounting** page provides a dynamic report that describes accesses (as reported by the network access device by means of RADIUS or TACACS+ accounting records) in the **Monitoring > Live Monitoring > Accounting** page. Click a row to display the corresponding **Accounting** page. The following figure displays a sample **Accounting** page followed by parameter definition.

Figure 11: *Accounting Page (Edit Mode)*

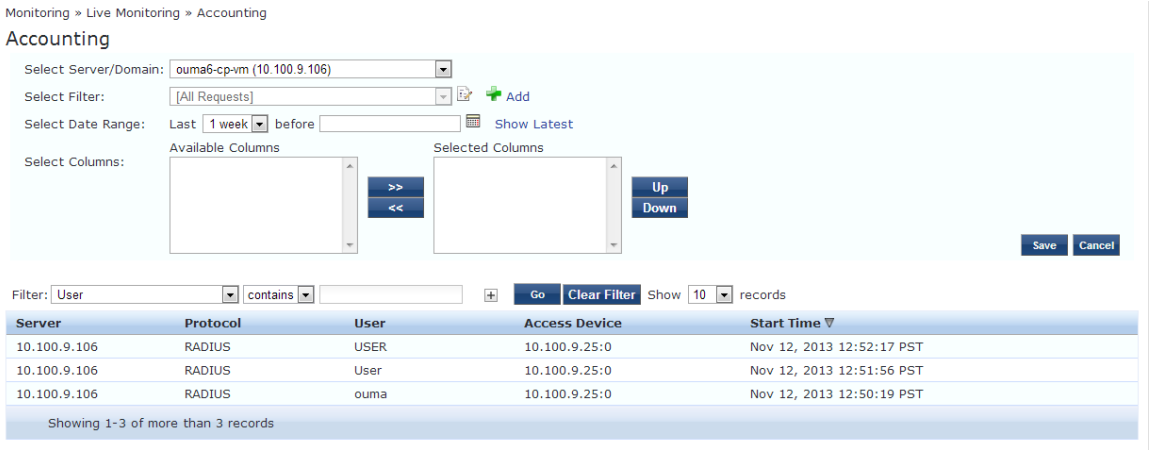


Table 7: *Accounting Page (Edit Mode) Parameters*

Parameter	Description
Select Server/Domain	Select server for which the dashboard data to be displayed.
Select Filter	Select filter to constrain data display.
Modify 	Modify the currently displayed data filter.
Add 	Go to **Data Filters** page to create a new data filter.
Select Date Range	Select the number of days prior to the configured date for which the accounting data to be displayed. You can specify the number from 1 day to a week.
Show Latest	Set the date to **Today** to view the latest information.
Select Columns	Click the right or left arrows to move data between **Available Columns** and **Selected Columns**. Click the **Up** or **Down** buttons to rearrange columns.

For more information, see:

- RADIUS Accounting Record Details (Auth Sessions tab) on page 26
- RADIUS Accounting Record Details (Details tab) on page 27
- RADIUS Accounting Record Details (Summary tab) on page 27
- RADIUS Accounting Record Details (Utilization tab) on page 29
- TACACS+ Accounting Record Details (Auth Sessions tab) on page 31
- TACACS+ Accounting Record Details (Details tab) on page 31
- TACACS+ Accounting Record Details (Request tab) on page 32

RADIUS Accounting Record Details (Auth Sessions tab)

This section describes the parameters of the **Accounting Record Details - Auth Sessions** tab for the RADIUS protocol.

Figure 12: *RADIUS Accounting Record Details Auth Sessions tab*

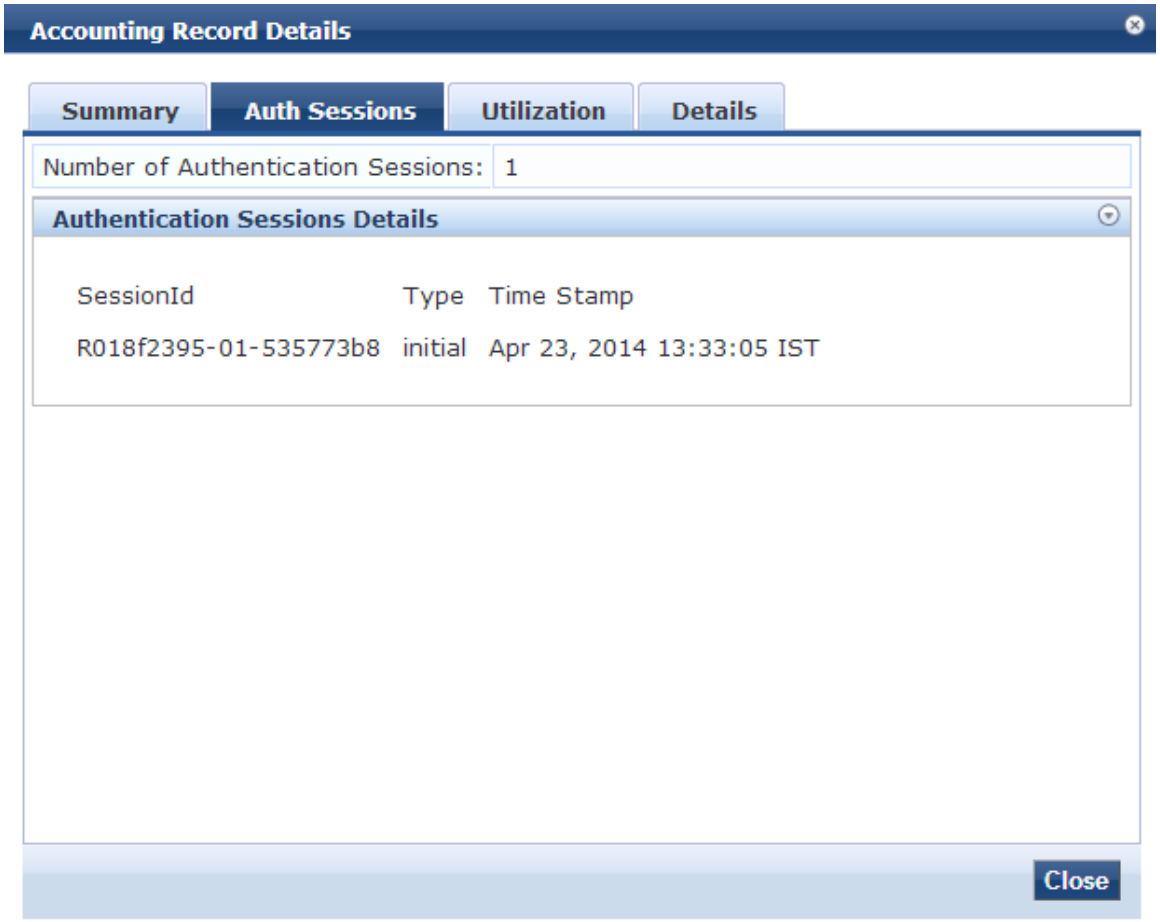


Table 8: *RADIUS Accounting Record Details Auth Sessions tab Parameters*

Parameter	Description
Number of Authentication Sessions	Specifies the total number of authentications (always 1) and authorizations in this session.
Authentication Sessions Details	
Session ID	Displays the Policy Manager session ID.
Type	Specifies the type of authentication from any the two options: Initial authentication or re-authentication.
Time Stamp	Specifies the time when the event occurred.

RADIUS Accounting Record Details (Details tab)

This section describes the parameters of the **Accounting Record Details - Details** tab for the RADIUS protocol.

Figure 13: *RADIUS Accounting Details tab*

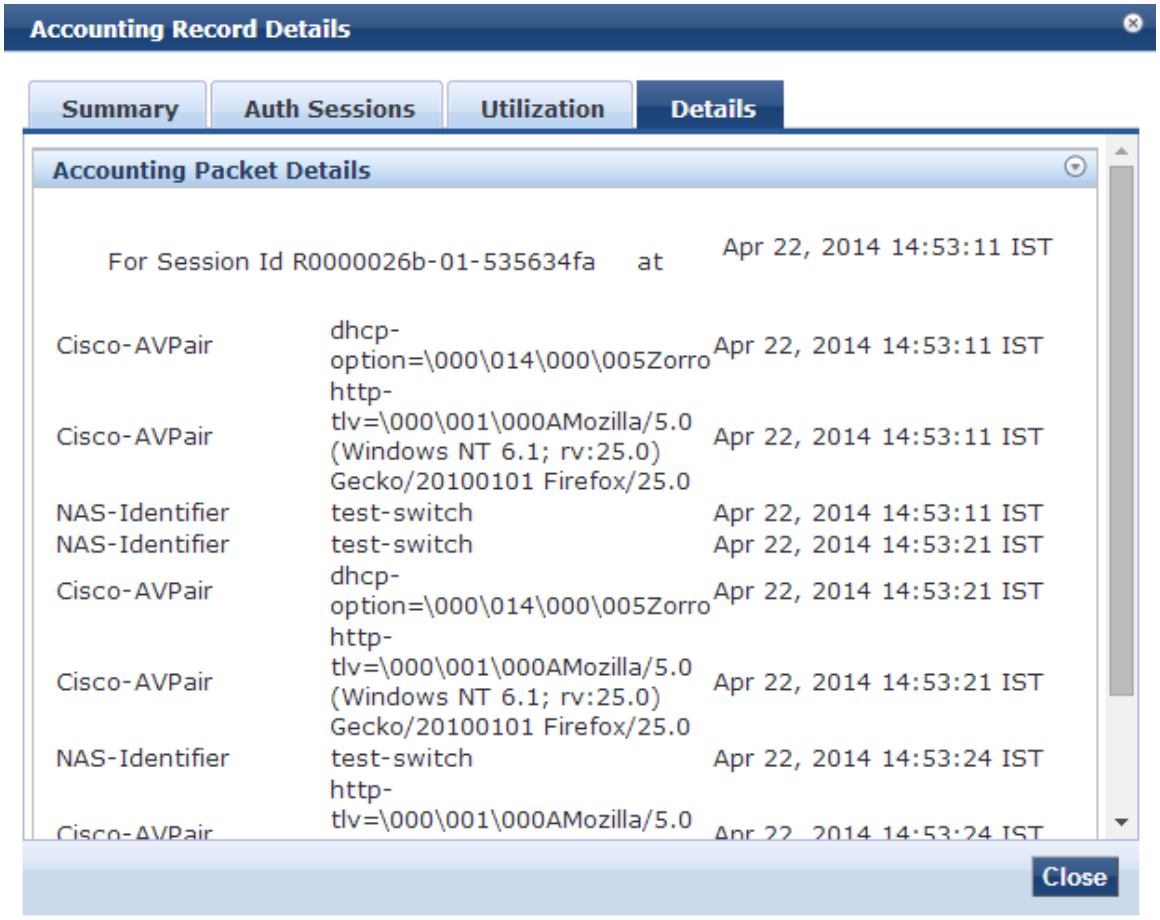


Table 9: *RADIUS Accounting Record Details tab Parameters*

Parameter	Description
Accounting Packet Details	Shows details of RADIUS attributes sent and received from the network device during an initial authentication and subsequent re-authentications (each section in the **Details** tab corresponds to a 'session' in Policy Manager).

RADIUS Accounting Record Details (Summary tab)

This section describes the parameters of the **Accounting Record Details - Summary** tab for the RADIUS Protocol.

Figure 14: *RADIUS Accounting Record Details Summary tab*

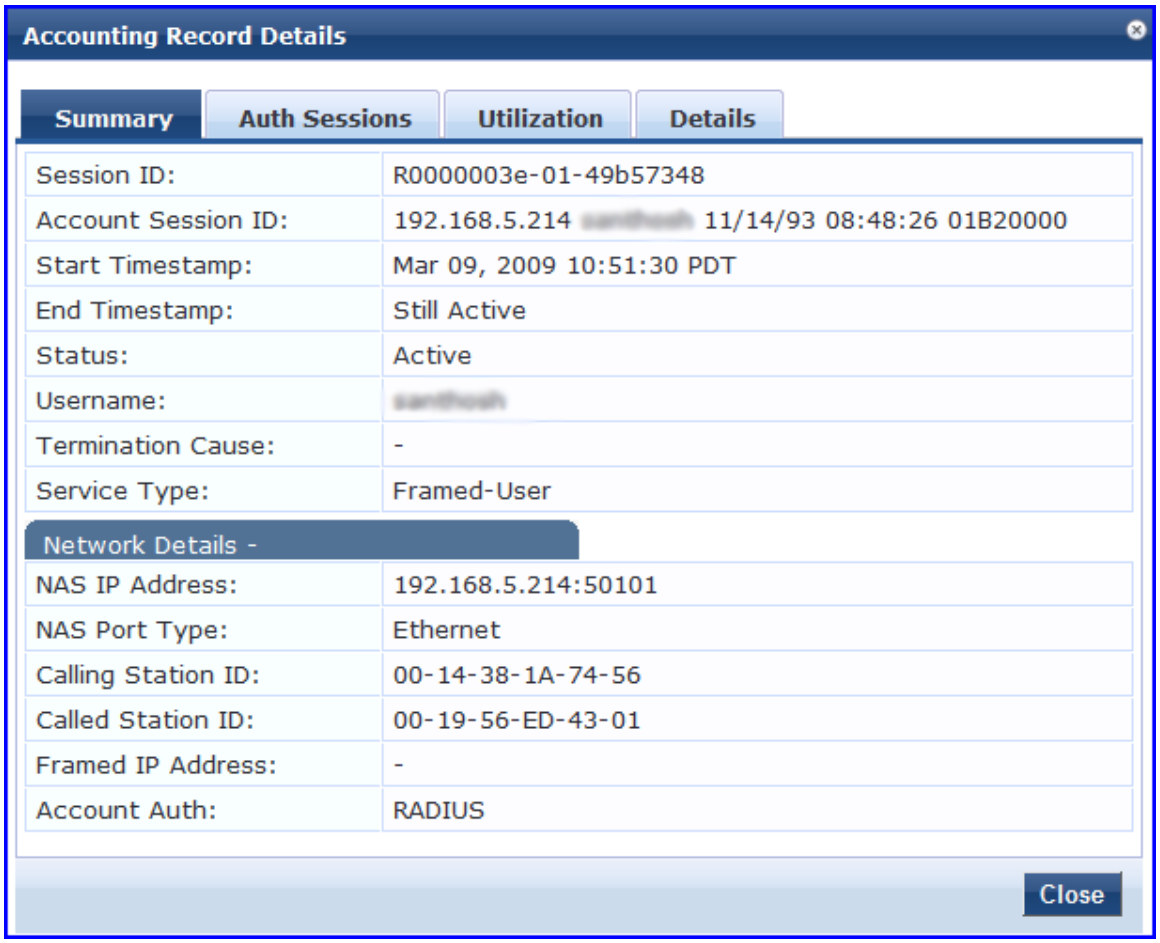


Table 10: *RADIUS Accounting Record Details Summary tab Parameters*

Parameter	Description
Session ID	Specifies the Policy Manager session identifier. You can correlate this record with a record in **Access Tracker**.
Account Session ID	Specifies a unique ID for this accounting record.
Start and End Timestamp	Shows the start and end time of the session.
Status	Shows the current connection status of the session.
Username	Username associated with this record.
Termination Cause	Specifies the reason for termination of this session.

Table 10: *RADIUS Accounting Record Details Summary tab Parameters (Continued)*

Parameter	Description
Service Type	Shows the value of the standard RADIUS attribute service type.
Network Details	
NAS IP Address	Shows the IP address of the network device.
NAS Port Type	Shows the access methods. For example, Ethernet, 802.11 Wireless, and so on.
Calling Station ID	Specifies the MAC address of the client that is supported by Policy Manager.
Called Station ID	Shows the MAC Address of the network device.
Framed IP Address	Shows the IP Address of the client (if available).
Account Auth	Specifies the type of authentication. Here this specifies the RADIUS authentication.

RADIUS Accounting Record Details (Utilization tab)

This section describes the parameters of the **Accounting Record Details - Utilization** tab for the RADIUS Protocol.

Figure 15: *RADIUS Accounting Record Details (Utilization tab)*

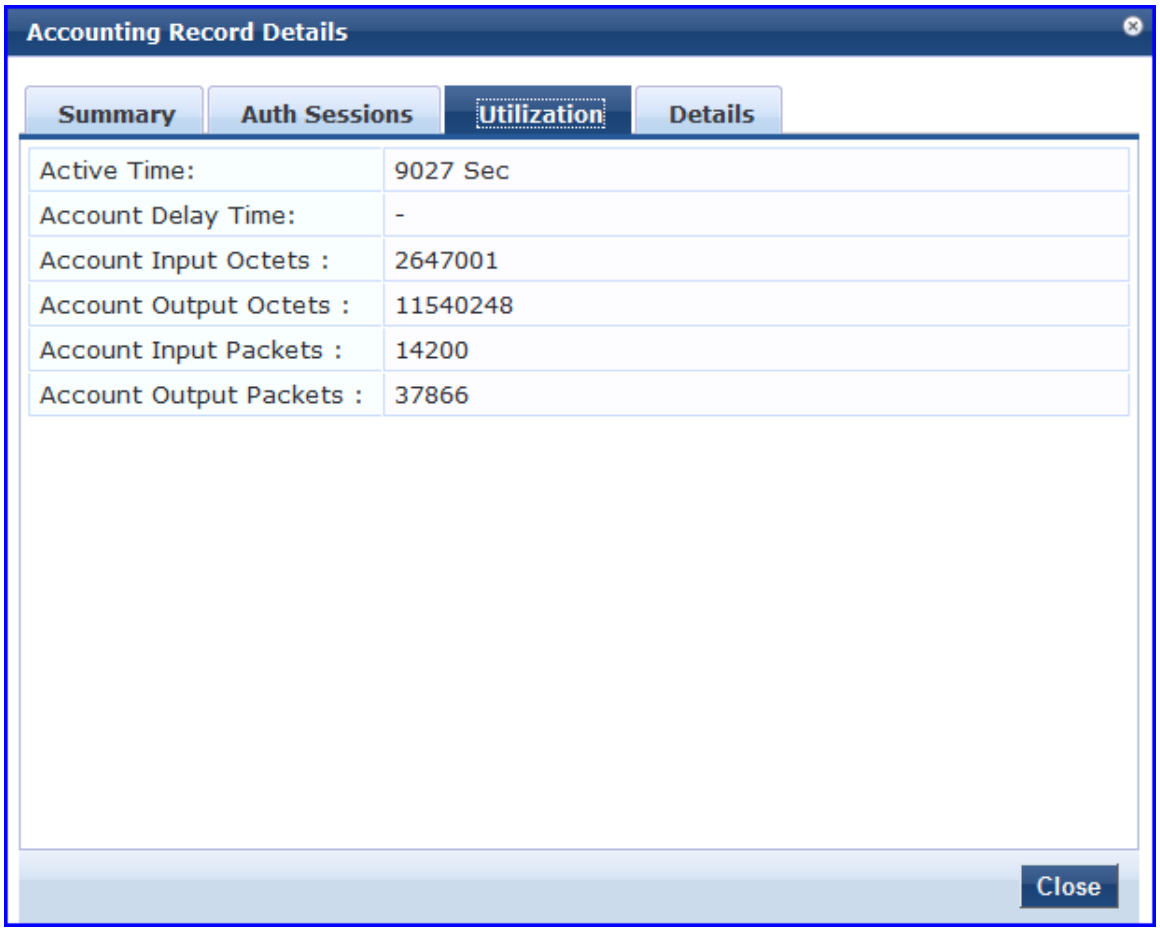


Table 11: *RADIUS Accounting Record Details Utilization tab Parameters*

Parameter	Description
Active Time	Displays how long the session was active.
Account Delay Time	Displays how many seconds the network device has been trying to send this record for (subtract from record time stamp to determine the time this record was actually generated by the device).
Account Input Octets	Specifies the quantity of octets sent to and received from the device port during the session.
Account Output Octets	
Account Input Packets	Specifies the packets sent and received from the device port during the session.
Account Output Packets	

TACACS+ Accounting Record Details (Auth Sessions tab)

This section describes the parameters of the **Accounting Record Details - Auth Sessions** tab for the TACACS+ Protocol.

Figure 16: *TACACS+ Accounting Record Details (Auth Sessions tab)*

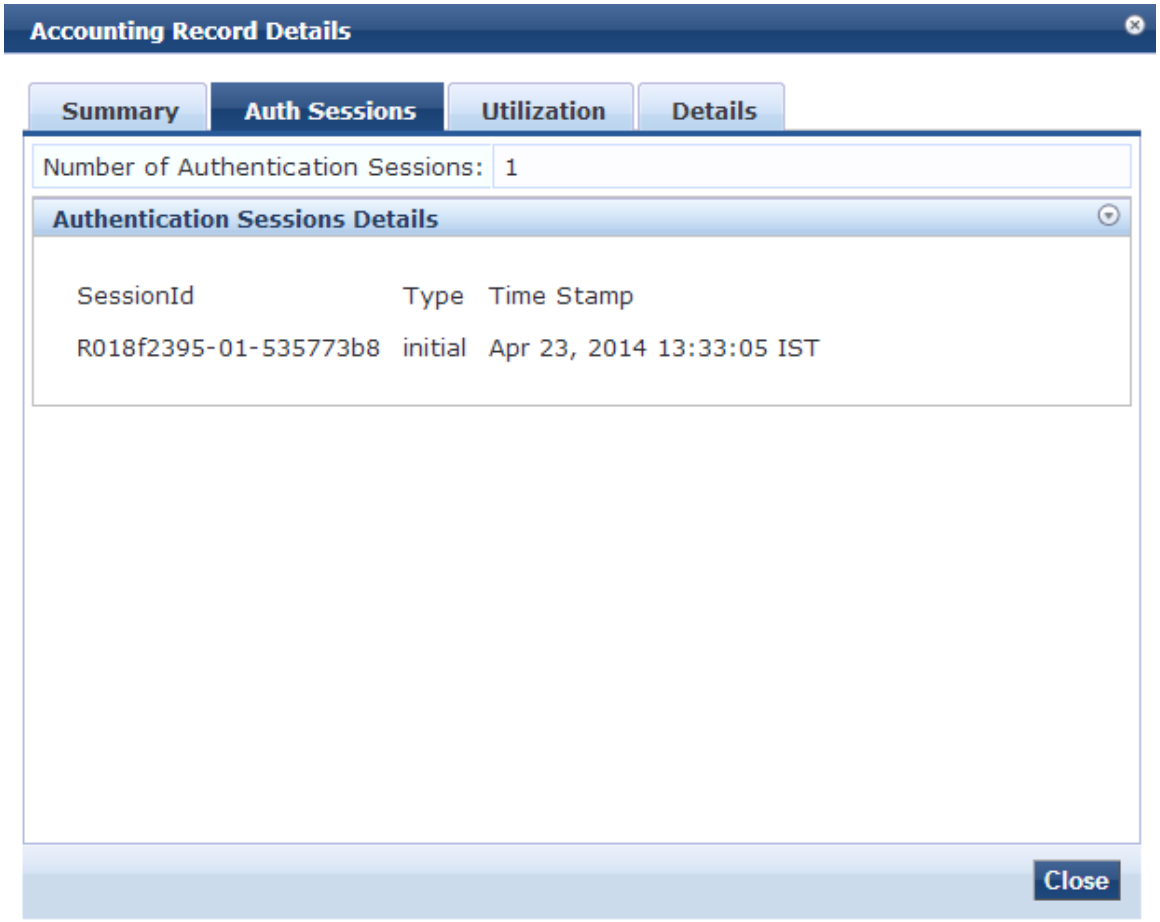


Table 12: *TACACS+ Accounting Record Details Auth Sessions tab Parameters*

Parameter	Description
Number of Authentication Sessions	Specifies the total number of authentications (always 1) and authorizations in this session.
Authentication Sessions Details	Denotes whether the request is an authentication or authorization request, and the time at which the request was sent for each request ID.

TACACS+ Accounting Record Details (Details tab)

This section describes the parameters of the **Accounting Record Details - Details** tab for the TACACS+ Protocol.

Figure 17: *TACACS+ Accounting Record Details (Details tab)*

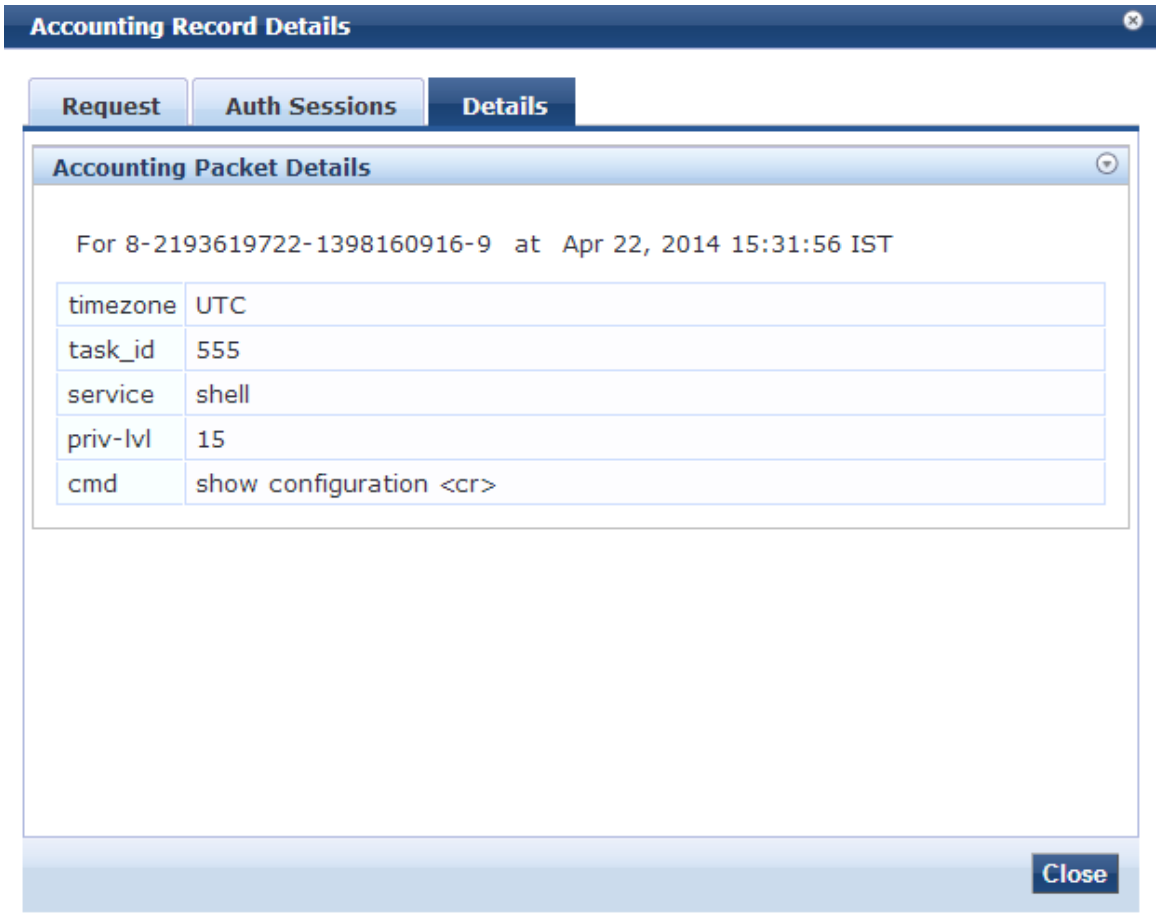


Table 13: *TACACS+ Accounting Record Details tab Parameters*

Parameter	Description
Accounting Packet Details	Shows cmd (command typed), priv-lvl (privilege level of the administrator executing the command), service (shell), and so on for each authorization request.

TACACS+ Accounting Record Details (Request tab)

This topic describes the parameters of the **Accounting Record Details - Request Sessions** tab for the TACACS+ Protocol.

Figure 18: *TACACS+ Accounting Record Details (Request tab)*

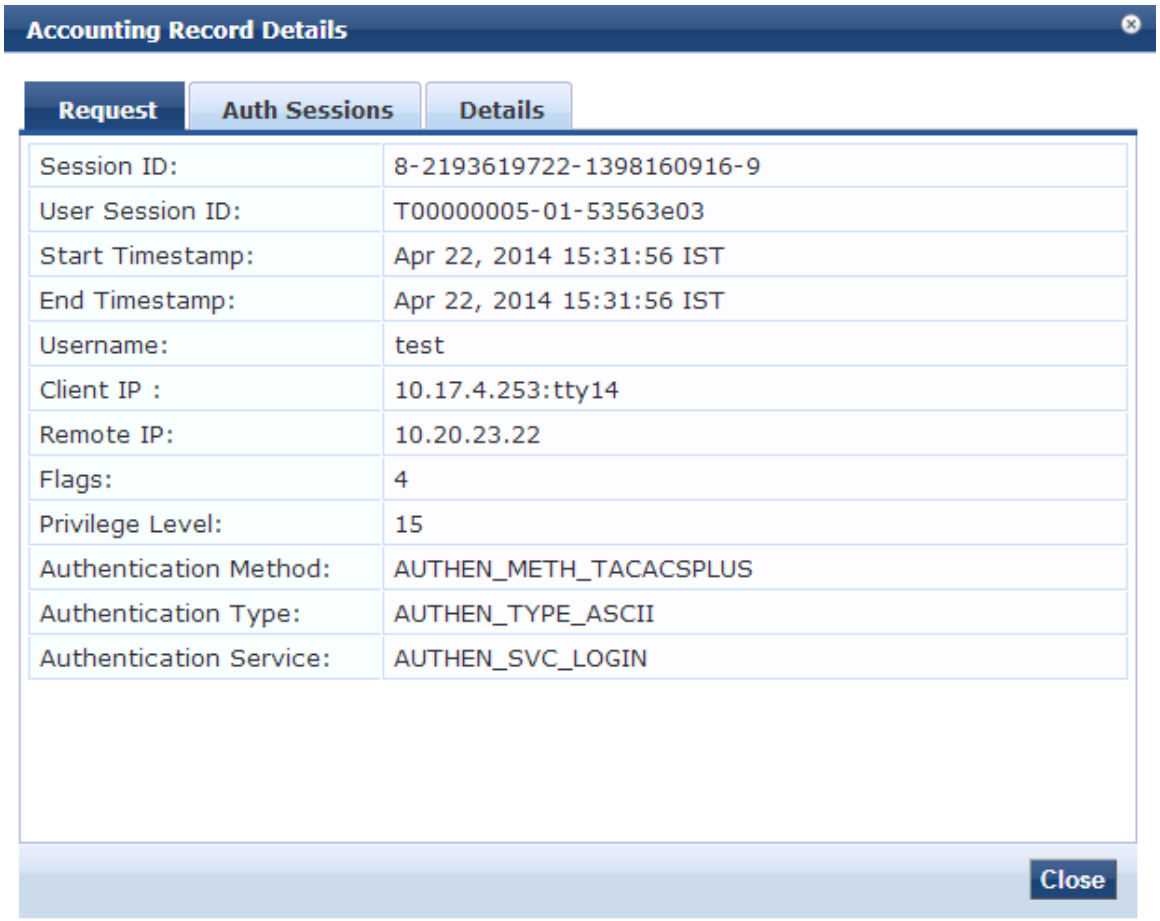


Table 14: *TACACS+ Accounting Record Request tab Parameters*

Parameter	Description
Session ID	Specifies the Session ID is a unique ID associated with a request.
User Session ID	Specifies a session ID that correlates authentication, authorization, and accounting records.
Start and End Timestamp	Shows the start and end time of the session.
Username	Shows the username associated with this record.
Client IP	Shows the IP address and tty of the device interface.
Remote IP	Shows the IP address from which Admin is logged in.
Flags	Shows the identifier corresponding to start, stop, or update accounting record.
Privilege Level	Specifies the privilege level of the administrator. The range is from

Table 14: *TACACS+ Accounting Record Request tab Parameters (Continued)*

Parameter	Description
	1 (lowest) to 15 (highest).
Authentication Method	Identifies the authentication method used for the access.
Authentication Type	Identifies the authentication type used for the access.
Authentication Service	Identifies the authentication service used for the access.

OnGuard Activity

The **OnGuard Activity** page shows the real-time status of all endpoints that have Dell W- OnGuard persistent or dissolvable agent in the **Monitoring > Live Monitoring > OnGuard Activity** page. This page also presents configuration tools to bounce an endpoint and to send unicast or broadcast messages to all endpoints running the W-OnGuard agent. The following figure displays a sample **OnGuard Activity** page followed by parameter definition.

Endpoint bounce only works with endpoints that run the persistent agent.

Figure 19: *OnGuard Activity*

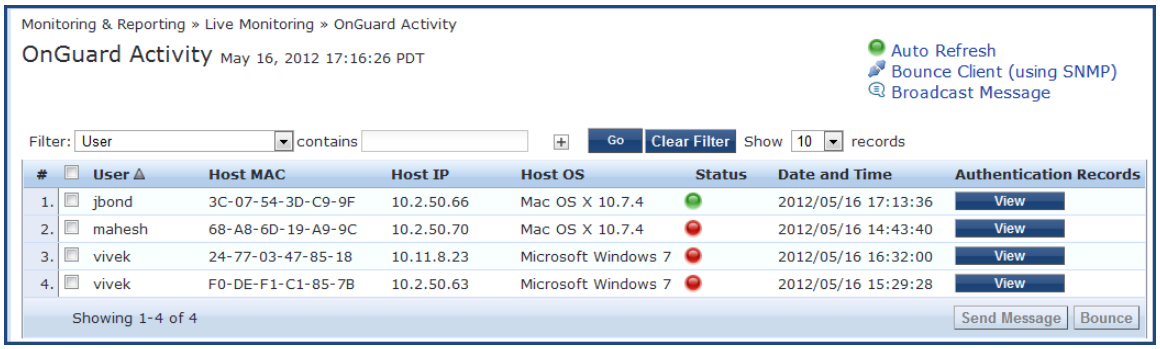


Table 15: *OnGuard Activity Parameters*

Parameter	Description
User	Displays the name of the user.
Host MAC	Displays the MAC address of the host.
Host IP	Displays the IP address of the host.
Host OS	Displays the operating system that runs on the host .

Table 15: *OnGuard Activity Parameters (Continued)*

Parameter	Description
Status	Displays the online status of the host. Green indicates online and red indicates offline.
Date and Time	Displays the date and time at which the user was created.
Authentication Records	Click the **View** button to see the **Endpoint Authentication Details** screen with the authentication records.

For more information, see:

- Bounce an Agent (non-SNMP) on page 35
- Bouncing a Client Using SNMP on page 38
- Broadcast Message on page 39
- Send Message on page 39

Bounce an Agent (non-SNMP)

This page is used to initiate a bounce on the managed interface on an endpoint. Initiating a bounce on the managed interface on the endpoint results in creating tags for the specified endpoint in the **Endpoints** table (see **Configuration** > **Identity** > **Endpoints**). One or more of the following tags are created:

- Disabled by
- Disabled Reason
- Enabled by
- Enabled Reason
- Info URL

To bounce an agent, click a row on the **OnGuard Activity** page. After clicking a row, the **Agent and Endpoint details** window opens. The following is an example of the **Agent and Endpoint details** screen:

Figure 20: *Agent and Endpoint details*

Table 16: *Agent and Endpoint details Parameters*

Parameter	Description
User	Displays the name of the user.
Host MAC	Displays the MAC address of the user.
Host IP	Displays the IP address of the host.
Status	Shows the online or offline status of the agent.
Agent Type	Specifies the type of the OnGuard agent.
Host OS	Displays the operating system that runs on the endpoint.
Registered Policy Manager Server	Displays the name and IP address of the Policy Manager server.
Registered at	Displays the date and time at which the Policy Manager was registered.
Last Seen Health Status	Displays the health status of the endpoint. For example, QUARANTINED or HEALTHY.

Table 16: *Agent and Endpoint details Parameters (Continued)*

Parameter	Description
Unhealthy Health Classes	Displays the health classes that are unhealthy. For example, AntiVirus and PatchAgent.
Description	
Status	Displays the status of the endpoint.
Added by	Displays the server name.

Click **Bounce** and the **Bounce Agents** window opens.

Figure 21: *Bounce Agents Page*

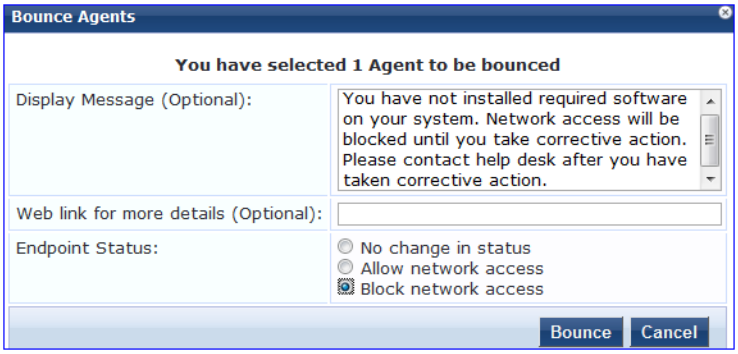


Table 17: *Bounce Agents Page Parameters*

Parameter	Description
Display Message (Optional)	An optional message to display on the endpoint using the OnGuard interface.
Web link for more details (Optional)	An optional clickable URL that is displayed along with the Display Message.
Endpoint Status	**No change in status** - No change is made to the status of the endpoint. The existing status of **Known**, **Unknown**, or **Disabled** continues to be applied. Access control is granted or denied based on the existing status of an endpoint. **Allow network access** - Allow network access by white-listing this endpoint. **NOTE:** Clicking **Allow network access** sets the status of the endpoint as **Known**. You must configure Enforcement Policy Rules to allow access to the endpoints with the status **Known**. **Block network access** - Block network access by blacklisting this endpoint. **NOTE:** Clicking **Block network access** sets the status of the endpoint to **Disabled**. You must configure **Enforcement Policy Rules** to allow access to the endpoints with the status **Disabled**.

Bouncing a Client Using SNMP

Perform a bounce operation (using SNMP) with the MAC or IP address of the endpoint on the switch port to which the endpoint is connected. This feature only works with wired Ethernet switches.

Requirements

To bounce a client using SNMP successfully, the following conditions are mandatory:

- The network device must be added to Policy Manager and SNMP read and write parameters must be configured.
- SNMP traps (link up and/or MAC notification) have to be enabled on the switch port.
- The DHCP snooper service on Policy Manager must receive DHCP packets from the endpoint to specify the IP address of the endpoint to bounce. Refer to your network device documentation to find out how to configure IP helper address.

Perform the following steps to bounce a client using SNMP:

1. Enter the client IP or MAC Address.
2. Click **Go**.
3. Click **Bounce**.

Figure 22: *Bounce Client (Using SNMP) Page*

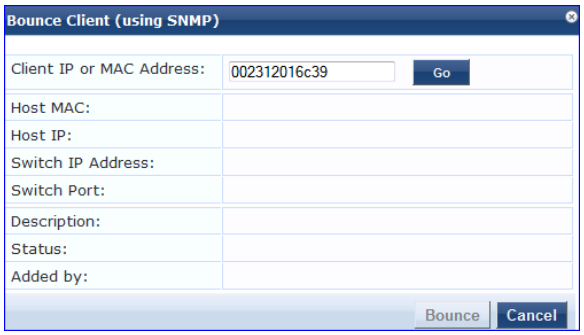


Table 18: *Bounce Client (Using SNMP) Page Parameters*

Parameter	Description
Client IP or MAC address	Enter the Client IP or MAC address of the bounce client.
Host MAC	Displays the MAC address of the host.
Host IP	Displays the IP address of the host.
Switch IP Address	Displays the IP address of the switch.
Switch Port	Displays the port number of the switch.
Description	Displays the description of the client.
Status	Displays the status of the client.
Added by	Displays the name of the user who added the client.

Broadcast Message

After you click the **Broadcast Message** link on the top right of the **OnGuard Activity** page, a page appears where you can write and send a message to all active endpoints.

Figure 23: *Broadcast Notification to Agents Page*

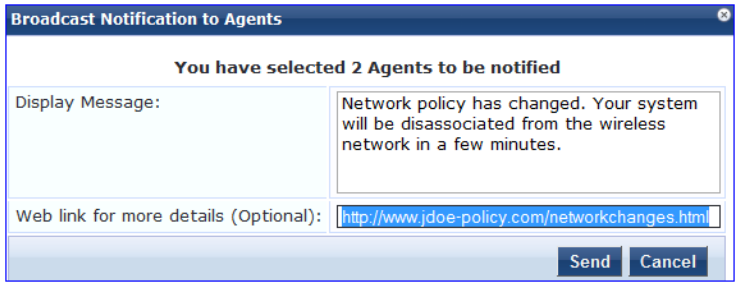


Table 19: *Broadcast Notification to Agents Page Parameters*

Parameter	Description
Display Message	Enter the message that needs to be notified to the active endpoints.
Web link for more details (Optional)	A clickable URL that is displayed along with the **Display Message**. This field is optional.

Send Message

Perform the following steps to send a message to a selected endpoint:

1. Select one or more rows on the **OnGuard Activity** page.
2. Click the **Send Message** button. The **Send Notification to Agents** screen opens.
3. Enter a message and click **Send** to send the message.

Figure 24: *Send Notifications to Agents*

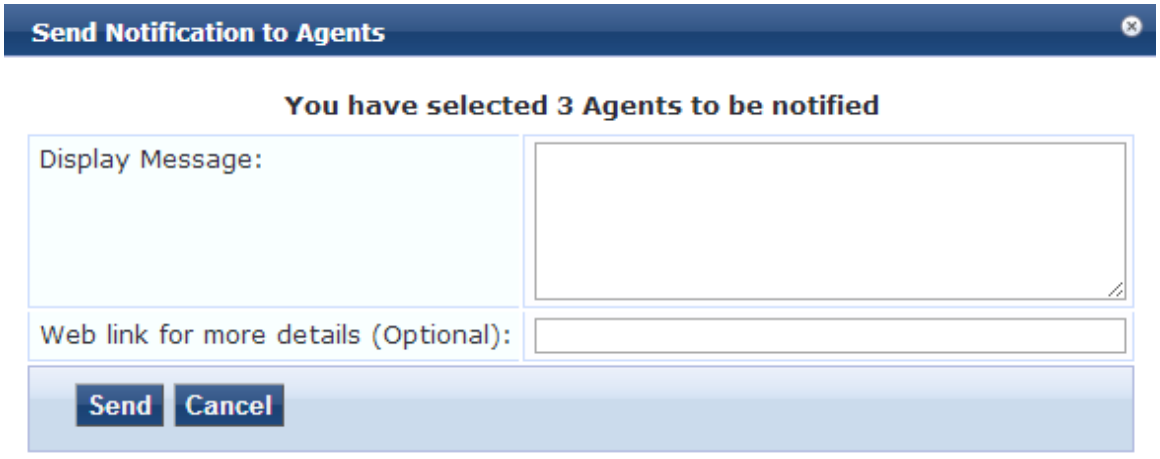


Table 20: *Send Notifications to Agents Page Parameters*

Parameter	Description
Display Message	Enter the message that needs to be notified to the active endpoints.
Web link for more details (Optional)	A clickable URL that is displayed along with the **Display Message**. This field is optional.

Analysis and Trending

The **Analysis and Trending** page displays monthly, bi-weekly, weekly, daily, or 12-hourly, 6-hourly, 3-hourly, or hourly quantity of requests for the subset of components included in the selected filters. The data can be aggregated by minute, hour, day, or week. The list at the end of this section shows the per-filter count for the aggregated data.

Each bar corresponding to each filter in the bar graph is clickable. Clicking a bar drills down into the Access Tracker on page 17 that shows session data for the specific time slice and for the specific requests.

For a line graph, click the circle corresponding to each plotted point in the graph to drill down into **Access Tracker** page.

Figure 25: *Analysis and Trending*

Use the following components in the GUI to customize and filter the **Analysis and Trending** page:

Component	Description
Select Server	Select a node from the cluster for which data to be displayed.
Update Now!	Click to update the display with the latest available data.
Customize This!	Click to customize the display by adding filters. You can add up to a maximum of 4 filters.

Component	Description
Toggle Chart Type	Click to toggle chart display between line and bar type.
Add new Data Filter	Click to add a data filter in the global filter list.

To add filters, refer to Data Filters on page 58.

Endpoint Profiler

If the Profile license is enabled, a list of the profiled endpoints are visible in the **Endpoints Profiler** table. The list of endpoints you view is based on the **Device Category**, **Device Family**, and **Device Name** items that you selected. Click **Change Selection** to modify the selection criteria used to list the devices. Click **Change View** to see graphs that show information about distribution and update frequency for devices and computers.

Figure 26: *Endpoint Profiler (view 1)*

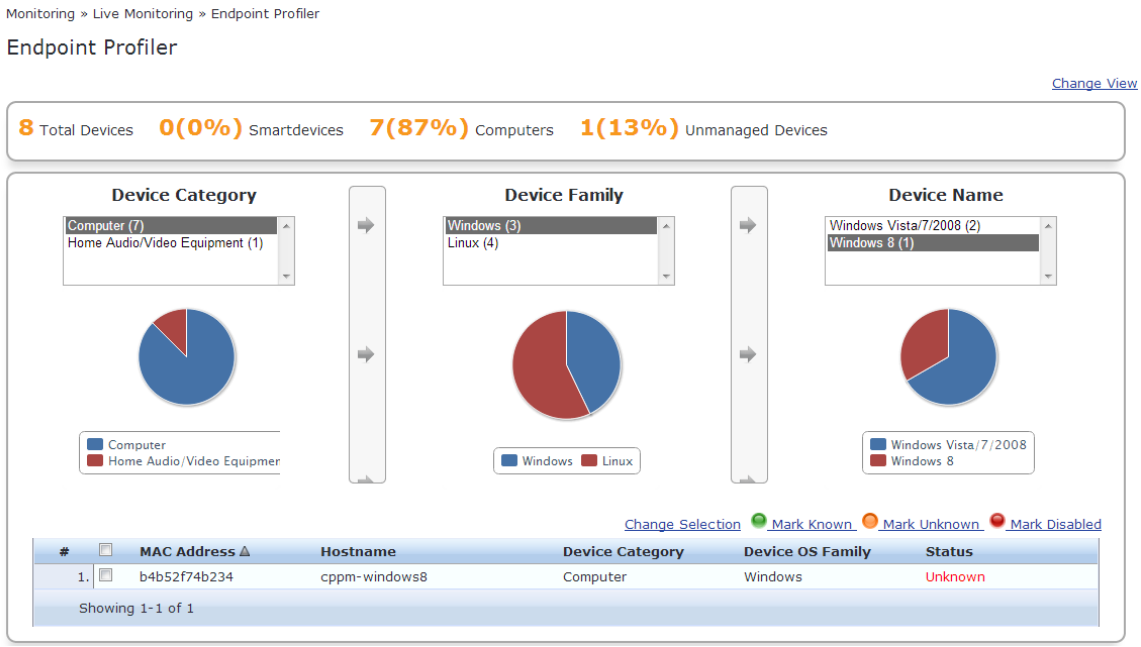
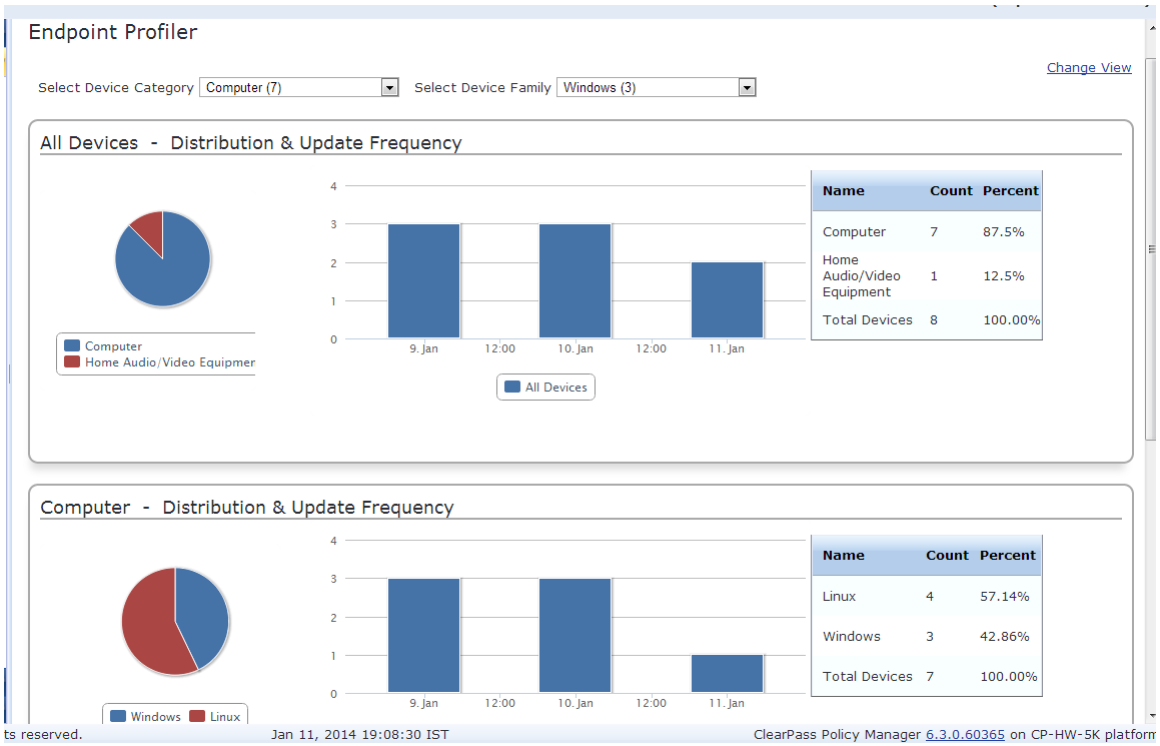


Figure 27: *Endpoint Profiler (view 2)*



Click a device in the table below the graphs to view endpoint details about a specific device. Select the **Cancel** button to return to the **Endpoint Profiler** page.

Figure 28: *Endpoint Profiler Details*

View Endpoint

MAC Address	181eb06005c9	IP Address	-
Description		Static IP	FALSE
Status	Known	Hostname	rfiler:Android 4.1:PDA 3
Added by	apiadmin	MAC Vendor	Samsung Electronics Co.,Ltd
		Device Category	SmartDevice
		Device OS Family	Android
		Device Name	Samsung-GT-N5110
		Added At	Nov 06, 2013 22:35:01 PST
		Updated At	Nov 19, 2013 16:15:13 PST
		Show Fingerprint	☑

Endpoint Fingerprint Details

Device Category:	SmartDevice
Device Family:	Android
Device Name:	Samsung-GT-N5110

	Attribute		Value
1.	Blacklisted App	=	False
2.	Carrier	=	PDA
3.	Compromised	=	False
4.	Display Name	=	Bob Filer
5.	Encryption Enabled	=	True
6.	Last Check In	=	3 d 5 h
7.	MDM Enabled	=	true
8.	MDM Identifier	=	b0cb2979-8280-45c6-94dd-3aef518a93f7
9.	Manufacturer	=	Samsung
10.	Model	=	GT-N5110
11.	OS Version	=	Android 4.1
12.	Owner	=	rfiler
13.	Ownership	=	Employee
14.	Phone Number	=	PDA 3

System Monitor

The **System Monitor** page has four tabs. Each tab provides one or more charts or graphs that give real-time information about various components.

System Monitor tab - Displays charts and graphs that include information about CPU load and usage, memory usage, and disk usage.

Process Monitor tab - Displays reports about a selected process. The processes that you can monitor include Policy server, TACACS server, stats collection service, and so on.

Network tab - Displays a graph about any selected network parameters such as web traffic, SSH, and so on.

ClearPass tab - ClearPass can plot graphs based on the performance monitoring counters and timers for the following categories:

- Service Categorization
- Authentication
- Authorization
- Posture Validation

- Audit Scan
- Enforcement
- End to End request processing

These components are actively monitored and the ClearPass tab displays the data collected for the last 30 minutes during the monitoring process.

Auto refresh ensures that the **System Monitor** page is updated for every 2 minutes. You can see the last updated time in the **Last updated at** field in the **System Monitor** page.

For more information, see:

- System Monitor tab on page 44
- Process Monitor tab on page 47
- Network tab on page 49
- ClearPass tab on page 50

System Monitor tab

The **System Monitor** tab displays information about component usage and load. The following figure displays a sample of the **System Monitor** tab:

Figure 29: *System Monitor Tab*

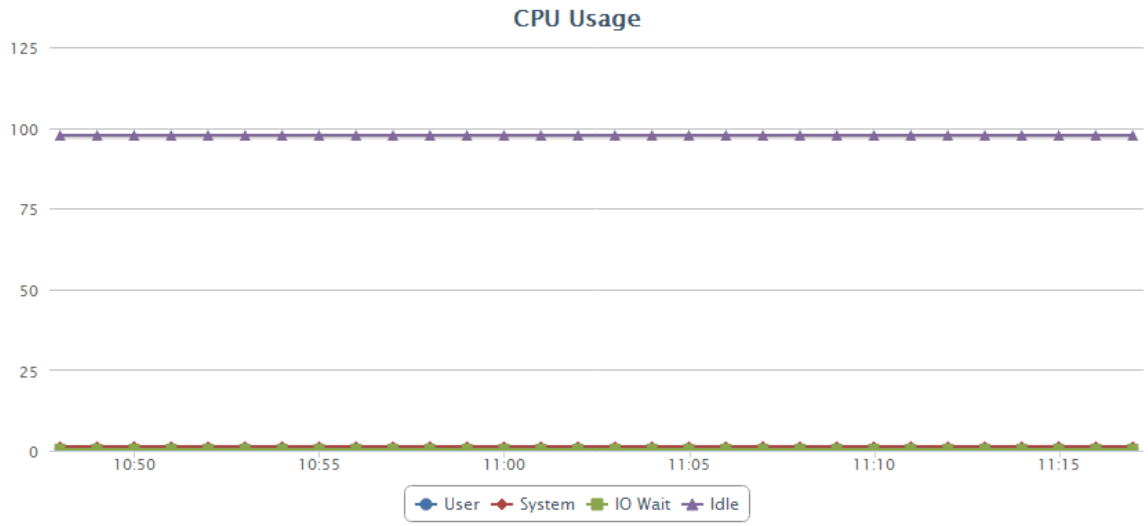
For more information, see:

- Monitoring CPU Usage on page 44
- Monitoring CPU Load on page 45
- Monitoring Memory Usage on page 45
- Monitoring Swap Memory Usage on page 46
- Monitoring Disk - / Usage on page 46
- Monitoring Disk Swap Usage on page 47

Monitoring CPU Usage

This graph shows the percentage of CPU usage based on User, System, IO Wait, and Idle time.

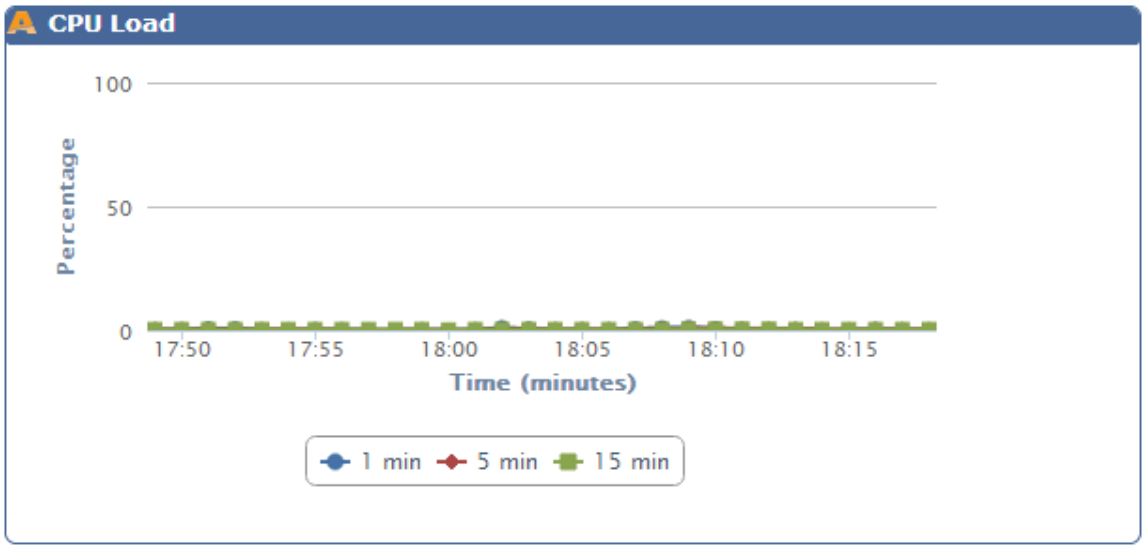
Figure 30: *CPU Usage Graph Example*



Monitoring CPU Load

This graph shows the percentage of CPU load in increments of 1, 5, and 15 minutes.

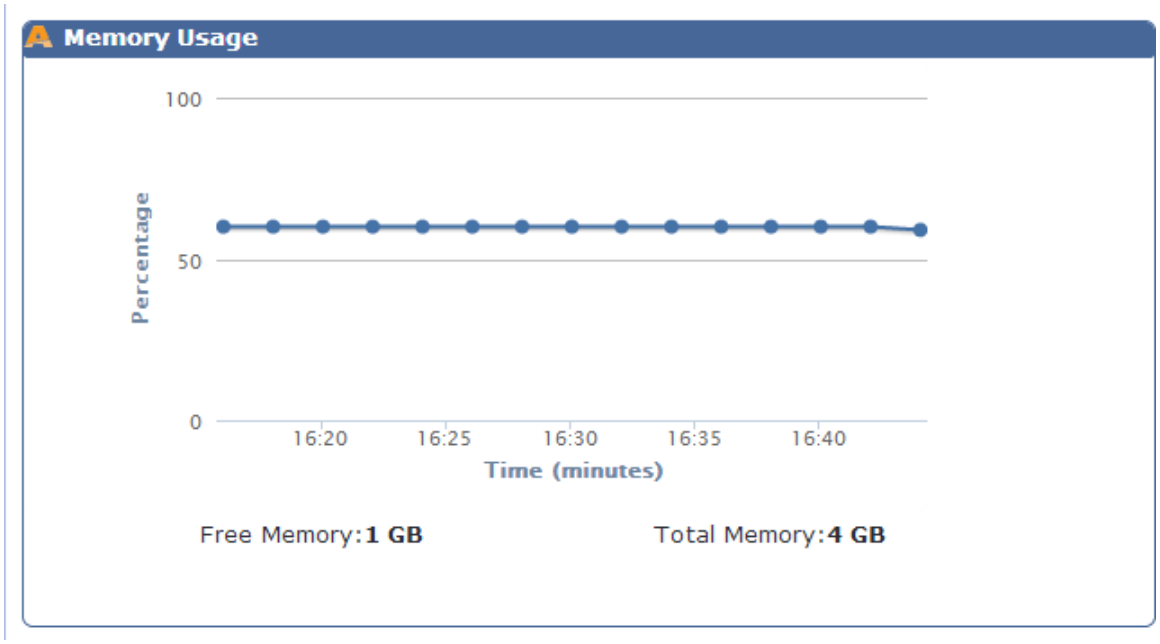
Figure 31: *CPU Load Graph Example*



Monitoring Memory Usage

This graph shows the percentage of free and total memory in Gigabytes.

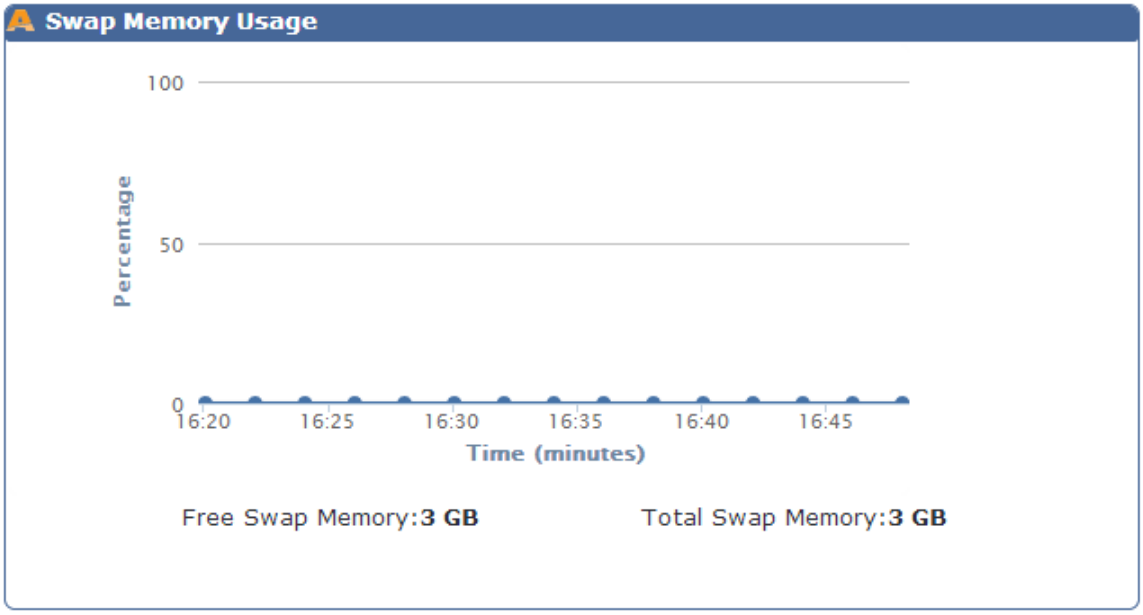
Figure 32: *Memory Usage Graph Example*



Monitoring Swap Memory Usage

This graph shows the percentage of free and total swap memory in Gigabytes.

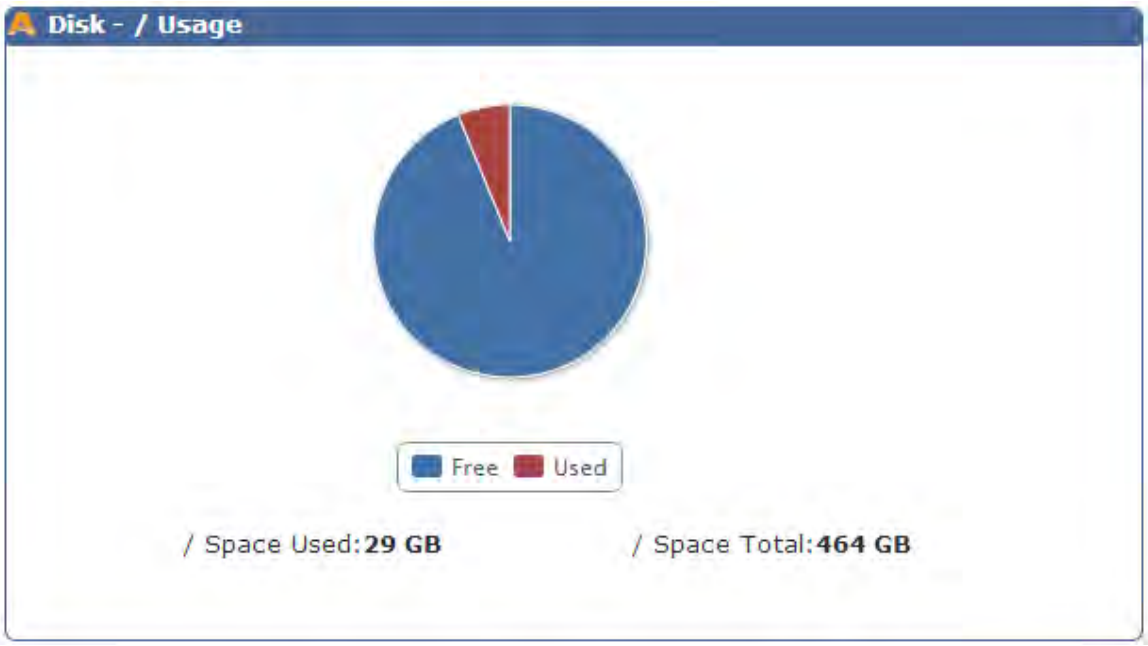
Figure 33: *Swap Memory Usage Graph Example*



Monitoring Disk - / Usage

This chart shows the percentage of used and free disk space.

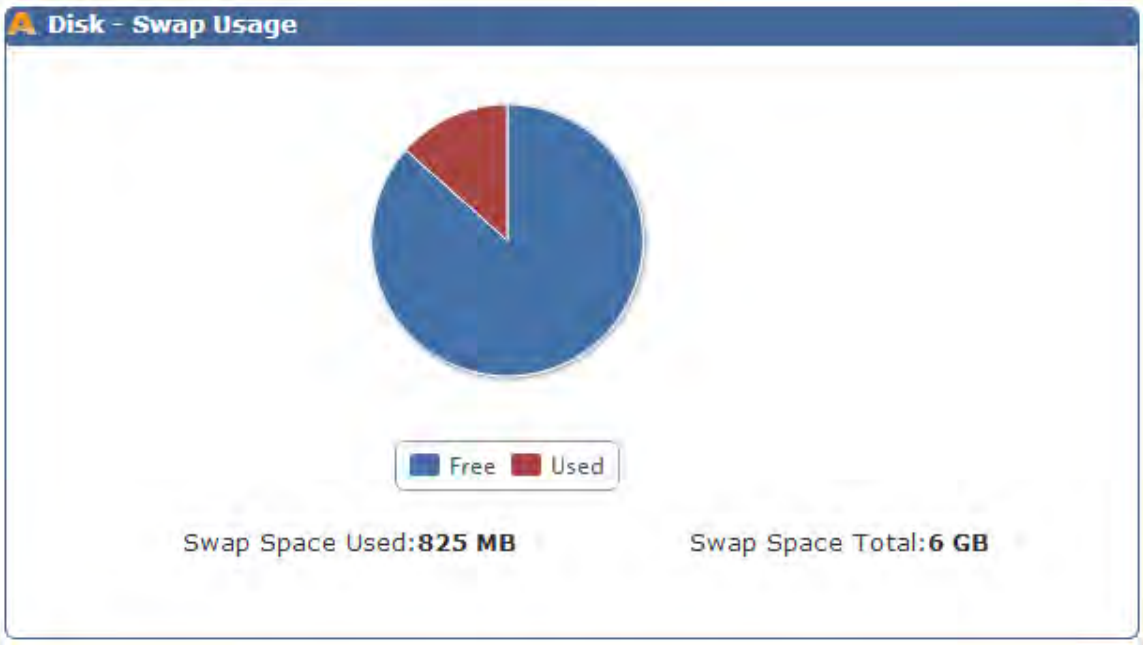
Figure 34: *Disk - / Usage Chart Example*



Monitoring Disk Swap Usage

The Disk - Swap Usage chart shows the used and total swap space.

Figure 35: *Disk Swap Usage Chart Example*



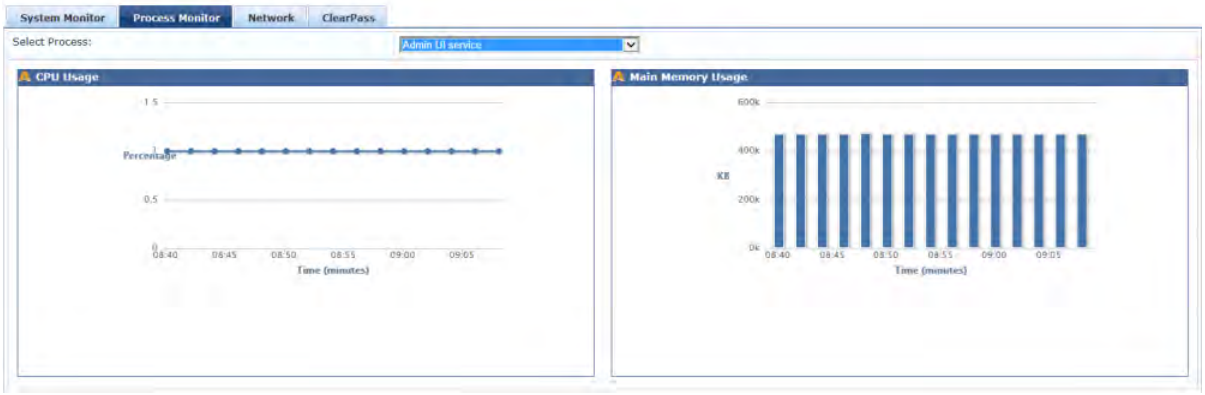
Process Monitor tab

Click this tab to view graphs that show data about CPU Usage and Main Memory Usage for the selected process or service. The **CPU Usage** graph on this tab shows only the percentage used and time in minutes for the selected process. Select a name any of the following processes from the drop-down list to view the CPU and Main Memory usage graphs:

- Admin UI service
- AirGroup notification service

- Async DB write service
- Async network services
- DB change notification server
- DB replication service
- Micros Fidelio FIAS
- Multi-master cache
- Policy server
- Radius server
- Stats aggregation service
- Stats collection service
- System auxiliary services
- System monitor service
- Tacacs server
- Virtual IP service

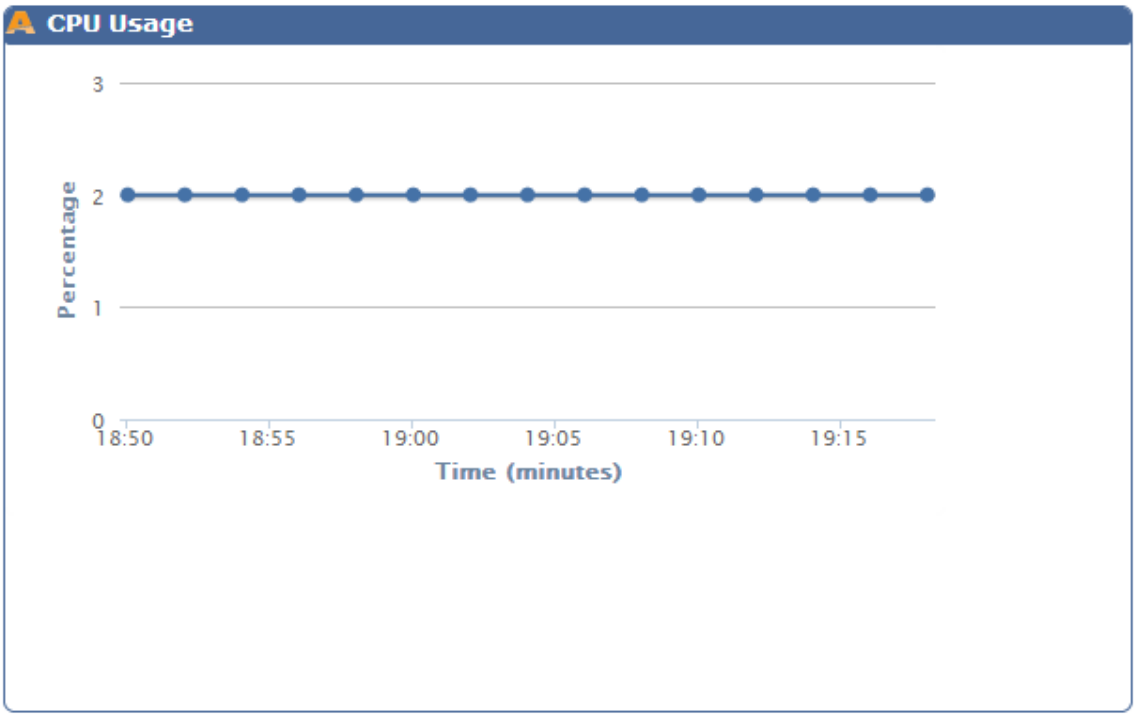
Figure 36: *Process Monitor tab Page Example*



Monitoring CPU Usage

This graph shows the CPU usage in time and percentage.

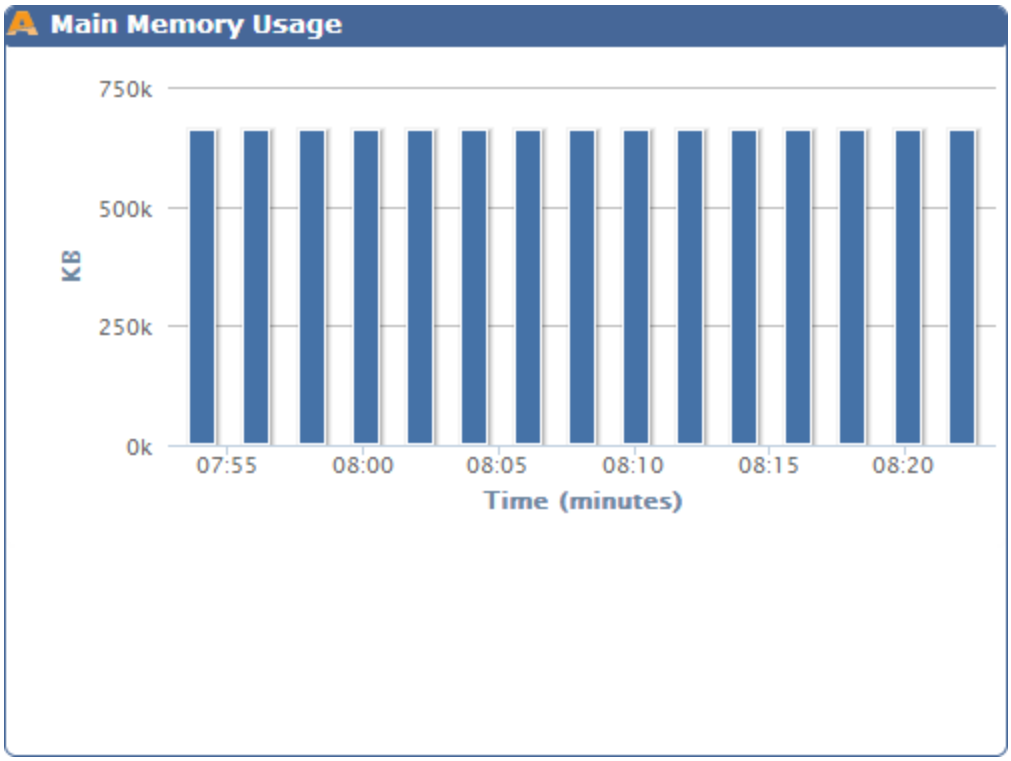
Figure 37: *CPU Usage Graph Example*



Monitoring Main Memory Usage

This graph shows the main memory usage in time and Kilobytes.

Figure 38: *Main Memory Usage Graph Example*

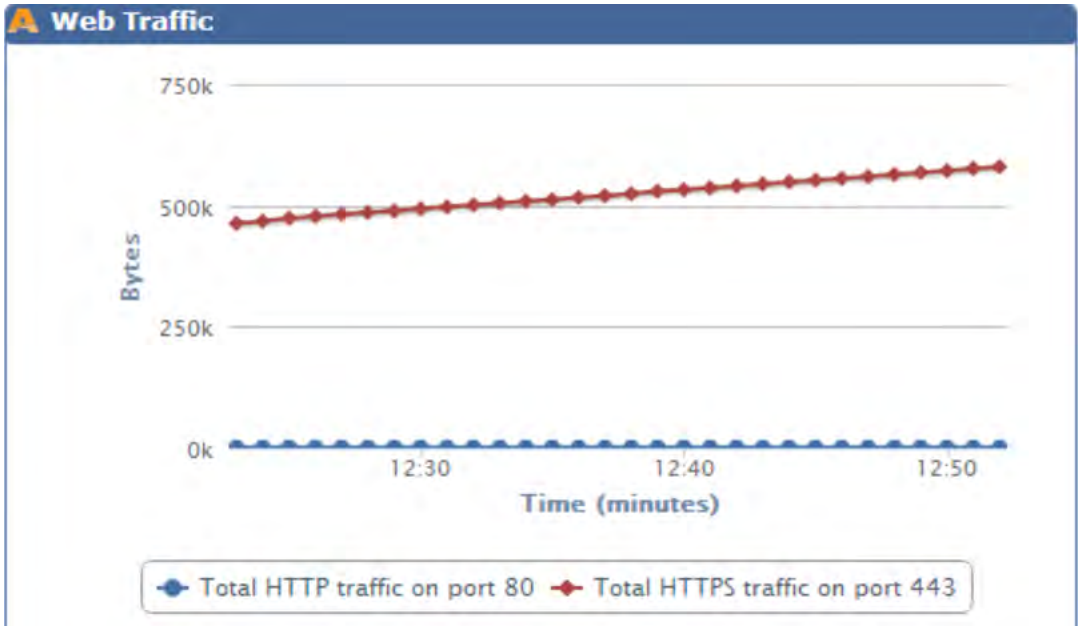


Network tab

Select the **Network** tab to view network activity charts and graphs for the following components:

- OnGuard
- Database
- Web Traffic
- RADIUS
- TACACS
- SSH
- NTP

Figure 39: *Network Monitor Tab Graph Example (Web Traffic)*



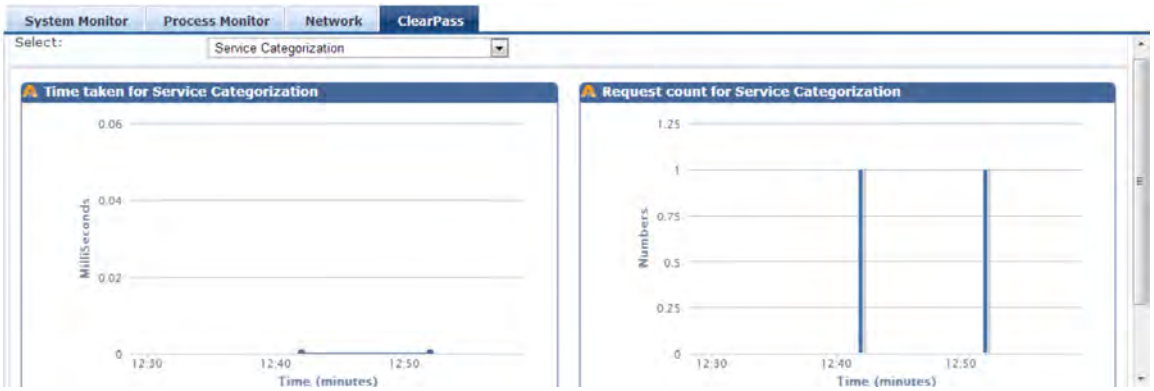
ClearPass tab

ClearPass can plot graphs based on the performance monitoring counters and timers for the following components:

- Service Categorization
- Authentication
- Authorization
- Role Mapping
- Posture Evaluation
- Audit Scan
- Enforcement
- End to End request processing for Radius, TACACS, and WebAuth based requests.

These components are actively monitored and the **ClearPass** tab displays the data for the past 30 minutes.

Figure 40: *Service Categorization Graph Example*



Audit Viewer

The **Audit Viewer** page provides a dynamic report on Actions, Name, Category of policy component, User, and Timestamp. The following figure displays the **Audit Viewer** page followed by parameter definition..

Figure 41: *Audit Viewer Page*

Table 21: *Audit Viewer Page Parameters*

Parameter	Description
Action	Displays the type of actions. For example, ADD, MODIFY, or REMOVE.
Name	Displays the name of the policy component.
Category	Displays the category of the user or endpoint.
User	Displays the user associated with the action.
Timestamp	Displays the server time when the status was last updated.

For more information, see:

- Viewing Audit Row Details (Add Page) on page 51
- Viewing Audit Row Details (Modify Page) on page 53
- Viewing Audit Row Details (Remove Page) on page 55

Viewing Audit Row Details (Add Page)

If you click a row with the **Action** type **ADD** on the main page, an **Audit Row Details** page opens. This page gives details that are specific to the **Action** category. The Audit Row Details Page Example 1 and Audit Row

Details Page Example 2 figures show the example of the **Audit Row Details** page.

Figure 42: *Audit Row Details Page Example 1*

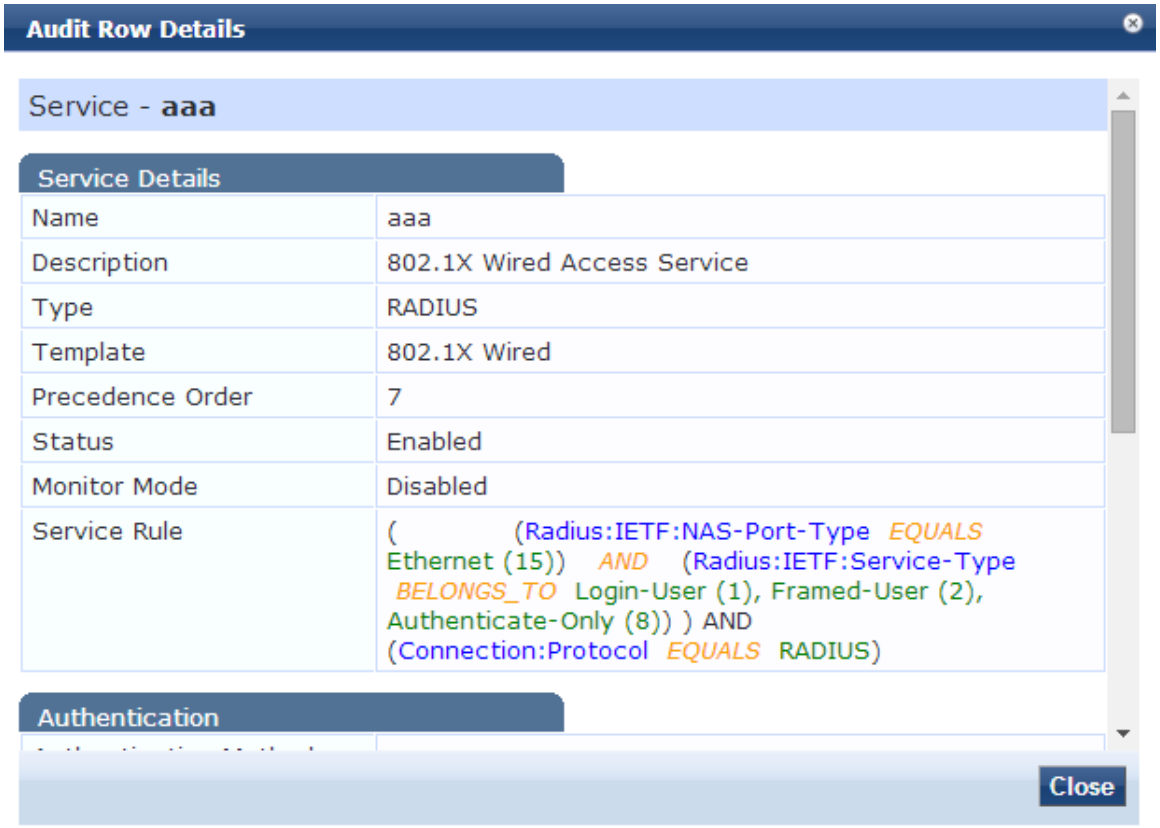
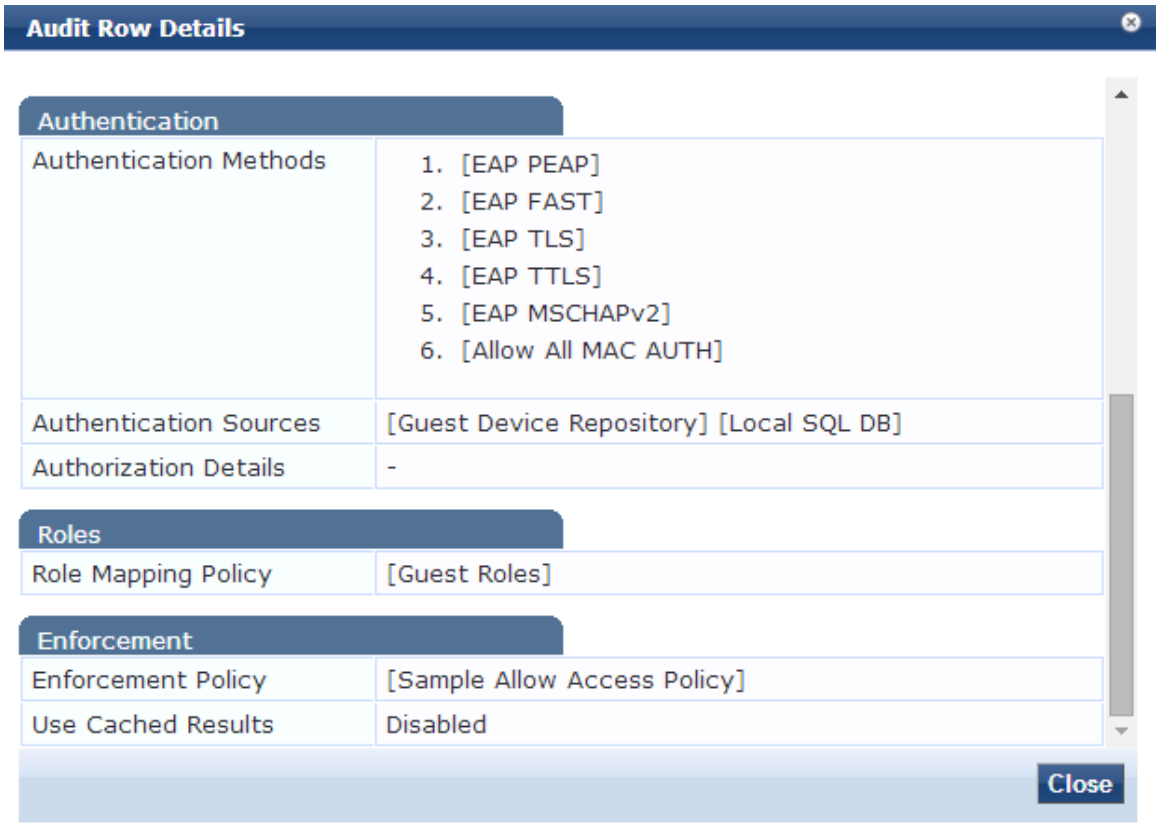


Figure 43: *Audit Row Details Page Example 2*



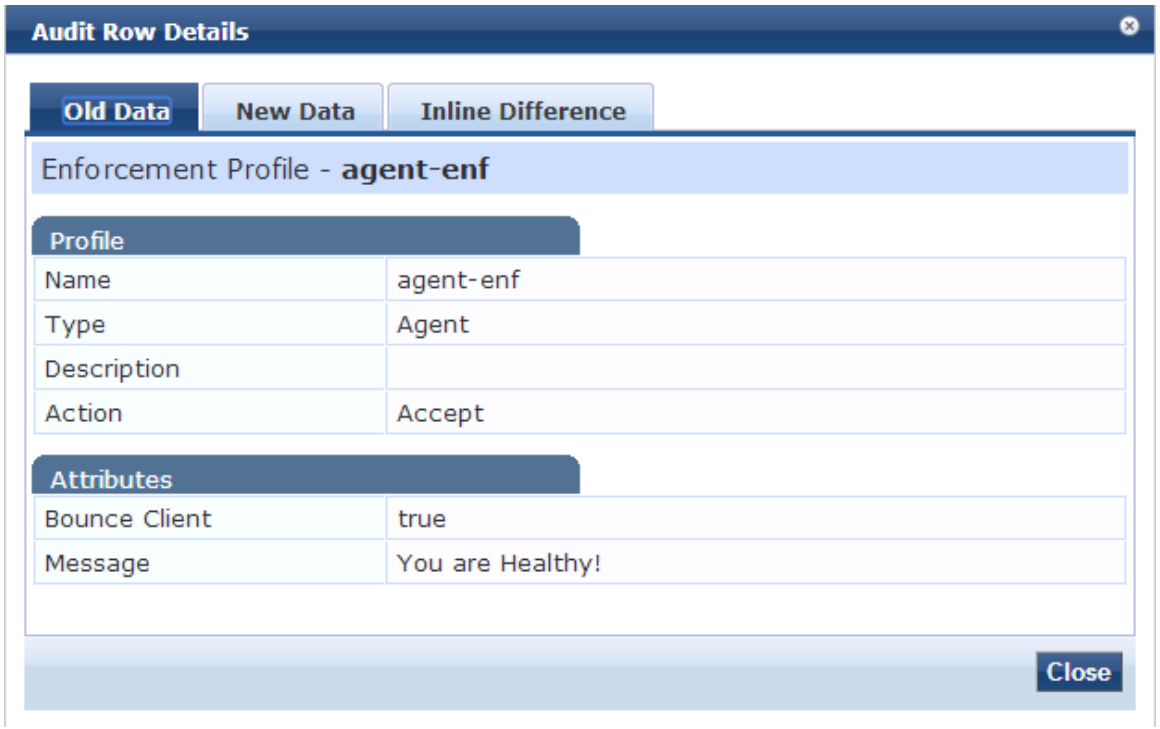
Viewing Audit Row Details (Modify Page)

If you click a row with the **Action** type **MODIFY** on the main page, an **Audit Row Details** page opens. The **Audit Row Details** page for the **MODIFY** category has three tabs.

Old Data Tab

The **Old Data** tab is a summary of details about the original data values. The **Attributes** section shows data about the original attributes and values. The following figure shows an example of an agent enforcement action that was taken in the **Enforcement Profile** category.

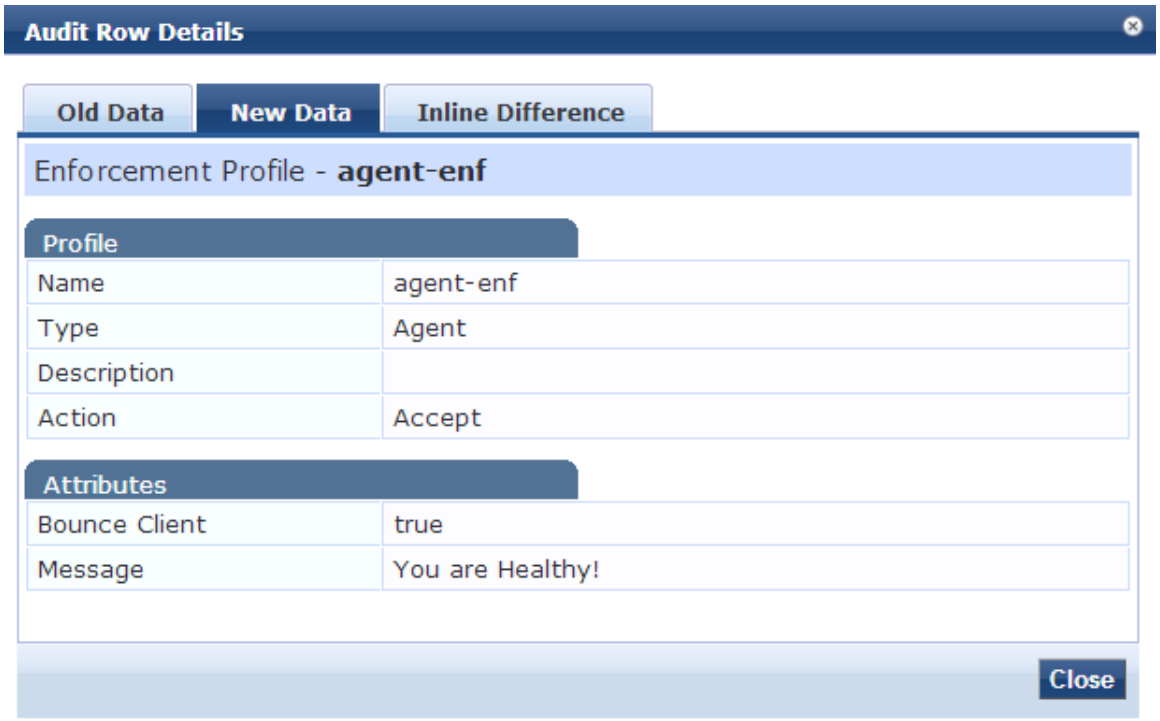
Figure 44: *Old Data tab*



New Data tab

The top section of the **New Data** tab is a summary of details about the original data values. The **Profile** section is a summary of the profile values. The **Attributes** section displays new and changed Attributes. The following figure shows an agent enforcement action that was taken in the **Enforcement Profile** category.

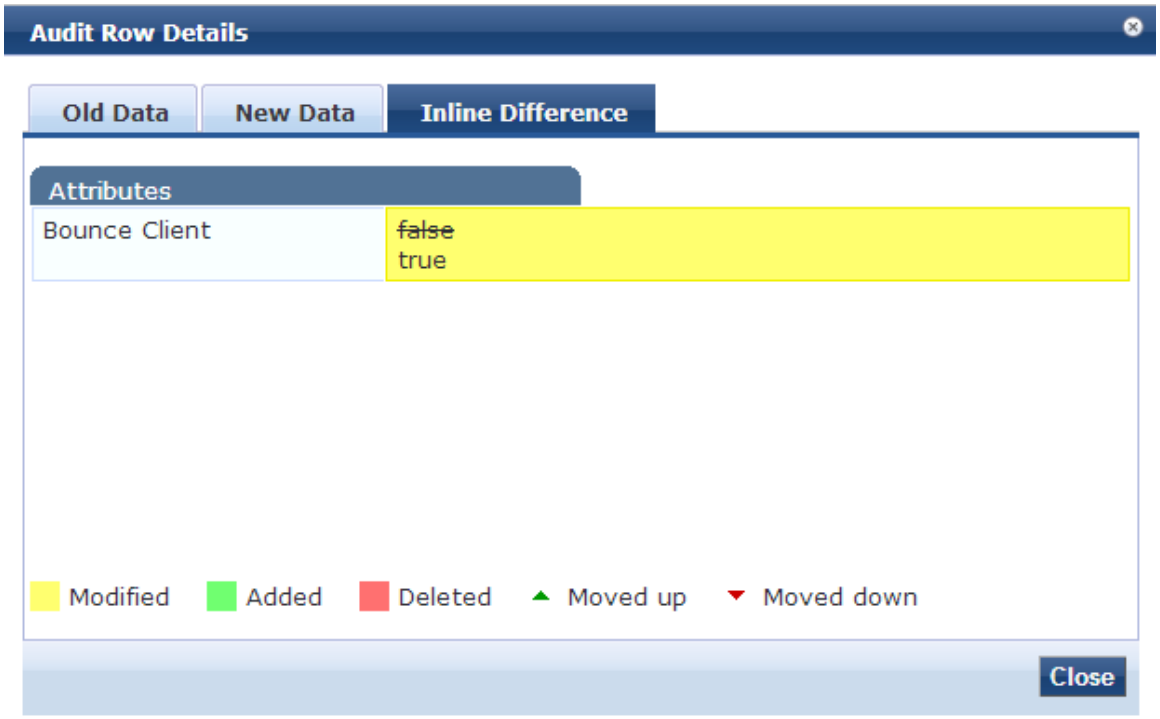
Figure 45: *New Data tab*



Inline Difference tab

The **Inline Difference** tab is a summary of the difference(s) between the old and new data. Modifications are highlighted in yellow, Additions are highlighted in green, and deletions are highlighted in red. A green arrow indicates that the value was moved up and a red arrow indicates the value was moved down.

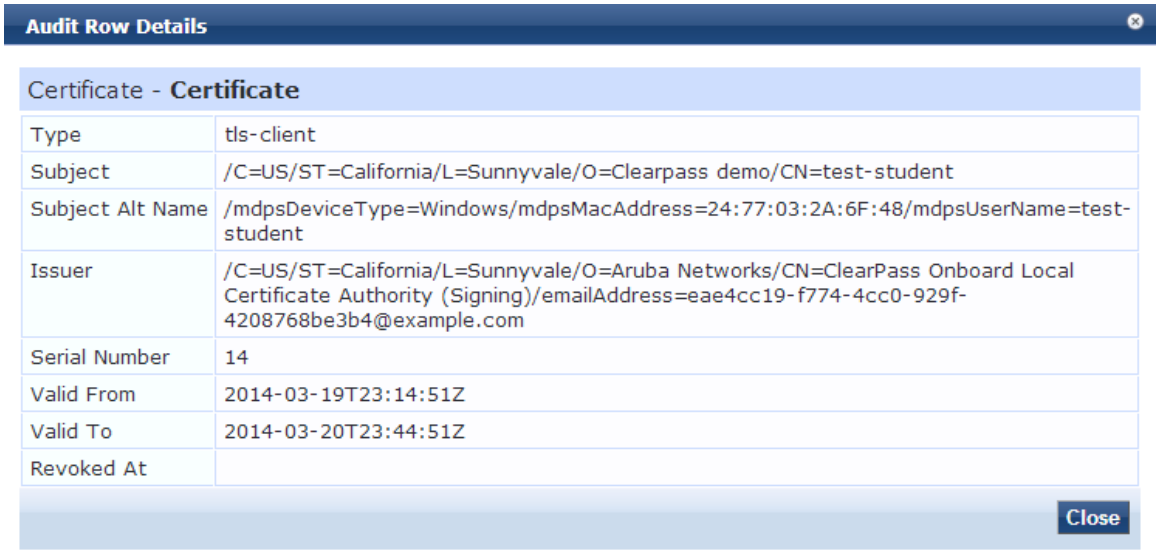
Figure 46: *Inline Difference tab*



Viewing Audit Row Details (Remove Page)

If you click on a row with the action **REMOVE** in the **Audit Viewer** page, a popup displays the details and attributes that were removed.

Figure 47: *Audit Row Details (Remove Page)*



Event Viewer

The **Event Viewer** page provides reports about system-level events. The following figure shows an example of the **Event Viewer** page followed by parameter definition:

Figure 48: *Event Viewer Page (Default Values)*

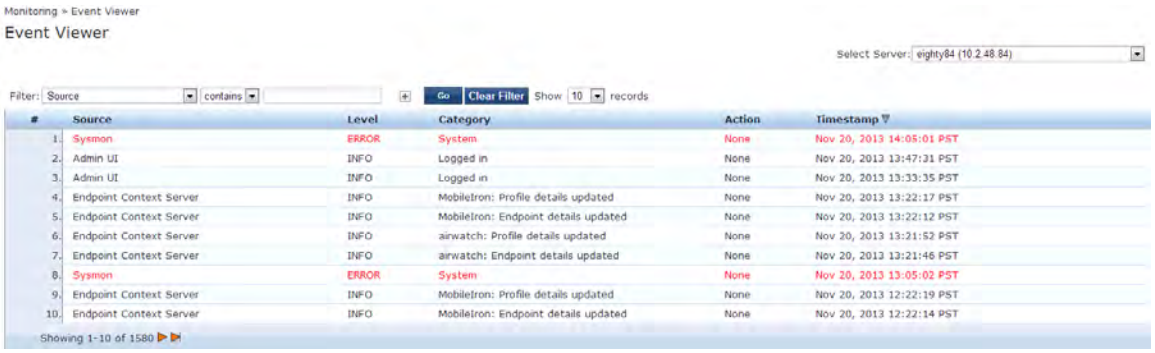


Table 22: *Event Viewer Page Parameters (Default Values)*

Parameter	Description
Source	Displays the source of the event. For example, AdminUI, RADIUS, SnmpService, and so on.
Level	Displays the level of the event from the following options: • INFO • WARN • ERROR
Category	Displays the category of the event. For example, Request, Authentication, System, and so on.
Action	Displays the action of the events. For example, Success, Failed, Unknown, and None.
Timestamp	Displays the date and time when the event was occurred.

For more information, see:

- Creating an Event Viewer Report Using Default Values on page 56
- Creating an Event Viewer Report Using Custom Values on page 56
- Viewing Report Details on page 57

Creating an Event Viewer Report Using Default Values

1. In the **Filter** field, select **Source** as the filter parameter.
2. Leave **contains** field with the default term.
3. Leave the text field blank.
4. Leave the Show records value at 10.
5. Click **Go**. The systems returns all event records.

Creating an Event Viewer Report Using Custom Values

1. Click the  icon. A new **Filter** field is added. You can add up to four **Filter** fields.

2. Click **Select ANY match**.
3. In the first **Filter** field, select **Level** as the **Filter** value.
4. Leave the search term set to **contains**.
5. Enter **ERROR** in the text field.
6. In the second **Filter** field, select **Source** as the **Filter** value.
7. Change the search field to **equals**.
8. Enter **SYSMON** in the text field.
9. Change the **Show records** value to 20.
10. Click **Go**.

Figure 49: *Event Viewer Report Example (Custom Values)*

Viewing Report Details

Click a row in the **Event Viewer** page to display **System Event Details**.

Figure 50: *System Event Details Page*

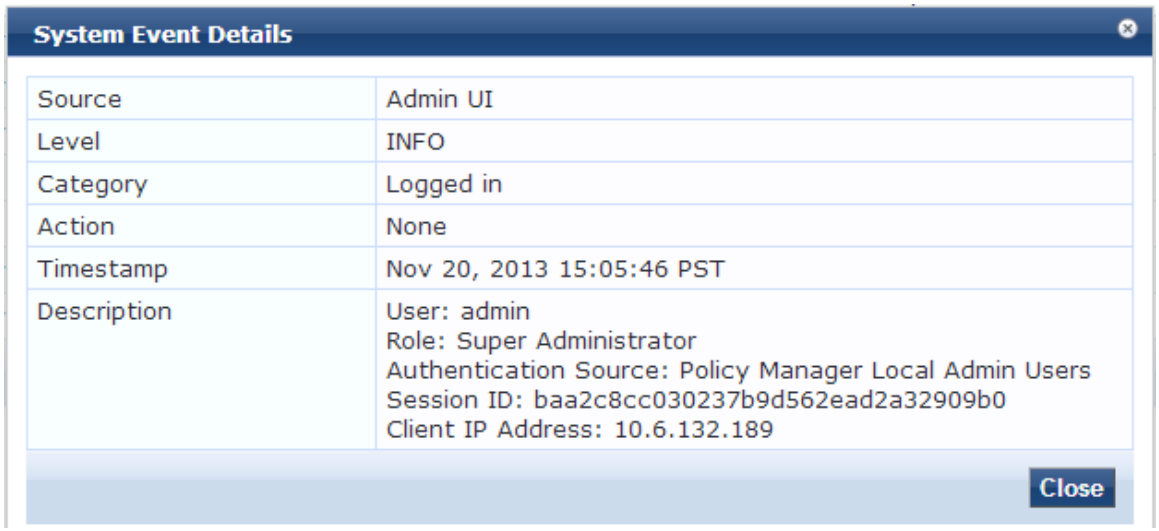


Table 23: *System Event Details Page Parameters*

Parameter	Description
Source	Displays the source of the event. For example, AdminUI, RADIUS, SnmpService, and so on.
Level	Displays the level of the event from the following options: • INFO • WARN • ERROR
Category	Displays the category of the event. For example, Request, Authentication, System, and so on.
Action	Displays the action of the events. For example, Success, Failed, Unknown, and None.
Timestamp	Displays the date and time when the event was occurred.
Description	Displays additional information about the event.

Data Filters

The **Data Filters** page provides a way to filter data (limit the number of rows of data shown by defining custom criteria or rules) that is shown in the Access Tracker on page 17, Syslog Export Filters on page 411, Analysis and Trending on page 40, and Accounting on page 24 components in Policy Manager. This is available in the **Monitoring > Data Filters** page.

Policy Manager is pre-configured with the following data filters:

- **All Requests -** Shows all requests (without any rows filtered).
- **ClearPass Application Requests** - All Application session log requests.
- **Failed Requests** - All authentication requests that were rejected or failed due to some reason. This includes RADIUS, TACACS+, and Web Authentication results.
- **Guest Access Requests** - All requests - RADIUS or Web Authentication - where the user was assigned with the built-in role called Guest.
- **Healthy Requests** - All requests that were deemed healthy by Policy Manager.
- **RADIUS Requests** - All RADIUS requests.
- **Successful Requests** - All authentication requests that were successful.
- **TACACS Requests** - All TACACS requests.
- **Unhealthy Requests** - All requests that were not deemed healthy by Policy Manager.
- **WebAuth Requests** - All Web Authentication requests (requests originated from the Dell Guest Portal).

For more information, see Add a Filter on page 59.

Figure 51: *Data Filters Page*

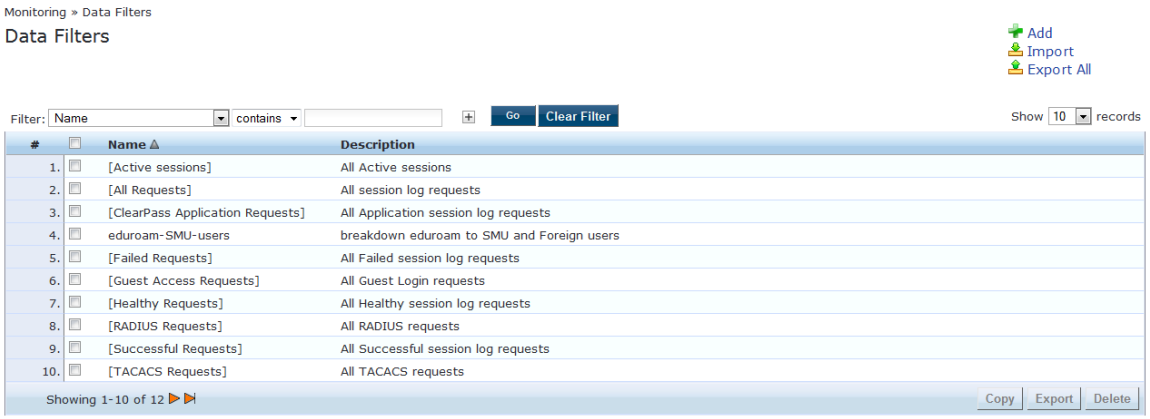


Table 24: *Data Filters Page Parameters*

Parameter	Description
Name	Displays the name of the data filter.
Description	Displays the description about the data filter.

Add a Filter

To add a filter, configure the name and description in the **Filter** tab and its rules in the **Rules** tab.

Figure 52: *Add Filter (Filter tab)*

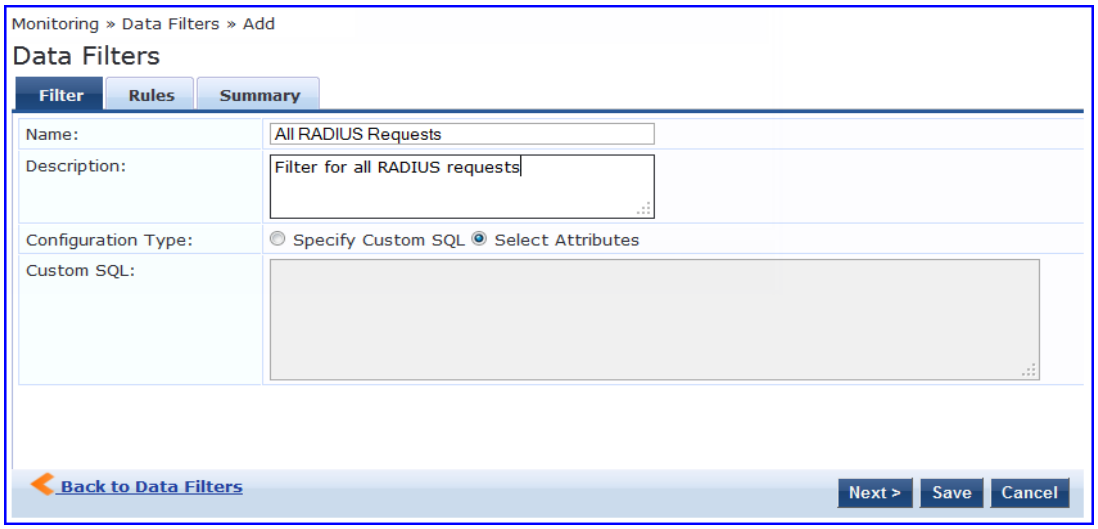


Table 25: *Add Filter (Filter tab)*

Parameter	Description
Name/Description	Name and description of the filter.
Configuration Type	Choose one of the following configuration types: • **Specify Custom SQL** - Specify a custom SQL entry for the filter. If this is specified, the **Rules tab** disappears and a SQL template displays in the **Custom SQL** field. **NOTE:** Using this option is not recommended. It is recommended to contact Support, if you want to use this option, • **Select Attributes** - This option is selected by default and enables the **Rules** tab. Use the **Rules** tab to configure rules for this filter.
Custom SQL	If **Specify Custom SQL** is selected, then this field populates with a default SQL template. In the text entry field, enter attributes for the type, attribute name, and attribute value. **NOTE:** It is recommended to contact Support, if you choose to use this option. Support can assist you with entering the correct information in this template.

The **Rules** tab displays only if **Select Attributes** is selected on the **Filter** tab.

Figure 53: *Add Filter (Rules tab)*

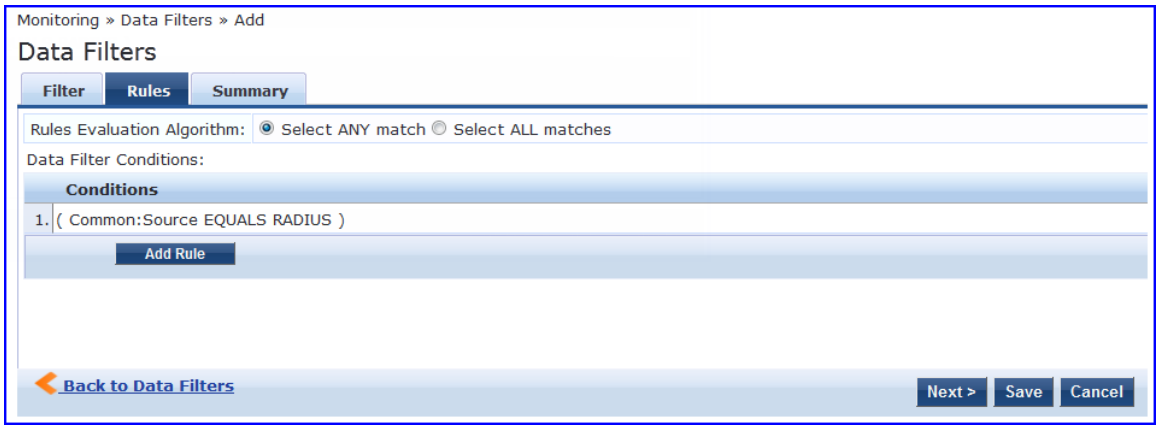


Table 26: *Add Filter (Rules tab)*

Parameter	Description
Rule Evaluation Algorithm	**Select ANY match** is a logical OR operation of all the rules. **Select ALL matches** is a logical AND operation of all the rules.
Add Rule	Add a rule to the filter.
Move Up/Down	Change the ordering of rules to Up and Down.
Edit/Remove Rule	Edit or remove a rule.

When you click on **Add Rule** or **Edit Rule**, the **Data Filter Rules Editor** appears.

Figure 54: *Add Filter (Rules tab) - Rules Editor*

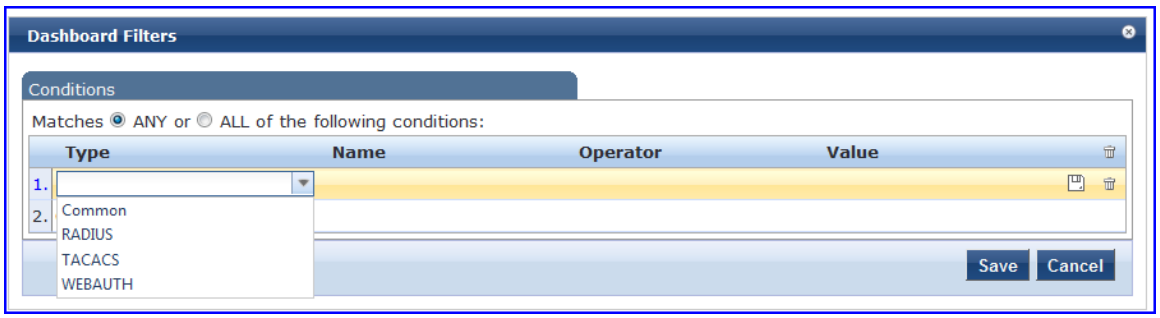


Table 27: *Add Filter (Rules tab)*

Parameter	Description
Matches	**ANY** matches one of the configured conditions. **ALL** indicates to match all of the configured conditions.
Type	This indicates the namespace for the attribute. • **Common** - Attributes common to RADIUS, TACACS, and WebAuth requests and responses. • **RADIUS** - Attributes associated with RADIUS authentication, accounting requests, and responses. • **TACACS** - Attributes associated with TACACS authentication, accounting, policy requests, and responses. • **Web Authentication Policy** - Policy Manager policy objects assigned after the evaluation of policies associated with Web Authentication requests. For example, Auth Method, Auth Source, and Enforcement Profiles.
Name	Name of the attributes corresponding to the selected namespace (Type).
Operator	Select any subset of string data type operators from the following list: • EQUALS • NOT_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS • GREATER_THAN • GREATER_THAN_OR_EQUALS • CONTAINS • NOT_CONTAINS • EXISTS • NOT_EXISTS
Value	The value of the attribute.

Blacklisted Users

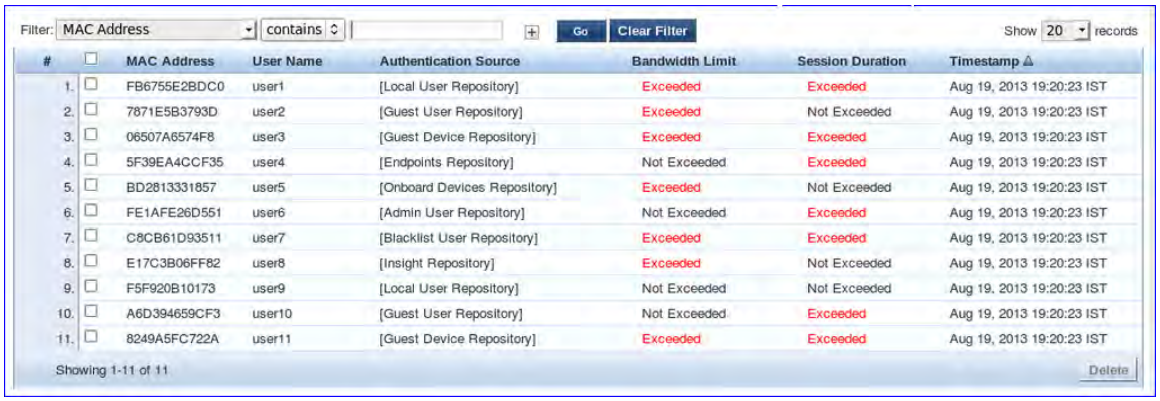
The **Blacklisted Users** page lists all blacklisted users with the reason(s) why they are blacklisted. This page shows whether the following attributes are exceeded:

- Bandwidth limit

- Session duration

You can delete a user from this blacklist by selecting the user row and then clicking **Delete**. After deletion, the user is eligible to access the network again.

Figure 55: *Monitoring Blacklisted Users*



The network devices or other entities that need authentication and authorization services view the Policy Manager as a RADIUS, TACACS+, or HTTP/S based authentication server. However, the Policy Manager's rich and extensible policy model allows it to broker security functions across a range of existing network infrastructure, identity stores, health/posture services, and client technologies within an enterprise. For more information, see:

- Services Paradigm on page 63
- Policy Simulation on page 70

Services Paradigm

Services are the highest level element in the Policy Manager policy model. They have two purposes:

- Unique **Categorization Rules** (per Service) enable Policy Manager to test **Access Requests** (Requests) against available **Services** to provide robust differentiation of requests by access method, location, or other network vendor-specific attributes.

Policy Manager is shipped with a number of basic **Service** types configured. You can extend these **Service** types to copy them and use as templates, import other **Service** types from another implementation (from which you have previously exported them), or develop new services from scratch.

- By wrapping a specific set of **Policy Components**, a **Service** can coordinate the flow of a request from authentication to role and health evaluation to determine the **Enforcement** parameters for network access.

For more information, see:

- Viewing Existing Services on page 66
- Adding and Removing Services on page 67
- Links to Use Cases and Configuration Instructions on page 68

The following image and table illustrate the basic Policy Manager flow of control and its underlying architecture:

Figure 56: *Generic Policy Manager Service Flow of Control*

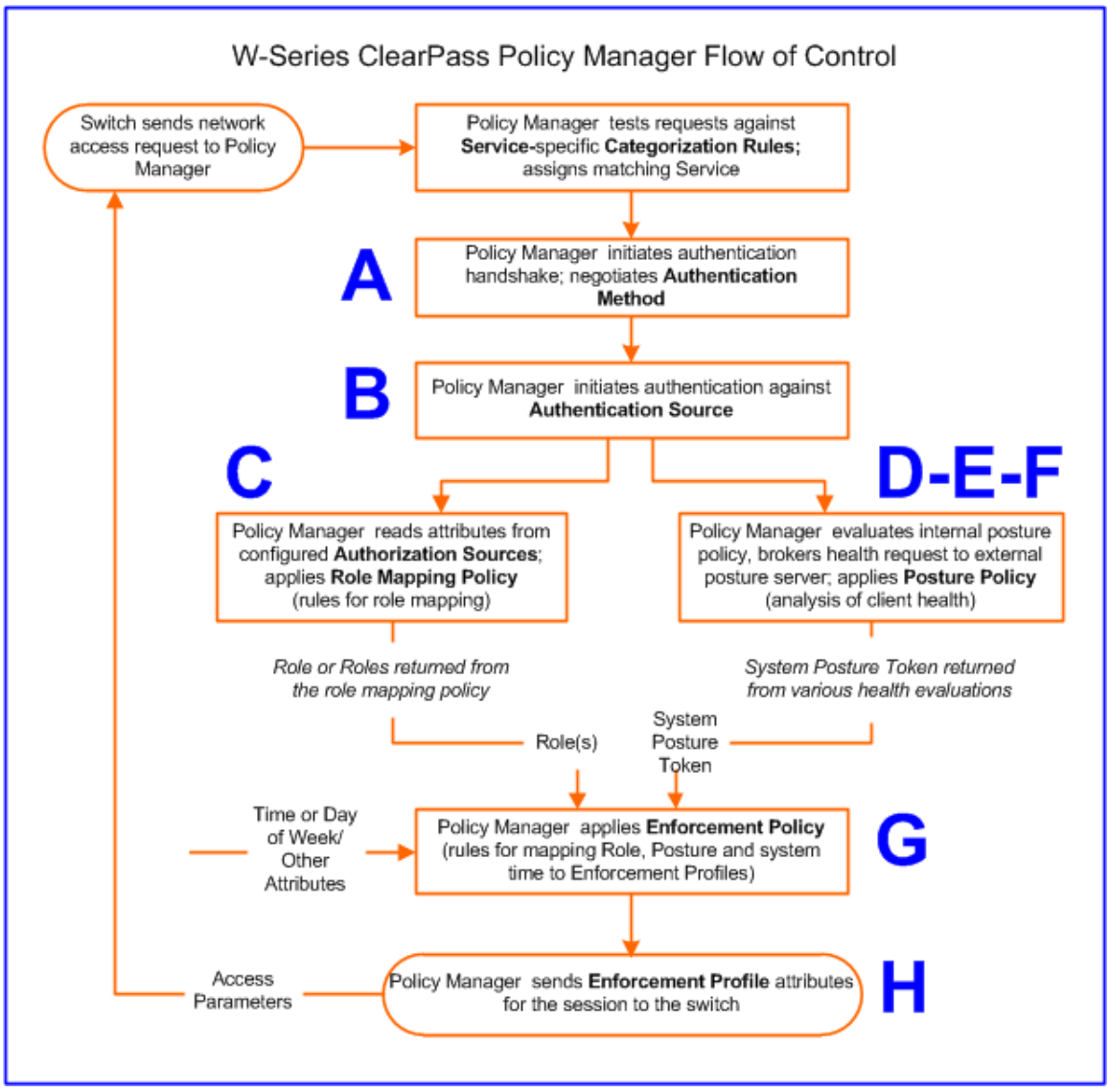


Table 28: *Policy Manager Service Components*

Component	Service: Component ratio	Description

A - Authentication Method	Zero or more per service	Specifies the EAP or non-EAP method for client authentication. Policy Manager supports the following classes of authentication methods:
		• **EAP, tunneled:** PEAP, EAP-FAST, or EAP-TTLS
		• **EAP, non-tunneled:** EAP-TLS or EAP-MD5
		• **Non-EAP, non-tunneled:** CHAP, MS-CHAP, PAP, or MAC-AUTH
		• **MAC_AUTH:** Must be used exclusively in a MAC-based Authentication Service. When the **MAC_ AUTH** method is selected, Policy Manager:
		  ▪ performs internal checks to verify that the request is a MAC Authentication request (and not a spoofed request)
		  ▪ ensures that the MAC address of the device is present in the authentication source
		Some services (for example, *TACACS+*) contain internal authentication methods. In such cases, Policy Manager does not make this method available.
		NOTE: The **EAP-MD5** authentication type is not supported, if you use the Dell Networking W-ClearPass Policy Manager in the FIPS mode.

B - Authentication Source	Zero or more per service	An **Authentication Source** is the identity repository against which the Policy Manager verifies an identity. It supports the following **Authentication Source** types: • Microsoft Active Directory and LDAP compliant directory • RSA or other RADIUS-based token servers • SQL database including the local user store • Static Host Lists (in case of MAC-based Authentication of managed devices)
C - Authorization Source	One or more per Authentication Source and zero, or more per service	An **Authorization Source** collects attributes for use in **Role Mapping** rules. Specify the attributes you want to collect, when you configure the authentication source. Policy Manager supports the following authorization source types: • Microsoft Active Directory and LDAP compliant directory • RSA or other RADIUS-based token servers • SQL database including the local user store
C - Role Mapping Policy	Zero or one per service	Policy Manager evaluates **Requests** against the **Role Mapping** Policy rules to match Clients to Role(s). All rules are evaluated and Policy Manager may return more than one role. If no rules match, the request takes the configured default role.

Table 28: *Policy Manager Service Components (Continued)*

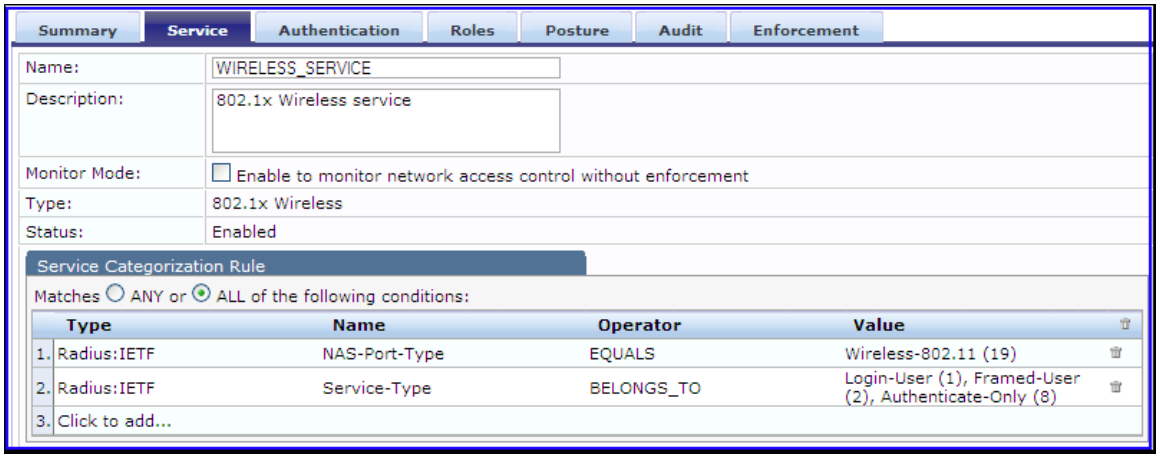
Component	Service: Component ratio	Description
		Some Services (for example, *MAC-based Authentication*) may handle role mapping differently: • For *MAC-based Authentication* Services, where role information is not available from an authentication source, an audit server can determine the role by applying post-audit rules against the client attributes gathered during the audit.
D - Internal Posture Policies	Zero or more per service	An Internal Posture Policy tests **Requests** against internal Posture rules to assess health. Posture rule conditions contain attributes present in vendor-specific posture dictionaries.
E - Posture Servers	Zero or more per service	Posture servers evaluate client health based on specified vendor-specific posture credentials. These posture credentials cannot be evaluated internally by Policy Manager (that is, not by internal posture policies). Currently, Policy Manager supports the following forms of posture server interfaces: • HCAP • RADIUS • GAMEv2
F - Audit Servers	Zero or more per service	**Audit Servers** evaluate the health of clients that do not have an installed agent, or which cannot respond to Policy Manager interactions. **Audit Servers** typically operate instead of authentication methods, authentication sources, internal posture policies, and posture server. In addition to returning posture tokens, **Audit Servers** can contain post-audit rules that map results from the audit into Roles.
G - Enforcement Policy	One per service (mandatory)	Policy Manager tests Posture Tokens, Roles, and system time against the **Enforcement Policy** rules to return one or more matching the **Enforcement Policy** rules to return one or more matching **Enforcement Profiles** that define scope of access for the client.
H - Enforcement Profile	One or more per service	**Enforcement Profiles** contain attributes that define a client's scope of access for the session. Policy Manager returns these **Enforcement Profile** attributes to the switch.

Viewing Existing Services

You can view all configured services in a list or drill down to individual services in the **Services** page. Click **Configuration > Services** to view a list of services that you can filter by phrase or sort by order. In the

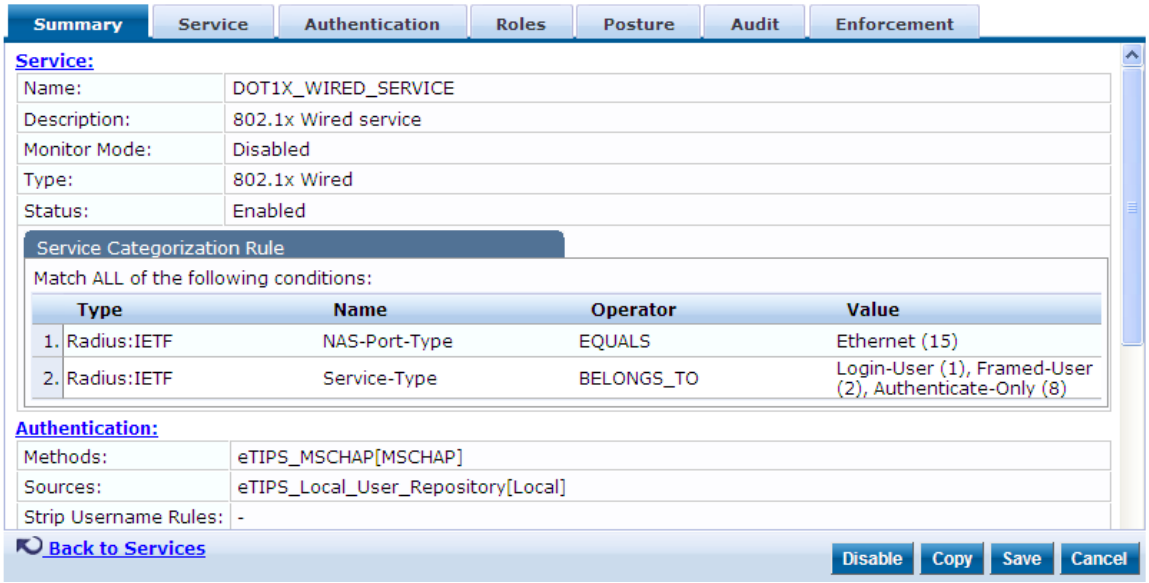
Services page, click the name of a **Service** to view its details. The following figure shows an example of the **Services** tab with the list of services with sorting tool:

Figure 57: *List of services with sorting tool*



The **Summary** tab provides the detailed information about the selected service with the link to other tabs. For example, you can click **Authentication** to view the **Authentication** tab and add authentication sources and authentication methods. The following figure shows an example of the **Summary** tab with service details:

Figure 58: *Details for an individual service*



Adding and Removing Services

You can add a service to the list of services by copying, importing from another configuration, or creating a new service as described below:

- **Create a template** by copying an existing service - From the **Services** page, select the check box of a service, then click **Copy**. This creates a new copy of the selected service.
- **Clone a service** by import (of a previously exported file from this or another configuration) - From the **Services** page, select the check box of a service, then click the **Export** button and provide the output file path where you want to export. You can import this service later by clicking **Import** and providing the file path.

- **Create a new service** - In the **Services** page, click **Add**, then follow the configuration wizard by clicking **Next** as you complete each tab.
- **Remove a service -** From the **Services** page, select the check box for a service and then click the **Delete** button. You can also disable or enable a service from the **Service** details page by clicking **Disable** or **Enable** in the lower right of page. The following figure shows an example of the **Disable** or **Enable** toggle buttons from the **Services** page:

Figure 59: *Disable or Enable toggle for a Policy Manager Service*

Links to Use Cases and Configuration Instructions

For the policy components of each service that you can configure, the following table provides an illustrative use case and detailed instructions on configuration.

Table 29: *Policy Component Use Cases and Configuration Instructions*

Policy Component	Illustrative Use Cases	Configuration Instructions
Service	• 802.1X Wireless Use Case on page 549 • Web Based Authentication Use Case on page 556 • MAC Authentication Use Case on page 564 • TACACS+ Use Case on page 567	Adding Services on page 119
Authentication Method	802.1X Wireless Use Case on page 549 demonstrates the principle of multiple authentication methods in a list. When Policy Manager initiates the authentication handshake, it tests the methods based on priority until an authentication method is accepted by the client. Web Based Authentication Use Case on page 556 has only a single authentication method, which is specifically designed for authentication of the request attributes received from the Dell Web Portal.	• Adding and Modifying Authentication Methods on page 130 • Adding and Modifying Authentication Methods on page 130
Authentication Source	• 802.1X Wireless Use Case on page 549 demonstrates the principle of multiple authentication sources in a list. Policy Manager tests the sources based on priority until the client can be authenticated. In this case, Active Directory is listed first.	• Adding and Modifying Authentication Sources on page 154 • Adding and Modifying Authentication Sources on page 154

Table 29: *Policy Component Use Cases and Configuration Instructions (Continued)*

Policy Component	Illustrative Use Cases	Configuration Instructions
	• Web Based Authentication Use Case on page 556 uses the local Policy Manager repository. This is a common practice among administrators configuring ClearPass Guest users. • MAC Authentication Use Case on page 564uses a **Static Host List** for authentication of the MAC address sent by the switch as the device's username. • TACACS+ Use Case on page 567 uses the local Policy Manager repository. Other authentication sources also accepted.	
Role Mapping	802.1X Wireless Use Case on page 549 has an explicit **Role Mapping Policy** that tests request attributes against a set of rules to assign a role.	• Adding and Modifying Role Mapping Policies on page 203 • Adding and Modifying Roles on page 202 • Adding and Modifying Local Users on page 193 • Adding and Modifying Static Host Lists on page 200
Posture Policy	Web Based Authentication Use Case on page 556 uses an internal posture policy that evaluates the health of the originating client based on attributes submitted with the request by the Dell Web Portal, and returns a corresponding posture token.	Adding a Posture Policy on page 210

Table 29: *Policy Component Use Cases and Configuration Instructions (Continued)*

Policy Component	Illustrative Use Cases	Configuration Instructions
Posture Server	802.1X Wireless Use Case on page 549 appends a third-party posture server to evaluate health policies based on vendor-specific posture credentials.	Adding and Modifying Posture Servers on page 247
Audit Server	MAC Authentication Use Case on page 564uses an audit server to provide port scanning for health.	Configuring Audit Servers on page 250
Enforcement Policy and Profiles	All Use Cases have an assigned Enforcement Policy and corresponding Enforcement Rules.	• Configuring Enforcement Profiles on page 264 • Configuring Enforcement Policies on page 298

Policy Simulation

After creating the policies, use the **Policy Simulation** utility to evaluate those policies before deployment. The **Policy Simulation** utility applies a set of request parameters as input against a given policy component and displays the outcome in the **Configuration > Policy Simulation** page.

The following types of simulations are supported:

- **Service Categorization** - The **Service Categorization** simulation allows you to specify a set of attributes in RADIUS or Connection namespace and test in which configured service request will be categorized into. The request attributes that you specify represent the attributes sent in the simulated request.
- **Role Mapping** - The **Role Mapping** simulation maps the user into a role or set of roles with the following inputs:
  - Service name and associated role mapping policy
  - Authentication source and the user name

  You can also use the **Role Mapping** simulation to test whether the specified authentication source is reachable.
- **Posture Validation** - The **Posture Validation** simulation allows you to specify a set of posture attributes in the posture namespace and test the posture status of the request. The posture attributes that you specify represent the attributes sent in the simulated request.
- **Audit** - The **Audit** simulation allows you to specify an audit server (Nessus Server or Nmap Audit based) and the IP address of the device you want to audit. The **Audit** simulation triggers an audit on the specified device and displays the results.

- **Enforcement Policy** - The **Enforcement Policy** simulation evaluates the rules in the enforcement policy and displays the resulting enforcement profiles with the following inputs:
  - Service name and the associated enforcement policy
  - A role or a set of roles
  - System posture status
  - Date and time (optional)
- **Chained Simulation** - The **Chained Simulation** combines the results of role mapping, posture validation, and enforcement policy simulations and displays the corresponding results with the following inputs:
  - Service name
  - Authentication source
  - User name
  - Date and time (optional)

For more information, see:

- Adding Simulation Test on page 71
- Import and Export Simulations on page 76

The following figure shows an example of the **Policy Simulation** page followed by parameter definition:

Figure 60: *Policy Simulation page*

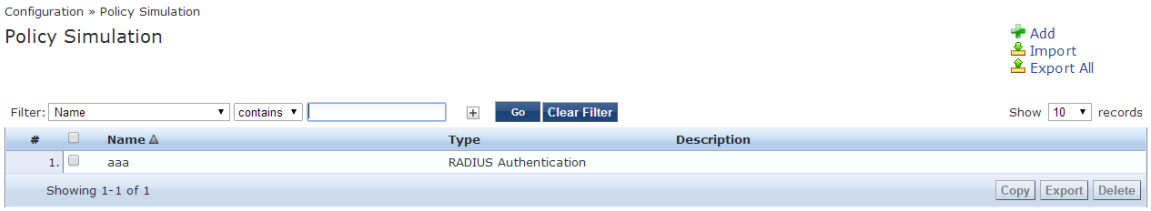


Table 30: *Policy Simulation page Parameters*

Parameter	Description
Name	Displays the name of the name of the policy simulation.
Type	Displays the type of the policy simulation.
Description	Displays additional information about the policy simulation.

Adding Simulation Test

Navigate to the **Configuration > Policy Simulation** page and click on the **Add** link. Different **Simulation** tabs are displayed depends on the simulation type selected as described in the following table:

Table 31: *Add Policy Simulation - Simulation tab Parameters*

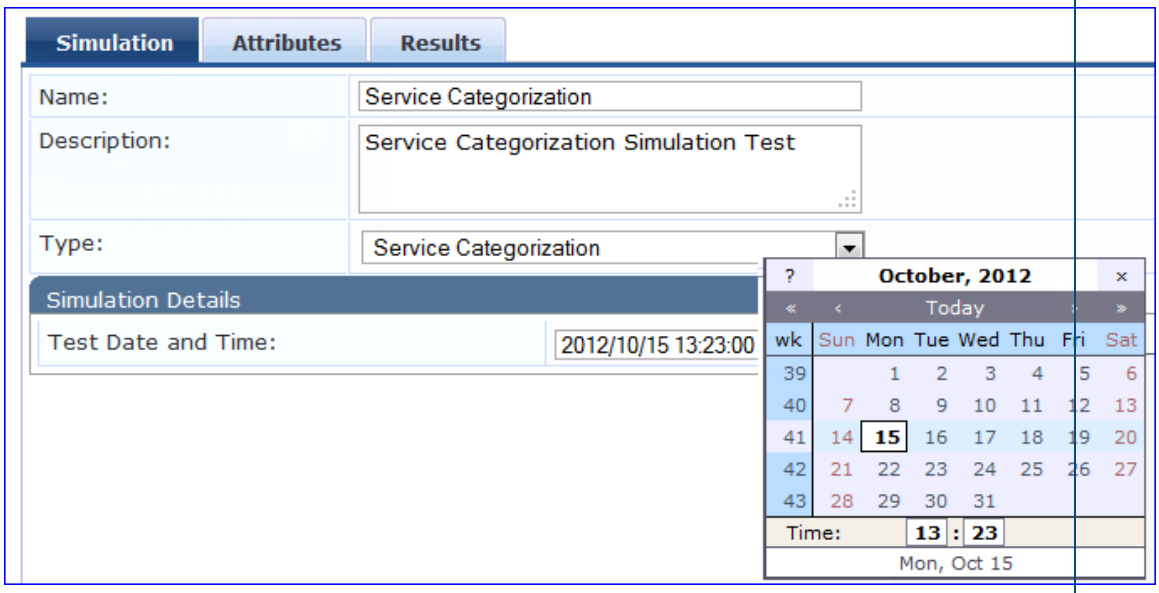
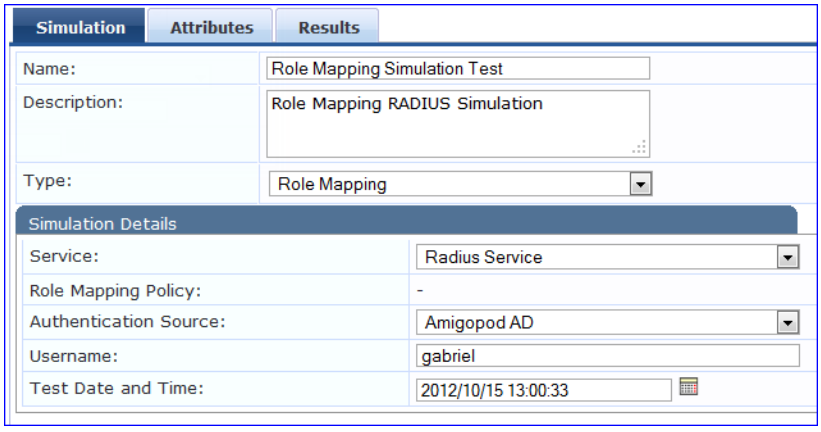
Parameter	Description
Name/Description	Specify name and description (freeform).
Type **Service Categorization**	• Input (**Simulation** tab): Select **Test Date and Time**. This field is optional and use if you want to create time based service rules.  • Input (**Attributes** tab): Use **Rules Editor** to create a request with the attributes you want to test. All namespaces relevant to service rules creation are loaded in the **Attributes** editor. • Returns (**Results** tab): **Service Name** (or status message in case of no match)
Type **Role Mapping**	• Input (**Simulation** tab): Select **Service** (**Role Mapping Policy** is implicitly selected, because there is only one such policy associated with a service), **Authentication Source**, **User Name**, and **Date/Time**.  • Input (**Attributes** tab): Use **Rules Editor** to create a request with the attributes you want to test. All namespaces relevant for role mapping policies are loaded in the **Attributes** editor. • Returns (**Results** tab): **Role(s)** includes authorization source attributes fetched as roles.

Table 31: *Add Policy Simulation - Simulation tab Parameters (Continued)*

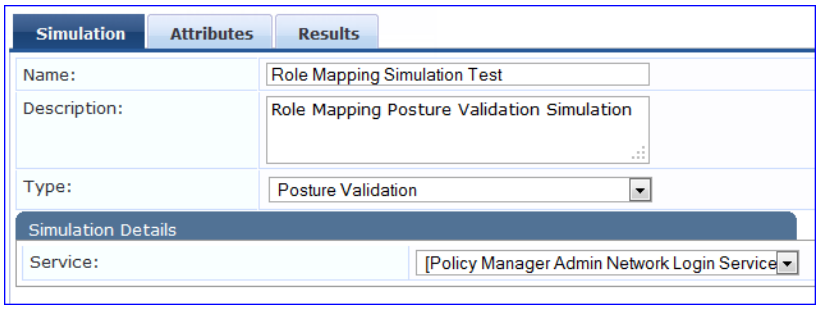
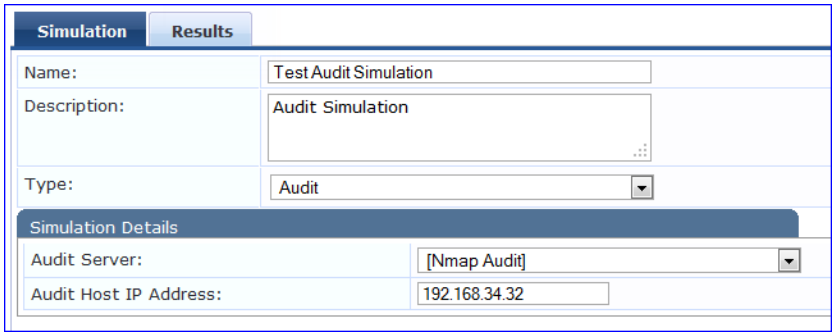
Parameter	Description
Type **Posture Validation**	• Input (**Simulation** tab): Select **Service** (Posture policies are implicitly selected by their association with the service).  • Input (**Attributes** tab): Use **Rules Editor** to create a request with the attributes you want to test. All namespaces relevant to posture evaluation (posture dictionaries) are loaded in the **Attributes** editor. • Returns (**Results** tab): **System Posture Status** and **Status Messages**.
Type **Audit**	• Input (**Simulation** tab): Select **Audit Server** and host to be audited (IP address or hostname).  • Returns (**Results** tab): **Summary Posture Status**, **Audit Attributes**, and **Status**. **NOTE: Audit** simulations can take a while; an **Audit In Progress** status is shown until the audit is completed.
Type **Enforcement Policy**	• Input (**Simulation** tab): Select **Service** (**Enforcement Policy** is implicit by its association with the service), **Authentication Source** (optional), **User Name** (optional), **Roles**, **Dynamic Roles** (optional), **System Posture Status**, and **Date/Time** (optional).

Table 31: *Add Policy Simulation - Simulation tab Parameters (Continued)*

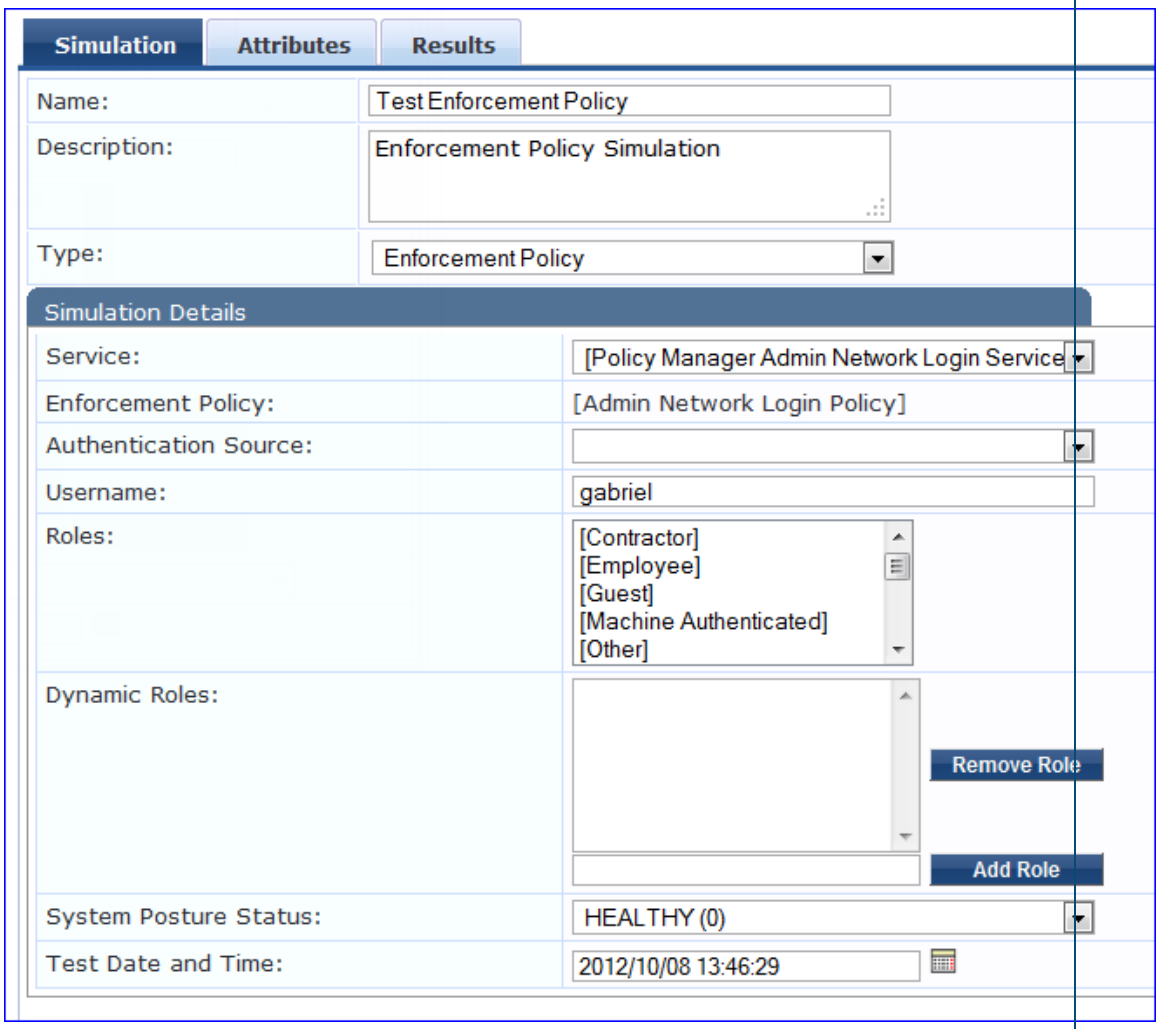
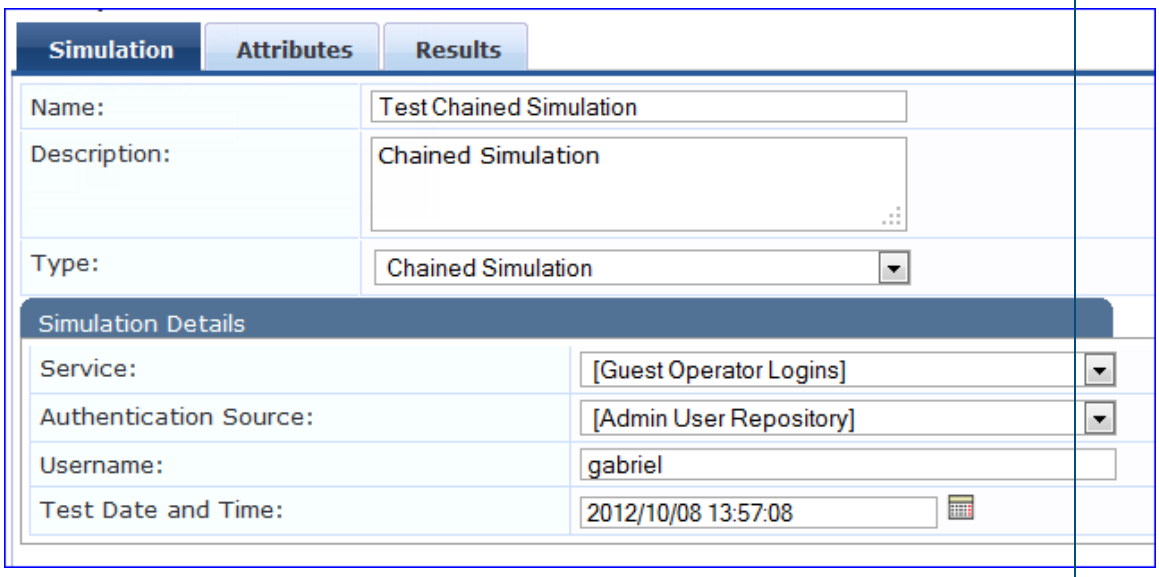
Parameter	Description
	 • Input (**Attributes** tab): Use the **Rules** Editor to create a request with the attributes you want to test. Connection and RADIUS namespaces are loaded in the **Attributes** editor. • Returns (**Results** tab): Enforcement Profile(s) and the attributes sent to the device. **NOTE: Authentication Source** and **User Name** inputs are used to derive dynamic values in the enforcement profile that are fetched from authorization source. These inputs are optional. **NOTE:** Dynamic Roles are attributes (that are enabled as a role) fetched from the authorization source. For an example of enabling attributes as a role, see Generic LDAP and Active Directory on page 155.
Type **Chained Simulations**	• Input (**Simulation** tab): Select **Service**, **Authentication Source**, **User Name**, and **Date/Time**.

Table 31: *Add Policy Simulation - Simulation tab Parameters (Continued)*

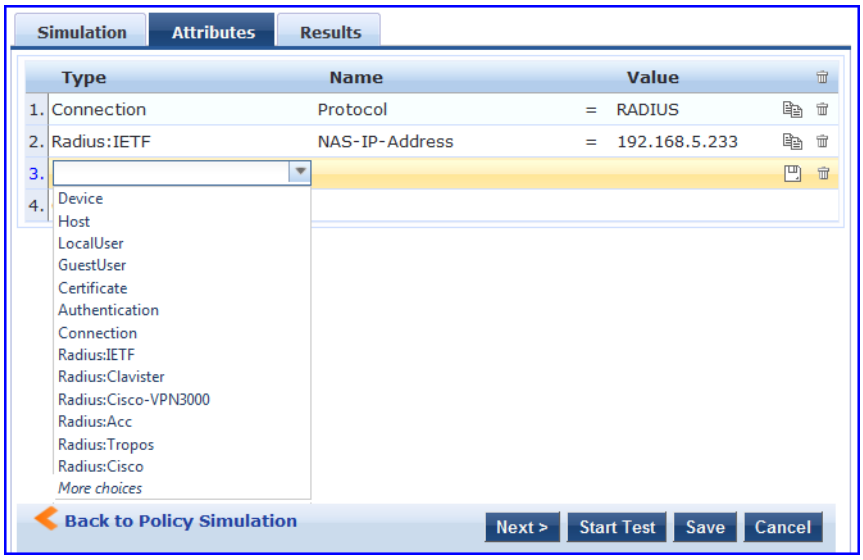
Parameter	Description
	 • Input (**Attributes** tab): Use **Rules Editor** to create a request with the attributes you want to test. All namespaces that are relevant in the **Role Mapping Policy** context are loaded in the **Attributes** editor. • Returns (**Results** tab): **Role(s)**, **Post Status**, **Enforcement Profiles**, and **Status Messages**.
Test Date/Time	Use the calendar widget to specify date and time for simulation test.
Next	After providing inputs in this tab, click **Next** to open the **Attributes** tab.
Start Test	Run test. You can see the result displayed in the **Results** tab.

In the **Attributes** tab, enter the attributes of the policy component to be tested. The namespaces loaded in the **Type** column depending on the type of simulation (See above).

The **Attributes** tab is not displayed if you select the **Audit Policy** component in the **Simulation** tab.

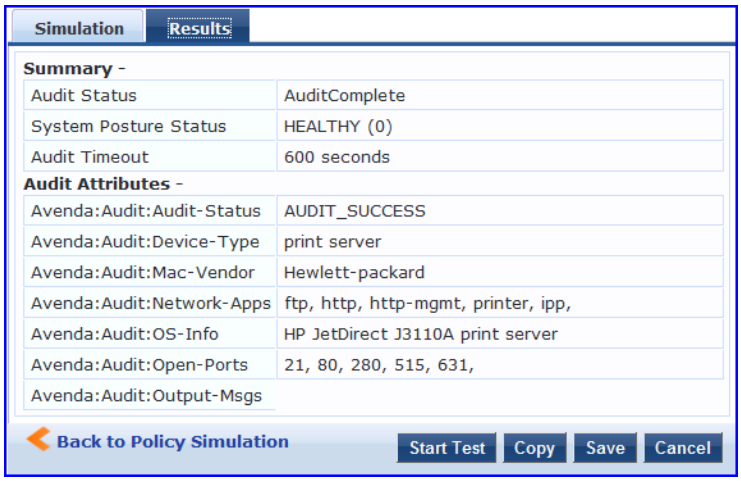
The following figure shows an example of the **Add Simulation - Attributes** tab:

Figure 61: *Add Simulation - Attributes Tab*



In the **Results** tab, Policy Manager displays the results of applied test request parameters against the specified policy component(s). The result shown in the **Results** tab is depend on the type of simulation selected. The following figure shows an example of the **Add Simulation - Results** tab:

Figure 62: *Add Simulation - Results Tab*



Import and Export Simulations

Navigate to **Configuration > Policy Simulation** and select the **Import** link. The following figure shows an example of the **Import from file** page followed by parameter definition:

Figure 63: *Import Simulations*

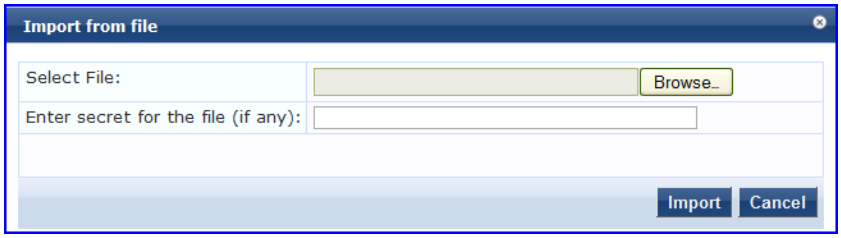


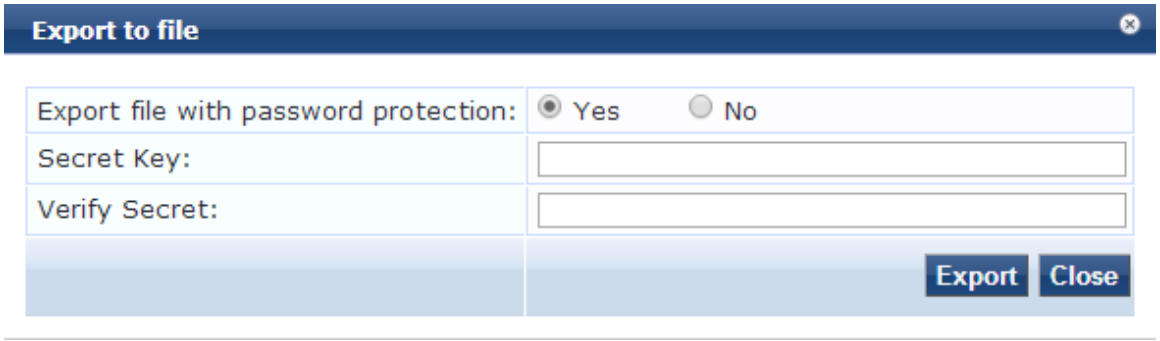
Table 32: *Import from file page Parameters*

Parameter	Description
Select file	Browse to select name of simulations to import.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.

Export Simulations

Click the **Export All** link to export all simulations. The browser displays the **Save As** dialog box in which you can enter the name of the XML file to export all simulations. The following image shows an example of the **Export** page to file page followed by parameter definition:

Figure 64: *Export Simulations*



To export a specific simulation, click **Export.** In the **Save As** dialog box, enter the name of the XML file to contain the export data.

Table 33: *Export Simulations*

Parameter	Description
Export file with password protection	Select **Yes** to export the file with password protection.
Secret Key	Enter the secret key in this field.
Verify Secret	Enter the same secret key to confirm and complete export.

The Policy Manager policy model groups policy components that serve a specific type of request into **Services** page, which is at the top of the policy hierarchy.

For more information, see:

- Architecture and Flow on page 79
- Start Here on page 79
- Policy Manager Service Types on page 98
- Services on page 118
- Identity on page 191

Architecture and Flow

Architecturally, Policy Manager Services are classified into the following:

- **Parents** of their policy components, which are wrapped (hierarchically) and coordinated in processing requests.
- **Siblings** of other Policy Manager Services within an ordered priority that determine the sequence in which they are tested against requests.
- **Children** of Policy Manager, which test requests against their rules to find a matching service for each request.

The flow-of-control for requests follows this hierarchy:

- *Policy Manager* tests for the first Request-to-Service-Rule match.
- The matching Service coordinates execution of its policy components.
- Those *policy components* process the request to return Enforcement Profiles to the network access device and optionally, posture results to the client.

There are two approaches to creating a new service in Policy Manager:

- **Bottom - Up**: Create all policy components (Authentication Method, Authentication Source, Role Mapping Policy, Posture Policy, Posture Servers, Audit Servers, Enforcement Profiles, and Enforcement Policy) first, as needed, and then create the service using the **Service** creation wizard.
- **Top-Down**: Start with the **Service** creation wizard and create the associated policy components as and when required, all in the same flow.

To help you get started, Policy Manager provides 14 Service types or templates. If these service types do not suit your needs, you can create a service using custom rules.

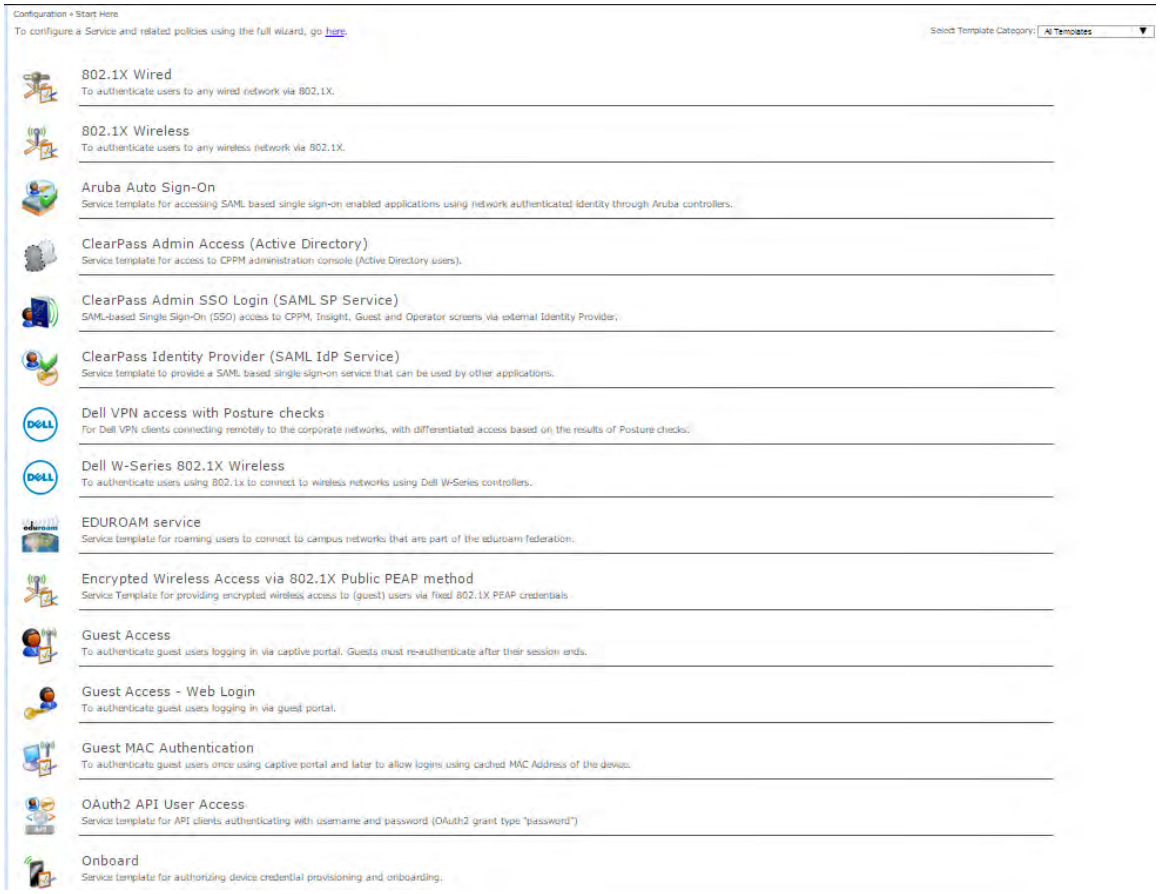
Start Here

The Dell Networking W-ClearPass Policy Manager **Start Here** page provides the ability to create templates for services where you can define baseline policies and require specific data, when you create services. Service templates create services and define components such as role-mapping policies, enforcement policies, and network devices with a **fill-in-the-blanks** approach. Fill in various fields; Policy Manager creates the different configuration elements that are needed for the service. These various configuration elements are added back to the service, when it is created. ClearPass provides the following service templates:

- 802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless on page 81
- Dell VPN Access with Posture Checks on page 84
- Aruba Auto Sign-On on page 86
- ClearPass Admin Access on page 87
- ClearPass Admin SSO Login (SAML SP Service) on page 89
- ClearPass Identity Provider (SAML IdP Service) on page 89
- EDUROAM Service on page 90
- Encrypted Wireless Access via 802.1X Public PEAP method on page 92
- Guest Access Web Login on page 93
- Guest Access on page 94
- Guest MAC Authentication on page 95
- Onboard on page 96

The following figure shows an example of the **Service Templates** page:

Figure 65: *Service Templates page (partial view)*



The following service templates are supported when the High Capacity Guest (HCG) mode is enabled:

- ClearPass Admin Access (Active Directory)
- ClearPass Admin SSO Login (SAML SP Service)
- ClearPass Identity Provider (SAML IdP Service)
- Encrypted Wireless Access via 802.1X Public PEAP method
- Guest Access
- Guest Access - Web Login

- Guest MAC Authentication
- OAuth2 API User Access

The following service types are supported when the HCG mode is enabled:

- MAC Authentication
- RADIUS Authorization
- 1RADIUS Enforcement
- RADIUS Proxy
- Dell Application Authentication
- Dell Application Authorization
- TACACS+ Enforcement
- Web-based Authentication
- Web-based Open Network Access

The following authentication methods are used in service templates in the HCG mode:

- PAP
- CHAP
- MSCHAP
- EAP_MD5
- MAC_AUTH
- AUTHORIZE
- EAP_PEAP_PUBLIC

802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless

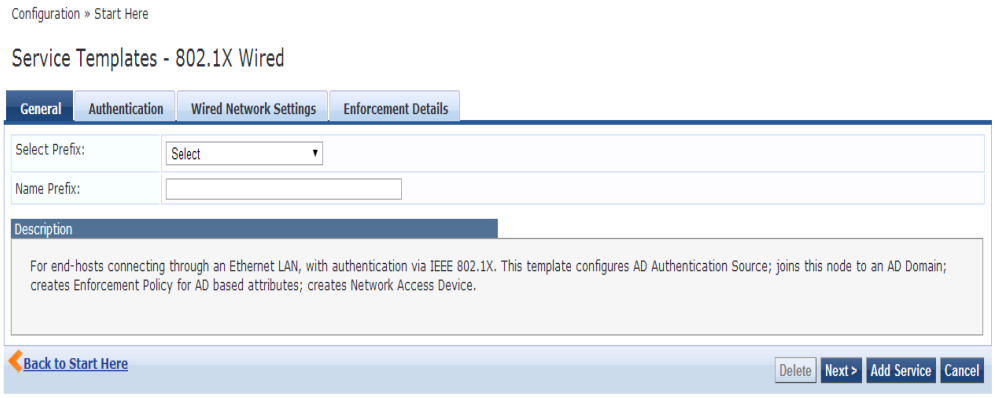
The **802.1X Wired** template is designed for wired end-hosts connecting through an Ethernet LAN with authentication using IEEE 802.1X. The **802.1X Wired** template allows configuring both identity and posture based policies.

The **802.1X Wireless** template is intended for wireless end-hosts connecting through an 802.11 wireless access device or controller with authentication using IEEE 802.1X. The **802.1X Wireless** template allows configuring both identity and posture based policies.

The Dell W-Series **802.1X Wireless** template is designed for wireless end-hosts connecting through an Dell 802.11 wireless access device or controller with authentication using IEEE 802.1X (Service rules customized for Dell WLAN Mobility Controllers).

All three templates are configured using identical parameters.

Figure 66: *Adding, Editing, or Deleting from a Service Template*



To add a new service for the selected Service Template, specify a unique **Name Prefix** (applies only to the selected template) in the **General** tab and update the required fields in the **Authentication** and **Enforcement Details** sections and click **Add Service**. Subsequently, an entry for the new set of configuration is created under the **Services**, **Roles**, **Role Mapping**, **Enforcement Policies** and **Profiles** menu.

NOTE

The sections shown in the figure and listed above are not same for all service templates. It is recommended to specify the appropriate sections for the respective templates when you add a new service.

Once you add a new service for the service template, the service denoted by the **Name Prefix** appears in the **Select Prefix** dropdown. Selecting a prefix from the dropdown populates the existing configuration for the service. Edit the changes and click **Edit Service** to save the changes.

To delete a service, select the appropriate service from the **Select Prefix** dropdown and click **Delete**. All the configured entries under the **Services**, **Authentication Source, Roles**, **Role Mapping**, **Enforcement Policies** and **Profiles** menu are deleted if these entities were created from the Service Template.

NOTE

When you edit or delete the entities of a service, a message is displayed at the top of the entity page stating that the selected entity was created through the Service Template.

Do not delete entities used in service configurations that are not created using the Service Template.

The following table describes the parameter definition used in the 802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless service templates:

Table 34: *802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication** and **Enforcement Details** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that is appended to services using this template. Use this to identify the services that use templates.
Authentication	

Table 34: *802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters (Continued)*

Parameter	Description
Select Authentication Source	Select any available Authentication Source from the list, the information updated in the **Authentication** and **Enforcement Details** tabs will be auto-populated.
Active Directory Name	Enter the active directory name. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter DN of the node in your directory tree from which to start searching for records. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for connection. This field is mandatory.
Enforcement Details	
Attribute Name	The attributes defined in the **Authentication Source** are listed here. Configure an optional enforcement policy based on the following attributes: • Email • Name • Phone • UserDN • Company • member of • Title For example, you can configure an enforcement policy for a contractor specifying that "If Name equals <contractor_name>, then assign the [Contractor] Role."
Attribute Value	Enter the active directory attribute value for the selected name in the **Attribute Name** field.
VLAN ID	Enter the Standard RADIUS-IETF VLAN ID.
Wired Network Settings	
Select Switch	Select any switch from the drop-down list.

Table 34: *802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters (Continued)*

Parameter	Description
Device Name	Enter the name of the device.
IP Address	Enter the IP address of the device.
Vendor Name	Select the manufacturer of the wired controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated Change of Authorization (CoA) on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Wireless Network Settings	
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.

Dell VPN Access with Posture Checks

This template authenticates Dell VPN clients connecting remotely to corporate networks. Differentiated access is based on the result of Posture checks. This template:

- Configures an AD Authentication Source
- Joins this node to the AD Domain
- Creates Enforcement Policy for AD based attributes
- Creates Network Access Device

NOTE

Posture checks are not performed if the **High Capacity Guest** mode is enabled in the cluster.

NOTE

You can view only the default user role in the **Dell User Roles for different access privileges** tab if the **High Capacity Guest** mode is enabled in the cluster.

The following table describes the parameter definitions of **Dell VPN Access with Posture Checks** service template:

Table 35: *Dell VPN Access with Posture Checks Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication Dell Wireless Controller for VPN Settings** and **Dell User Roles for different access privileges** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an Authentication Source from the list. The information provided in the **Authentication**, **Dell Wireless Controller for VPN Settings**, and **Dell User Roles for different access privileges** sections are auto-populated.
Active Directory Name	Enter your active directory name.
Description	Enter a description that helps you to identify the characteristics of this template.
Server	Enter the hostname or the IP address of the Active Directory server.
Identity	Enter the Distinguished Name of the administrator account.
NETBIOS	Enter the server Active Directory domain name.
Base DN	Enter DN of the node in your directory tree from which to start searching for records.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
Dell Wireless Controller for VPN Access	
Select Wireless Controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.

Table 35: *Dell VPN Access with Posture Checks Service Template Parameters (Continued)*

Parameter	Description
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Dell User Roles for different access privileges	
Create a new Enforcement Policy	
Initial Role (before posture checks)	Enter the initial role of the client before posture checks are performed.
Quarantined Role (failed posture checks)	Enter the role of clients that fail posture checks.
Healthy Role (passed posture checks)	Enter the role of the client after a posture check is passed and deemed healthy.

Aruba Auto Sign-On

This service template allows you to access the SAML based single sign on enabled applications (such as Policy Manager, Guest, Onboard, and Insight) using network authenticated (802.1X) identity through Dell controllers. The following table describes the parameter definition of the **Aruba Auto Sign-On** service template:

Table 36: *ClearPass Aruba Auto Sign-On Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This field populates the pre-configured information in the **Authentication**, **SP details**, and **Enforcement Details** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an Authentication Source from the list. The information provided in the **Authentication**, **Enforcement Details**, and **SP details** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This

Table 36: *ClearPass Aruba Auto Sign-On Service Template Parameters (Continued)*

Parameter	Description
	field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the Distinguished Name of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the Distinguished Name of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for connection. This value defaults to 389. This field is mandatory.
Enforcement Details	
Create new Enforcement Policy	The attribute defined in the Authentication Source are listed here. Configure an optional enforcement policy based on the following attributes: • Department • Email • Name • Phone • UserDN • company • memberOf • Title For example, you can configure an enforcement policy for a contractor as "If Name equals <contractor_name>, then assign the [Contractor] Role."
SP Details	
SP URL	Enter the Service Provider (SP) URL.
Attribute Name	Enter attribute names and assign values to those names. These name/value pairs are included in SAML responses.
Attribute Value	

ClearPass Admin Access

This template is designed for services that authenticate users against Active Directory (AD). Use AD attributes to determine appropriate privilege levels for Dell Networking W-ClearPass Policy Manager admin access. The following table describes the parameter definition of the **ClearPass Admin Access** service template:

Table 37: *ClearPass Admin Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication** and **Role Mapping** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an Authentication Source from the list. The information updated in the **Authentication** and **Role Mapping** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the Distinguished Name of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the Distinguished Name of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for connection. This field is mandatory.
Role Mapping	
Attribute Name	Select the active directory attribute.
Super Admin Condition	Defines the various privilege levels.
Read Only Admin Condition	
Help Desk Condition	

ClearPass Admin SSO Login (SAML SP Service)

This application service template allows SAML-based Single Sign-On (SSO) authenticated users to access Policy Manager, Guest, Insight, and Operator pages. The following table describes the parameter definition of the **ClearPass Admin SSO Login** service template:

Table 38: ClearPass *Admin SSO Login Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Service Rule** tab. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Application	Select the application that single-sign-on-authenticated administrative users can access.

ClearPass Identity Provider (SAML IdP Service)

This template is designed for services that act as an Identity Provider (IdP). This IdP feature allows the layer-2 device, RADIUS server, and Security Asserting Markup Language (SAML) IdP to work together and deliver application-based single sign-on using network authentication information. The following table describes the parameter definition of the **ClearPass Admin Access** service template:

Table 39: *ClearPass Admin Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication** and **SP Details** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an Authentication Source from the list, the information updated in the **Authentication** and **SP Details** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.

Table 39: *ClearPass Admin Access Service Template Parameters (Continued)*

Parameter	Description
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the Distinguished Name of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the Distinguished Name of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for connection. This field is mandatory.
SP Details	
SP URL	Enter the Service Provider (SP) URL.
Attribute Name	Enter the name of the attributes and assign values to those names. These name/value pairs are included in SAML responses.
Attribute Value	

EDUROAM Service

This template is designed for the following scenarios:

- Local campus users connecting to eduroam from the local wireless network.
- Roaming users from an eduroam campus connecting to their campus network.
- Roaming users connecting from local campus or other campuses that are part of the eduroam federation.

You cannot view the **EDUROAM** service template if the **High Capacity Guest** mode is enabled in the cluster.

The following table describes the parameter definition of the **EDUROAM** service template:

Table 40: *EDUROAM Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication, Service Rule, Wireless,** and **Federation Level Radius Server (FLR) tabs**. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	**Service Rule**

Table 40: *EDUROAM Service Template Parameters (Continued)*

Parameter	Description
Enter domain details	Enter the domain name of the network. For example, @edunet.ucla.com. This field is mandatory.
Select Vendor	Select the vendor of the network device. This field is mandatory.
Authentication	
Select Active Directory	Select an Authentication Source from the list, the information updated in the **Authentication**, **Wireless** and **Federation Level Radius Server (FLR)** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the Distinguished Name of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the Distinguished Name of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for connection. This field is mandatory.
Wireless Network Settings	
Select wireless controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.

Table 40: *EDUROAM Service Template Parameters (Continued)*

Parameter	Description
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Federation Level RADIUS Server (FLR)	
Host Name	The hostname of the federation RADIUS server.
IP Address	The IP address of the federation RADIUS server.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
RADIUS Authentication Port	Enter a port number here.
RADIUS Accounting Port	Enter a port number here.

Encrypted Wireless Access via 802.1X Public PEAP method

This template is designed for providing encrypted wireless access to users using fixed 802.1X PEAP credentials. This template configures an **EAP PEAP Public** type authentication method and creates enforcement policy for network access. The following table describes the parameter definition of the **Encrypted Wireless Access via 802.1X Public PEAP method** service template:

Table 41: *Encrypted Wireless Access via 802.1X Public PEAP Method Service Template Parameters*

Parameter	Description
General	
Name Prefix	Enter a prefix that you want to append to services using this template. You can use this to identify services that use templates.
Wireless Network Settings	
Select wireless controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.

Table 41: *Encrypted Wireless Access via 802.1X Public PEAP Method Service Template Parameters (Continued)*

Parameter	Description
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Authentication Method	
Public Username	Enter public username for EAP PEAP Public type authentication method.
Public Password	Enter password for EAP PEAP Public type authentication method.
Access Restrictions	
Days allowed for access	Select the days on which network access is allowed.

Guest Access Web Login

This service authenticates guests logging in using the Guest portal. To use this service, create a **Guest Web Login** page that sets the **Pre-Auth Check** option to **AppAuth - Check using** Dell **Application Authentication**. The following table describes the parameter definition of the **Guest Access Web Login** service template:

Table 42: *Guest Web Login Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select any one prefix from the existing list of prefixes. This populates the pre-configured information in the **Service Rule** and **Guest Web Login** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Page name	Enter the name of the **Guest Web Login** page.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.

Guest Access

This template is designed for authenticating guest users who log in using captive portal. Guests must re-authenticate after session expiry. Guest access can be restricted based on day of the week, bandwidth limit, and number of unique devices used by the guest user. The following table describes the parameter definition of the **Guest Access** service template:

Table 43: *Guest Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select any one prefix from the existing list of prefixes. This populates the pre-configured information in the **Wireless Network Settings** and **Guest Access Restrictions** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Wireless SSID for Guest access	Enter the SSID value here.
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

Guest MAC Authentication

This template is designed for authenticating guest accounts based on the cached MAC Addresses used during authentication. A guest can belong to a specific role such as Contractor, Guest, or Employee, and each role can have different lifetime for the cached MAC Address. The following table describes the parameter definition of the **Guest MAC Authentication** service template:

Table 44: *Guest MAC Authentication Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Wireless Network Settings, MAC Caching Settings,** and **Guest Access restrictions** tabs. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Wireless SSID for Guest access	Enter the SSID name of your network.
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
MAC Caching Settings	
Cache duration for Guest Role	Enter the duration in number of days the MAC account will remain valid for the **Guest** role. After this the guest must re-authenticate using captive portal. **NOTE:** You must enter cache duration for at least one role.
Cache duration for Employee role	Enter the duration in number of days the MAC account will remain valid for the **Employee** role. After this the guest must re-authenticate using captive portal.

Table 44: *Guest MAC Authentication Service Template Parameters (Continued)*

Parameter	Description
Cache duration for Contractor role	Enter the duration in number of days the MAC account will remain valid for the **Contractor** role. After this the guest must re-authenticate using captive portal.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum number of devices allowed per user	Enter a number to define how many devices users can connect to the network.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

OAuth2 API User Access

This template is designed for configuration that supports Dell Networking W-ClearPass Policy Manager to authenticate API clients with username and OAuth2 grant type password. The **OAuth2 API User Access** service template uses the **Guest Operator Logins** as the default enforcement policy. The **Local User Repository** and **Admin User Repository** repositories are used as the default authentication sources. The following table describes the parameter definition of the **OAuth2 API User Access** service template:

Table 45: *OAuth2 API User Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes.
Name Prefix	Enter a prefix that is appended to services using this template. You can use this prefix to identify the services that use templates.

Onboard

This template is designed for configuration that allows to perform checks before allowing Onboard provisioning for Bring Your Own Device (BYOD) use-cases. This service creates an Onboard Pre-Auth service to check the user's credentials before starting the device provisioning process. This also creates an authorization service that checks whether a user's device can be provisioned using Onboard. Use an **802.1X Wireless** service to authenticate users prior to device provisioning with Onboard and after device provisioning is completed.

You cannot view the **Onboard** service template if the **High Capacity Guest** mode is enabled in the cluster.

The following table describes the parameter definition of the **Onboard Authorization** service template:

Table 46: *Onboard Authorization Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Wireless Network Settings**, **Device Access Restrictions**, and **Provisioning Wireless Network Settings** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	The name given to the wireless controller.
Controller IP Address	The wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Device Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Provisioning Wireless Network Settings	
Wireless SSID for Onboard Provisioning	Enter the SSID of your network.

Policy Manager Service Types

The following service types are available in Policy Manager:

Dell 802.1X Wireless

Configure this service for wireless hosts by connecting through a Dell 802.1X wireless access device or controller with authentication using IEEE 802.1X. Service rules are customized for a typical Dell W-Series Mobility Controller deployment. By default, Dell W-Series 802.1X service includes a rule that specifies that a Dell ESSID exists. The following are the default configuration tabs available in the **Add Service (Configuration > Services > Add)** page:

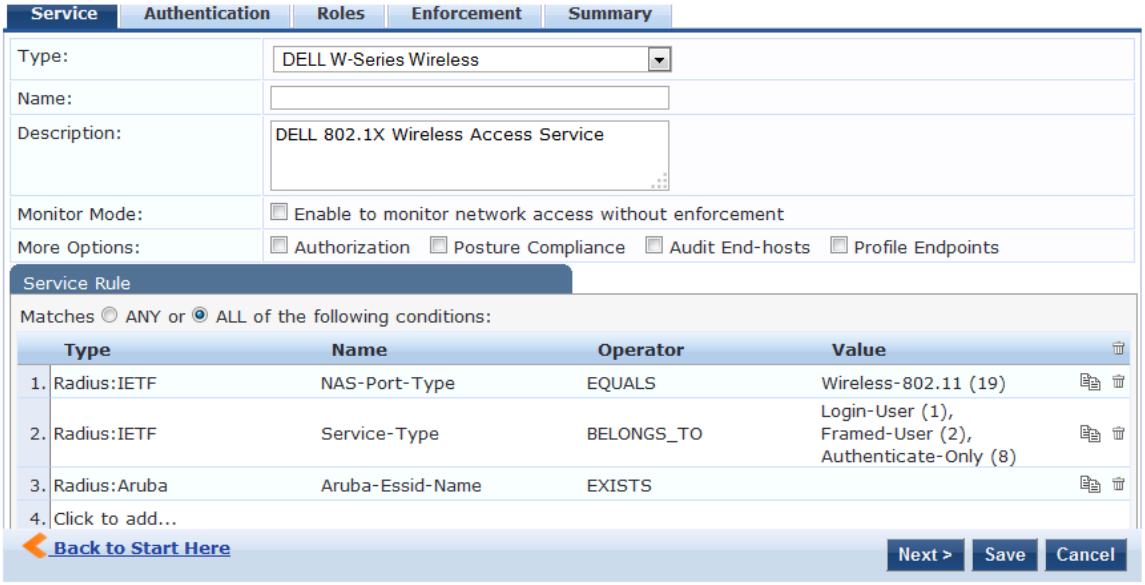
- Service
- Authentication
- Roles
- Enforcement
- Summary

You can also select the following additional tabs by checking the **More Options** field to access these configuration tabs:

- Authorization
- Posture Compliance
- Audit End-hosts
- Profile Endpoints

The following figure shows an example of the **Dell 802.1X Wireless** service:

Figure 67: *Dell 802.1X Wireless Service*



Service Tab

The **Service** tab includes basic information about the service. The **Service Rules** section defines a set of criteria that supplicants must match to trigger the service. Some service templates have one or more rules pre-defined. You can click on a service rule to modify any of its options. The following figure shows an example of the **Service** tab followed by parameter definition:

Figure 68: *Dell 802.1X Wireless Service - Service Tab*

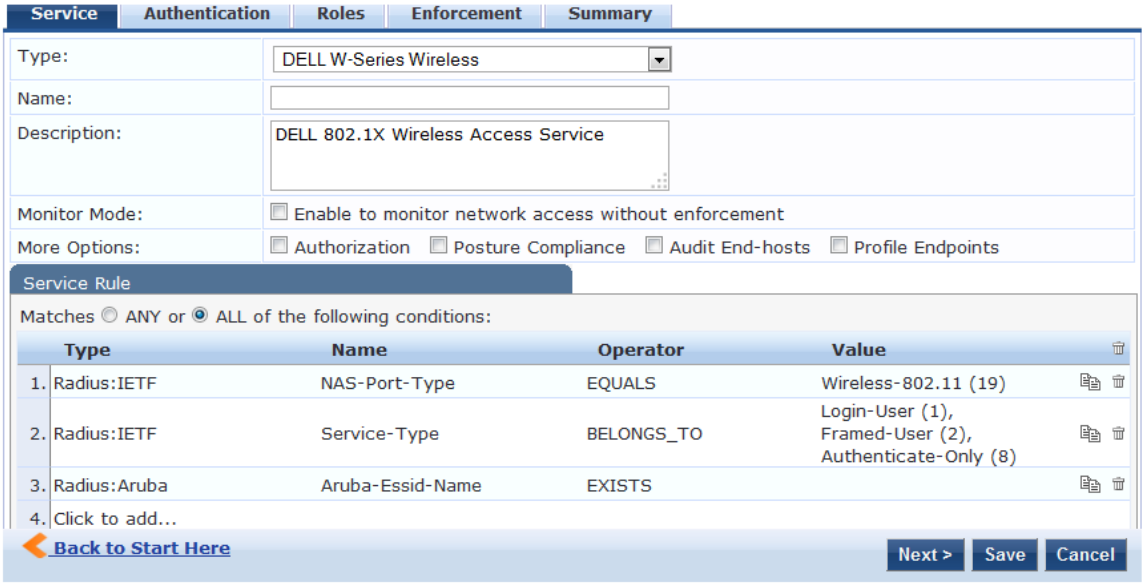


Table 47: *Dell 802.1X Wireless Service - Service tab Parameters*

Parameter	Description
Type	Select a service from the drop-down list that defines what type of service can be configured.
Name	Enter the name of the service.
Description	Provide additional information that helps to identify what the service does.
Monitor Mode	Check this box to exclude enforcement.
More Options	Check these boxes to access the category of configuration options.
Service Rule	
Type	Select the service rule type from the drop-down list.
Name	Select the name of the service rule from the drop-down list.
Operator	Select an appropriate operator from the list of operators for the data type of the attribute. For example, you can select from BELONGS_TO, NOT_BELONGS_TO, CONTAINS, EQUALS, and so on.
Value	Select the value from the drop-down list depends on the operator selected.

Service Rules define a set of criteria that supplicants must match to trigger the service. Some service templates have one or more rules pre-defined. Click on a service rule to modify its options.

If you want to administer the same set of policies for wired and wireless access, you can combine the service rule to define one single service. The other option is to keep two services for wired and wireless access, but re-use the policy components (authentication methods, authentication source, authorization source, role mapping policies, posture policies, and enforcement policies) in both services.

Authentication Tab

The **Authentication** tab contains options for configuring authentication methods and authentication sources. The following figure shows an example of the **Authentication** tab followed by parameter definition:

Figure 69: *Dell 802.1X Wireless Service - Authentication Tab*

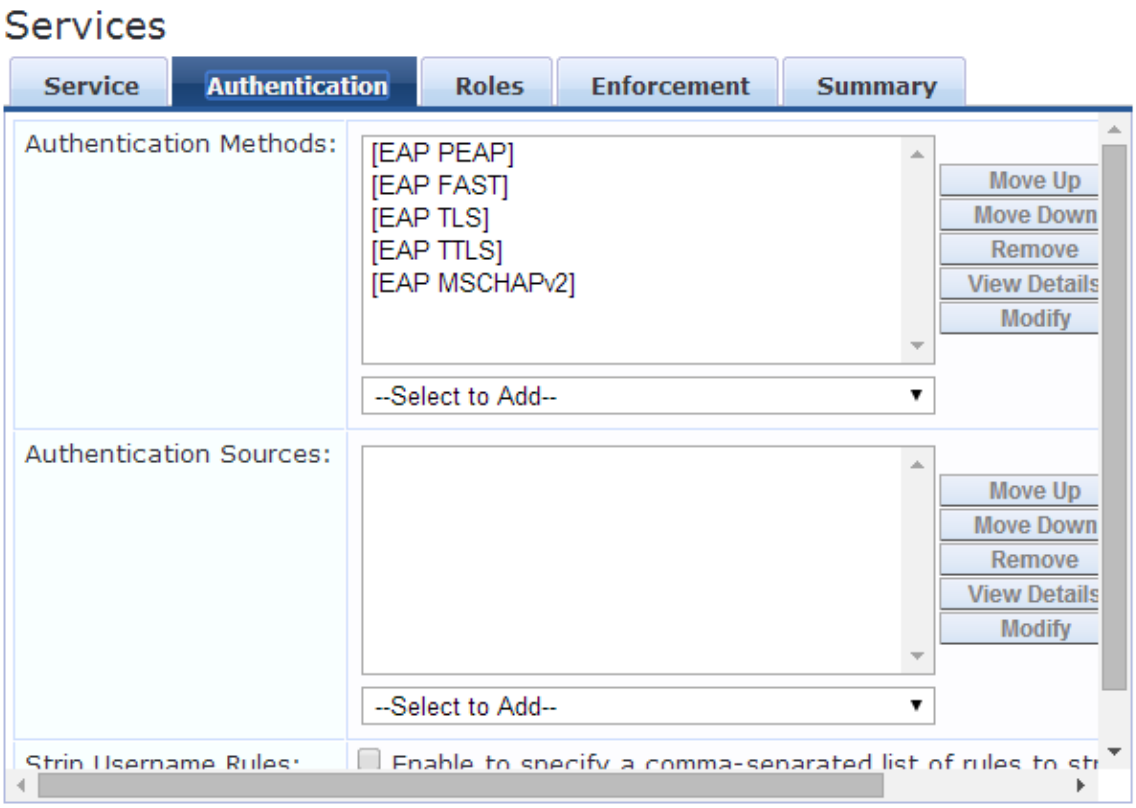


Table 48: *Dell 802.1X Wireless Service - Authentication tab Parameters*

Parameter	Description
Authentication Methods	Select authentication methods using the **Select to Add** field used for this service depend on the 802.1X supplicants and the type of authentication methods you choose to deploy. Policy Manager automatically selects the appropriate method for authentication, when a user attempts to connect. The common types, which are automatically selected include the following examples: • EAP PEAP • EAP FAST • EAP TLS • EAP TTLS **NOTE:** You can also use non-tunneled EAP method such as EAP-MD5 as an authentication method. **NOTE:** The **EAP-MD5** authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS mode. The order of authentication is significant, when a client tries to perform an 802.1X authentication. Policy Manager proposes the first authentication method configured. However, the client can accept the authentication method proposed by Policy Manager and continue authentication or send a Negative-Acknowledgment (NAK) and propose a different authentication method. If the newly proposed authentication method is also configured, then the authentication proceeds, otherwise authentication fails. **NOTE:** If most of the clients in the network use a specific authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged. For more information, see Adding and Modifying Authentication Methods on page 130 and Adding and Modifying Authentication Sources on page 154.
Authentication Sources	Specify the authentication sources using the **Select to Add** field used for this type of service. This can be one or more instances of the following examples: • Active Directory • LDAP Directory • SQL DB • Token Server • Policy Manager local DB
Strip Username Rules	Select the check box to pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

Use the **Authorization** tab to select the authorization sources for this service. Policy Manager fetches role mapping attributes from the authorization sources associated with the service, regardless of which authentication source was used to authenticate the user. For a given service, role mapping attributes are fetched from the following authorization sources:

- Authorization sources associated with the authentication source
- Authorization sources associated with the service

The **Authorization** tab is not displayed by default. To access this tab, select the **Authorization** check box from the **More Options** on the **Services** tab. The following figure shows an example of the **Authorization** tab followed by parameter definition:

Figure 70: *Dell 8021X Wireless Service - Authorization Tab*

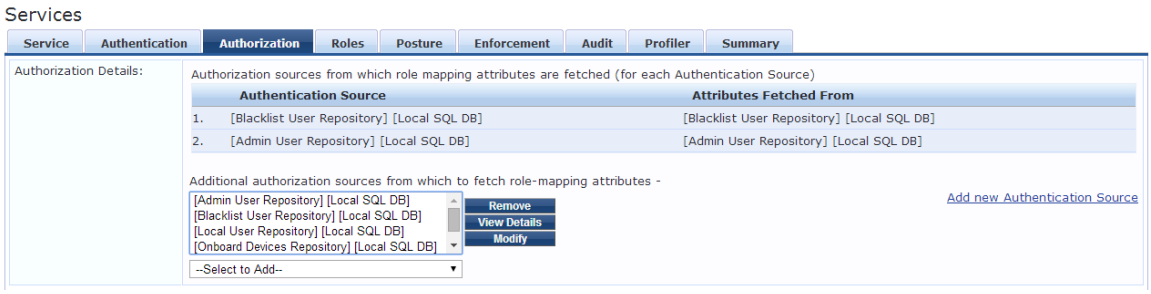


Table 49: *Dell 8021X Wireless Service - Authorization tab Parameters*

Parameter	Description
Authentication Source	Displays the authorization sources from which role mapping attributes are fetched for each Authentication Source.
Attributes Fetched From	Displays the source of attributes.
Additional authorization sources from which to fetch role-mapping attributes	Select the additional authorization sources using the **Select to Add** drop-down list.

For more information on configuring authorization sources, see Adding and Modifying Authentication Methods on page 130.

Roles Tab

Use the **Roles** tab to associate a role mapping policy with this service. The following figure shows an example of the **Dell 8021X Wireless Service - Roles** tab followed by parameter definition:

Figure 71: *Dell 8021X Wireless Service - Roles Tab*

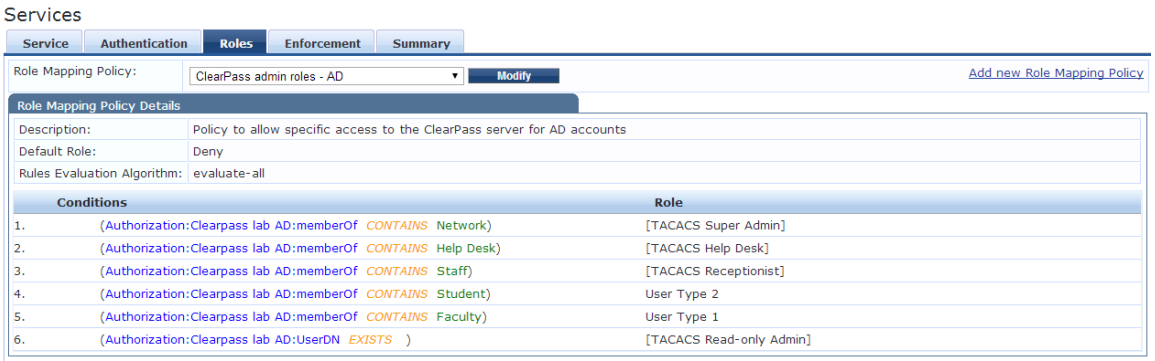


Table 50: *Dell 802.1X Wireless Service - Roles tab Parameters*

Parameter	Description
Role Mapping Policy	Select a Role Mapping Policy from the drop-down list. **NOTE:** A service can be configured without a Role Mapping Policy, but only one Role Mapping Policy can be configured for each service.
Role Mapping Policy Details	
Description	Provides additional information about the selected Role Mapping Policy.
Default Role	Specifies the role to which Policy Manager defaults, when the role mapping policy does not produce a match.
Rules Evaluation Algorithm	Shows first matched rule and return the role or Select all matched rules and return a set of roles.

For information on configuring role mapping policies, see Configuring a Role and Role Mapping Policy on page 202.

Posture Tab

The **Posture** tab is not enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box from the **More Options** field on the **Service** tab. You can enable the posture checking for this kind of service, if you deploy any of the following:

- Policy Manager in a Microsoft Network Access Protection (NAP)
- Cisco Network Admission Control (NAC) Framework environment
- Dell hosted captive portal that performs posture checks through a dissolvable agent

You cannot view the **Posture** tab if you enable the **High Capacity Guest** mode in the cluster.

The following figure shows an example of the **Posture** tab followed by parameter definition:

Figure 72: *Dell 8021X Wireless Service - Posture Tab*

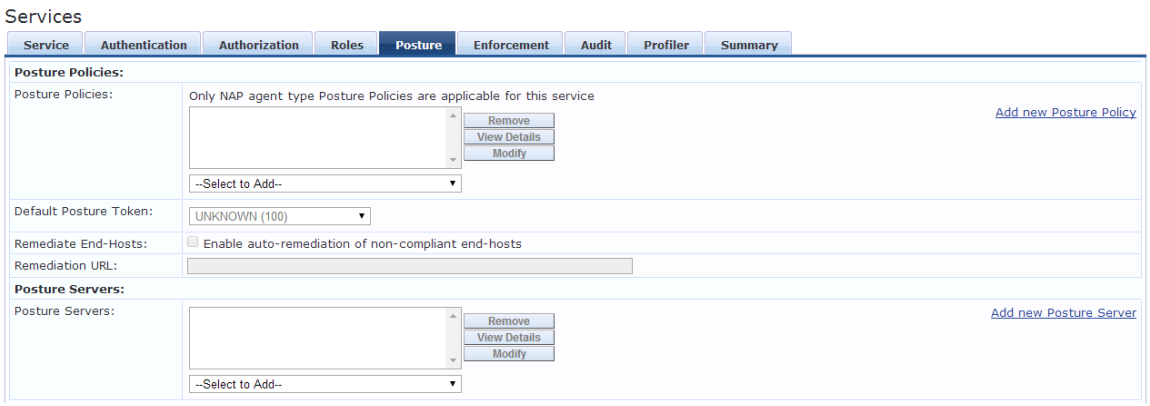


Table 51: *Dell 802.1X Wireless Service - Posture tab Parameters*

Parameter	Description
Posture Policies	
Posture Policies	Select the Posture Policy from the **Select to Add** drop-down list. If you do not have any pre-configured Posture Policies, click **Add new Posture Policy** to create a new Posture Policy. Only NAP agent type Posture Policies are applicable for this service.
Default Posture Token	Select the default Posture Token from the drop-down list.
Remediate End-Hosts	Select the **Enable auto-remediation of non-compliant end-hosts** check box to perform remediation action, when a client is quarantined.
Remediation URL	Enter the web link of a server resource to perform the remediation.
Posture Servers	
Posture Servers	Select the Posture Server from the **Select to Add** drop-down list. If you do not have any pre-configured Posture Servers, click **Add new Posture Server** to create a new Posture Server.

For more information on configuring Posture Polices and Posture Servers, see Adding a Posture Policy on page 210 and Adding and Modifying Posture Servers on page 247.

Enforcement Tab

Use this tab to select an enforcement policy for a service. You must select one. The following figure shows an example of the **Enforcement** tab followed by parameter definition:

Figure 73: *Dell 8021X Wireless Service - Enforcement Tab*

Table 52: *Dell 802.1X Wireless Service - Enforcement tab Parameters*

Parameter	Description
Use Cached Results	Select this check box to use cached Roles and Posture attributes from previous sessions.
Enforcement Policy	Select the pre-configured Enforcement Policy from the drop-down list. This is mandatory. If you do not have any pre-configured Enforcement Policies, click **Add new Enforcement Policy** to create a new Enforcement Policy.
Enforcement Policy Details	
Description	Displays additional information about the selected Enforcement Policy.
Default Profile	Displays a default profile applied by Policy Manager.
Rules Evaluation Algorithm	Shows first matched rule and return the role or Select all matched rules and return a set of roles.

See Configuring Enforcement Policies on page 298 for more information.

Audit Tab

Table 53: *Dell 802.1X Wireless Service - Audit tab Parameters*

Parameter	Description
Audit Server	Select the Audit Server from the following options: • **Nessus Server** - Interfaces with Policy Manager primarily to perform vulnerability scanning • **Nmap Audit** - Performs specific audit functions You can click the **View Details** button to view the **Policy Manager Entity Details** pop-up with the summary of Audit Server details. Click the **Modify** button to view the **Summary** tab with Audit Server details.
Audit Trigger Conditions	Select an Audit Trigger Condition from the following conditions: Known end hosts are the clients that are found in the authentication source(s) associated with this service.
Action after audit	Specifies the audit that can be performed only after the MAC authentication request is completed and the client has acquired an IP address through DHCP. Once the audit results are available, Policy Manager re-applies policies on the network device in one of the following ways: • **No Action** - The audit does not apply policies on the network device after completing this audit.

Table 53: *Dell 802.1X Wireless Service - Audit tab Parameters (Continued)*

Parameter	Description
	• **Do SNMP bounce** - This option bounces the switch port or force an 802.1X re-authentication (both done using SNMP). Bouncing the port triggers a new 802.1X or MAC authentication request by the client. If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager. • **Trigger RADIUS CoA action** - This option sends a RADIUS CoA command to the network device by Policy Manager.

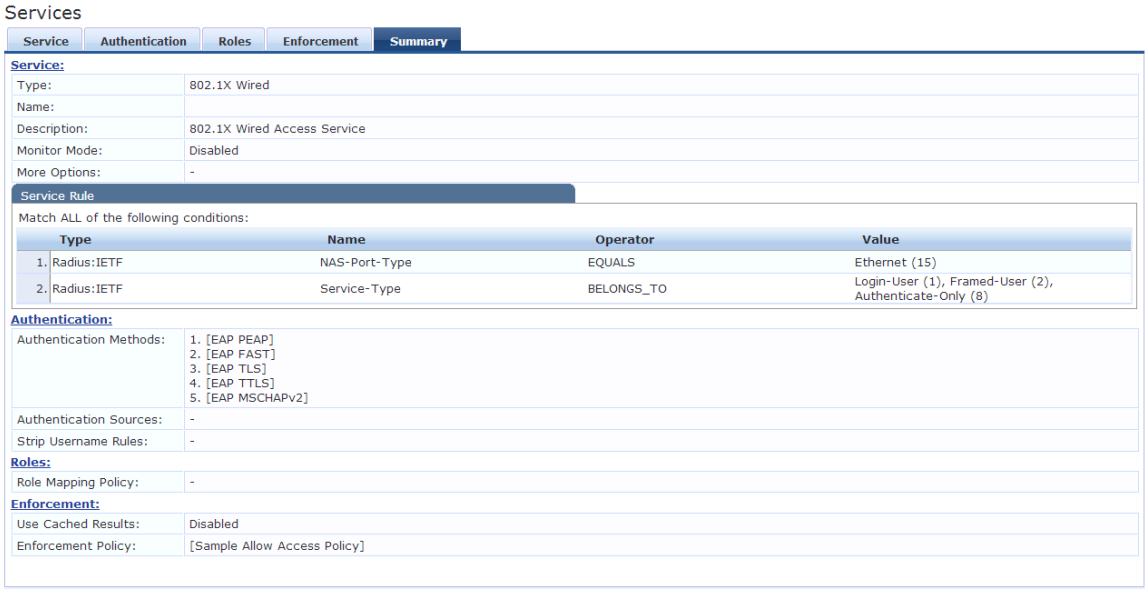
Table 54: *Dell 802.1X Wireless Service - Profiler tab Parameters*

Parameter	Description
Endpoint Classification	Select one or more Endpoint Classification items from the drop-down list.
RADIUS CoA Action	Select the RADIUS CoA action from the drop-down list. Click the **View Details** button to view the **Policy Manager Entity Details** page with the summary of Enforcement Profile details. Click the **Modify** button to view the **Summary** tab with profile details. You can click the **Add new RADIUS CoA Action** link to create a new RADIUS CoA action.

Summary Tab

The **Summary** tab presents the summary of parameters used in other tabs when you created a new service. The following figure shows an example of the **Summary** tab:

Figure 74: *Dell 8021X Wireless Service - Summary Tab*



802.1X Wireless

Configure the 802.1X Wireless service for wireless clients connecting through an 802.11 wireless access device or controller with authentication using IEEE 802.1X. You can view the following default configuration tabs in the **Add Service** (**Configuration** > **Services** > **Add**) page:

- Service
- Authentication
- Roles
- Enforcement

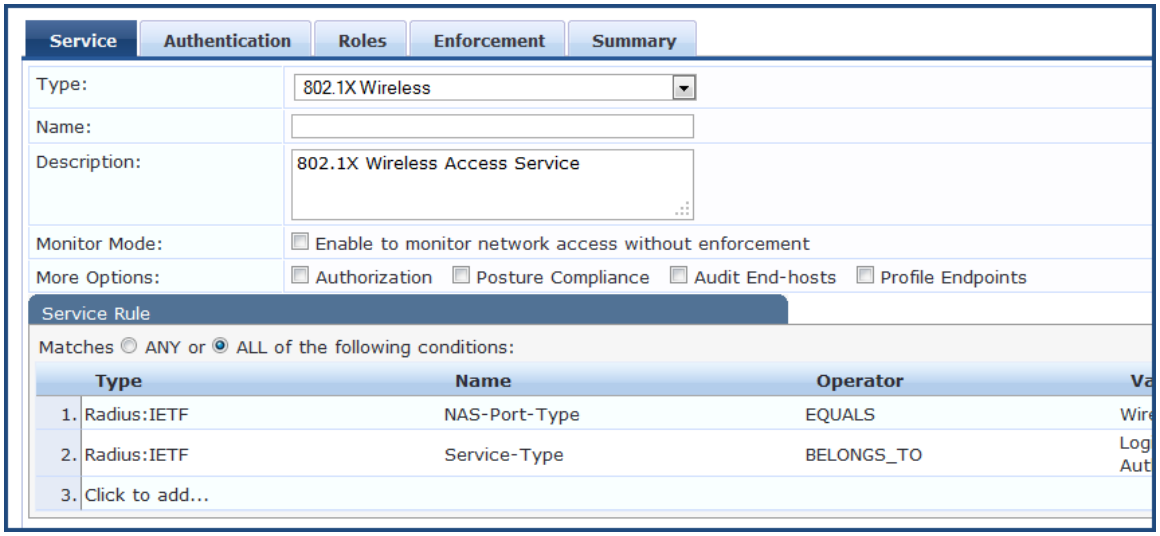
You can also select the following additional tabs by checking the **More Options** field to access these configuration tabs:

- Authorization
- Posture Compliance
- Audit End Hosts
- Profile Endpoints

Posture checks are not performed if the **High Capacity Guest** mode is enabled in the cluster.

The following figure displays an example of the **802.1X Wireless** service:

Figure 75: *802.1X Wireless Service*



If you want to administer the same set of policies for wired and wireless access, you can combine the service rule to define one single service. The other option is to keep two services for wired and wireless access, but re-use the policy components (authentication methods, authentication source, authorization source, role mapping policies, posture policies, and enforcement policies) in both services.

Configuring the 802.1X Wireless service for wireless clients connecting through an 802.11 wireless access device is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see Dell 802.1X Wireless on page 98

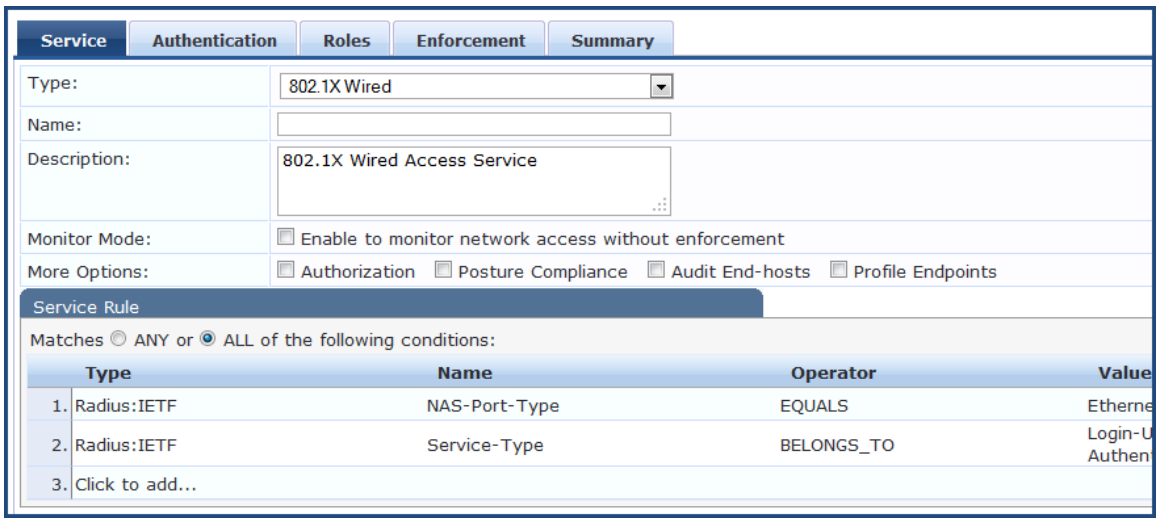
802.1X Wired

Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X.

Except for the NAS-Port-Type service rule value (which is Ethernet for 802.1X Wired and Wireless 802.11 for 802.1X Wireless), configuration for the rest of the tabs is similar to the Dell 802.1X Wireless service. See Dell 802.1X Wireless on page 98 for details.

The following figure shows an example of the **802.1X Wired** service page:

Figure 76: *802.1X Wired Service*



MAC Authentication

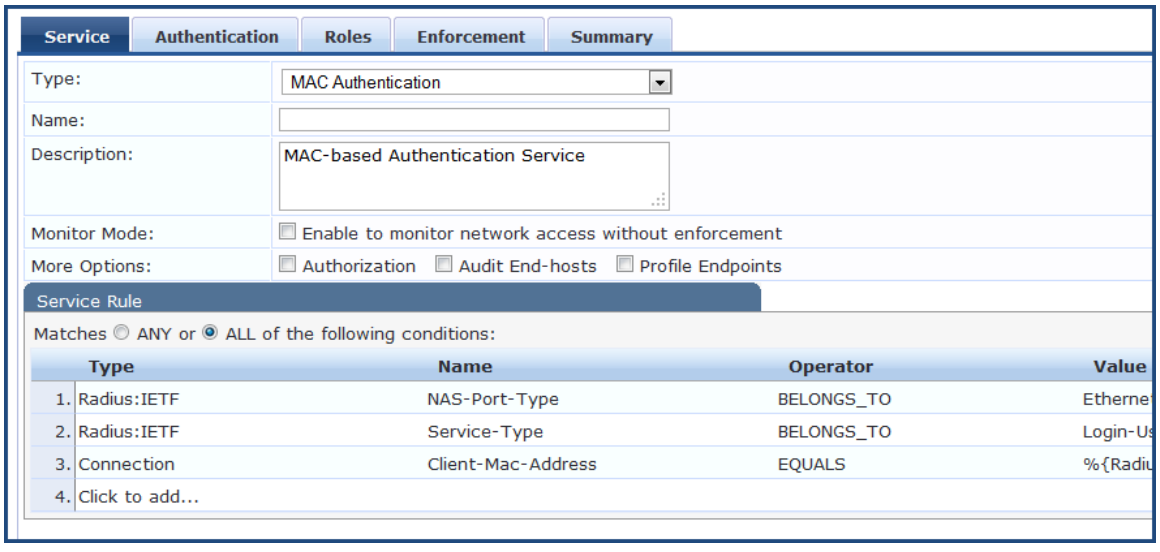
MAC-based authentication service, for clients without an 802.1X supplicant or a posture agent (printers, other embedded devices, and computers owned by guests or contractors). The network access device sends a MAC authentication request to Policy Manager. Policy Manager can look up the client in a white list or a black list, authenticate and authorize the client against an external authentication/authorization source, and optionally perform an audit on the client.

NOTE

You cannot configure Posture for this type of service.

The following figure shows an example of **MAC Authentication** service:

Figure 77: *MAC Authentication Service*



Except for the **Posture** tab, configuration for the rest of the tabs is similar to the **Dell 802.1X Wireless** service. For more information on configuration tabs, See Dell 802.1X Wireless on page 98 for details.

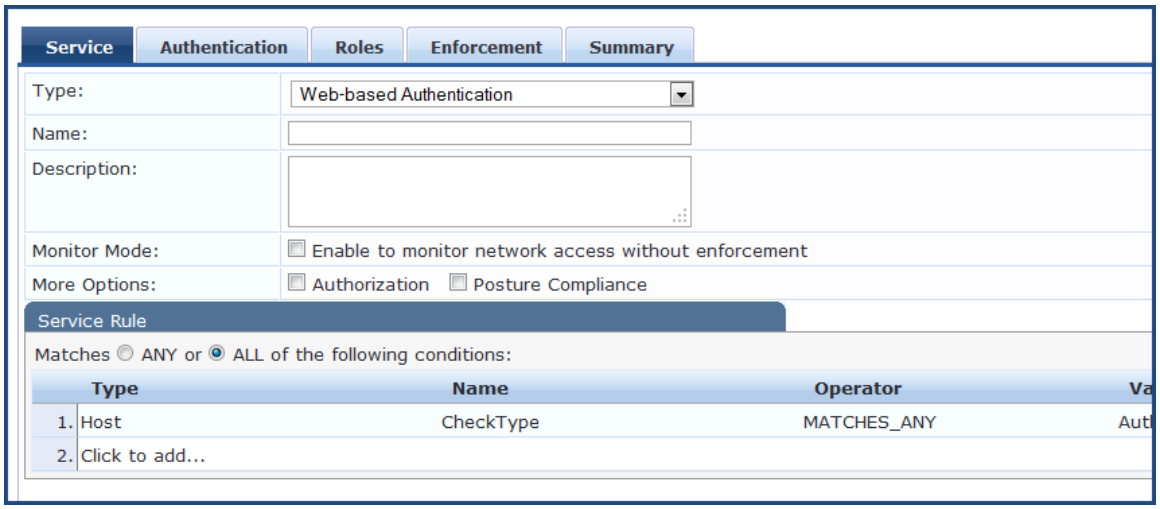
Web-based Authentication

Configure this service for guests or agent-less hosts that connect through the Dell built-in Portal. The user is redirected to the Dell captive portal by the network device or by a DNS server that is set up to redirect traffic on a subnet to a specific URL. The web page collects username and password, and also optionally collects health information on the following Operating Systems:

- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008
- Windows Server 2003
- Linux

An internal service rule **Connection:Protocol EQUALS WebAuth** categorizes requests into this type of service. You can add additional rules if needed. The following figure shows an example of the **Web-based Authentication** service:

Figure 78: *Web-based Authentication Service*



NOTE

The **Audit End-hosts** and **Profile Endpoints** options are not available for the **Web-based Authentication** service.

Configuring the **Web-based Authentication** service for guests or agent-less hosts is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see Dell 802.1X Wireless on page 98

Web-based Health Check Only

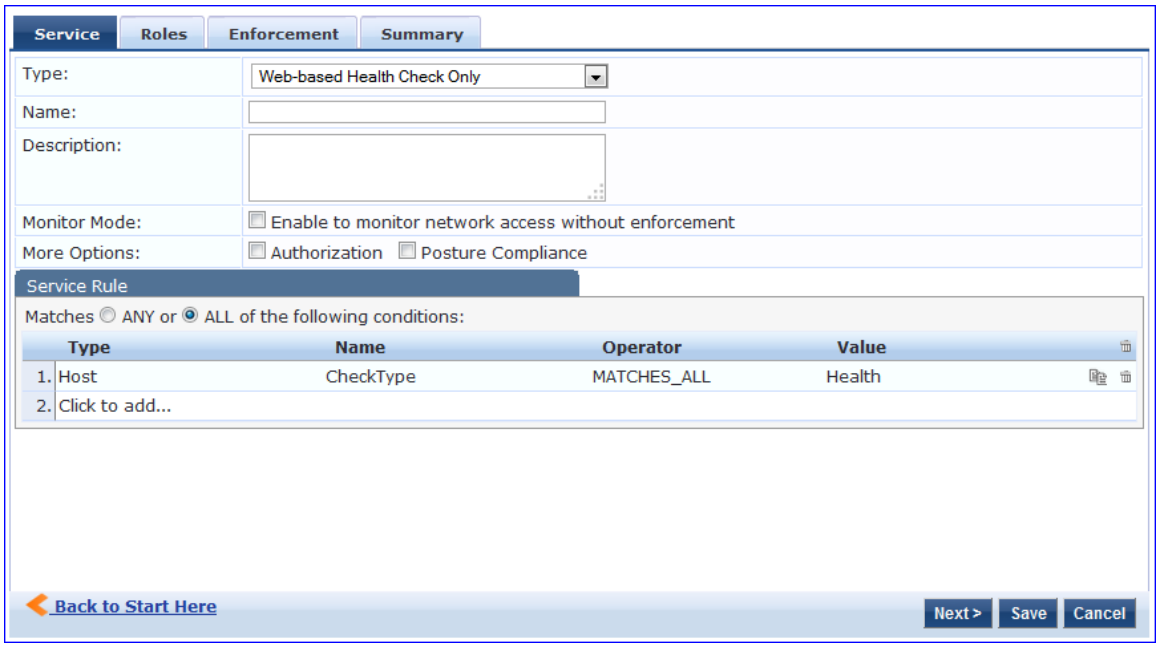
This type of service is the same as the **Web-based Authentication** service except that there is no authentication performed; only health check is done. The internal service rule **Connection:Protocol EQUALS WebAuth** categorizes requests into this type of service. The external service rule **Host:CheckType EQUALS Health** is automatically added when you select this type of service. For more information, see Web-based Authentication.

NOTE

This service does not include authentication options. This service performs health checks only.

The following figure shows an example of the **Web-Based Health Check Only** service:

Figure 79: *Web-Based Health Check Only Service*



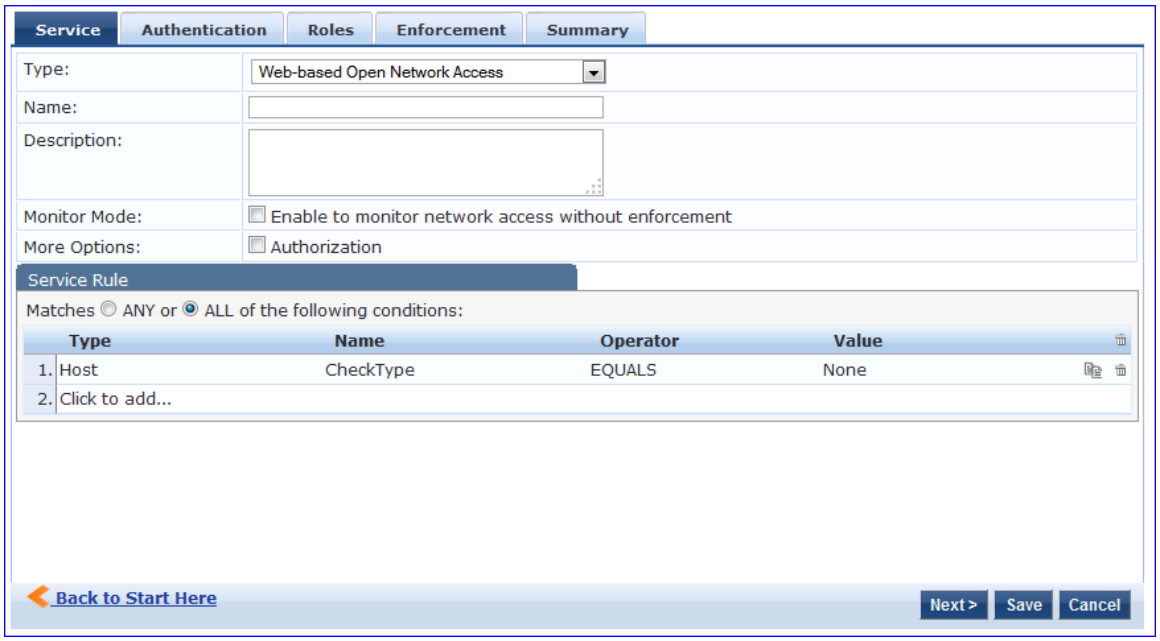
For more information on configuration tabs, see Dell 802.1X Wireless on page 98

Web-based Open Network Access

This type of service is similar to other **Web-based Authentication** service, except that health check is not performed on the endpoints. A **Terms of Service** page (as configured on the **Dell Networking W-ClearPass Policy Manager Guest Portal** page) is presented to the user. Network access is granted, when you click **Submit Action**.

Configuration for this service is the same as **Web-based Authentication** service except that the **Posture** option is not available. For more information, see Web-based Authentication. The following figure shows an example of the **Web-based Open Network** service page:

Figure 80: *Web-based Open Network Access Service*



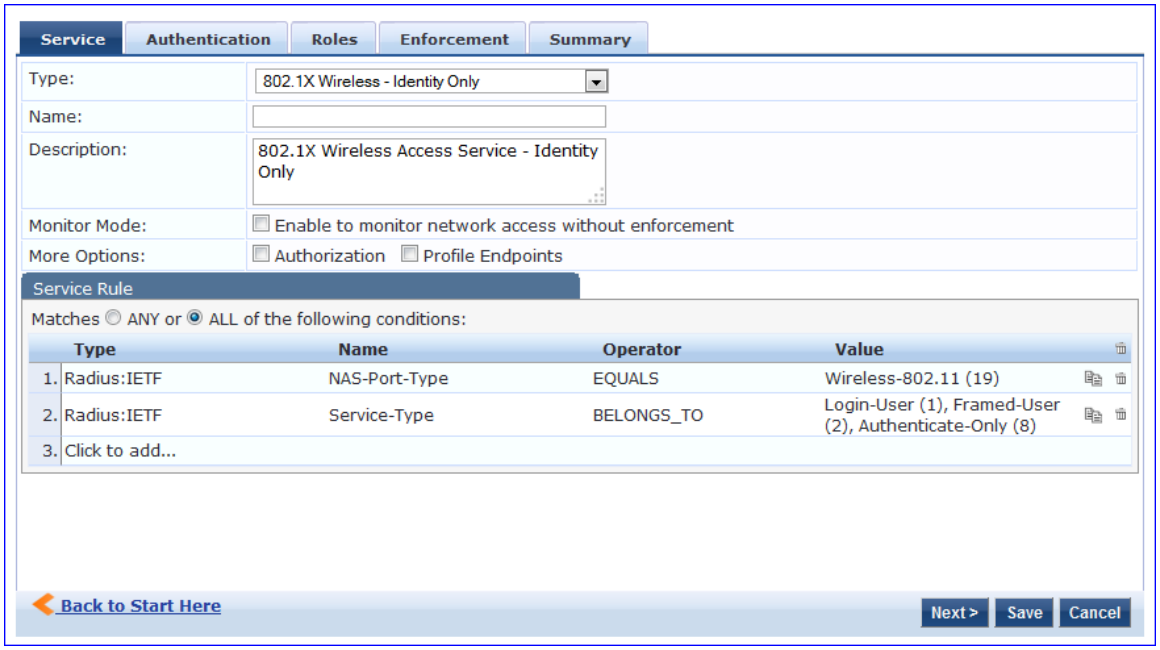
For more information on configuration tabs, see Dell 802.1X Wireless on page 98

802.1X Wireless - Identity Only

Configuration for this type of service is the same as the **Dell 802.1X Wireless** service except that **Posture** and **Audit** policies are not configurable, when you use this template. For more information, see 802.1X Wireless on page 108.

The following figure shows an example of the **802.1X Wireless - Identity Only** service:

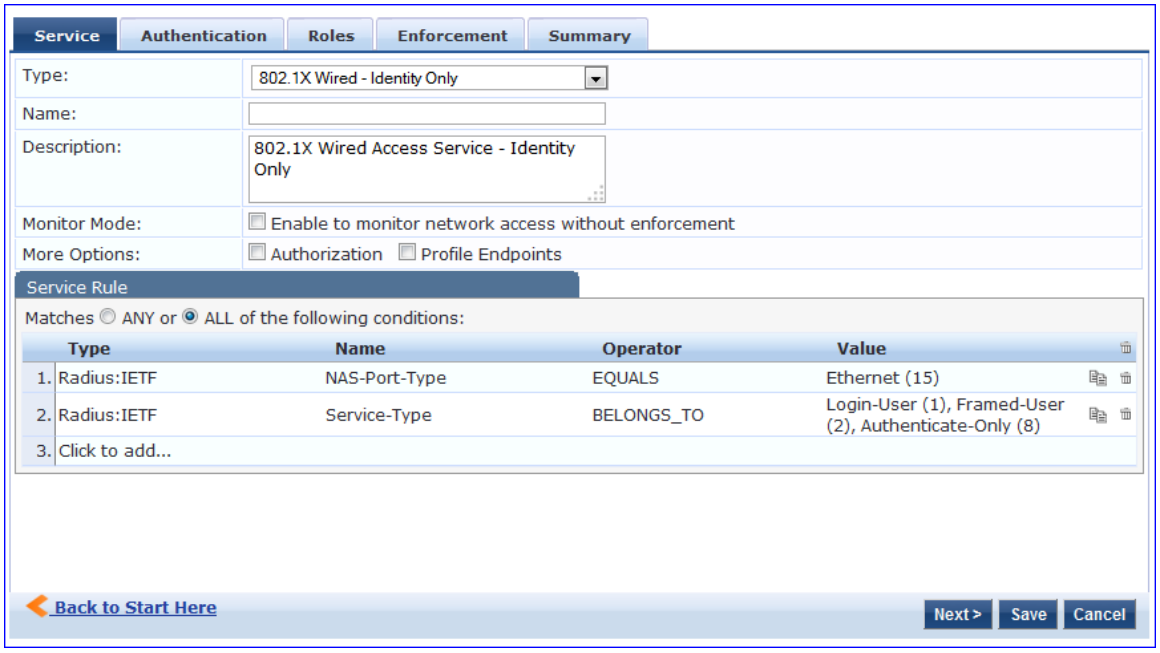
Figure 81: *802.1X Wireless - Identity Only Service*



802.1X Wired - Identity Only

Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X. Configuration for the **802.1X Wired - Identity Only** service is same as the **802.1X Wired** service except that **Posture** and **Audit** policies are not configurable, when you use this template. For more information, see 802.1X Wired on page 108. The following figure shows an example of the **802.1X Wired - Identity Only** service:

Figure 82: *802.1X Wired - Identity Only Service*



RADIUS Enforcement (Generic)

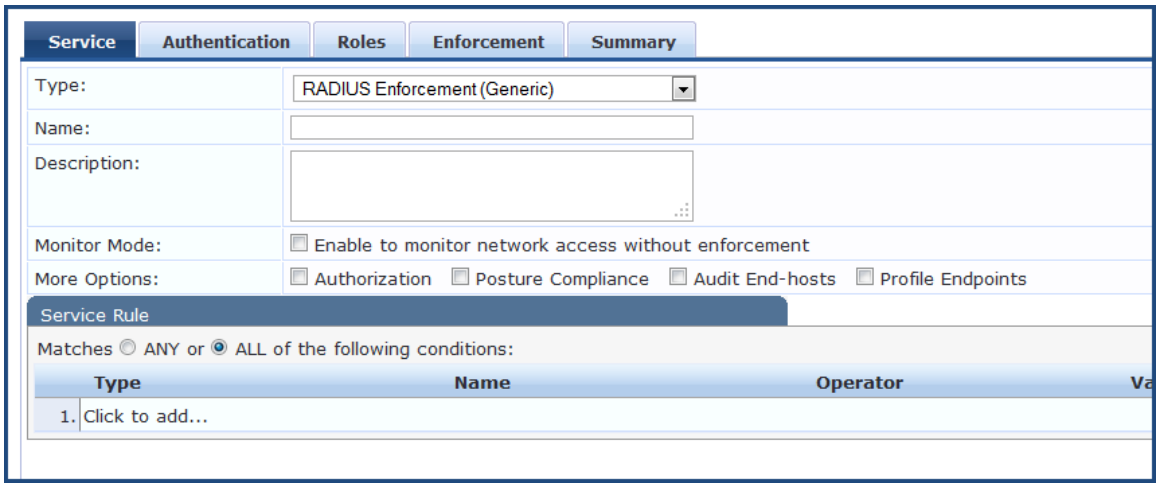
Configure the **RADIUS Enforcement (Generic)** service for any kind of RADIUS requests.

The **[AirGroup Authorization Service]** service is the only **RADIUS Enforcement (Generic)** service that is available by default.

The default configuration tabs include Service, Authentication, Roles, and Enforcement. You can also select Authorization, Posture Compliance, Audit End Hosts, and Profile Endpoints in the **More Options** field on the **Service** tab.

There are no default rules associated with this service type. Rules can be added to handle any type of standard or vendor-specific RADIUS attributes (any attribute that is loaded through the pre-packaged vendor-specific or standard RADIUS dictionaries, or through other dictionaries imported into Policy Manager). The following figure shows an example of the **RADIUS Enforcement (Generic)** service:

Figure 83: *RADIUS Enforcement (Generic) Service*



Configuring a service for RADIUS requests is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see Dell 802.1X Wireless on page 98

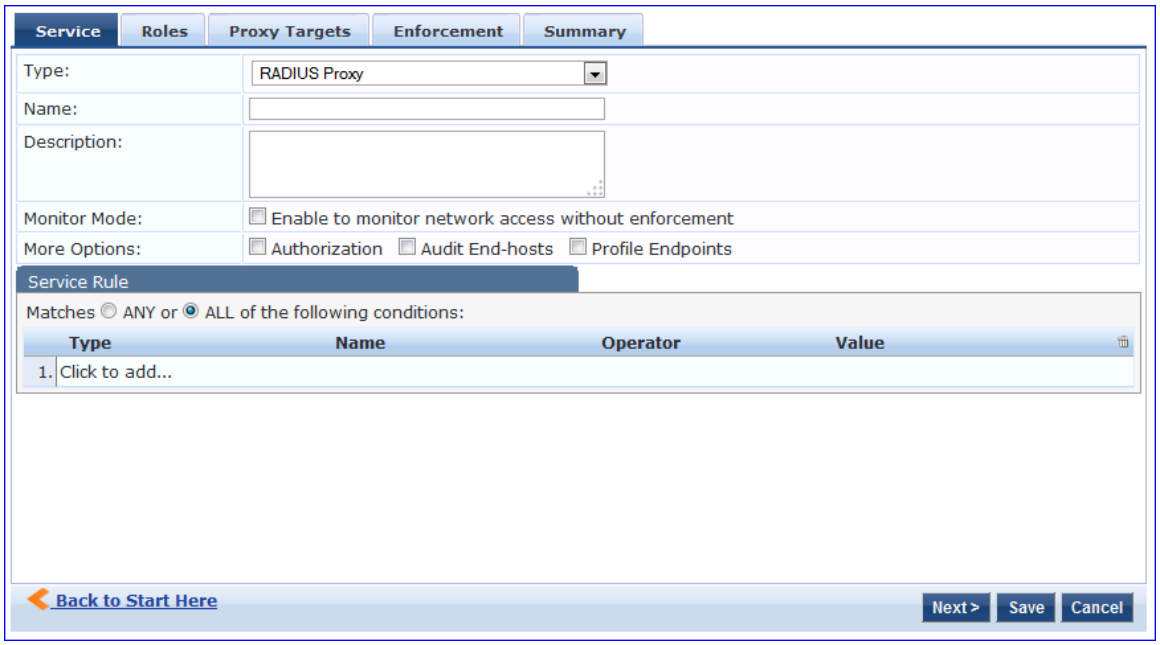
RADIUS Proxy

Configure the **RADIUS Proxy** service for any kind of RADIUS request that needs to be proxied to another RADIUS server (a Proxy Target). There are no default rules associated with this service type. Rules can be added to handle any type of standard or vendor-specific RADIUS attributes. Typically, proxying is based on a realm or the domain of the user trying to access the network.

Configuration of this service is the same as the **RADIUS Enforcement (Generic)** service except that you do not configure **Authentication** or **Posture** policies with this service type. However, you need to configure Proxy targets (the servers to which requests are proxied). Requests can be dispatched to the proxy targets randomly. Subsequently, these requests are load balanced. However, in the **Failover** mode, requests can be dispatched to the first proxy target in the ordered list of targets and subsequently to the other proxy targets if the prior requests failed. When you select the **Enable proxy for accounting requests** accounting requests are also sent to the proxy targets.

The following figure shows an example of the **RADIUS Proxy** service:

Figure 84: *RADIUS Proxy Service*

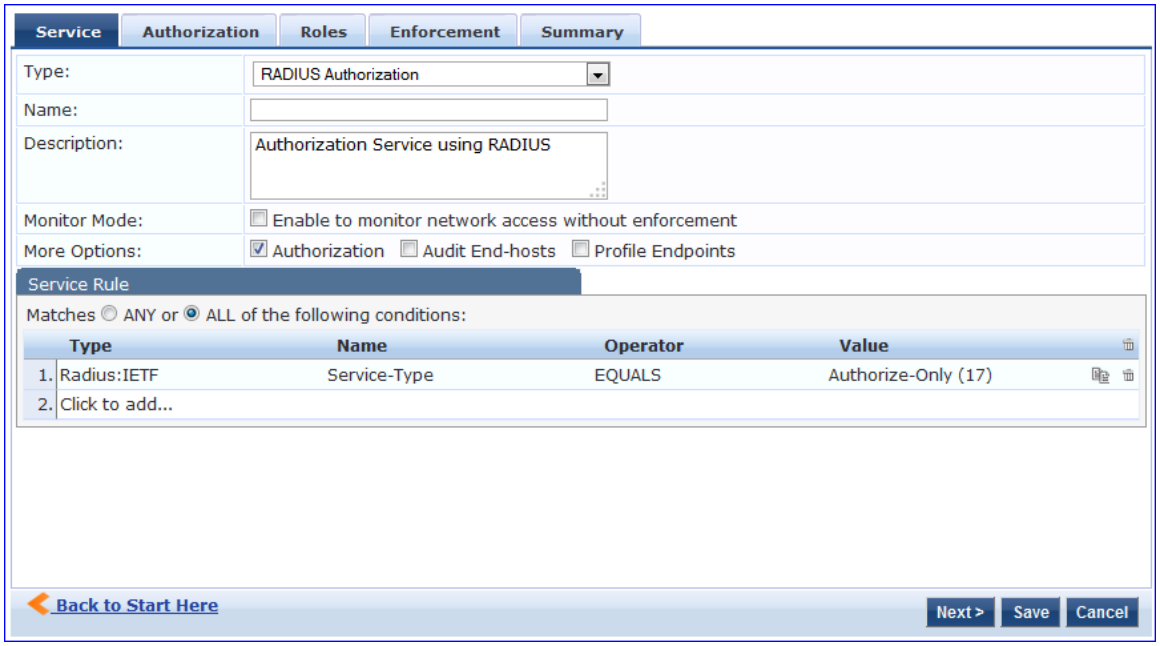


For more information, see RADIUS Enforcement (Generic) on page 113.

RADIUS Authorization

Configure the **RADIUS Authorization** service type for services that perform authorization using RADIUS. When this service is selected, the **Authorization** tab is enabled by default. The following figure shows an example of the **RADIUS Authorization** service:

Figure 85: *RADIUS Authorization Service*



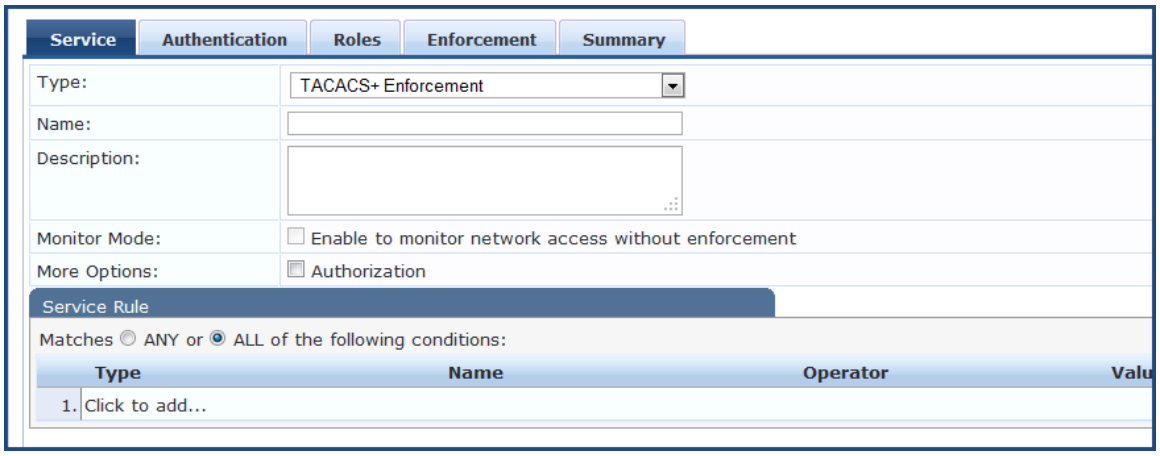
Configuration for this service is the same as the **RADIUS Enforcement (Generic)** service except that you do not configure Authentication or Posture with this service type. Refer to RADIUS Enforcement (Generic) on page 113 for more information.

TACACS+ Enforcement

Configure the **TACACS+ Enforcement** service for any kind of TACACS+ request. TACACS+ users can be authenticated against any of the supported authentication source types: Local DB, SQL DB, Active Directory, LDAP Directory, or Token Servers with a RADIUS interface. Similarly, service level authorization sources can be specified from the **Authorization** tab. Note that this tab is not enabled by default. Select the **Authorization** check box from the **More Options** on the **Service** tab to enable this tab. A role mapping policy can be associated with this service from the **Roles** tab.

The result of evaluating a TACACS+ enforcement policy is one or more TACACS+ enforcement profiles. For more information on TACACS+ enforcement profiles, see TACACS+ Based Enforcement on page 295 for more information. The following figure shows an example of the **TACACS+ Enforcement** service:

Figure 86: *TACACS+ Enforcement Service*

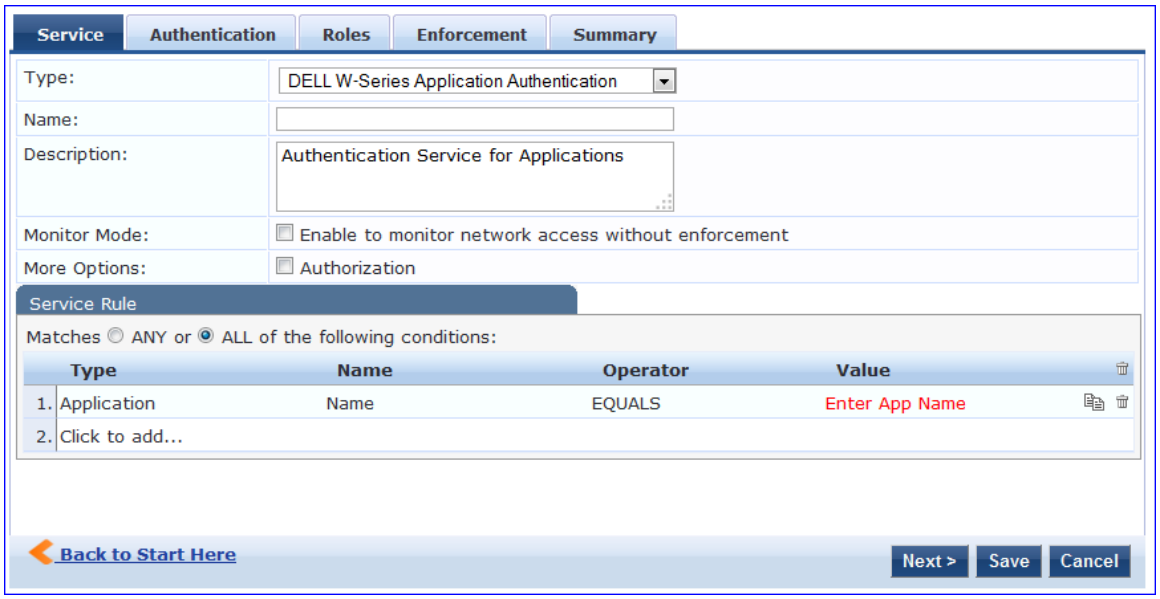


Configuring the **TACACS+ Enforcement** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 98

Dell W-Series Application Authentication

This type of service provides authentication and authorization to users of Dell applications: W-Series ClearPass Guest and W-Series ClearPass Insight. You can send Generic Application Enforcement on page 285 to these or other generic applications for authenticating and authorizing the users. The following figure shows an example of the **Dell W-Series Application Authentication** service:

Figure 87: *Dell W-Series Application Authentication*

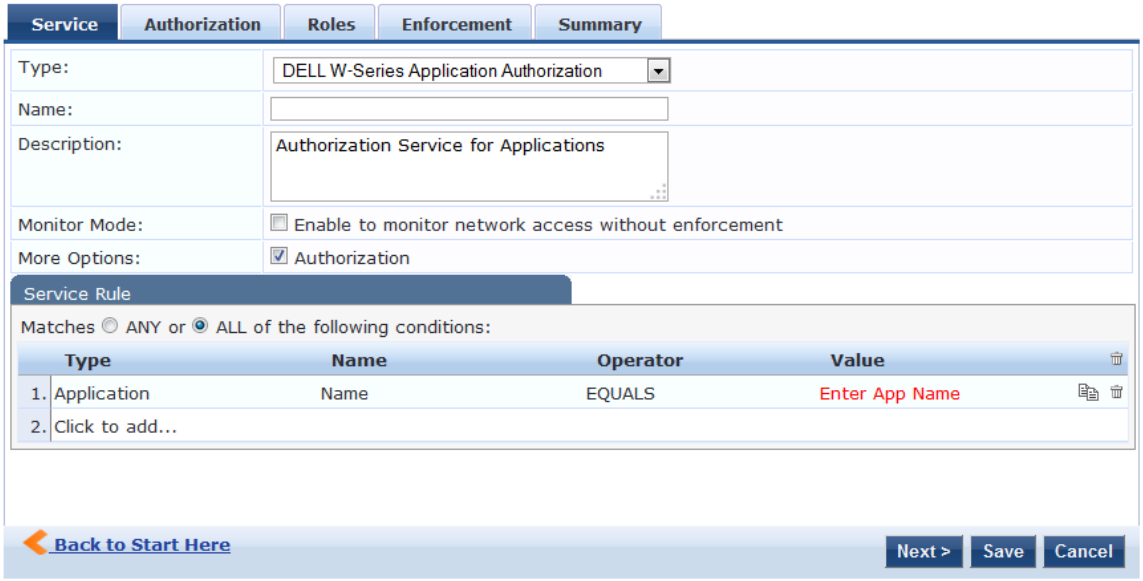


Configuring the **Dell W-Series Application Authentication** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 98

Dell W-Series Application Authorization

This type of service provides authorization for users of Dell applications: W-Series ClearPass Guest and W-Series ClearPass Insight. Generic Application Enforcement on page 285 can be sent to these or other generic applications for authorizing the users. The following figure shows an example of the **Dell W-Series Application Authorization** service:

Figure 88: *Dell W-Series Application Authorization*

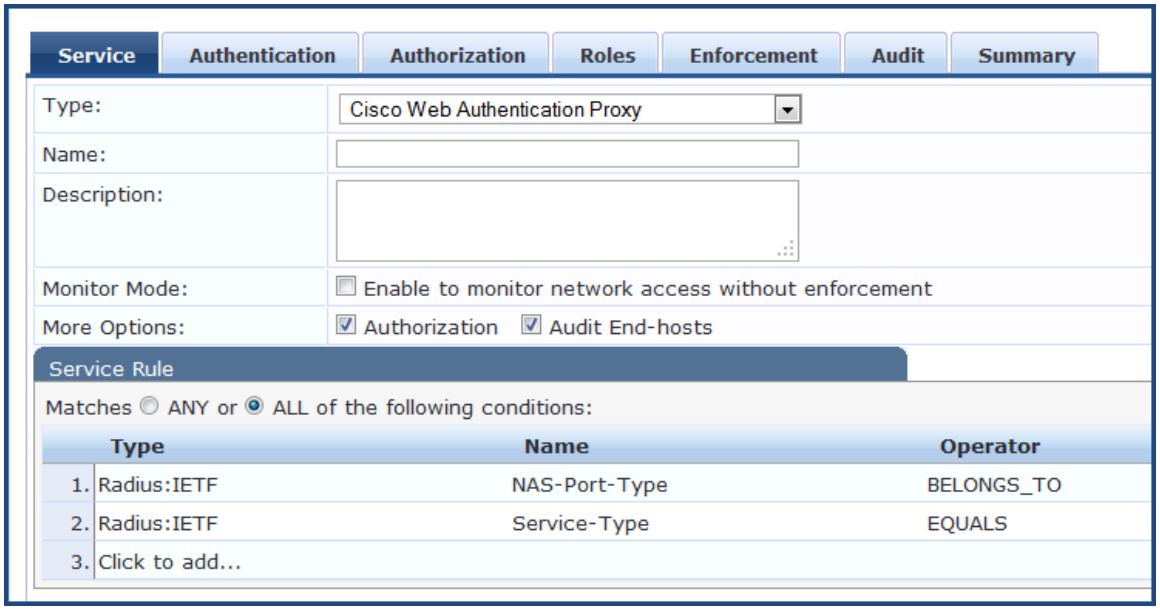


Configuring the Dell W-Series Application Authorization service is similar to configuring the Dell 802.1X Wireless service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 98

Cisco Web Authentication Proxy

This service is a web-based authentication service for guests or agent-less hosts. The Cisco switch hosts a captive portal and the portal web page that collects username and password information. Subsequently, the switch sends a RADIUS request in the form of a password authentication protocol (PAP) authentication request to Policy Manager. By default, this service uses the **PAP** authentication method. You can click on the **Authorization** and **Audit End-hosts** options to enable additional tabs. The following figure shows an example of the **Cisco Web Authentication Proxy** service:

Figure 89: *Cisco Web Authentication Proxy Service*



Configuring the **Cisco Web Authentication Proxy** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance** and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 98

Services

The **Services** page shows the current list and order of services that Dell Networking W-ClearPass Policy Manager follows during authentication and authorization. You can use the configured default service types or you can add additional services. Services included in "[ ]" indicate default services. The following figure shows an example of the **Services** page followed by parameter definition:

Figure 90: *Service Listing Page*

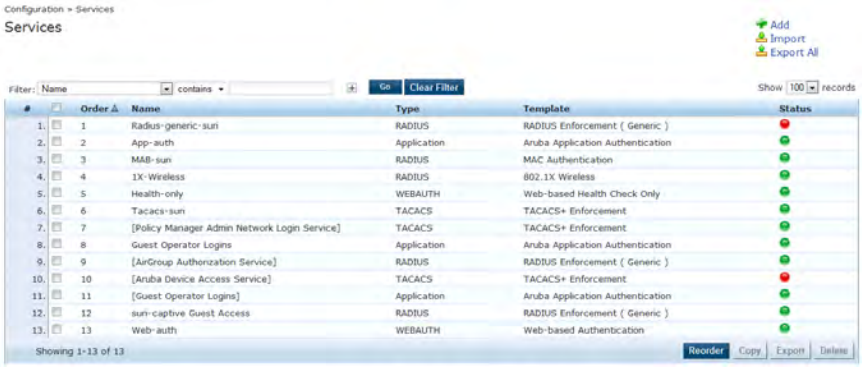


Table 55: *Services page Parameters*

Parameter	Description
Name	Displays the name of the service.
Type	Displays the type of authentication associated with the service. For example, RADIUS, Web Authentication, and TACACS.
Template	Specifies the type of the service template to create a service.
Status	Displays the status of the service. A green/red icon indicates enabled/disabled state. Click the icon to toggle the status of a service between **Enabled** and **Disabled**. **NOTE:** If a service is in **Monitor** mode, an [*m*] indicator is displayed next to the **Status** icon.

For more information, see:

- Adding Services on page 119
- Modifying Services on page 122
- Reordering Services on page 124

Adding Services

From the **Services** page (**Configuration > Services**) or from the **Start Here** page (**Configuration > Start Here**), you can create a new service using the **Add Service** option. Click on **Add** in the upper-right corner to add a new service. The following figure shows an example of the **Add Service** tab followed by parameter definition:

Figure 91: *Add Service Page (all options enabled)*

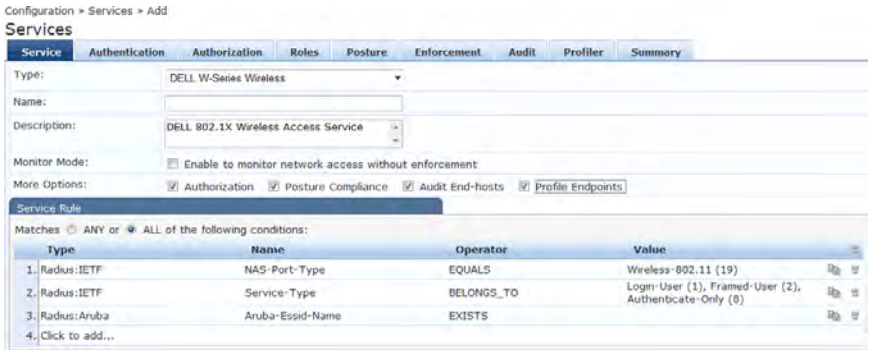


Table 56: *Service Page (General Parameters)*

Label	Description
Type	Select the desired service type from the drop-down list. When working with service rules, you can select from the following namespace dictionaries: • **Application**: The type of application for this service. • **Authentication**: The Authentication method to be used for this service. • **Connection:** Originator address (Src-IP-Address, Src-Port), Destination address (Dest-IP-Address, Dest-Port), and Protocol • **Device:** Filter the service based on a specific device type, vendor, operating system location, or controller ID. • **Date:** Time-of-Day, Day-of-Week, or Date-of-Year • **Endpoint**: Filter based on endpoint information such as enabled/disabled, device, OS, location, and more. • **Host**: Filter based on host Name, OSType, FQDN, UserAgent, CheckType, UniqueID, Agent-Type, and InstalledSHAs, • **RADIUS:** Policy Manager ships with a number of vendor-specific namespace dictionaries and distinguishes vendor-specific RADIUS namespaces with the notation *RADIUS:vendor* (sometimes with an additional suffix for a particular device). To add a dictionary for a vendor-specific RADIUS namespace, navigate to **Administration > Dictionaries > Radius > Import** (link). The notation **RADIUS:IETF** refers to the RADIUS attributes defined in RFC 2865 and associated RFCs. As the name suggests, RADIUS namespace is only available if the request type is RADIUS. • **Any other supported namespace:** See Rules Editing and Namespaces on page 513 for an exhaustive list of namespaces and their descriptions. To create new services, you can copy or import other services for use *as is* or as templates, or you can create a new service.
Name	Enter the name or label for the service you want to create.
Description	Enter a description/additional information for the service that helps to identify the service. This field is optional.

Table 56: *Service Page (General Parameters) (Continued)*

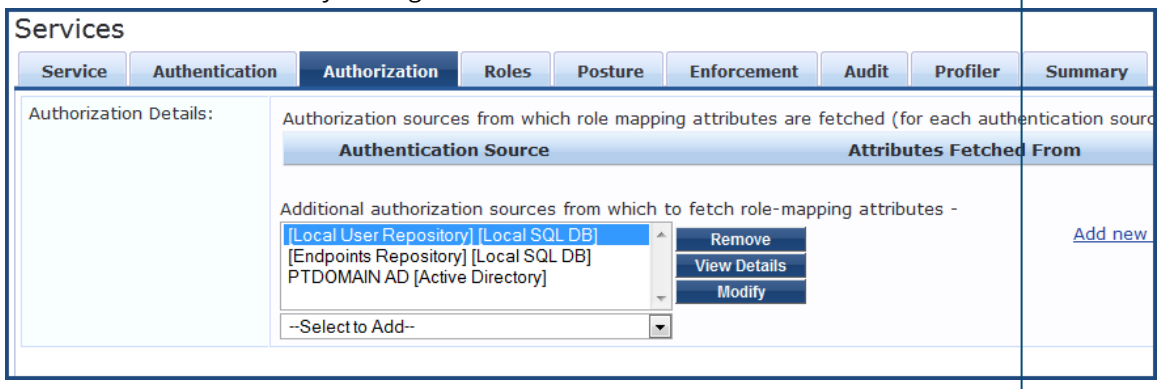
Label	Description
Monitor Mode	Optionally check the **Enable to monitor network access without enforcement** to allow authentication and health validation exchanges to take place between endpoint and Policy Manager, but without enforcement. In **Monitor Mode**, no enforcement profiles (and associated attributes) are sent to the network device. Policy Manager also allows *Policy Simulation* (**Monitoring > Policy Simulation**), where the administrator can test the results of a particular configuration of policy components.
More Options	Select any of the available check boxes to enable the configuration tabs for those options. The available check boxes varies based on the type of service that is selected and may include one or more of the following: • **Authorization**: Select an authorization source from the drop-down list to add the source or select the **Add new Authentication Source** link to create a new source. • **Posture Compliance:** Select a Posture Policy from the drop-down list to add the policy or create a new policy by clicking the link. Select the default Posture token. Specify whether to enable auto-remediation of non-compliant end hosts. If this is enabled, then enter the Remediation URL. You can specify the **Posture Server** from the drop-down list or add a new server by clicking the **Add new Posture Server** link.  • **Audit End-hosts:** Select an **Audit Server**, either built-in or customized. Refer to Configuring Audit Servers on page 250 for audit server configuration steps. For this type of service, you can perform audit **Always**, **When posture is not available**, or **For MAC authentication requests**. You can specify to trigger an audit always, when posture is not available, or for MAC authentication requests. If **For MAC authentication requests** is specified, then you can perform an audit **For known end-hosts only** or **For unknown end hosts only**, or **For all end hosts**. Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service. Performing audit on a client is an asynchronous task, which means the audit can be performed only after the MAC authentication request has been completed and the client has acquired an IP address through DHCP. Once the audit results are available, Policy Manager re-applies policies on the network deviceby one of the following ways: ▪ **No Action:** The audit does not apply policies on the network device after this audit. ▪ **Do SNMP bounce:** This option bounces the switch port or force an 802.1X re-authentication (both done using SNMP). **NOTE:** Bouncing the port triggers a new 802.1X or MAC authentication request by the client. If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager. ▪ **Trigger RADIUS CoA action:** This option sends a RADIUS CoA command to the network device by Policy Manager.

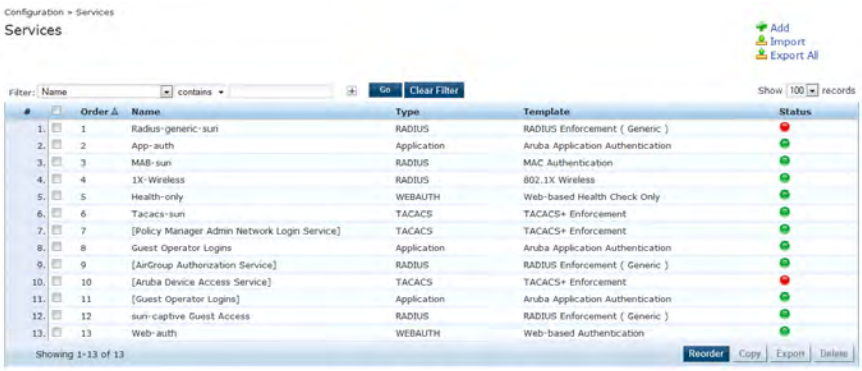
Table 56: *Service Page (General Parameters) (Continued)*

Label	Description
	• Optionally configure **Profiler** settings. Select one or more Endpoint Classification items from the drop down list, then select the RADIUS CoA action. You can also create a new action by selecting the **Add new RADIUS CoA Action** link.

Modifying Services

Navigate to the **Configuration > Services** page to view available services. You can use these service types as configured, or you can edit their settings. The following figure shows an example of the **Services** page with the list of services:

Figure 92: *Service Listing Page*



To modify an existing service, click the check box of a service row in the **Configuration > Services** page. This opens the **Services > Edit - <*service_name*>** form. Select the **Service** tab on this form to edit the service information. The following figure shows an example of the **Service** tab followed by parameter definition:

Figure 93: *Services Configuration*

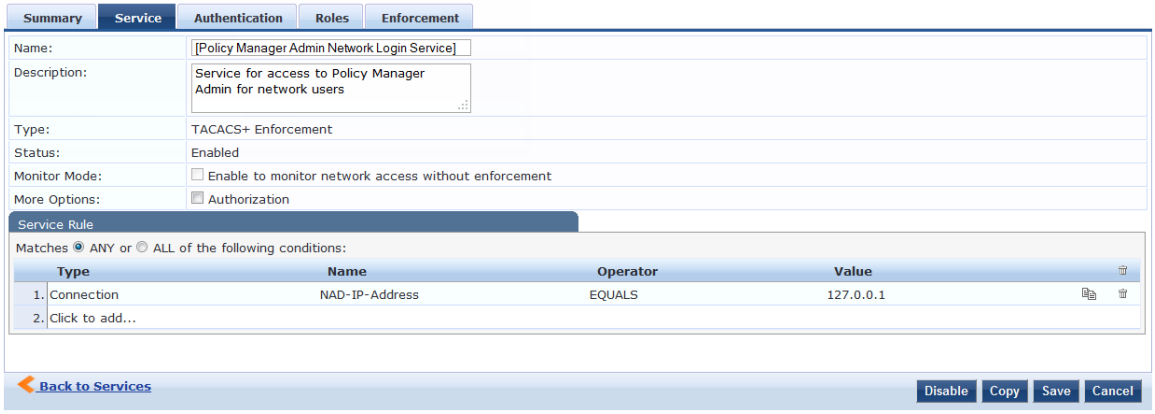


Table 57: *Service Page - General Parameters*

Parameter	Description
Name	Enter or modify the label for a service.
Description	Enter or modify the service description. This field is optional.
Type	This is a non-editable label that shows the type of service as it was originally configured.
Status	This non-editable label indicates whether the service is enabled or disabled. **NOTE:** You can disable a service by clicking the **Disable** button on the bottom-right corner of the form. Use this button to toggle between **Enable** and **Disable** depending on the Service's current status.
Monitor Mode	This non-editable check box indicates whether authentication and health validation exchanges take place between endpoint and Policy Manager, but without enforcement. In monitor mode, no enforcement profiles (and associated attributes) are sent to the network device.
More Options	Select the available check box(es) to view additional configuration tab(s). The options that are available depend on the type of service currently being modified. TACACS+ service, for example, allows for authorization configuration. RADIUS service allows for configuration of posture compliance, end hosts, profile endpoints, and authorization.

On the lower half of the form, select an available rule within the **Service Rule** table. The following fields are available in the **Service Rule** table:

Table 58: *Service Page (Rules Editor)*

Label	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on Service type. When working with service rules, you can select from the following namespace dictionaries: • **Application**: The type of application for this service. • **Authentication**: The Authentication method to be used for this service. • **Connection:** Originator address (Src-IP-Address, Src-Port), Destination address (Dest-IP-Address, Dest-Port), and Protocol. • **Device**: Filter the service based on a specific device type, vendor, operating system location, or controller ID. • **Date:** Time-of-Day, Day-of-Week, or Date-of-Year • **Endpoint**: Filter based on endpoint information such as enabled/disabled, device, OS, and location. • **Host**: Filter based on host Name, OSType, FQDN, UserAgent, CheckType, UniqueID, Agent-Type, and InstalledSHAs, • **RADIUS:** Policy Manager ships with a number of vendor-specific namespace dictionaries and distinguishes vendor-specific RADIUS namespaces with the notation *RADIUS:vendor* (sometimes with an additional suffix for a particular device). To add a dictionary for a vendor-specific RADIUS namespace, navigate to **Administration > Dictionaries > Radius > Import Dictionary** (link). The notation **RADIUS:IETF** refers to the RADIUS attributes defined in RFC 2865 and associated RFCs. RADIUS namespace is available only when the request type is RADIUS. • Any other supported namespace. See Rules Editing and Namespaces on page 513 for an exhaustive list of namespaces and their descriptions.
Name (of attribute)	Shows the drop-down list of attributes present in the selected namespace.
Operator	Shows the drop-down list of context-appropriate (with respect to the attribute) operators. See Operators on page 524 for an exhaustive list of operators and their descriptions.
Value of attribute	Displays the free-form (one or many lines) edit box, a drop-down list, or a time/date widget depending on attribute data type,

Reordering Services

Policy Manager evaluates requests against the service rules of each service that is configured, in the order in which these services are defined. The service associated with the first matching service rule is then associated with this request. To change the order in which service rules are processed, you can change the order of services.

1. To reorder services, navigate to the **Configuration > Services** page.
2. Click the **Reorder** button located on the lower-right portion of the page to open the **Reorder Services** page.

The following figures shows the examples of the **Services** page and the **Reorder Services** page followed by parameter definition:

Figure 94: *Service Reorder Button*

Figure 95: *Reordering Services*

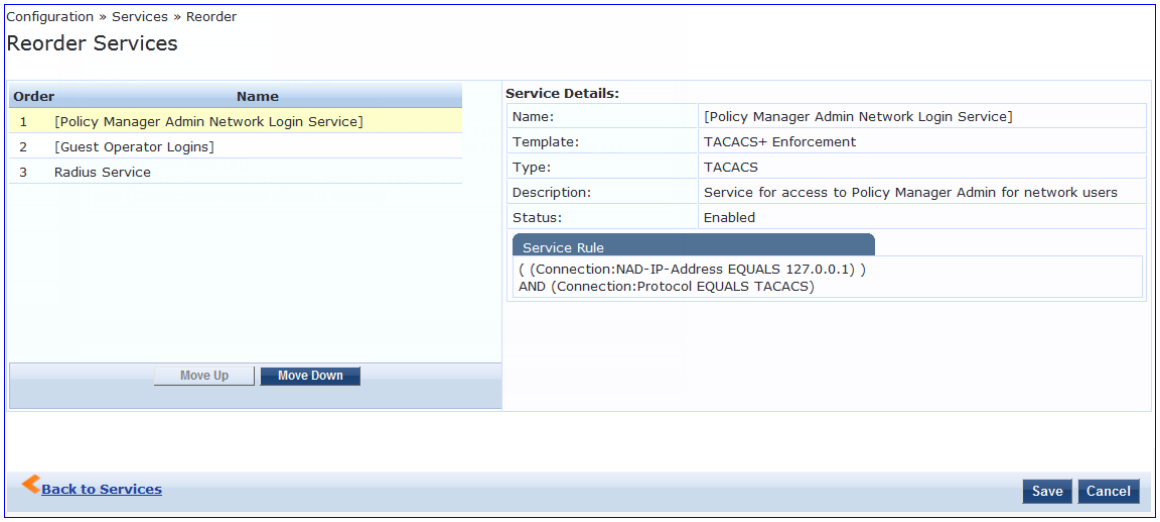


Table 59: *Reordering Services*

Label	Description
Name	Shows the name of the service selected.
Service Details	
Name	Shows the name of the service selected.
Template	Displays the name of the service template used to create the service.
Type	Displays the type of authentication used to create the service.
Description	Shows additional information about the service.
Status	Shows the status of the service from the options: Enabled or Disabled.
Service Rule	Displays the rules used to create the service.

As a first step in Service-based processing, Policy Manager uses an authentication method to authenticate the user or device against an authentication source. After the user or device is authenticated, Policy Manager fetches attributes for Role Mapping policies from the authorization sources associated with this authentication source. For more information, see:

- Authentication and Authorization Architecture and Flow on page 127
- Configuring Authentication Components on page 128
- Adding and Modifying Authentication Methods on page 130
- Adding and Modifying Authentication Sources on page 154

Authentication and Authorization Architecture and Flow

Policy Manager divides the architecture of authentication and authorization into the following three components:

- Authentication Method
- Authentication Source
- Authorization Source

Authentication Method

Policy Manager initiates the authentication handshake by sending available methods in priority order until the client accepts a method or until the client rejects the last method (with NAKs) with the following possible outcomes:

- Successful negotiation returns a method, which is used to authenticate the client against the Authentication Source.
- Where no method is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this service.
- Policy Manager rejects the connection.

An authentication method is configurable only for some service types (Refer to Policy Manager Service Types on page 98). All 802.1X services (wired and wireless) have an associated authentication method. An authentication method (of type MAC_AUTH) can be associated with MAC authentication service type.

Authentication Source

In Policy Manager, an authentication source is the identity store (Active Directory, LDAP directory, SQL DB, token server) against which users and devices are authenticated. Policy Manager first tests whether the connecting entity - device or user - is present in the ordered list of configured authentication sources. Policy Manager looks for the device or user by executing the first filter associated with the authentication source. After the device or user is found, Policy Manager then authenticates this entity against this authentication source. The flow is outlined below:

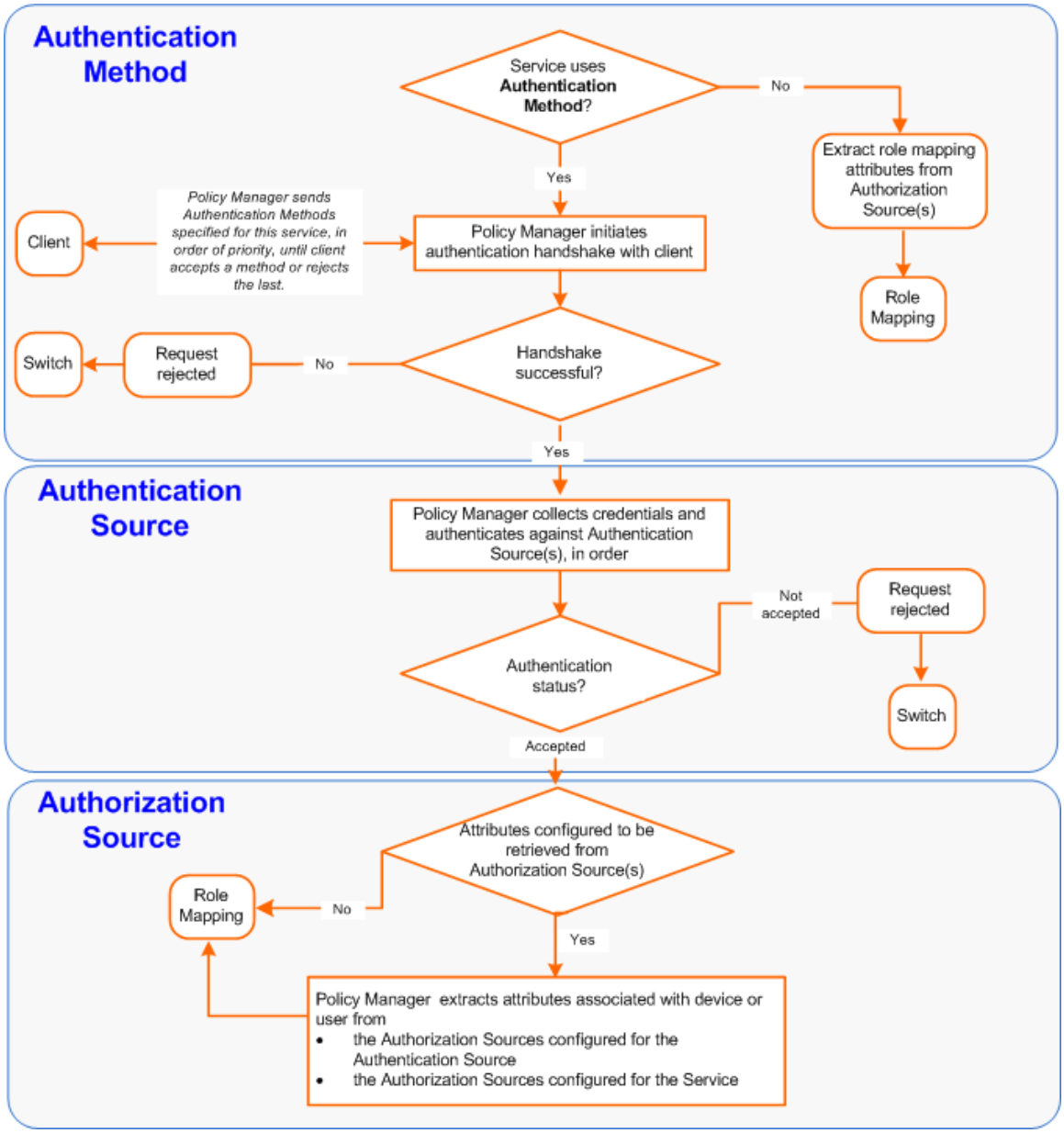
On successful authentication, Policy Manager moves on to the next stage of policy evaluation, which collects role mapping attributes from the authorization sources.

Where no authentication source is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this service.

If Policy Manager does not find the connecting entity in any of the configured authentication sources, it rejects the request.

After Policy Manager successfully authenticates the user or device against an authentication source, it retrieves role mapping attributes from each of the authorization sources configured for that authentication source. It also, optionally, can retrieve attributes from authorization sources configured for the service. The flow of control for authentication takes these components in sequence:

Figure 96: *Authentication and Authorization Flow of Control*



Configuring Authentication Components

The following summarizes the methods for configuring authentication:

For an existing service, you can add or modify an authentication method or source by opening the **Services** (**Configuration > Services** page > **Authentication** tab) page. For a new service, the **Policy Manager** wizard automatically opens the **Authentication** tab for configuration. You can open an authentication method or source from the **Configuration > Authentication > Methods** or **Configuration > Authentication > Sources** page. The following figure shows an example of the **Authentication** tab followed by parameter definition:

Figure 97: *Authentication Components*

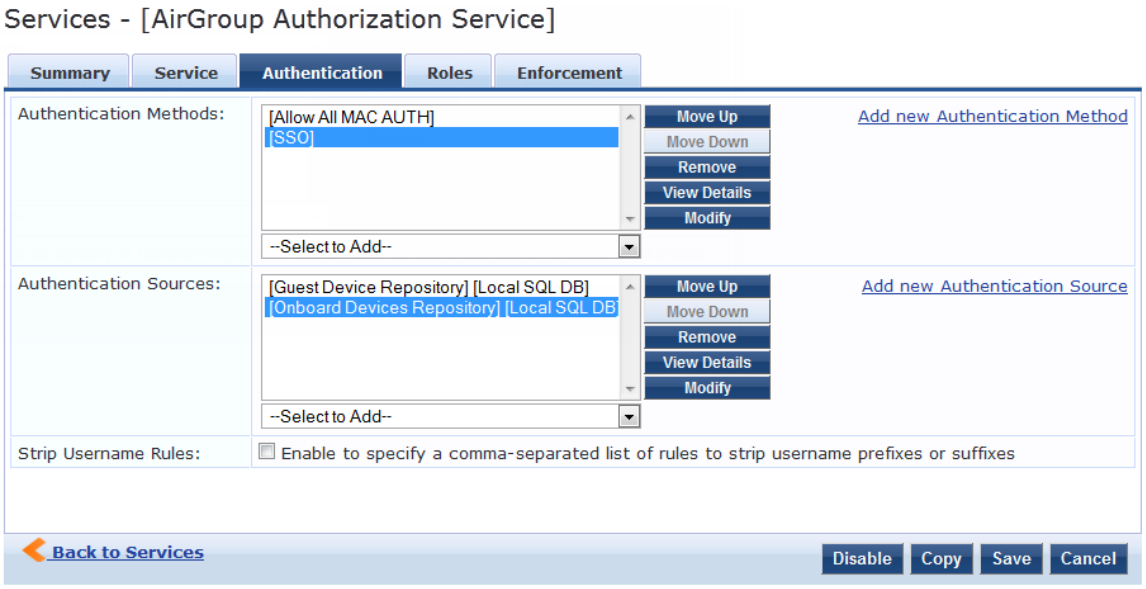


Table 60: *Authentication Features at the Service Level*

Component	Configuration Steps
Sequence of Authentication Methods	1. Select a method, then select **Move Up**, **Move Down**, or **Remove**. 2. Select **View Details** to view the details of the selected method. 3. Select **Modify** to modify the selected authentication method. This displays a popup with the edit widgets for the select authentication method. a. To add a previously configured authentication method, select from the **Select** drop-down list, then click **Add**. b. To configure a new method, click the **Add New Authentication Method** link. For more information about authentication methods, see Adding and Modifying Authentication Methods on page 130. **NOTE:** An authentication method is only configurable for some service types. For more information, refer to Policy Manager Service Types on page 98.
Sequence of Authentication Sources	1. Select a source, then **Move Up**, **Move Down**, or **Remove**. 2. Select **View Details** to view the details of the selected authentication source. 3. Select **Modify** to modify the selected authentication source. This displays the **Authentication Source Configuration** wizard for the selected authentication source. 4. To add a previously configured authentication source, select from the **Select** drop-down list, then click **Add**. 5. To configure a new authentication source, click the **Add New Authentication Source** link. For more information about authentication sources, see Adding and Modifying Authentication Sources on page 154.
Whether to standardize the form in which usernames are present	Select the **Enable to specify a comma-separated list of rules to strip usernames** check box to pre-process the user name and to remove prefixes and suffixes before authenticating it to the authentication source.

Adding and Modifying Authentication Methods

Policy Manager supports specific EAP, non-EAP, tunneled, and non-tunneled methods.

In tunneled EAP methods, authentication and posture credential exchanges occur inside a protected outer tunnel.

Table 61: *Policy Manager Supported Authentication Methods*

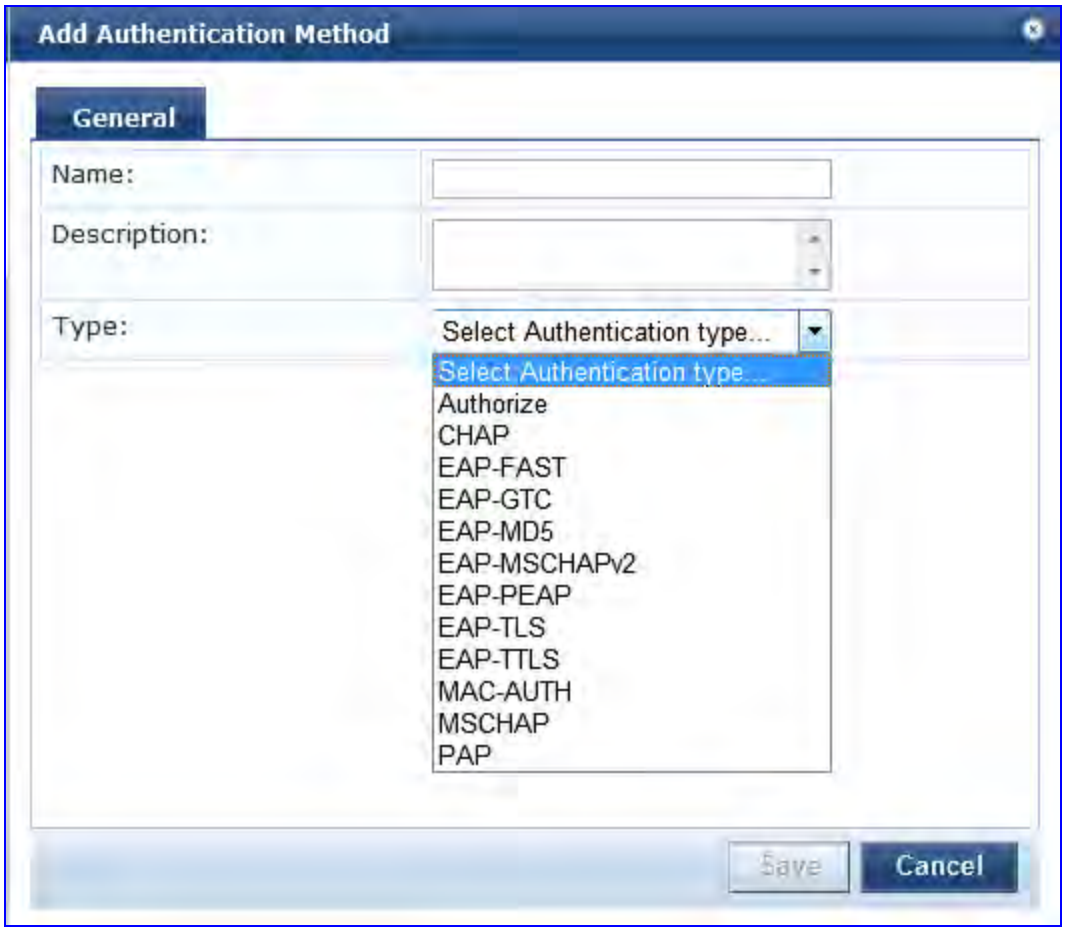
	EAP	Non-EAP
Tunneled	• EAP Protected EAP (EAP-PEAP) • EAP Flexible Authentication Secure Tunnel (EAP-FAST) • EAP Transport Layer Security (EAP-TLS) • EAP Tunneled TLS (EAP-TTLS)	
Non-Tunneled	• EAP Message Digest 5 (EAP-MD5) • EAP Microsoft Challenge Handshake Authentication Protocol version 2 (EAP- MSCHAPv2) • EAP Generic Token Card (EAP-GTC)	• Challenge Handshake Authentication Protocol (CHAP) • Password Authentication Protocol (PAP) • Microsoft CHAP version 1 and version 2 • MAC Authentication Method (MAC-AUTH) MAC-AUTH must be used exclusively in a MAC-based Authentication Service. When the MAC_AUTH method is selected, Policy Manager makes internal checks to verify that the request is a **MAC_Authentication** request (and not a spoofed request). **NOTE:** The **EAP-MD5** authentication method is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

The Authorize authentication method does not fit into any of these categories.

From the **Services** (**Configuration > Service**) page, you can configure authentication for a new service (using the **Add Service** wizard) or modify an existing authentication method directly (**Configuration > Authentication > Methods**, then click any row in the **Authentication Methods** page).

When you click **Add** from any of these locations, Policy Manager displays the **Add Authentication Method** popup. The following figure shows an example of the **Add Authentication Method** page:

Figure 98: *Add Authentication Method Page*



NOTE

The **EAP-MD5** authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

Depending on the **Type** selected, you can view the following different tabs:

- Authorize on page 132
- CHAP and EAP-MD5 on page 133
- EAP-FAST on page 135
- EAP-GTC on page 141
- EAP-MSCHAPv2 on page 142
- EAP-PEAP on page 143
- EAP-TLS on page 148
- EAP-TTLS on page 149
- MAC-AUTH on page 151
- MSCHAP on page 152
- PAP on page 153

Authorize

This is an authorization-only method that you can add with a custom name. The following figure shows an example of the **Authorization - General** tab followed by parameter definition:

Figure 99: *Add Authentication - General tab*

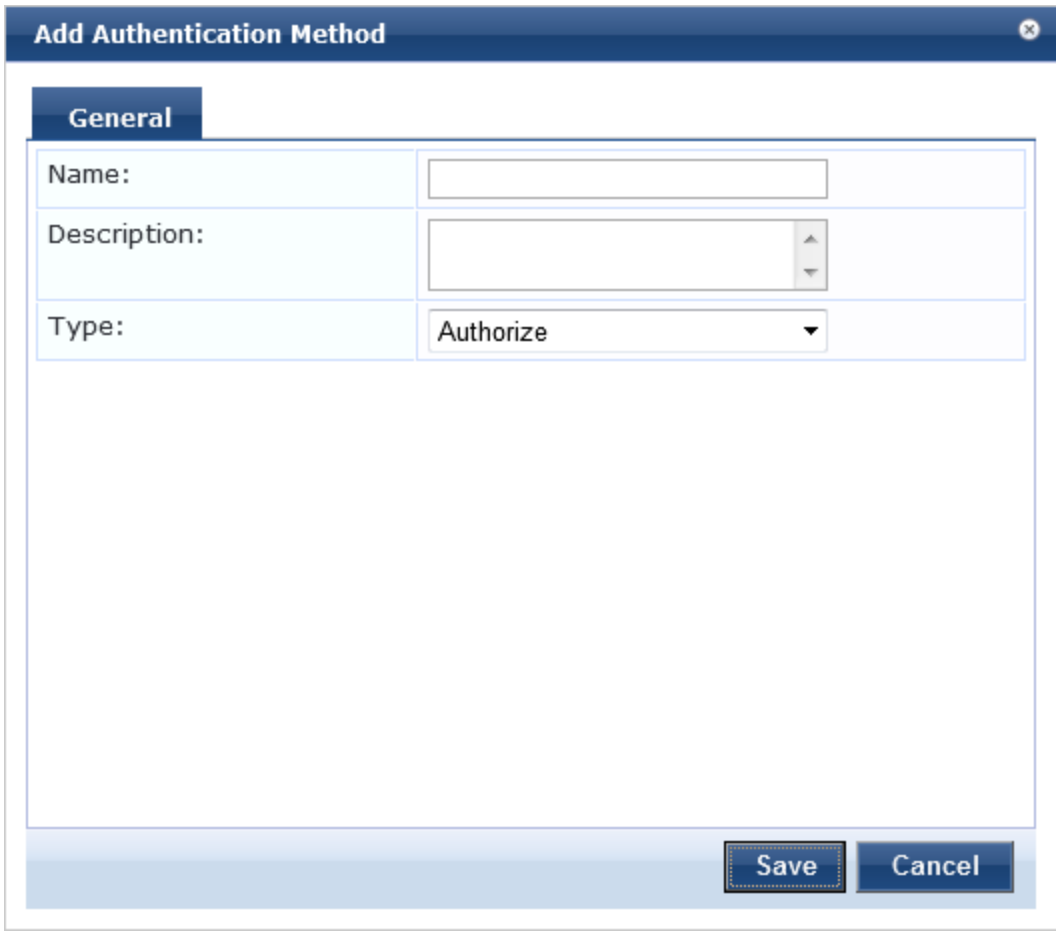


Table 62: *Authorize General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **Authorize.**

CHAP and EAP-MD5

Policy Manager also comes packaged with **CHAP** and **EAP-MD5** methods. You can add methods of this type with a custom name. These methods can also be associated to a **Service** as authentication methods. The following figures show the examples of the **CHAP General** tab and the **EAP-MD5 - General** tab:

Figure 100: *CHAP General Tab*

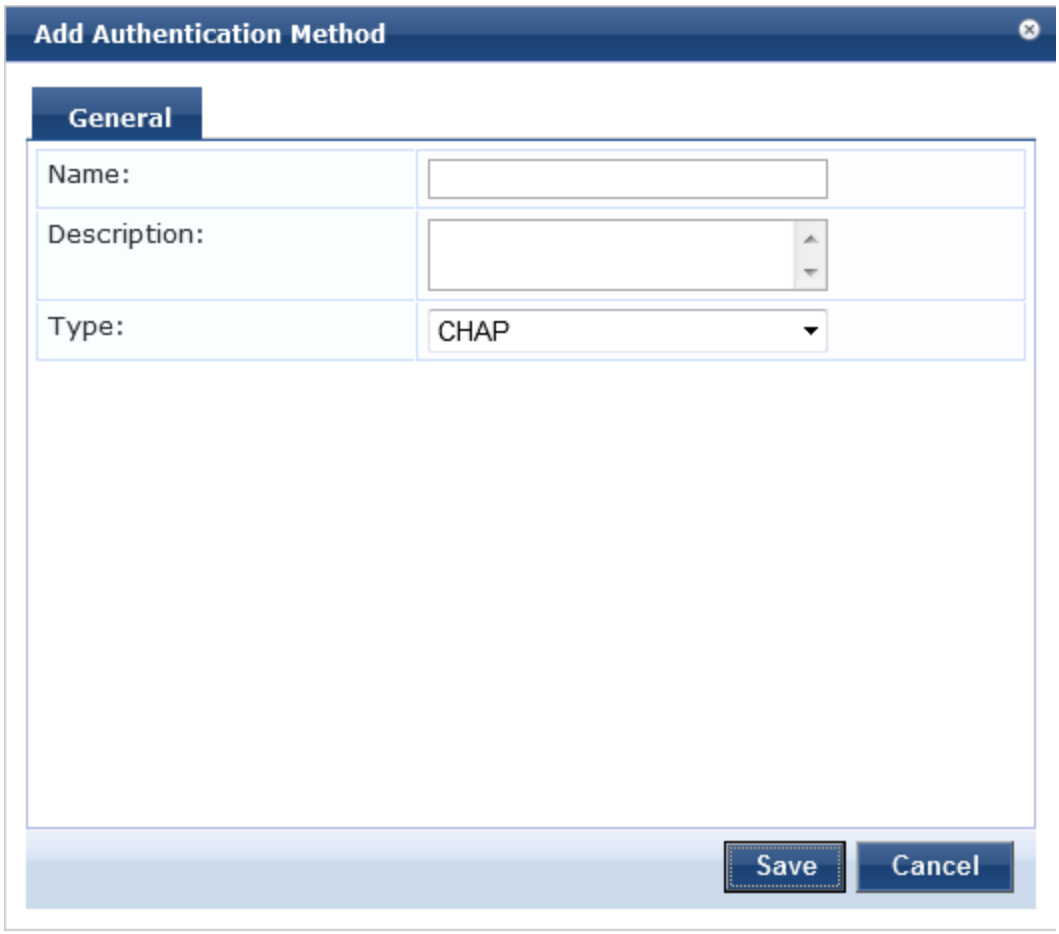
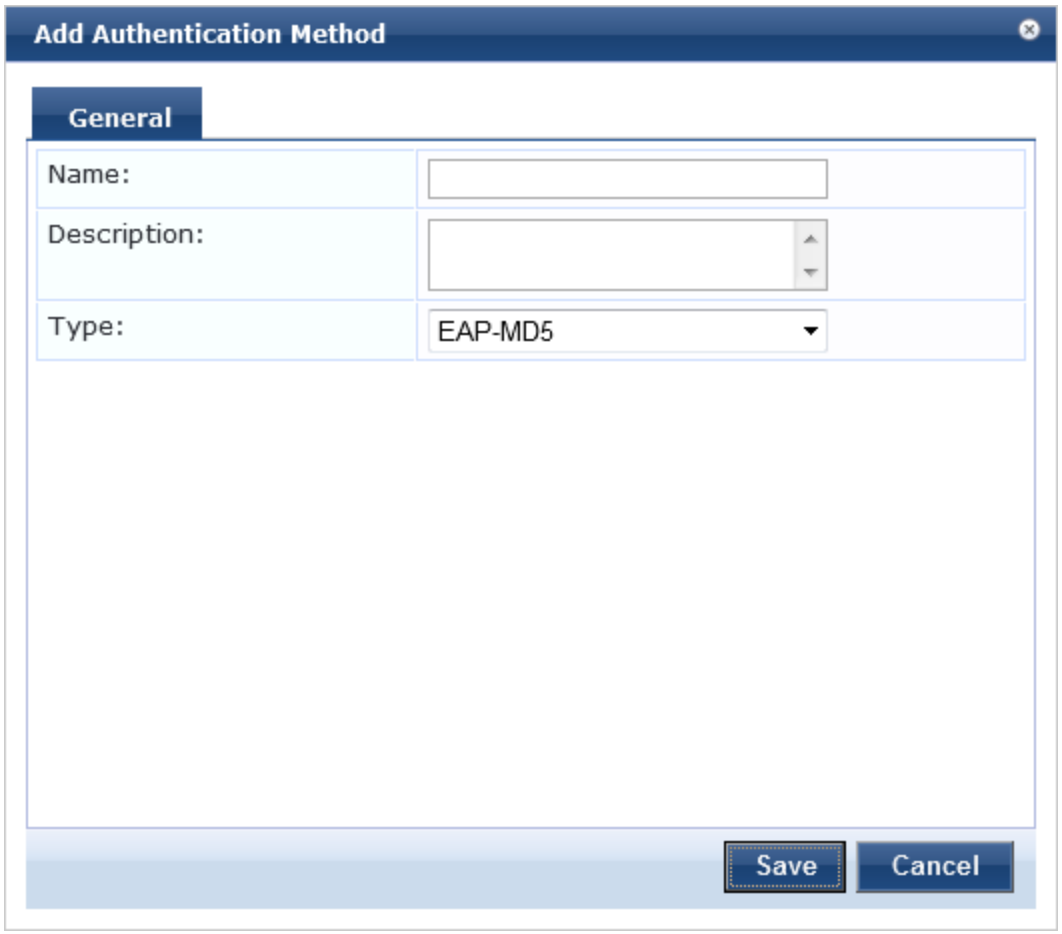


Figure 101: *EAP-MD5 General tab*



NOTE

The **EAP-MD5** authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

Table 63: *CHAP and EAP-MD5 - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, always **CHAP** or **EAP-MD5**.

EAP-FAST

The EAP-FAST method contains the following four tabs:

- General
- Inner Methods
- PACs
- PAC Provisioning

NOTE

The PACs and PAC Provisioning tabs are only available when **Using PACs** is specified on the **General** tab for the **End-Host Authentication** setting.

General Tab

The **General** tab labels the method and defines session details. The following figure shows an example of the **EAP-FAST - General** tab followed by parameter definition:

Figure 102: *EAP-FAST - General Tab*

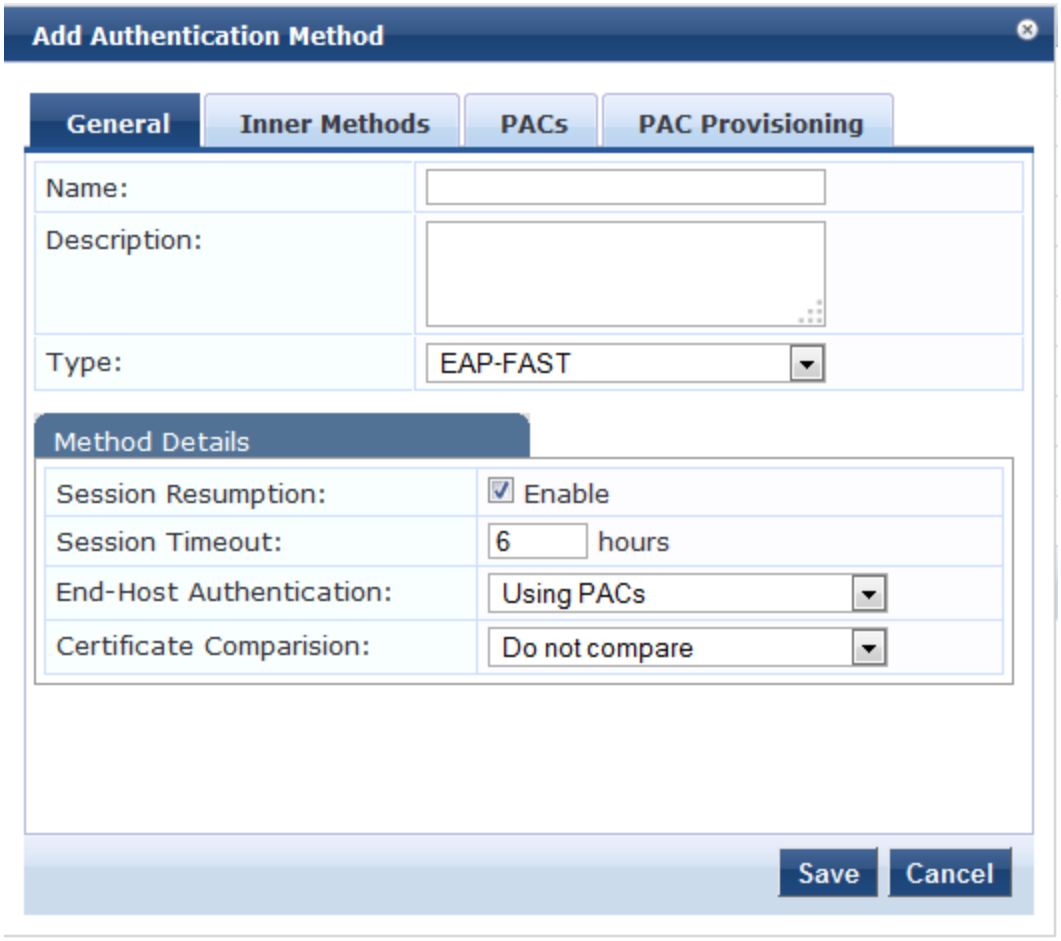


Table 64: *EAP_FAST - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **EAP_FAST**.

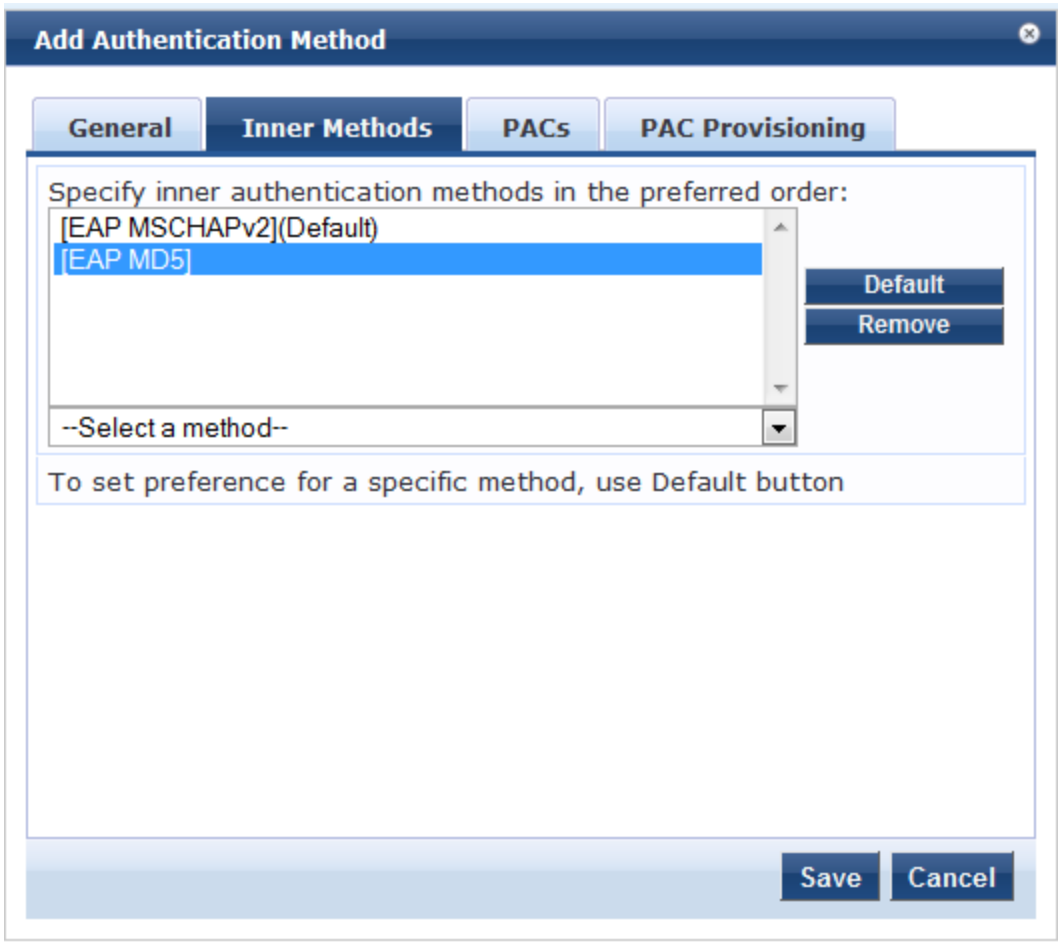
Table 64: *EAP_FAST - General tab Parameters (Continued)*

Parameter	Description
Session Resumption	Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to Policy Manager within the session timeout interval.
Session Timeout	Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to Policy Manager within the session timeout interval. If session timeout value is set to 0, the cached sessions are not purged.
Fast Reconnect	Enable this check box to allow fast reconnect. When **Fast Reconnect** is enabled, the inner method of the server-authenticated outer tunnel is also bypassed. This makes the process of re-authentication faster. For the fast reconnect to work, **session resumption** must be enabled.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-FAST** method. The following figure shows an example of the **EAP-FAST - Inner Methods** tab followed by parameter definition:

Figure 103: *Add Authentication - Inner Methods tab*



The **EAP-MD5** authentication method is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

Table 65: *EAP-FAST - Inner Methods tab Parameters*

Parameter	Description
Specify inner authentication methods in the preferred order	Select any method available in the current context from the drop-down list. Functions available in this tab include: • To append an inner method to the displayed list, select from the drop-down list. The list can contain multiple inner methods, which Policy Manager sends in priority order until negotiation succeeds. • To remove an inner method from the displayed list, select the method and click **Remove**. • To set an inner method as the default (the method tried first), select a method and click **Default**.

PACs tab

The **PACs** tab enables or disables Protected Access Credential (PAC) types. The following figure shows an example of the **EAP-FAST - PACs** tab followed by parameter definition:

Figure 104: *EAP_FAST PACs Tab*

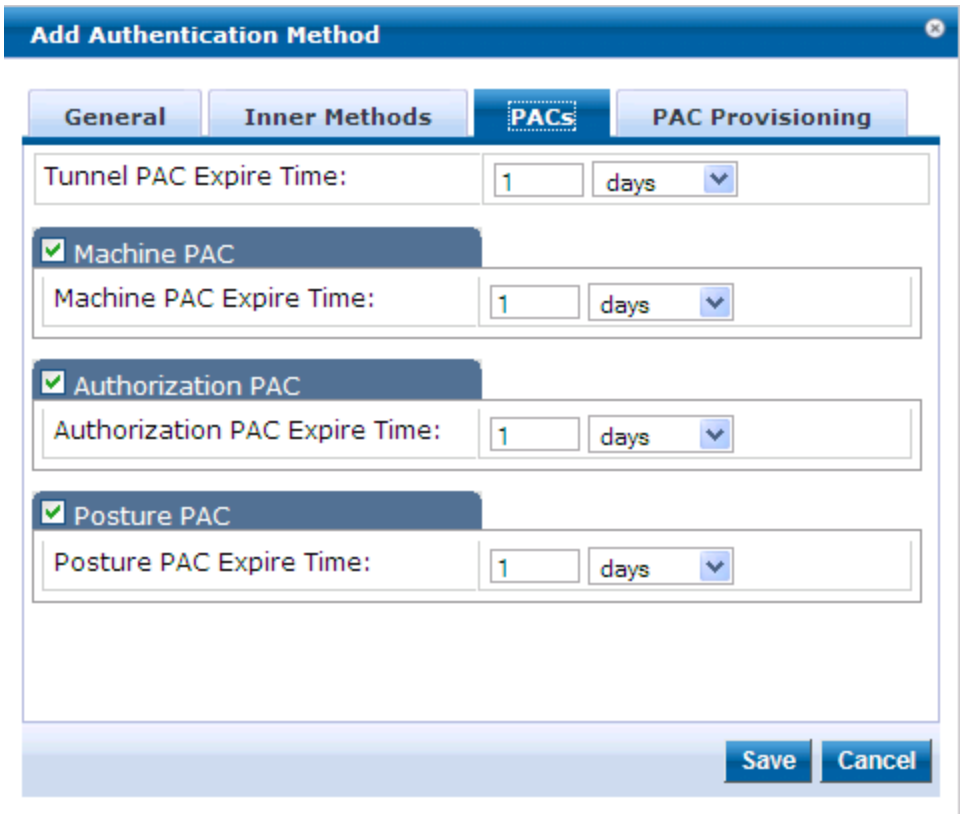


Table 66: *EAP-FAST PACs tab Parameters*

Parameter	Description
Tunnel PAC Expire Time	Specify **Tunnel PAC Expire Time** (the time until the PAC expires and must be replaced by automatic or manual provisioning) in hours, days, weeks, months, or years. To provision a Tunnel PAC on the end-host after initial successful machine authentication, Policy Manager can use the Tunnel PAC shared secret to create the outer EAP-FAST tunnel during authentication.
Machine PAC Expire Time	Select the **Machine PAC** check box to provision a Machine PAC on the end-host after initial successful machine authentication. During authentication, Policy Manager can use the Machine PAC shared secret to create the outer EAP-FAST tunnel. Specify the **Machine PAC Expire Time** (the time until the PAC expires and must be replaced by automatic or manual provisioning) in hours, days, weeks, months, or years. This can be a long-lived PAC (specified in months and years).
Authorization PAC Expire Time	Select the **Authorization PAC** check box to provision an authorization PAC upon successful user authentication. Authorization PAC results from a prior user authentication and authorization. When presented with a valid Authorization PAC, Policy Manager skips the inner user authentication handshake within EAP-FAST. Specify the **Authorization PAC Expire Time** (the time until the PAC expires and must be replaced by automatic or manual provisioning) in hours, days, weeks, months, or years. This is typically a short-lived PAC (specified in hours).
Posture PAC Expire Time	Select the **Posture PAC** check box to provision a posture PAC upon successful posture validation. Posture PACs result from prior posture evaluation. When presented with a valid Posture PAC, Policy Manager skips the posture validation handshake within the EAP-FAST protected tunnel; the prior result is used to ascertain end-host health. Specify **Posture PAC Expire Time** (the time until the PAC expires and must be replaced, by automatic or manual provisioning) in hours, days, weeks, months, or years. This is typically a short-lived PAC (specified in hours).

PAC Provisioning tab

The **PAC Provisioning** tab controls anonymous and authenticated modes. The following figure shows an example of the **EAP-FAST PAC - Provisioning** tab followed by parameter definition:

Figure 105: *EAP_FAST PAC Provisioning Tab*

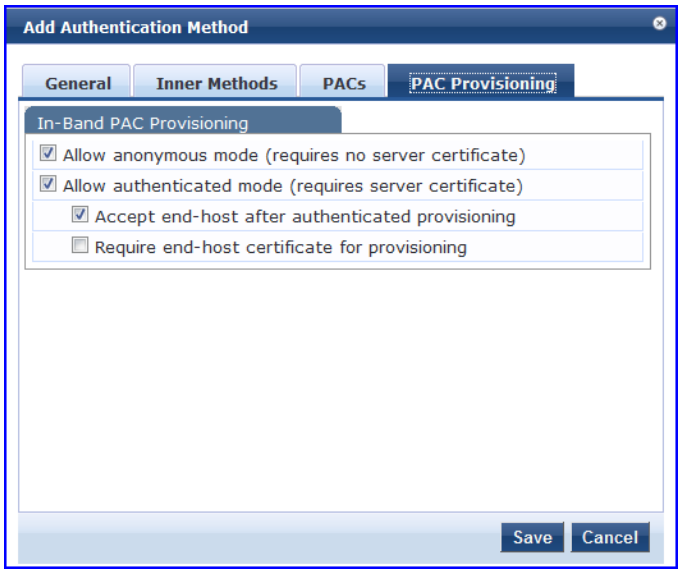


Table 67: *EAP_FAST PAC Provisioning tab Parameters*

Parameter	Description	Considerations
Allow Anonymous Mode	When in anonymous mode, *phase 0* of EAP_FAST provisioning establishes an outer tunnel without end-host/Policy Manager authentication (not as secure as the authenticated mode). After the tunnel is established, end-host and Policy Manager perform mutual authentication using MSCHAPv2, then Policy Manager provisions the end-host with an appropriate PAC (tunnel or machine).	Authenticated mode is more secure than anonymous provisioning mode. After the server is authenticated, the phase 0 tunnel is established. The end-host and Policy Manager perform mutual authentication and provision the end-host with an appropriate PAC (tunnel or machine): • If both anonymous and authenticated provisioning modes are enabled and the end-host sends a cipher suite that supports server authentication, Policy Manager picks the authenticated provisioning mode. • Otherwise, if the appropriate cipher suite is supported by the end-host, Policy Manager performs anonymous provisioning.
Allow Authenticated Mode	Enable to allow **Authenticated Mode** provisioning. When **Allow Authenticated Mode** is in *phase 0*, Policy Manager establishes the outer tunnel inside of a server-authenticated tunnel. The end-host authenticates the server by validating the Policy Manager certificate.	
Accept end-host after authenticated provisioning	After the authenticated provisioning mode is complete and the end-host is provisioned with a PAC, Policy Manager rejects end-host authentication; the end-host subsequently re-authenticates using the newly provisioned PAC. When enabled, Policy Manager accepts the end-host authentication in the provisioning	

Table 67: *EAP_FAST PAC Provisioning tab Parameters (Continued)*

Parameter	Description	Considerations
	mode itself; the end-host does not have to re-authenticate.	
Required end-host certificate for provisioning	In authenticated provisioning mode, the end-host authenticates the server by validating the server certificate resulting in a protected outer tunnel; the end-host is authenticated by the server inside this tunnel. When enabled, the server can require the end-host to send a certificate inside the tunnel for the purpose of authenticating the end-host.	

EAP-GTC

The **EAP-GTC** method contains the **General** tab that labels the method and defines session details. The following figure shows an example of the **EAP-GTC - General** tab followed by parameter definition:

Figure 106: *EAP-GTC - General Tab*

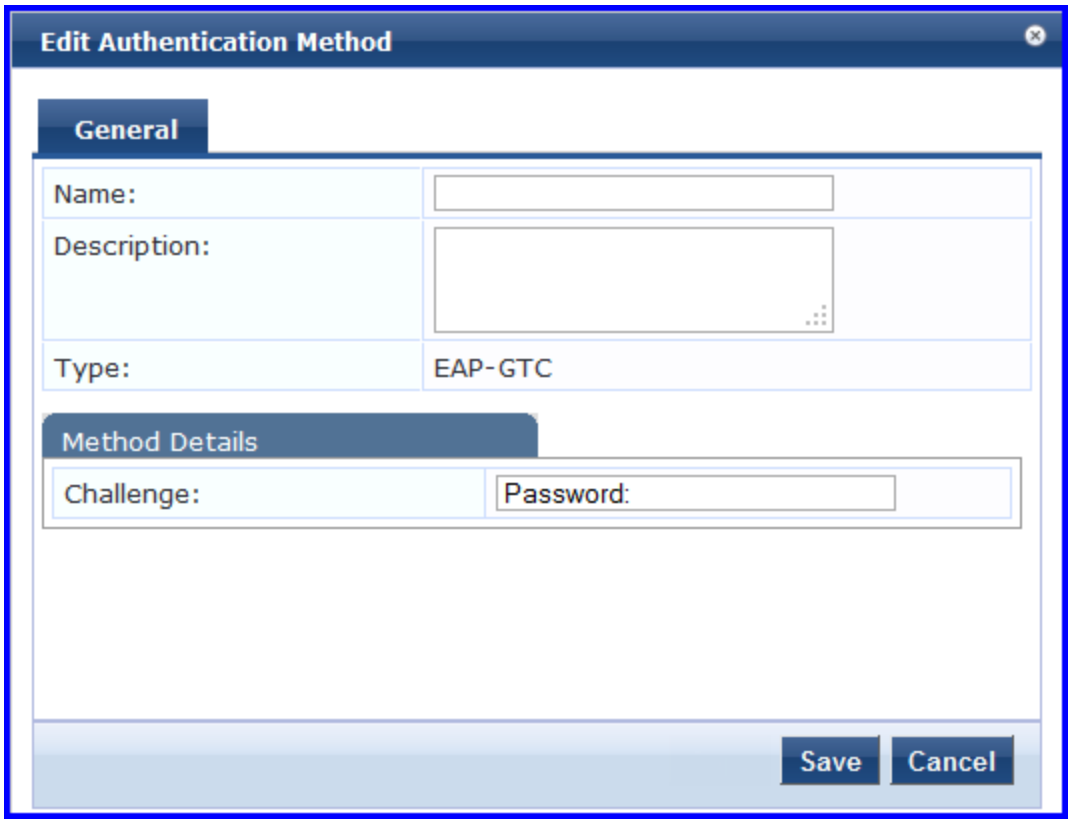


Table 68: *EAP-GTC General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **EAP-GTC**.
Method Details	
Challenge	Specify an optional password.

EAP-MSCHAPv2

The **EAP-MSCHAPv2** method contains the **General** tab that labels the method and defines session details. The following figure shows an example of the **EAP-MSCHAPv2 - General** tab followed by parameter definition:

Figure 107: *EAP-MSCHAPv2 - General Tab*

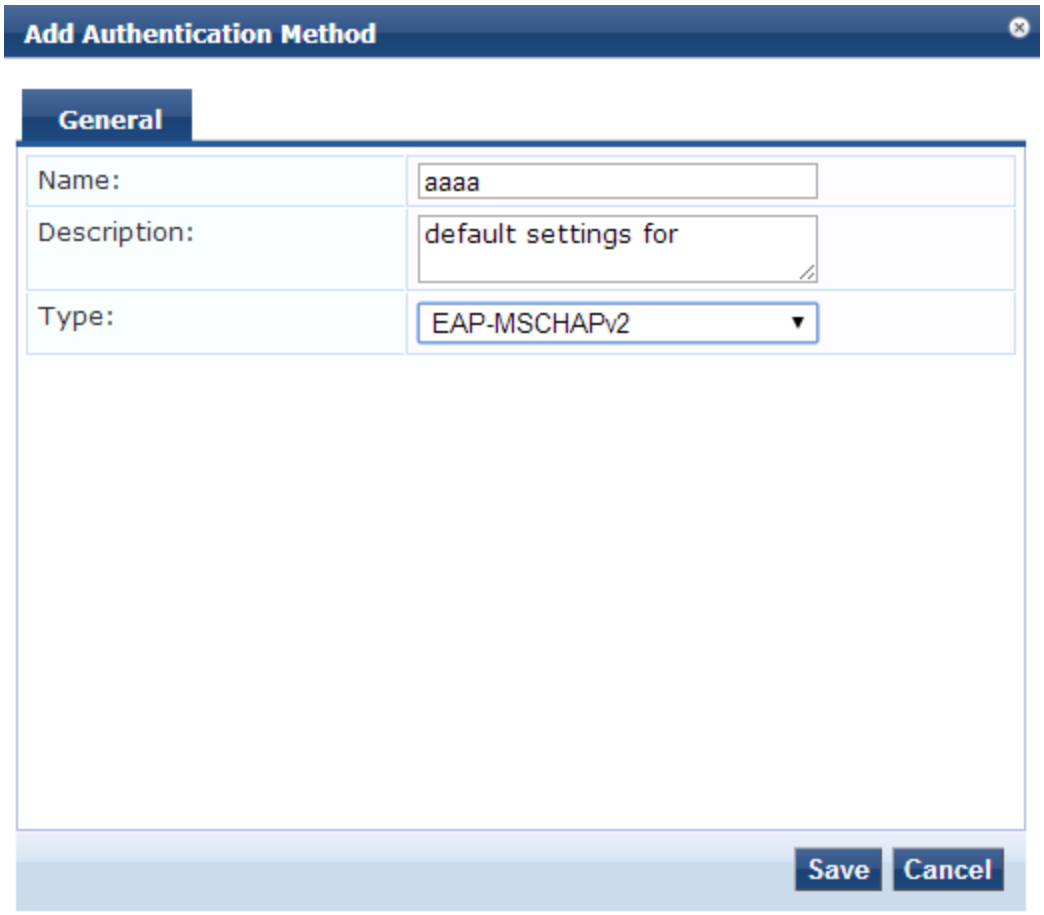


Table 69: *EAP-MSCHAPv2 - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **EAP-MSCHAPv2**.

EAP-PEAP

The **EAP-PEAP** method contains two tabs:

- General
- Inner Methods

General Tab

The **General** tab labels the method and defines session details. The following figure shows an example of the **EAP-PEAP General** tab followed by parameter definition:

Figure 108: *EAP-PEAP - General Tab*

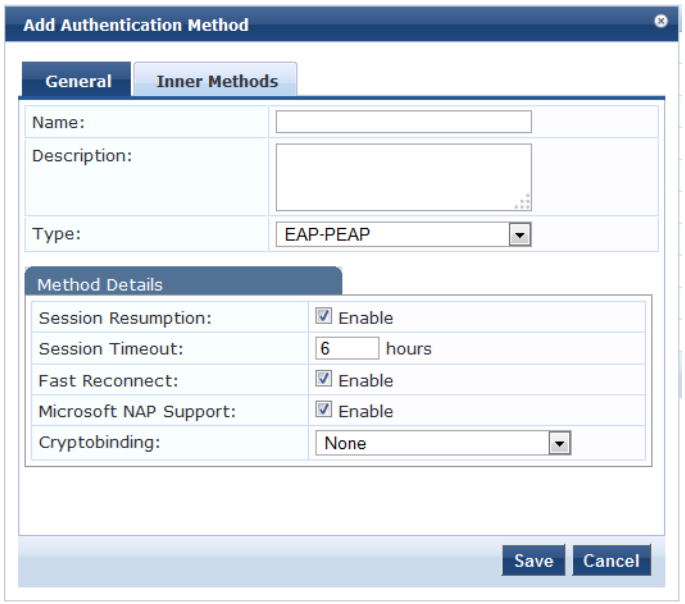


Table 70: *EAP-PEAP - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select **EAP-PEAP.**

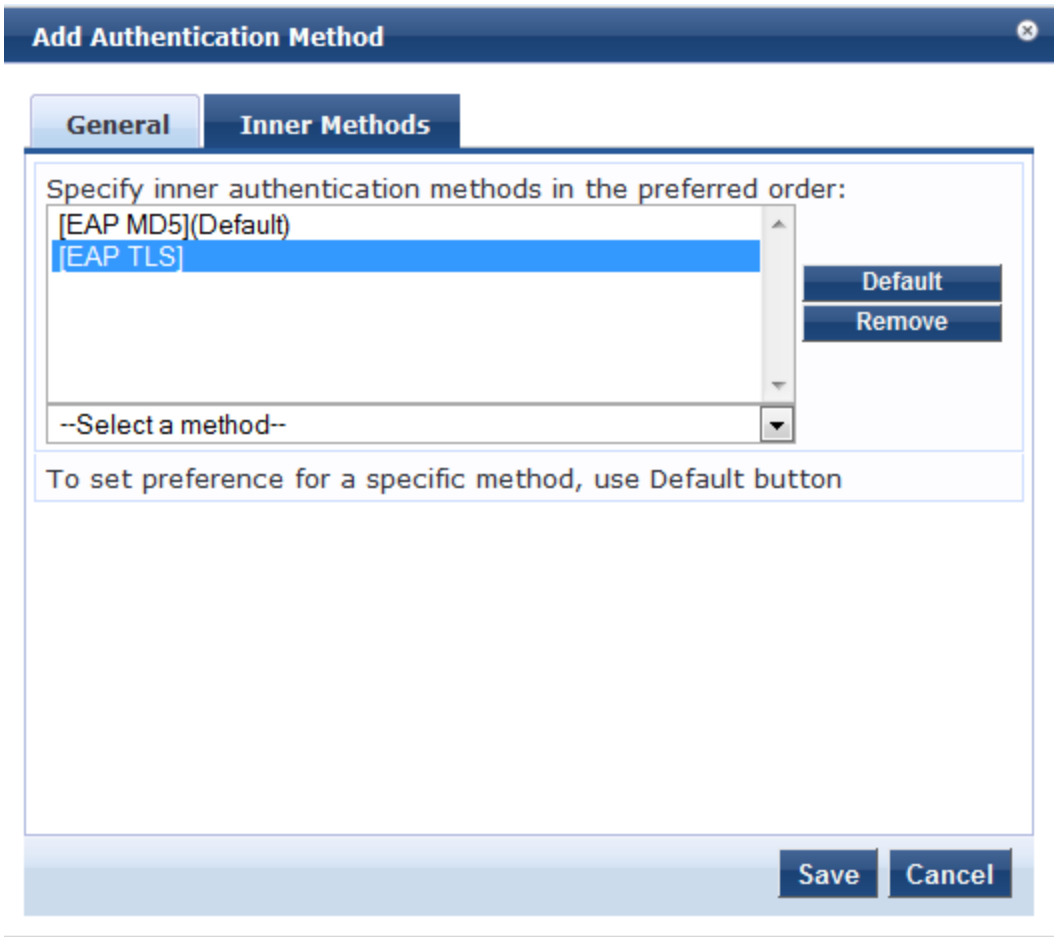
Table 70: *EAP-PEAP - General tab Parameters (Continued)*

Parameter	Description
Session Resumption	Caches EAP-PEAP sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.
Session Timeout	Caches EAP-PEAP sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval. If session timeout value is set to 0, the cached sessions are not purged.
Fast Reconnect	Enable this check box to allow fast reconnect. When fast reconnect is enabled, the inner method that happens inside the server authenticated outer tunnel is also bypassed. This makes the process of re-authentication faster. For the fast reconnect to work, session resumption must be enabled.
EAPoUDP Support	Enable EAPoUDP support. When EAPoUDP support is enabled, Policy Manager does not expect user authentication to happen within the protected tunnel.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-PEAP** method. The following figure shows an example of the **EAP-PEAP - Inner Methods** tab followed by parameter definition:

Figure 109: *EAP-PEAP - Inner Methods Tab*



NOTE

The **EAP-MD5** authentication method is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

Table 71: *EAP-PEAP Inner Methods tab Parameters*

Parameter	Description
Specify inner authentication methods in the preferred order	Select any method available in the current context from the drop-down list. Functions available in this tab include: • To append an inner method to the displayed list, select it from the drop-down list. The list can contain multiple inner methods, which Policy Manager sends in priority order until negotiation succeeds. • To remove an inner method from the displayed list, select the method and click **Remove**. • To set an inner method as the default (the method tried first), select it and click **Default**.

EAP-PEAP-Public

The **EAP-PEAP-Public** method is used for authenticating and providing a secured wireless guest access to the endpoints. To provide a secured wireless guest access, the Wi-Fi Protected Access (WPA) is provided for publicly known username and password. This ensures that every device gets a unique wireless session key that is used to encrypt the traffic and provide secured wireless access without intruding the privacy of others though the same username and password is shared to all devices.

The **EAP-PEAP-Public** method contains the following two tabs:

- General
- Inner Methods

General

The **General** tab labels the method and defines session details. The following figure shows an example of the **EAP-PEAP-Public - General** tab followed by parameter definition:

Figure 110: *EAP-PEAP-Public - General Tab*

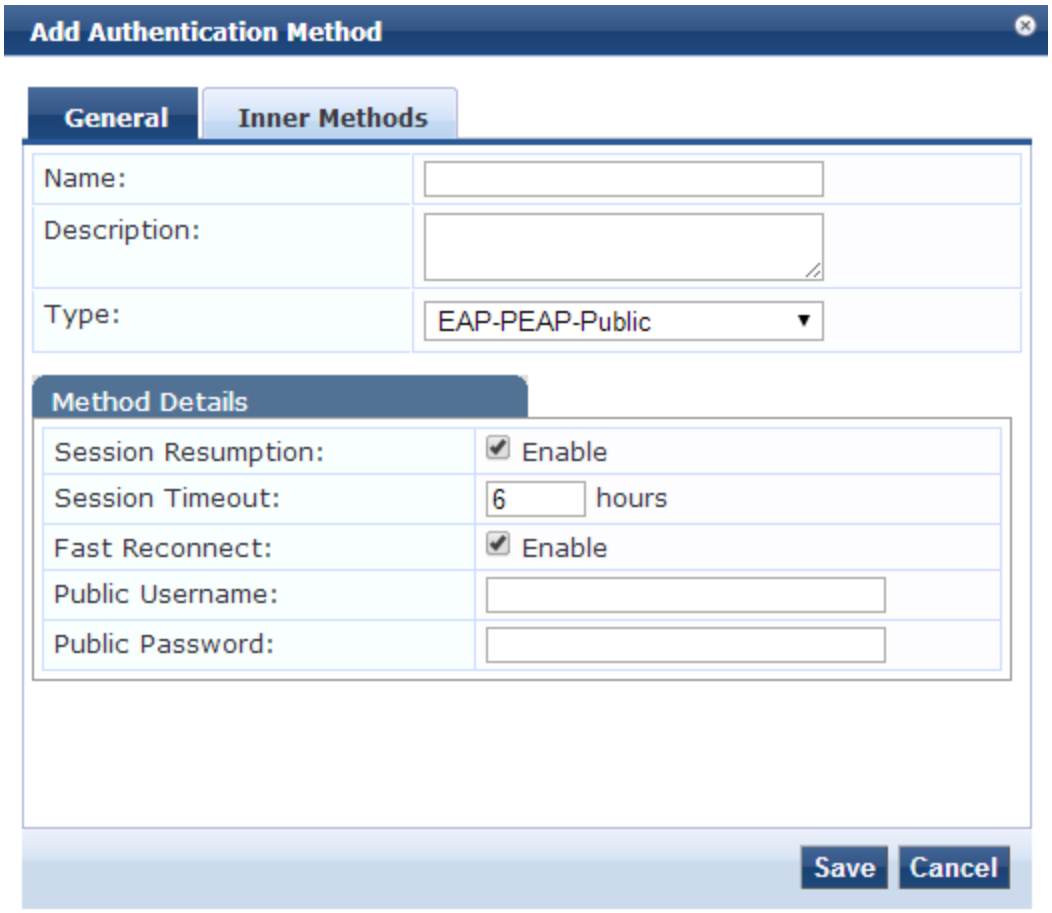


Table 72: *EAP-PEAP-Public - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select **EAP-PEAP-Public.**
Session Resumption	Caches EAP-PEAP-Public sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval. By default, this option is enabled.
Session Timeout	Caches EAP-PEAP-Public sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval in hours. If session timeout value is set to 0, the cached sessions are not purged. The default session timeout is 6 hours.
Fast Reconnect	Enable this check box to allow fast reconnect. When fast reconnect is enabled, the inner method that happens inside the server authenticated outer tunnel is also bypassed. This makes the process of re-authentication faster. For the fast reconnect to work,

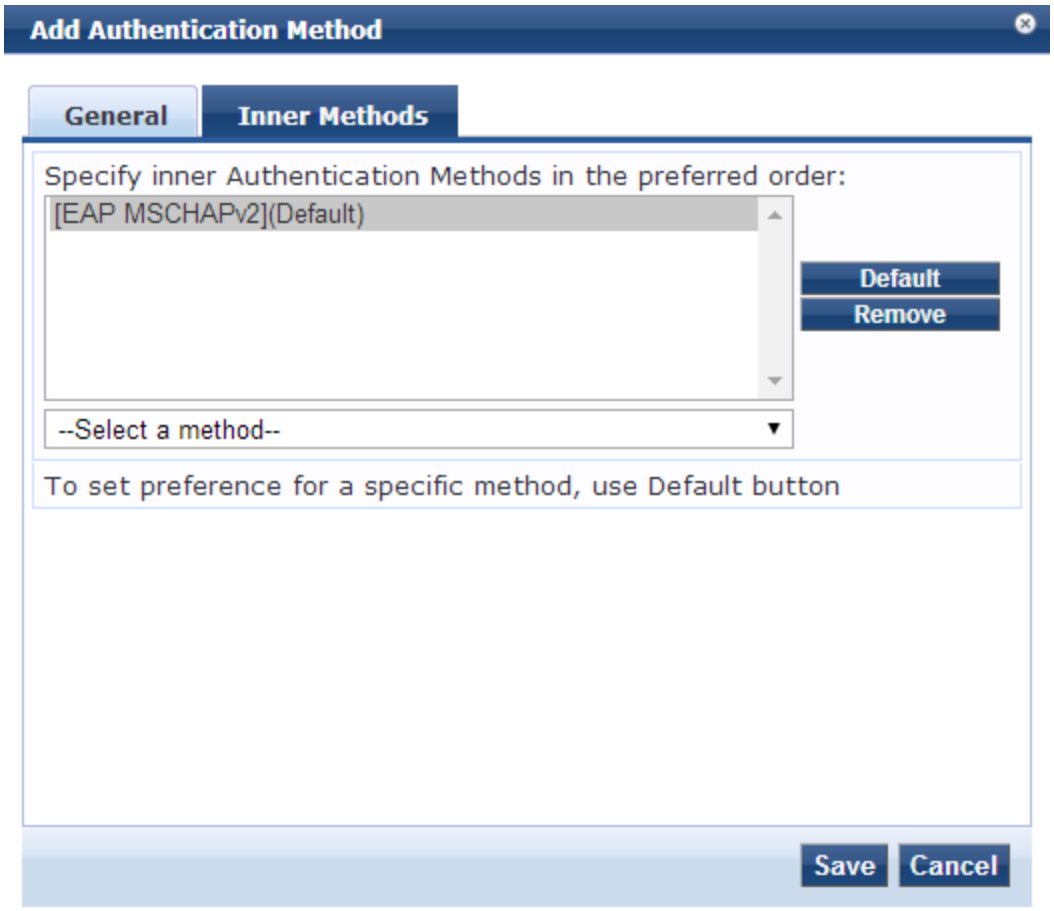
Table 72: *EAP-PEAP-Public - General tab Parameters (Continued)*

Parameter	Description
	session resumption must be enabled.
Public Username	Enter the Guest username. In this context, enter 'public'.
Public Password	Enter the Guest password. In this context, enter 'public'.

Inner Methods

The **Inner Methods** tab controls the inner methods for the **EAP-PEAP-Public** method. The following figure shows an example of the **EAP-PEAP-Public - Inner Methods** tab followed by parameter definition:

Figure 111: *EAP-PEAP-Public - Inner Methods Tab*



NOTE

The **EAP-MD5** authentication method is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

Table 73: *EAP-PEAP-Public Inner Methods tab Parameters*

Parameter	Description
Specify inner authentication methods in the preferred order	Select the inner authentication method available from the drop-down list. In this context, only the EAP-MSCHAPv2 method is available. The following functions are available in this tab: • To append an inner method to the displayed list, select it from the drop-down list. The list can contain multiple inner methods, which Policy Manager sends in priority order until negotiation succeeds. • To remove an inner method from the displayed list, select the method and click **Remove**. • To set an inner method as the default (the method tried first), select it and click **Default**.

EAP-TLS

The **EAP-TLS** method contains the **General** tab that labels and defines session details. The following figure shows an example of the **EAP-TLS - General** tab followed by parameter definition:

Figure 112: *EAP-TLS - General Tab*

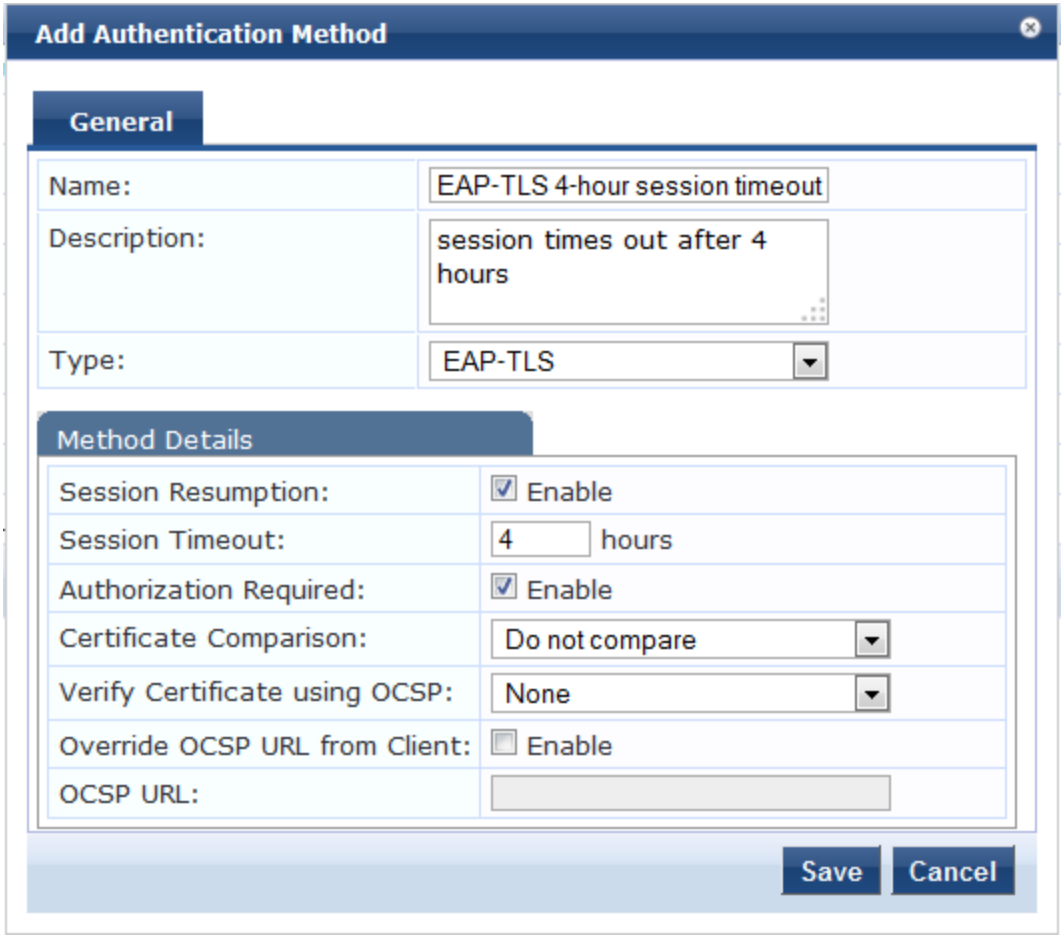


Table 74: *EAP_TLS - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select **EAP_TLS**.
Session Resumption	Caches EAP-TLS sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.
Session Timeout	Specifies the duration in hours for the cached EAP-TLS sessions to be retained.
Authorization Required	Check **Enable** to specify whether to perform an authorization check.
Certificate Comparison	Specify the type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate: • To skip the certificate comparison, choose **Do not compare.** • To compare specific attributes, choose **Compare Common Name (CN)**, **Compare Subject Alternate Name (SAN)**, or **Compare CN or SAN**. • To perform a binary comparison of the stored (in the client record in Active Directory or another LDAP-compliant directory) and presented certificates, choose **Compare Binary**.
Verify Certificate using OCSP	Select **Optional** or **Required** if the certificate must be verified by the Online Certificate Status Protocol (OCSP). Select **None** to not to verify the certificate.
Override OCSP URL from the Client	Select this option to use a different URL for OCSP. After this option is enabled, you can enter a new URL in the **OCSP URL** field.
OCSP URL	If the **Override OCSP URL from the Client** field is enabled, then enter the replacement URL here.

EAP-TTLS

The **EAP-TTLS** method contains two tabs; **General** and **Inner Methods**.

General Tab

The **General** tab labels the method and defines session details. The following figure shows an example of the **EAP-TTLS - General** tab followed by parameter definition:

Figure 113: *EAP-TTLS - General Tab*

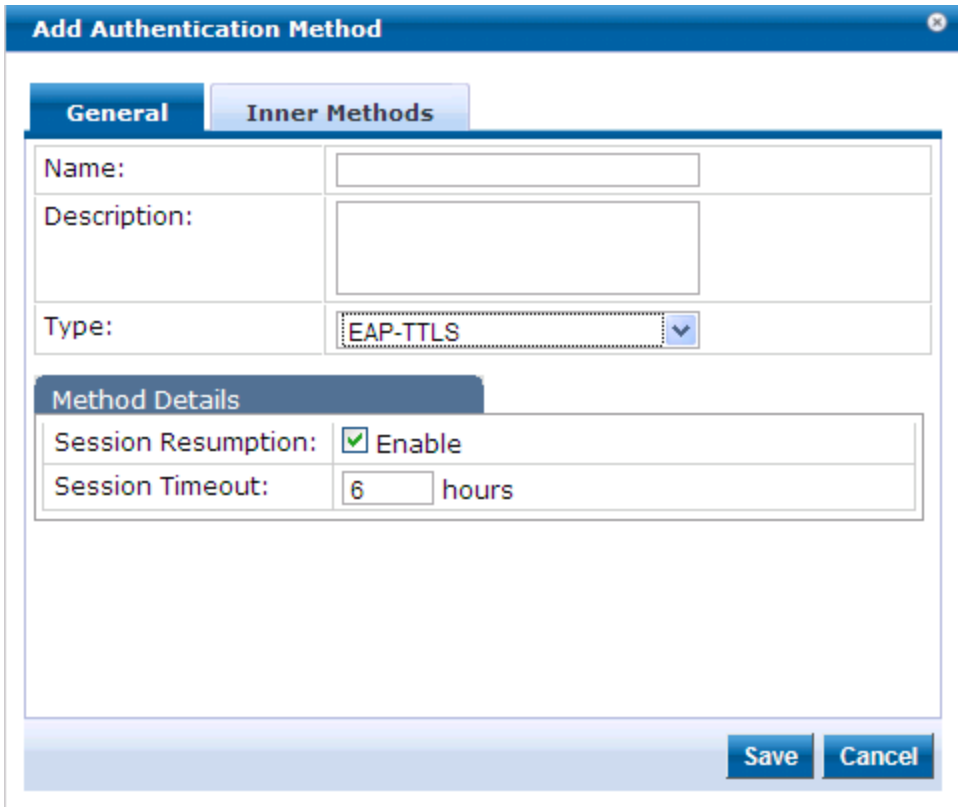


Table 75: *EAP-TTLS - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **EAP-TTLS**. **NOTE:** The **EAP-MD5** authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS mode.
Method Details	
Session Resumption	Caches EAP-TTLS sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.
Session Timeout	Specify the duration in hours for the EAP-TTLS sessions to be cached.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-TTLS** method. The following figure shows an example of the **EAP-TTLS - Inner Methods** tab followed by parameter definition:

Figure 114: *EAP_TTLS - Inner Methods Tab*

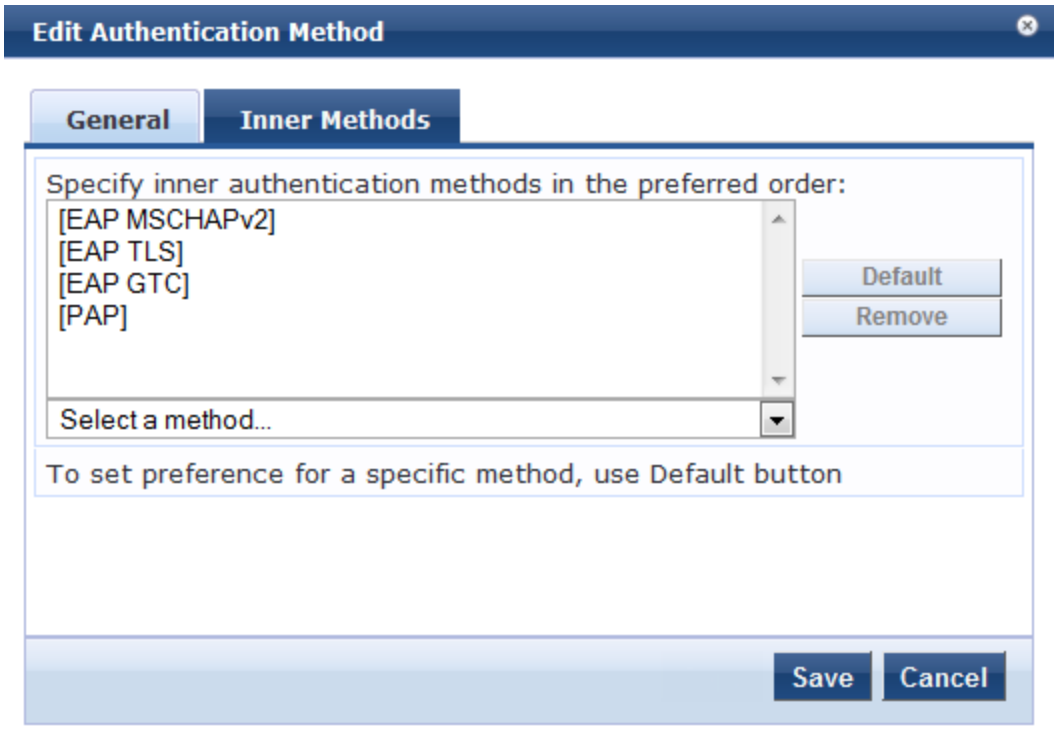


Table 76: *EAP-TTLS - Inner Methods tab Parameters*

Parameter	Description
Specify inner authentication methods in the preferred order	Select any method available in the current context from the drop-down list. Functions available in this tab include: • To append an inner method to the displayed list, select it from the drop-down list. The list can contain multiple inner methods, which Policy Manager sends in priority order until negotiation succeeds. • To remove an inner method from the displayed list, select the method and click **Remove**. • To set an inner method as the default (the method that tried first), select it and click **Default**. **NOTE:** The **EAP-MD5** authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS mode.

MAC-AUTH

The MAC-AUTH method contains the **General** tab that labels the method and defines session details. The following figure shows an example of the **MAC-AUTH - General** tab followed by parameter definition:

Figure 115: *MAC-AUTH - General Tab*

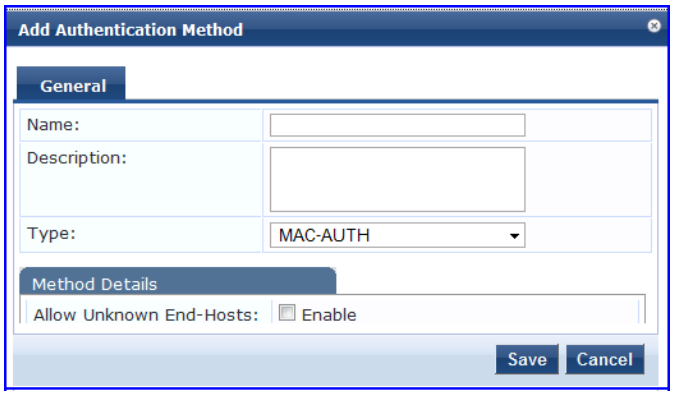


Table 77: *MAC-Auth - General tab Parameters*

Parameter	Description
General	
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **MAC-AUTH.**
Method Details	
Allow Unknown End-Hosts	Enables further policy processing of MAC authentication requests of unknown clients. If this is not enabled, Policy Manager automatically rejects a request whose MAC address is not in a configured authentication source. This setting is enabled, for example, when you want Policy Manager to trigger an audit for an unknown client. By selecting this check box and enabling audit (See Configuring Audit Servers on page 250), you can trigger an audit of an unknown client.

MSCHAP

The **MSCHAP** method contains the **General** tab that labels the method and defines session details. The following figure shows an example of the **MSCHAP - General** tab followed by parameter definition:

Figure 116: *MSCHAP - General Tab*

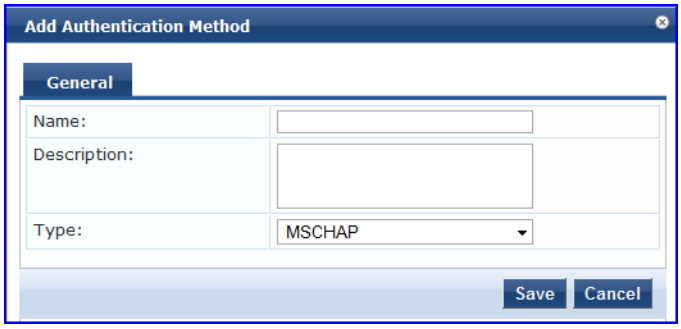


Table 78: *MSCHAP - General Tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **MSCHAP**.

PAP

The **PAP** method contains the **General** tab that labels the method and defines session details. The following figure shows an example of the **PAP - General** tab followed by parameter definition:

Figure 117: *PAP - General Tab*

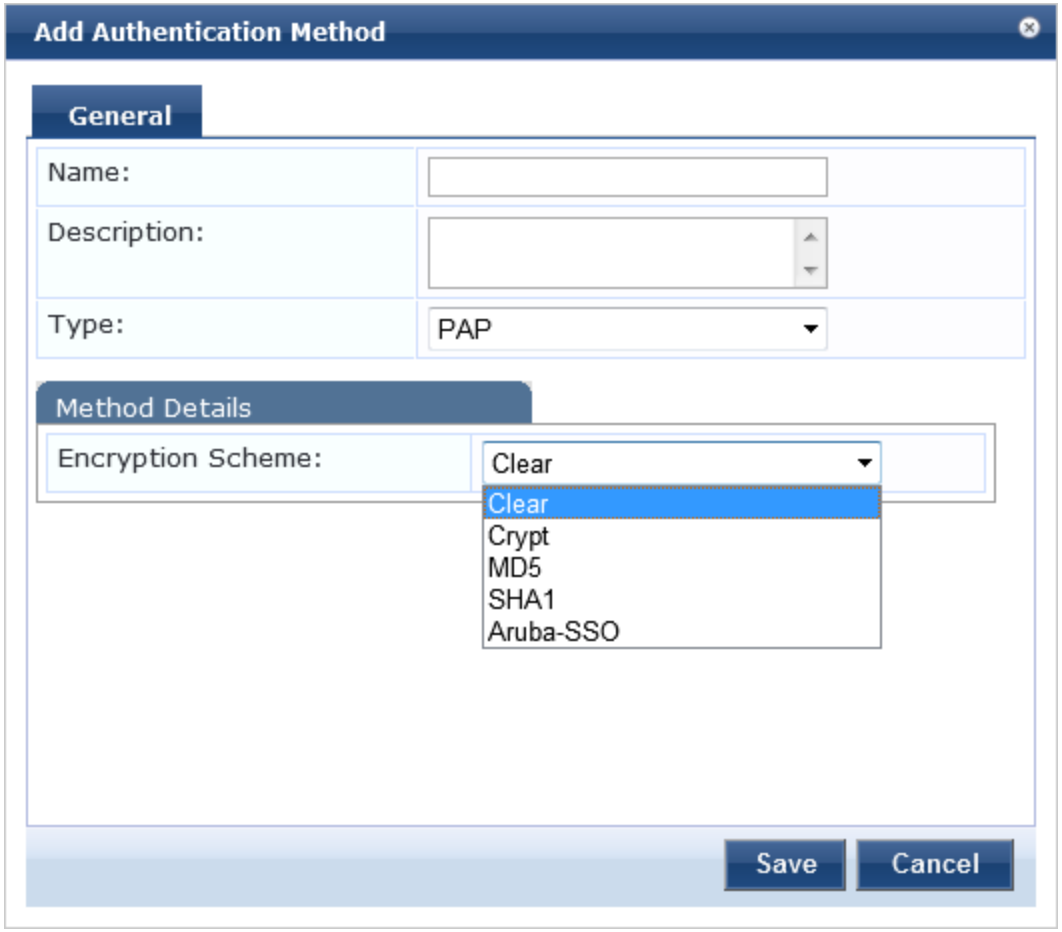


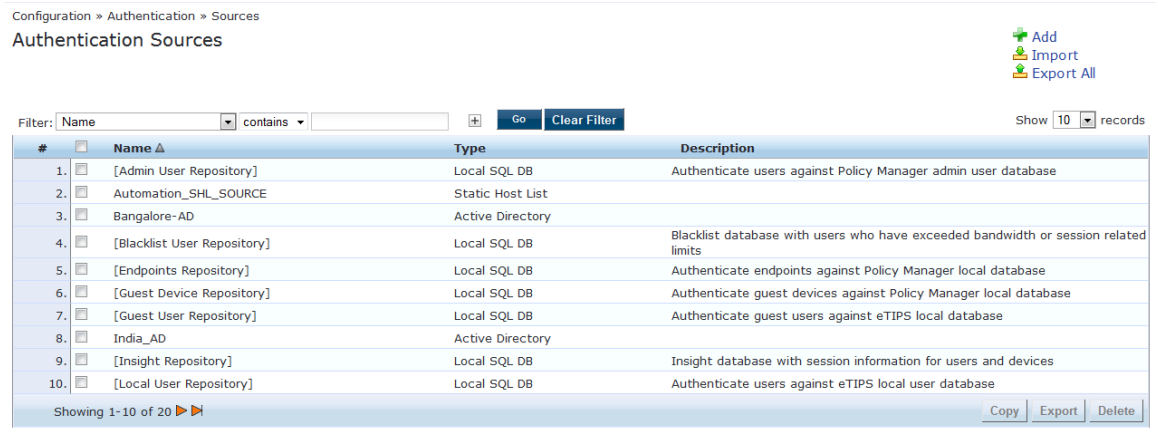
Table 79: *PAP - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **PAP.**
Method Details	
Encryption Scheme	Select the PAP authentication encryption scheme. The following schemes are supported: • Clear • Crypt • MD5 • SHA1 • SHA256 • NT Hash • LM Hash • Aruba-SSO **NOTE:** The **MD5** encryption scheme is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

Adding and Modifying Authentication Sources

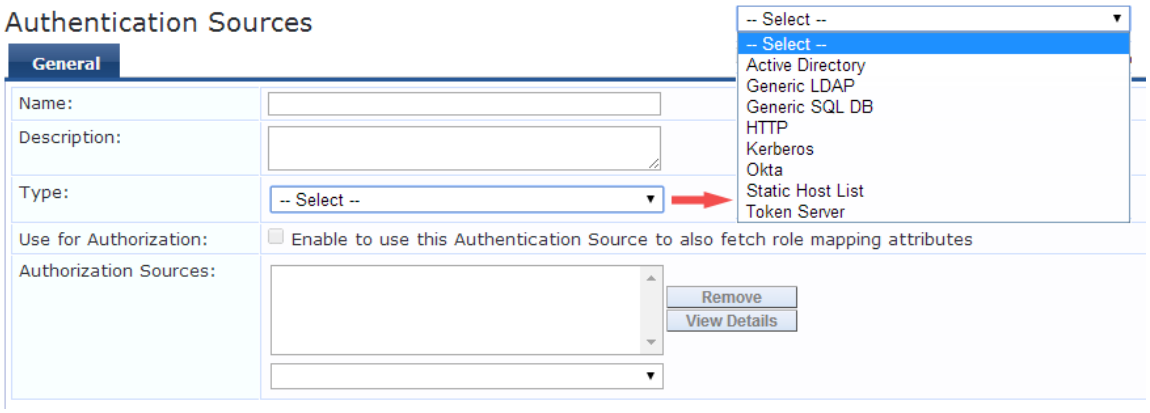
Policy Manager supports multiple authentication sources. From the **Services** (**Configuration > Service**) page, you can configure the authentication source for a new service as part of the flow of the **Add Service** wizard) or modify an existing authentication source directly (**Configuration > Authentication > Sources**, then click any row in the **Authentication Sources** page). The following figure shows an example of the **Authentication Sources** page:

Figure 118: *Authentication Sources Page*



After clicking **Add Authentication Source** from any of these locations, Policy Manager displays the **Add** page. Depending on the **Authentication Source** selected, different tabs and fields appear.

Figure 119: *Add Authentication Source Page*



For more information, see:

- Generic LDAP and Active Directory on page 155
- Generic SQL DB on page 169
- HTTP on page 174
- Kerberos on page 178
- Okta on page 181
- Static Host List on page 185
- Token Server on page 187

Generic LDAP and Active Directory

Policy Manager can perform NTLM/MSCHAPv2, PAP/GTC, and certificate-based authentications against Microsoft Active Directory and against any LDAP-compliant directory (For example, Novell eDirectory, OpenLDAP, or Sun Directory Server). Both LDAP and Active Directory based server configurations are similar. You can retrieve role mapping attributes by using filters. For more information, see Adding and Modifying Role Mapping Policies on page 203.

Configure Generic LDAP and Active Directory authentication sources on the following tabs:

- General Tab on page 155
- Primary Tab on page 157
- Attributes Tab on page 160
- Summary Tab

General Tab

The **General** tab labels the authentication source and defines session details. The following figure shows an example of the **Generic LDAP or Active Directory - General** tab followed by parameter definition:

Figure 120: *Generic LDAP or Active Directory - General Tab*

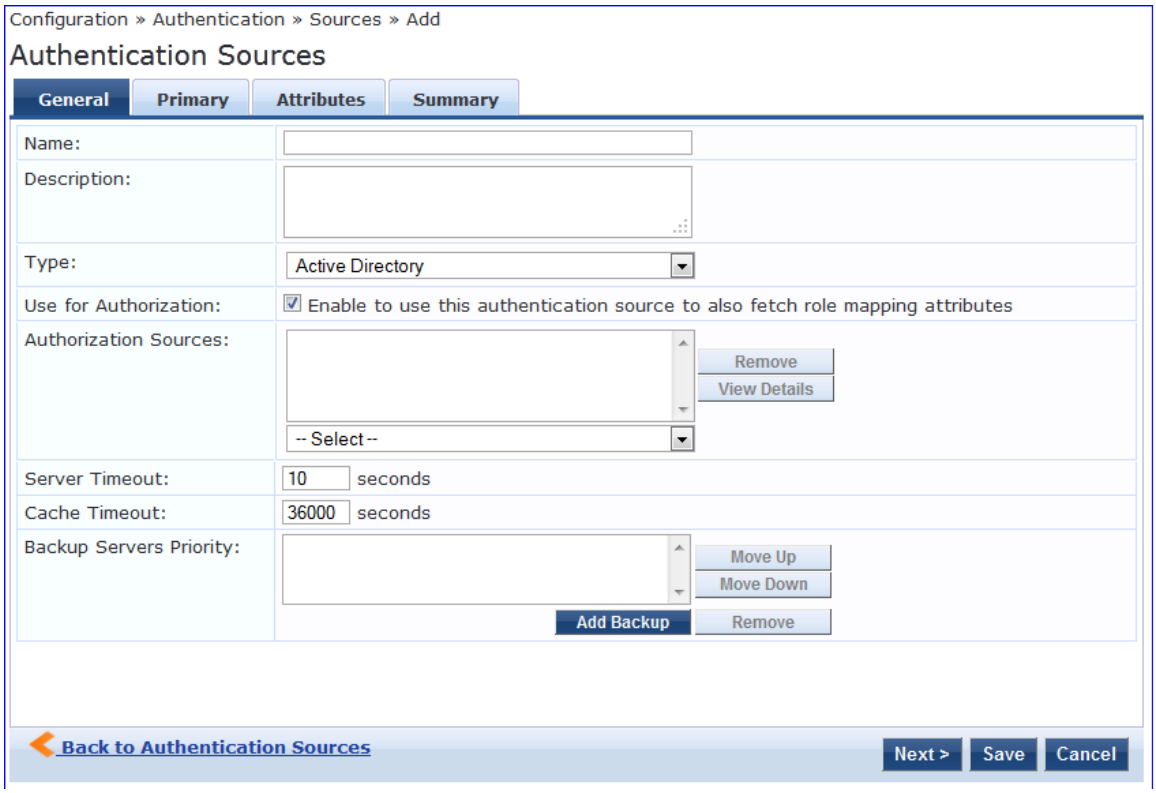


Table 80: *Generic LDAP or Active Directory - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **General LDAP** or **Active Directory.**
Use for Authorization	Enable this check box instruct Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This box is checked (enabled) by default.
Authorization Sources	Specifies additional sources from which role mapping attributes to be fetched. Select a previously configured authentication source from the drop-down list and click **Add** to add authentication source to the list of authorization sources. Click **Remove** to remove the authentication source from the list. If Policy Manager authenticates the user or device from this authentication source, then also fetches role mapping attributes from these additional authorization sources.

Table 80: *Generic LDAP or Active Directory - General tab Parameters (Continued)*

Parameter	Description
	NOTE: As described in Services on page 79, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.
Server Timeout	Specifies the duration in number of seconds that Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the duration in number of seconds that Policy Manager waits before attempting to fail over from the primary to the backup servers in the order in which they are configured.
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.
Backup Servers Priority	Click **Add Backup** to add a backup server. If the **Backup 1** tab appears, you can specify connection details for a backup server (same fields as for primary server that is specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers if the primary server is unreachable.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure shows an example of the **Generic Active Directory - Primary** tab followed by parameter definition:

Figure 121: *Generic LDAP or Active Directory - Primary tab*

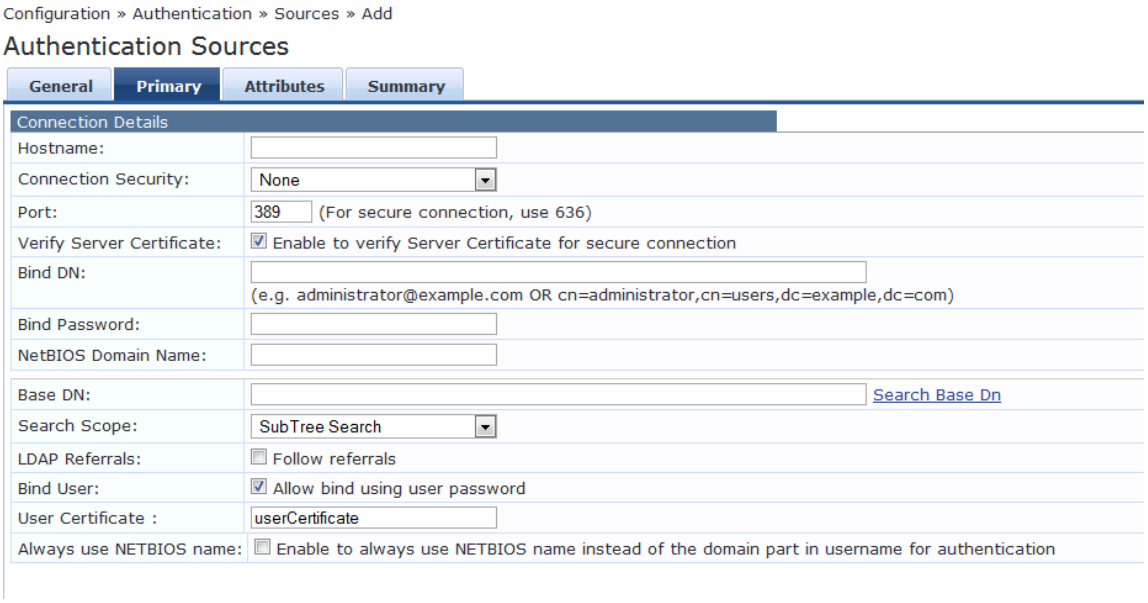


Table 81: *Generic LDAP or Active Directory - Primary Tab Parameters*

Parameter	Description
Hostname	Specify the hostname or the IP address of the LDAP or Active Directory server.
Connection Security	• Select **None** for default non-secure connection (usually port 389). • Select **StartTLS** for secure connection that is negotiated over the standard LDAP port. This is the preferred way to connect to an LDAP directory securely. • Select **LDAP over SSL** or **AD over SSL** to choose the legacy way of securely connecting to an LDAP directory. Port 636 must be used for this type of connection.
Port	Specifies the TCP port at which the LDAP or Active Directory server is listening for connections. (The default TCP port for LDAP connections is 389. The default port for LDAP over SSL is 636).
Verify Server Certificate	Select this checkbox to verify the Server Certificate as part of the authentication.
Bind DN	Specify the Distinguished Name (DN) of the administrator account. Policy Manager uses this account to access all other records in the directory. **NOTE:** For Active Directory, the bind DN can also be in the administrator@domain format (for example, administrator@acme.com).
Bind Password	Specify the password for the administrator DN entered in the **Bind DN** field.
NetBIOS Domain Name	Specify the Active Directory domain name for this server. Policy Manager prepends this name to the user ID to authenticate users found in this Active Directory. **NOTE:** This setting is available only for Active Directory.
Base DN	Enter the DN of the node in your directory tree from which to start searching for records. After entering the values for the fields described above, click **Search Base DN** to browse the directory hierarchy. The LDAP Browser opens. You can navigate to the DN that you want to use as the Base DN.

Table 81: *Generic LDAP or Active Directory - Primary Tab Parameters (Continued)*

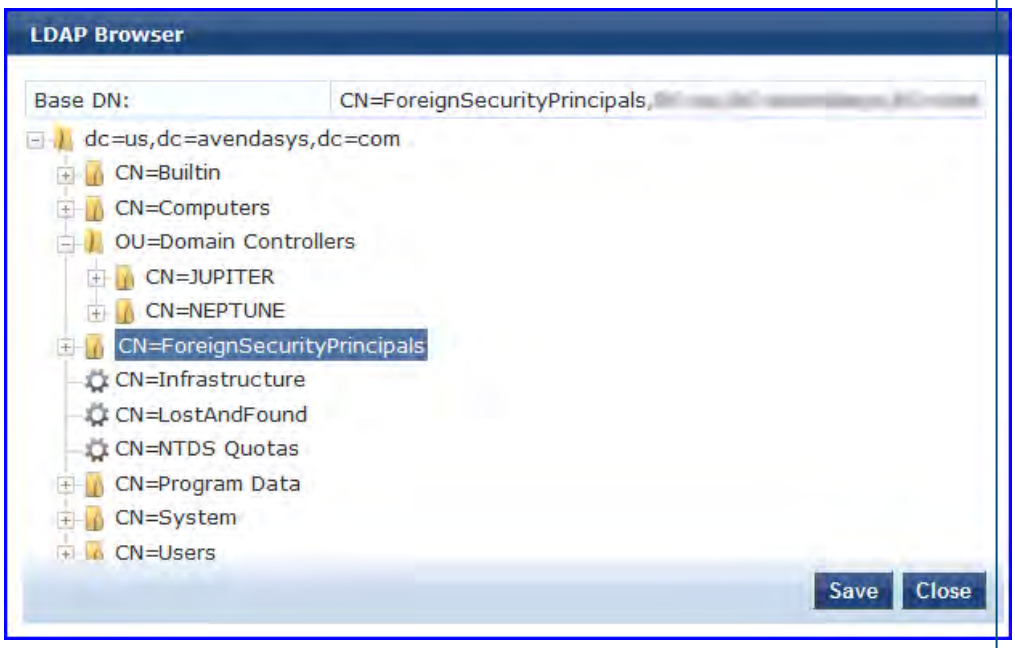
Parameter	Description
	 Click on any node in the tree structure that is displayed to select it as a Base DN. Note that the Base DN is displayed at the top of the LDAP Browser. **NOTE:** This is also a method to test the connectivity to your LDAP or AD directory. If the values entered for the primary server attributes are correct, you can browse the directory hierarchy by clicking **Search Base Dn**.
Search Scope	Select the scope of the search you want to perform, starting at the Base DN. • **Base Object Search** allows you to search at the level specified by the base DN. • **One Level Search** allows you to search up to one level lesser to the immediate children of the base DN. • **Subtree Search** allows you to search the entire subtree under the base DN (including at the base DN level).
LDAP Referral	Enable this check box to automatically follow referrals returned by your directory server in search results. Refer to your directory documentation for more information on referrals.
Bind User	Enable this checkbox to authenticate users by performing a bind operation on the directory using the credentials (user name and password) obtained during authentication. For clients to be authenticated by using the LDAP bind method, Policy Manager must receive the password in cleartext.
Password Attribute (Available only for **Generic LDAP**)	Enter the name of the attribute in the user record from which user password can be retrieved. This is not available for Active Directory.

Table 81: *Generic LDAP or Active Directory - Primary Tab Parameters (Continued)*

Parameter	Description
Password Type (Available only for **Generic LDAP**)	Specify whether the password type is Cleartext, NT Hash, or LM Hash.
Password Header (Available only for **Generic LDAP**)	Specifies the Oracle's LDAP implementation that prepends a header to a hashed password string. If using Oracle LDAP, enter the header in this field to correctly identify and read the password .
User Certificate	Enter the name of the attribute in the user record from which user certificate can be retrieved.
Always use NETBIOS name	Check this option to always use NETBIOS name instead of the domain part in username for authentication. **NOTE:** This field is available only if you select **Active Directory** as an authentication source.

Attributes Tab

The **Attributes** tab defines the Active Directory or LDAP Directory query filters and the attributes to be fetched by using those filters. The following figures show the examples of the **Active Directory - Attributes** tab and the **Generic LDAP Directory - Attributes** tab followed by parameter definition:

Figure 122: *Active Directory Attributes Tab (with default data)*

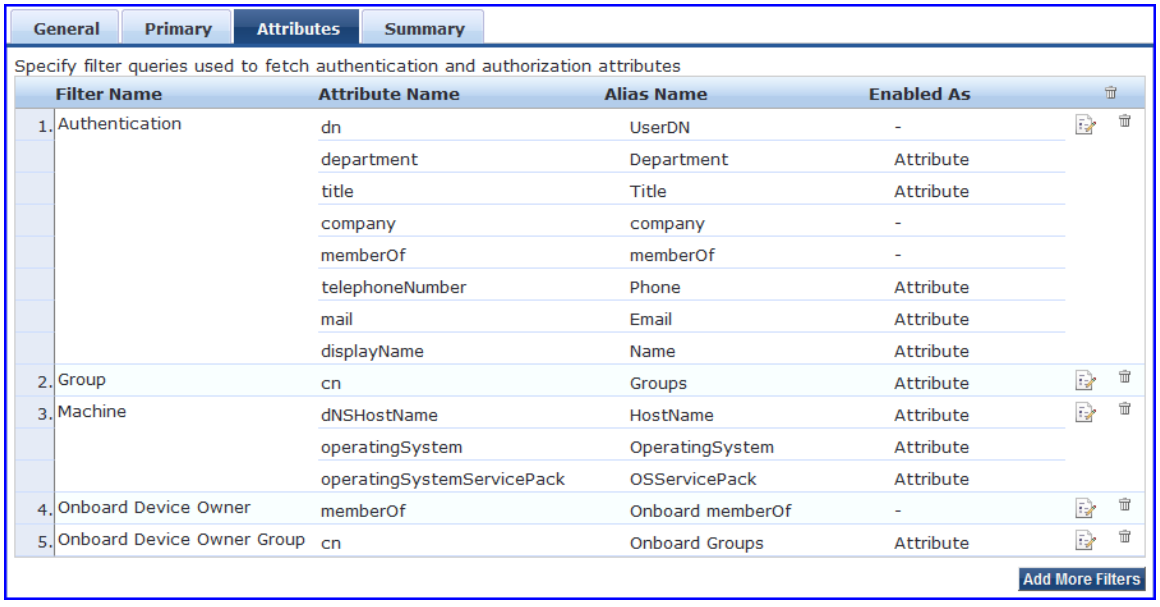


Figure 123: *Generic LDAP Directory Attributes Tab*

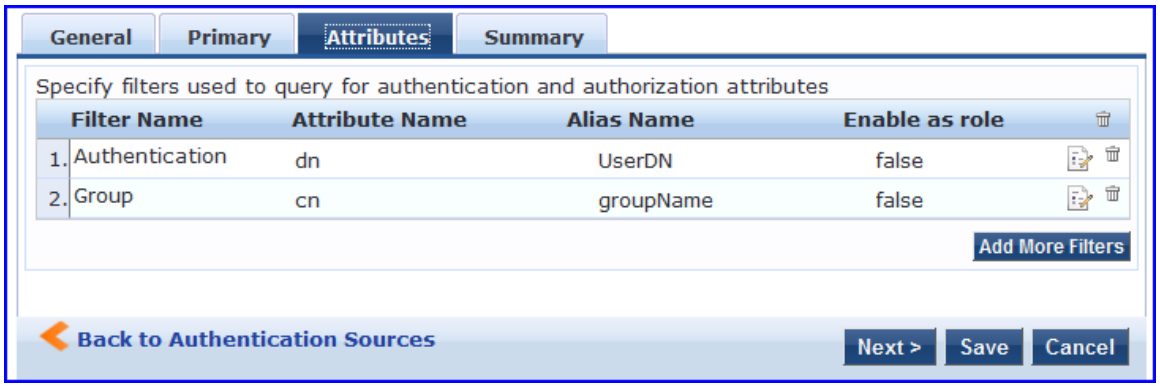


Table 82: *D/LDAP Attributes Tab (Filter Listing Screen) Parameters*

Tab	Parameter/Description
Filter Name	Specifies the name of the filter.
Attribute Name	Specify the name of the LDAP/AD attributes defined for this filter.
Alias Name	Specify the alias name for each attribute name selected for the filter.
Enable As	Specify whether the value is to be used directly as a role or attribute in an Enforcement Policy. This bypasses the step to assign a role in Policy Manager through a Role Mapping Policy.

The following table describes the available directories.

Table 83: *AD/LDAP Default Filters*

Directory	Default Filters

Active Directory	• **Authentication**: This filter is used for authentication. The query searches in the objectClass of type **user**. This query finds both user and machine accounts in Active Directory:
	`(&(objectClass=user)(sAMAccountName=%{Authentication:Username}))`
	After a request arrives, Policy Manager populates **%{Authentication:Username}** with the authenticating user or machine. This filter is also configured to fetch the following attributes based on this filter query:
	▪ **dn** (alias of UserDN): This is an internal attribute that is populated with the user or machine record's Distinguished Name (DN)
	▪ **department**
	▪ **title**
	▪ **company**
	▪ **memberOf**: In Active Directory, this attribute is populated with the groups that the user or machine belongs to. This is a multi-valued attribute.
	▪ **telephoneNumber**
	▪ **mail**
	▪ **displayName**
	▪ **accountExpires**
	• **Group**: This is a filter used for retrieving the name of the groups a user or machine belongs to.
	`(distinguishedName=%{memberOf})`
	This query fetches all group records, where the distinguished name is the value returned by the **memberOf** variable. The values for the **memberOf** attribute are fetched by the first filter (Authentication) described above. The attribute fetched with this filter query is **cn**, which is the name of the group.
	• **Machine**: This query fetches the machine record in Active Directory.
	`(&(objectClass=computer)(sAMAccountName=%{Host:Name}$))`
	%{Host:Name} is populated by Policy Manager with the name of the connecting host if available. dNSHostName, operatingSystem, and operatingSystemServicePack attributes are fetched with this filter query.
	• **Onboard Device Owner:** This is the filter for retrieving the name of the owner the onboard device belongs to. This query finds the user in the Active Directory
	`(&(sAMAccountName=%{Onboard:Owner})(objectClass=user))`
	%{Onboard:Owner} is populated by Policy Manager with the name of the onboarded user.
	• **Onboard Device Owner Group:** This filter is used for retrieving the name of the group the onboarded device owner belongs to.
	`(distinguishedName=%{Onboard memberOf})`
	This query fetches all group records where the distinguished name is the value returned by the Onboard **memberOf** variable. The attribute fetched with this filter query is cn, which is the name of the Onboard group.

Generic LDAP Directory	**Authentication**: This is the filter used for authentication. `(&(objectClass=*)(uid=%{Authentication:Username}))` When a request arrives, Policy Manager populates %{Authentication:Username} with the authenticating user or machine. This filter is also set up to fetch the following attributes based on this filter query:

Table 83: *AD/LDAP Default Filters (Continued)*

Directory	Default Filters
	▪ **dn** (aliased to UserDN): This is an internal attribute that is populated with the user record's Distinguished Name (DN) **Group**: This is the filter used for retrieving the name of the groups to which a user belongs. `(&(objectClass=groupOfNames)(member=%{UserDn}))` ▪ This query fetches all group records (of objectClass groupOfNames), where the member field contains the DN of the user record (UserDN, which is populated after the Authentication filter query is executed. The attribute fetched with this filter query is cn, which is the name of the group (this is aliased to a more readable name: groupName)).
Add More Filters	Click this button to open the filter creation page. Refer to Add More Filters on page 163 for more information.

Add More Filters

Click the **Add More Filters** button on the **Authentication Sources > Add** page to open the **Configure Filter** page. From this page, you can define a filter query and the related attributes to be fetched.

Browse Tab

The **Browse** tab shows an LDAP browser from which you can browse the nodes in the LDAP or AD directory, starting at the base DN. This is presented in read-only mode. Selecting a leaf node (a node that has no children) displays the attributes associated with that node. The following figure shows an example of the **AD/LDAP Configure Filter - Browse** tab followed by parameter definition:

Figure 124: *AD/LDAP Configure Filter - Browse tab*

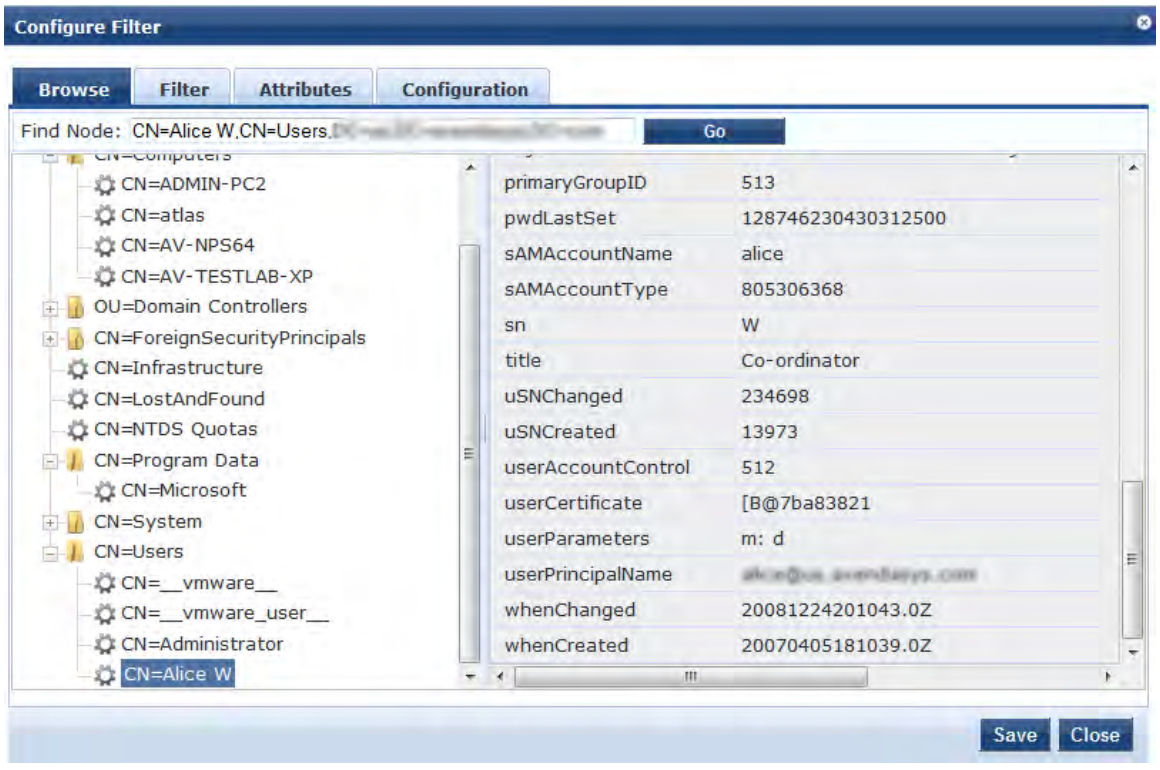


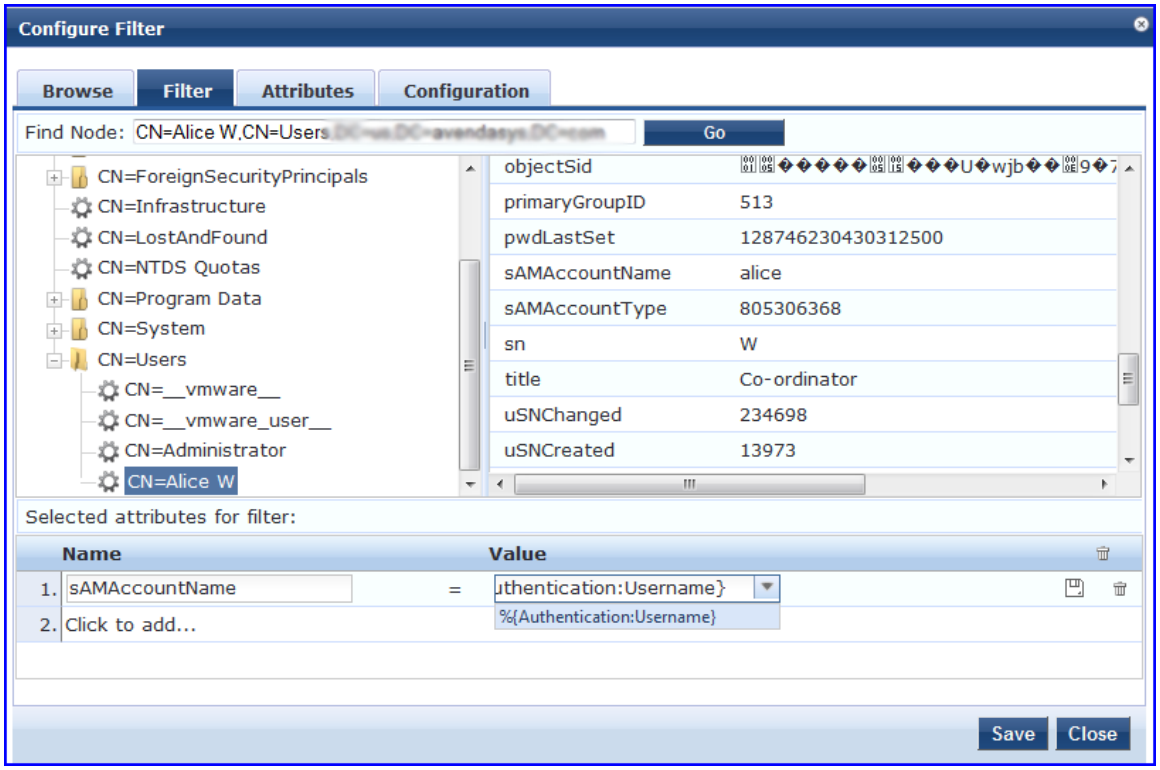
Table 84: *AD/LDAP Configure Filter Page - Browse tab Parameters*

Navigation	Description
Find Node	Find the node by entering the Distinguished Name (DN) and clicking on the **Go** button.

Filter Tab

The **Filter** tab provides an LDAP browser interface to define the filter search query. You can define the attributes used in the filter query using this interface. The following figure shows an example of the **AD/LDAP Create Filter Page - Filter** tab followed by parameter definition:

Figure 125: *AD/LDAP Create Filter Page - Filter tab*



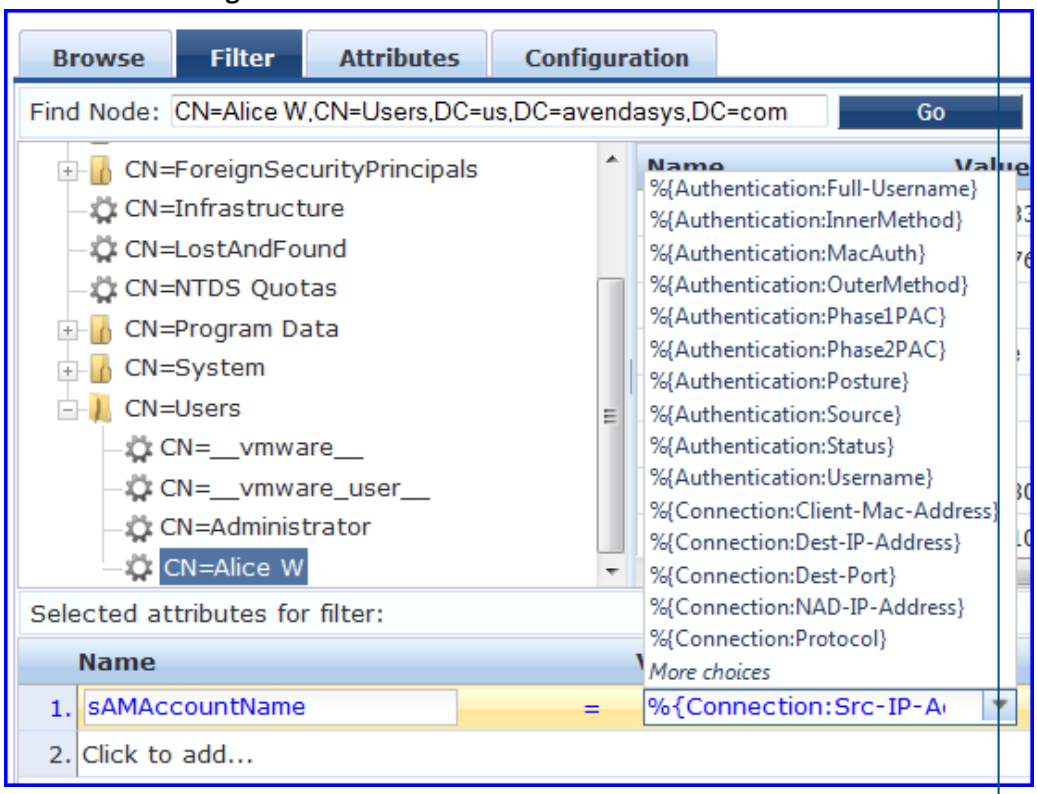
NOTE

Policy Manager is pre-configured with filters and selected attributes for Active Directory and generic LDAP directory. Create new filters only if you need Policy Manager to fetch role mapping attributes from a new type of record.

NOTE

You can fetch different types of records by specifying multiple filters that use different dynamic session attributes. For example, Policy Manager can fetch the user record associated with %{Authentication:Username} and a machine record associated with %{RADIUS:IETF:Calling-Station-ID} for a given request.

Table 85: *Configure Filter Page - Filter tab Parameters*

Parameter	Description
Find Node	Find a node by entering the Distinguished Name (DN) and clicking the **Go** button.
Select the attributes for filter	This table has a name and value column. There are two ways to enter the attribute name • By selecting a node, inspecting the attributes, and then manually entering the attribute name by clicking on **Click to add...** in the table row. • By selecting an attribute on the right hand side of the LDAP browser. The attribute name and value are automatically populated in the table. The attribute value field can be a value that is automatically populated by selecting an attribute from the browser, or it can be manually populated. To aid in populating the value with dynamic session attribute values, a drop-down with the commonly used namespace and attribute names is presented. The following figure shows an example of the **AD/LDAP Configure Filter - Filter** tab: 

The following table describes the steps used in creating a filter:

Table 86: *Filter Creation Steps*

Step	Description
Step 1 Select filter node	The goal of filter creation is to help Policy Manager to understand how to find a user or device connecting to the network in LDAP or Active Directory. From the **Filter** tab, click on a node that you want to extract user or device information from. For example, browse to the **Users** container in Active Directory and select the node for a user (Alice, for example). On the right hand side, you can view the attributes associated with that user.
Step 2 Select attribute	Click on attributes that helps Policy Manager to identify the user or device. For example, in Active Directory, an attribute called **sAMAccountName** stores the user ID. The attributes that you select are automatically populated in the **Filter** table displayed below the browser section with their values. In this example, if you select **sAMAccountName**, the row in the **Filter** table shows this attribute with a value of Alice (assuming you picked Alice's record as a sample user node).
Step 3 Enter value (optional)	After Step 2, you can have values for a specific record, Alice's record, in this context. Change the value to a dynamic session attribute that helps Policy Manager to associate a session with a specific record in LDAP/AD. For example, if you selected the **sAMAccountName** attribute in AD, click on the **Value** field and select **%{Authentication:Username}**. When Policy Manager processes an authentication request, **%{Authentication:Username}** is populated with the user ID of the user connecting to the network.
Step 4	Add more attributes from the selected node and continue with Step 2.

Attributes Tab

The **Attributes** tab defines the attributes to be fetched from Active Directory or LDAP directory. Each attribute can also be enabled as a Role, which means the value fetched for this attribute can be used directly in Enforcement Policies. For more information, see Configuring Enforcement Policies on page 298.

The following figure shows an example of the **AD/LDAP Configure Filter - Attributes** tab followed by parameter definition:

Figure 126: *AD/LDAP Configure Filter - Attributes Tab*

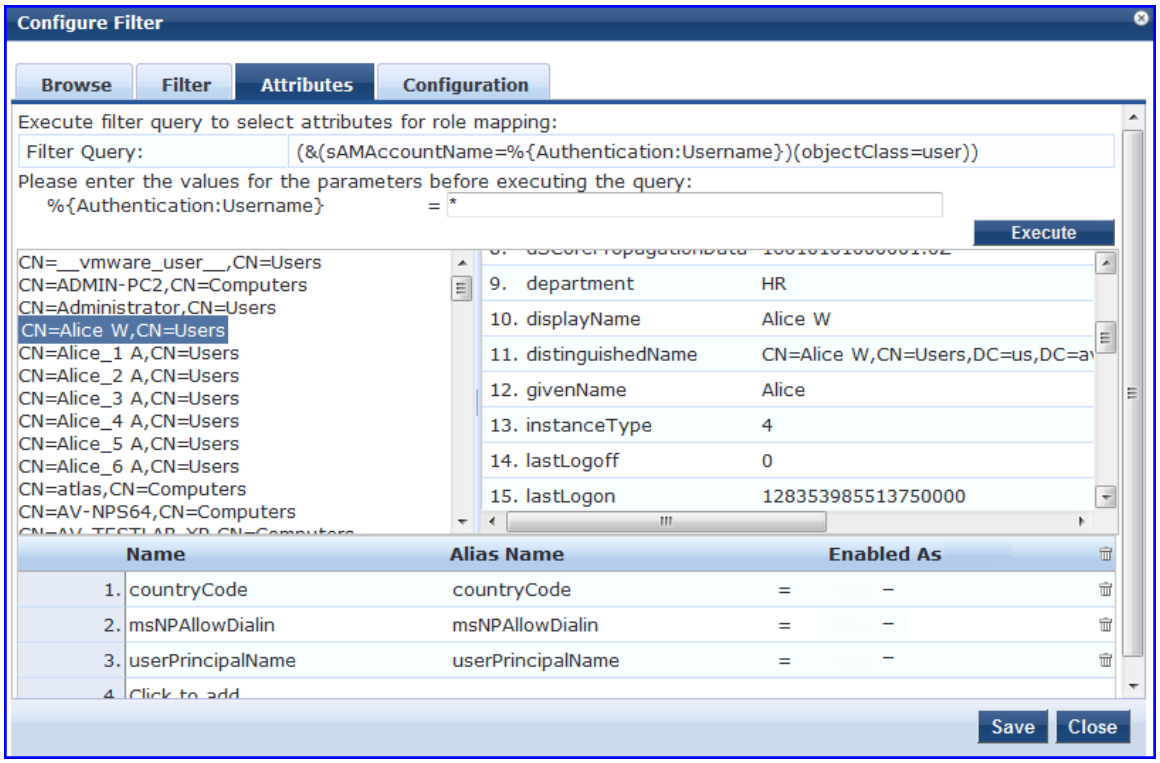


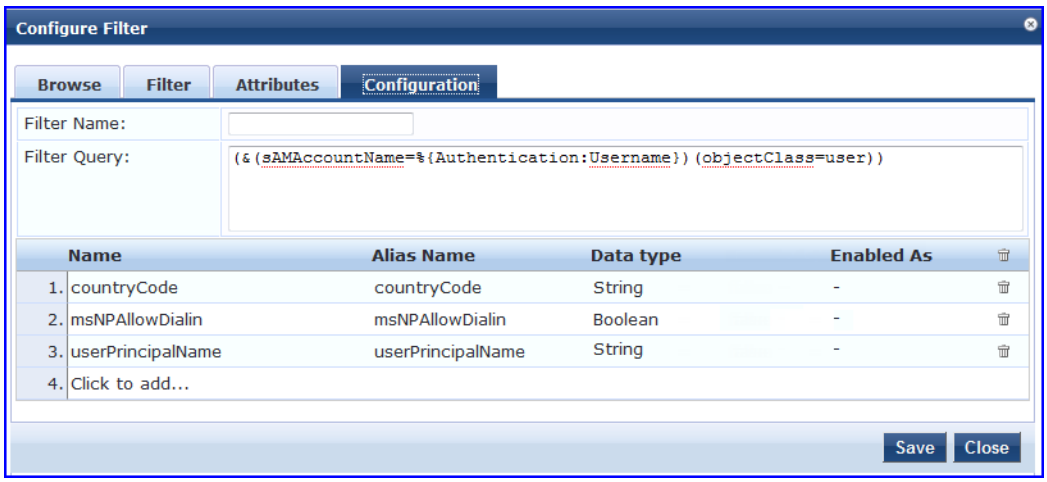
Table 87: *AD/LDAP Configure Filter Page - Attributes tab Paramters*

Parameter	Description
Enter values for parameters	Policy Manager parses the filter query (created in the **Filter** tab and shown at the top of the **Attributes** tab) and prompts to enter the values for all dynamic session parameters in the query. For example, if you have **%{Authentication:Username}** in the filter query, you are prompted to enter the value for it. You can enter wildcard character (*) here to match all entries. **NOTE:** If there are thousands of entries in the directory, entering the wildcard character (*) can take a while to fetch all matching entries.
Execute	After entering the values for all dynamic parameters, click **Execute** to execute the filter query. You can see all entries that match the filter query. Click on one of the entries (nodes) to view the list of attributes for that node. You can now click on the attribute names that you want to use as role mapping attributes.
Name	Specify the name of the attribute.
Alias Name	Specify the alternative name for the attribute. By default, this is the same as the attribute name.
Enable As	Click this to enable this attribute value to be used directly as a role in an Enforcement Policy. This bypasses the step of assigning a role in Policy Manager through a Role Mapping Policy.

Configuration Tab

The **Configuration** tab shows the filter and attributes configured in the **Filter** and **Attributes** tabs respectively. From this tab, you can also manually edit the filter query and attributes to be fetched. The following figure shows an example of the **Configure Filter - Configuration** tab:

Figure 127: *Configure Filter Popup - Configuration tab*



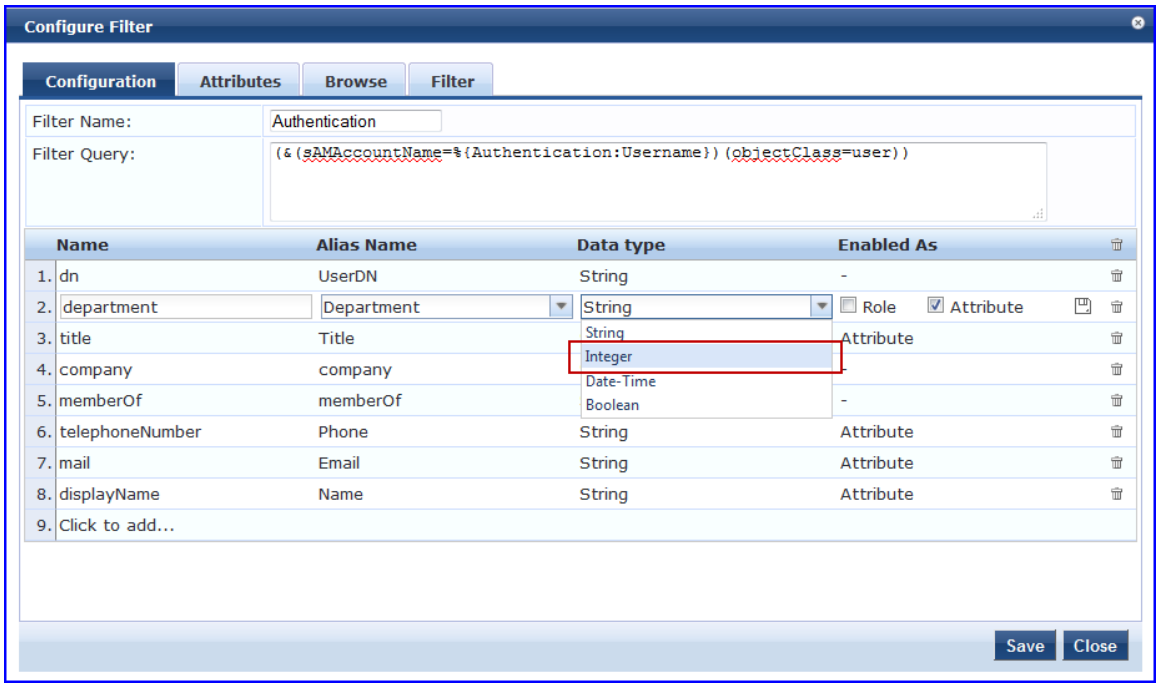
Modify Default Filters

When you add a new authentication source of type Active Directory or LDAP, a few default filters and attributes are populated. You can modify these pre-defined filters by selecting a filter on the **Authentication > Sources > Attributes** tab. This opens the **Configure Filter** page for the specified filter.

NOTE

A minimum of one filter must be specified for the LDAP and Active Directory authentication source. This filter is used by Policy Manager to search for the user or device record. If not specified, authentication requests are rejected.

Figure 128: *Modify Default Filters*



The attributes that are defined for the authentication source display as attributes in role mapping policy rules editor under the authorization source namespace. Then, on the **Role Mappings - Rules Editor** page, the Operator values that display are based on the **Data type** specified here. For example, if you modify the Active Directory **department** to be an integer rather than a string, then the list of operator values populate with values that are specific to integers.

The functionality that allows you to modify the data type available for Generic SQL DB, Generic LDAP, Active Directory, and HTTP authentication source types.

Summary Tab

You can use the **Summary** tab to view configured parameters.

Generic SQL DB

Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against any Open Database Connectivity (ODBC) compliant SQL database such as Microsoft SQL Server, Oracle, MySQL, or PostgrSQL. Specify a stored procedure to query the relevant tables and retrieve role mapping attributes by using filters.

Configure the primary and backup servers, session details, filter query, and role mapping attributes to fetch the Generic SQL authentication sources on the following tabs:

- General Tab on page 169
- Primary Tab on page 171
- Attributes Tab on page 172
- Summary Tab

For a configured Generic SQL DB authentication source, the following options on the main page enable you to:

- **Clear Cache**: Clears the attributes cached by Policy Manager for all entities that authorize against this server.
- **Copy**: Creates a copy of this authentication/authorization source.

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure shows an example of the **Generic SQL DB - General** tab followed by parameter definition:

Figure 129: *Generic SQL DB - General Tab*

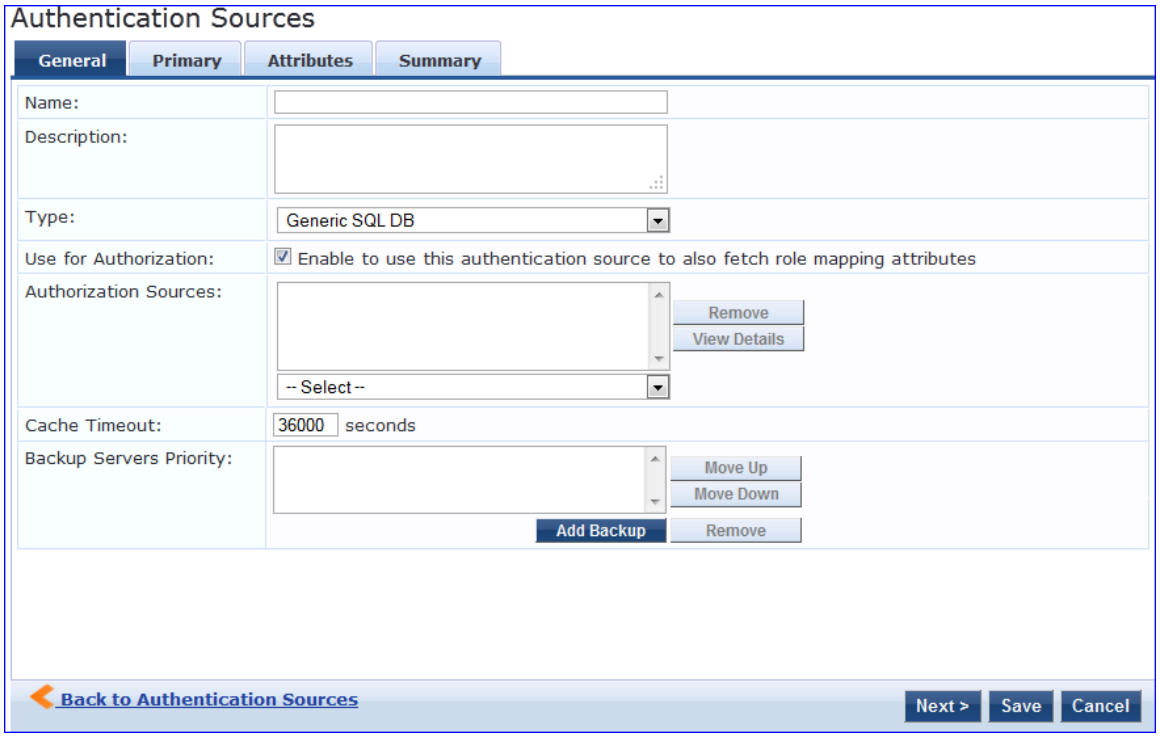


Table 88: *General SQL DB - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select **Generic SQL DB**.
Use for Authorization	Enable this option to request Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This check box is enabled by default.

Table 88: *General SQL DB - General tab Parameters (Continued)*

Parameter	Description
Authorization Sources	Specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop-down list and click **Add** to add to the list of authorization sources. Click **Remove** to remove the authorization source from the list. If Policy Manager authenticates the user or device from this authentication source, then Policy Manager also fetches role mapping attributes from these additional authorization sources. **NOTE:** As described in Services on page 79, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the time period for which the attributes are cached.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure shows an example of the **General SQL DB - Primary** tab followed by parameter definition:

Figure 130: *General SQL DB - Primary Tab*

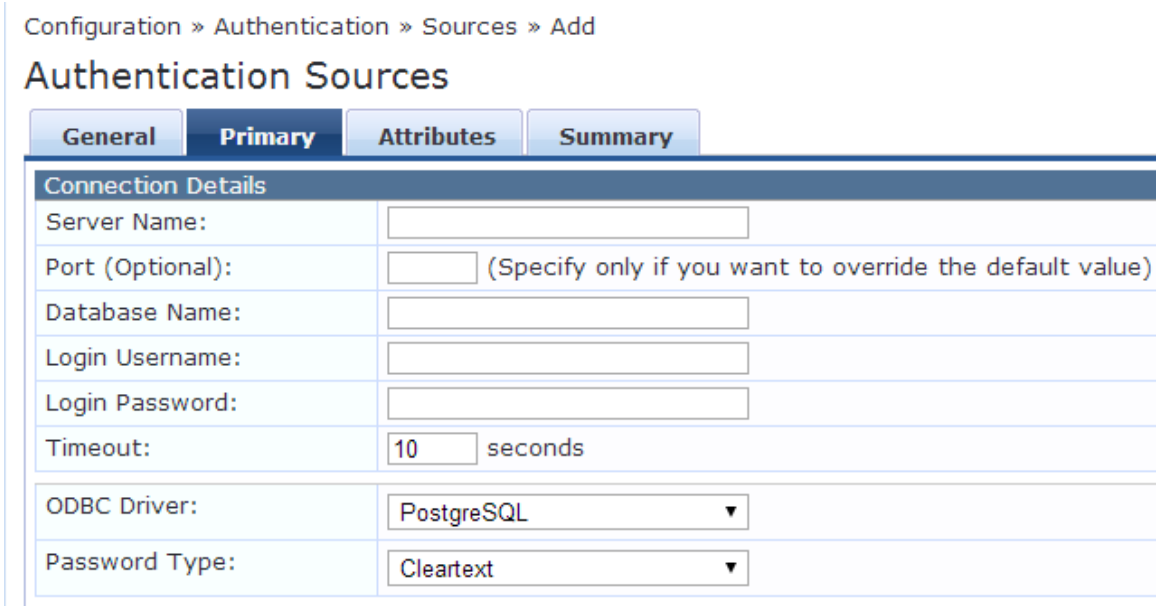


Table 89: *Generic SQL DB - Primary tab Parameters*

Parameter	Description
Server Name	Enter the hostname or IP address of the database server.
Port (Optional)	Specify a port value to override the default port.
Database Name	Enter the name of the database from which records can be retrieved.
Login Username	Enter the name of the user used to log into the database. This account must have read access to all the attributes that need to be retrieved by the specified filters.
Password	Enter the password for the user account entered in the **Login Username** field.
Timeout	Enter the duration in seconds that Policy Manager waits before attempting to fail over from primary to the backup servers (in the order in which they are configured).
ODBC Driver	Select the ODBC driver (Postgres, Oracle11g, or MSSQL) to connect to the database. **NOTE:** MySQL is supported in versions 6.0 and later. Dell does not ship MySQL drivers by default. If you require MySQL, contact Dell support at dell.com/support to get the required patch. This patch does not persist across upgrades. If you are using MySQL, you should contact support before upgrading.
Password Type	Set the type of user password stored in the database to one of the following: • Cleartext • NT Hash • LM Hash • SHA • SHA256

Attributes Tab

The **Attributes** tab defines the SQL DB query filters and the attributes to be fetched by using those filters. The following figure shows an example of the **Generic SQL DB - Attributes** tab followed by parameter definition:

Figure 131: *Generic SQL DB - Attributes Tab*

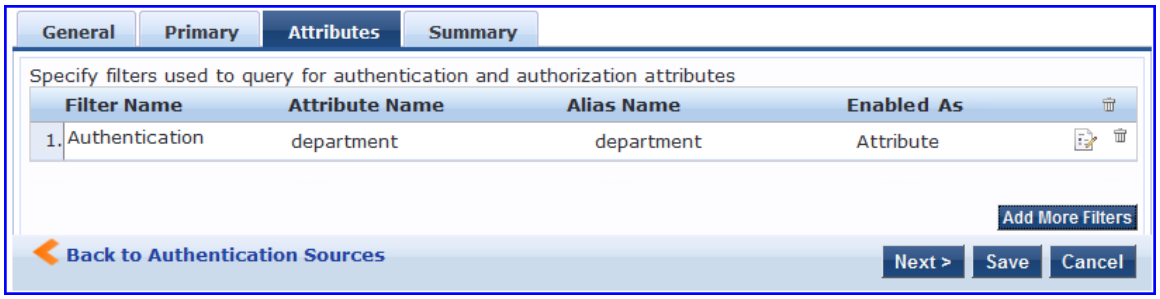


Table 90: *Generic SQL DB - Attributes tab (Filter List) Parameters*

Tab	Parameter/Description
Filter Name	Specifies the name of the filter.
Attribute Name	Specifies the name of the SQL DB attributes defined for this filter.
Alias Name	Specifies an alias name for each attribute name selected for the filter.
Enabled As	Indicates whether the filter is enabled as a role or attribute type. This can also be blank.
Add More Filters	Click this button to open the **Configure Filter** page. Refer to Add More Filters on page 173.

Add More Filters

The **Configure Filter** page defines a filter query and the related attributes to be fetched from the SQL DB store. The following figure displays the **Generic SQL DB - Configure Filter** page followed by parameter definition:

Figure 132: *Generic SQL DB - Configure Filter Page*

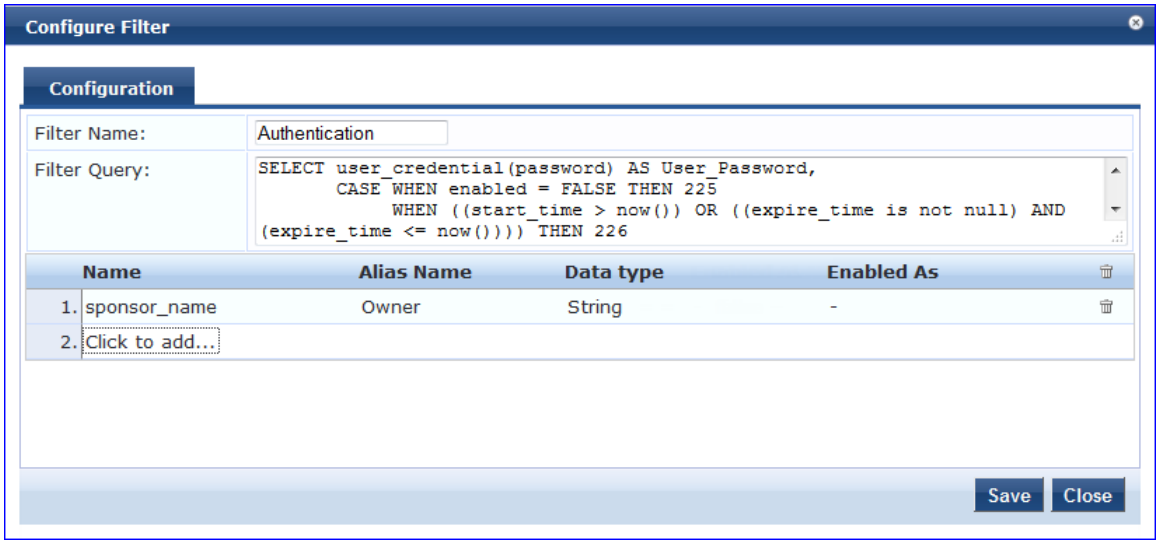


Table 91: *Generic SQL DB Configure Filter Page Parameters*

Parameter	Description
Filter Name	Enter the name of the filter.
Filter Query	Specifies an SQL query to fetch the attributes from the user or device record in DB.
Name	Specifies the name of the attribute.

Parameter	Description
Alias Name	Specifies the name for the attribute. By default, this is the same as the attribute name.
Data Type	Specify the data type for this attribute such as String, Integer, and Boolean.
Enabled As	Specify whether this value is to be used directly as a role or attribute in an Enforcement Policy. This bypasses the step of having to assign a role in Policy Manager through a Role Mapping Policy.

Summary Tab

You can use the **Summary** tab to view configured parameters.

HTTP

The HTTP authentication source relies on the GET method to retrieve information. The client submits a request, and then the server returns a response. All request parameters are included in the URL. For example:

URL: https//hostname/webservice/.../%{Auth:Username}?param1=%{...}&param2=value2

HTTP relies on the assumption that the connection between the client and server computers is secure and can be trusted.

You configure primary and backup servers, session details, filter query, and role mapping attributes to fetch HTTP authentication sources on the following tabs:

- General Tab on page 174
- Primary Tab on page 176
- Attributes Tab on page 177
- Summary Tab

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure shows an example of the **HTTP - General** tab followed by parameter definition:

Figure 133: *HTTP - General Tab*

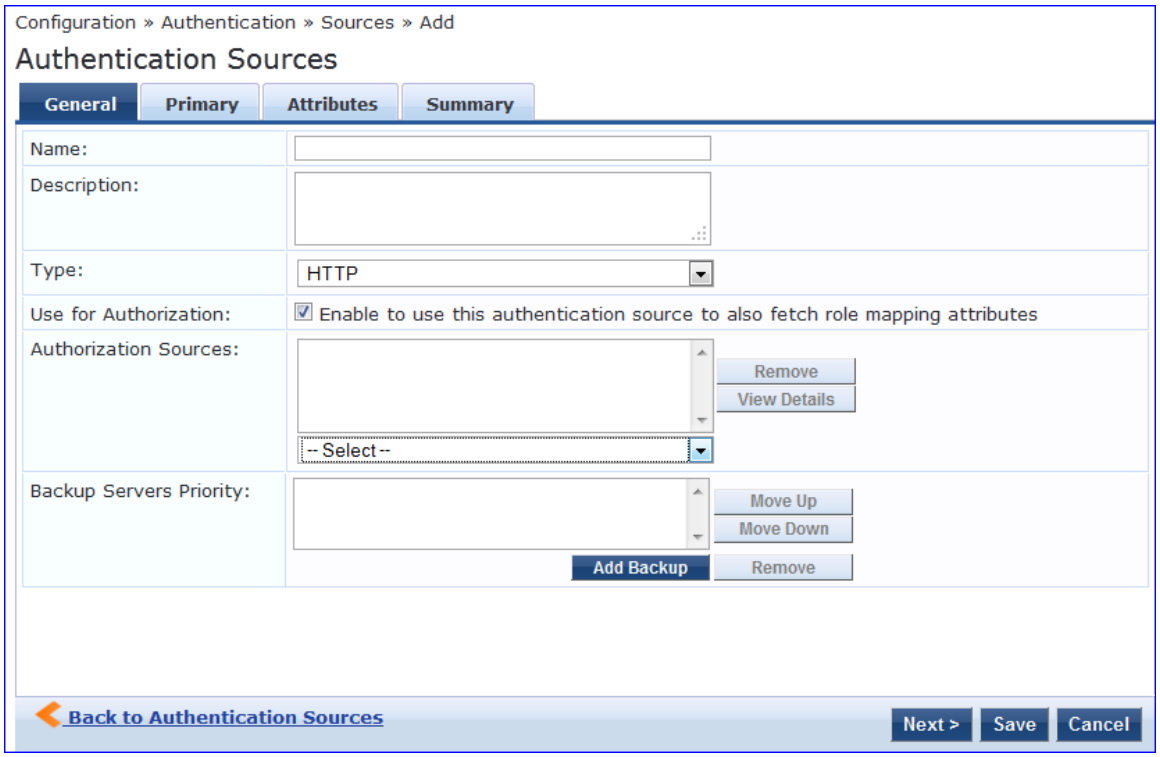


Table 92: *HTTP - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select **HTTP**.

Table 92: *HTTP - General tab Parameters (Continued)*

Parameter	Description
Use for Authorization	Enable this option to request Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This check box is enabled by default.
Authorization Sources	Specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop-down list and click **Add** to add it to the list of authorization sources. Click **Remove** to remove rhe selected additional resource from the list. If Policy Manager authenticates the user or device from this authentication source, then also fetches role mapping attributes from these additional authorization sources. **NOTE:** As described in Services on page 79, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields applicable for primary server specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure shows an example of the **HTTP - Primary** tab followed by parameter definition:

Figure 134: *HTTP - Primary Tab*

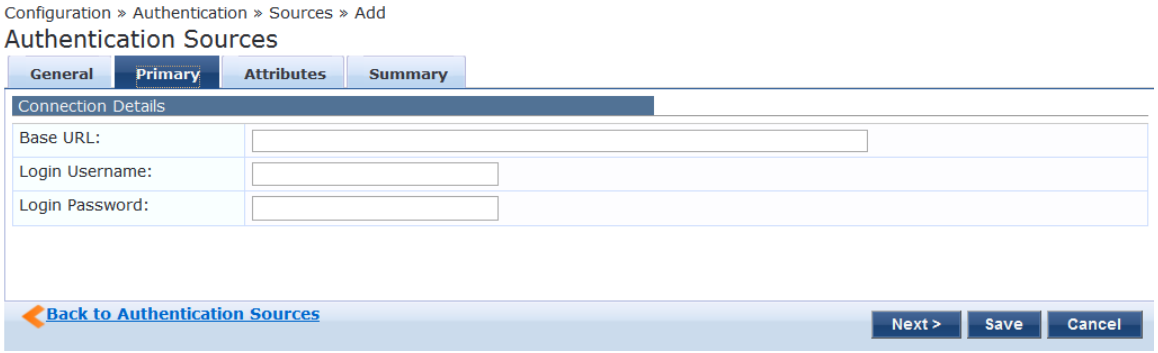


Table 93: *HTTP - Primary tab Parameters*

Parameter	Description
Base URL	Enter the base URL(host name) or IP address of the HTTP server. For example, http://<hostname> or <fully-qualified domain name>:xxxx, where xxxx is the port to access the HTTP Server.
Login Username	Enter the name of the user used to log into the database. This account must have read access to all the attributes that need to be retrieved by the specified filters.
Password	Enter the password for the user account entered in the **Login Username** field.

Attributes Tab

The **Attributes** tab defines the HTTP query filters and the attributes to be fetched by using those filters.

Figure 135: *HTTP - Attributes Tab*

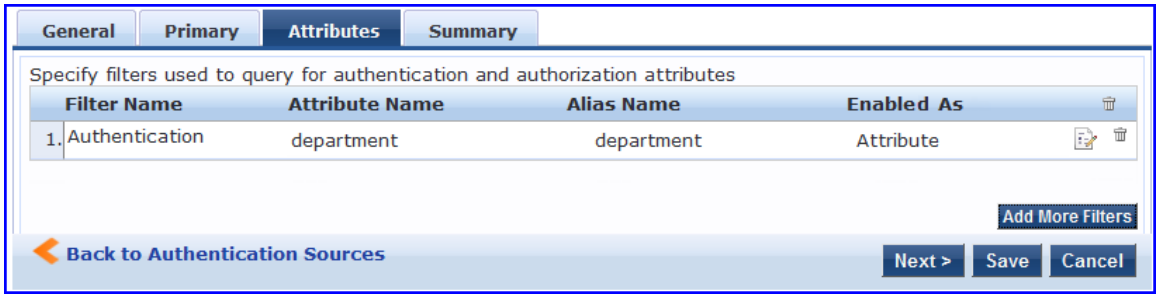


Table 94: *HTTP - Attributes tab (Filter List) Parameters*

Tab	Parameter/Description
Filter Name	Displays the name of the filter.
Attribute Name	Specifies the name of the SQL DB attributes defined for this filter.
Alias Name	Specifies the name of an alias name for each attribute name selected for the filter.
Enabled As	Indicates whether an attribute is enabled as a role.
Add More Filters	Opens the **Configure Filter** page. For more information, see Add More Filters on page 177.

Add More Filters

The **Configure Filter** page defines a filter query and the related attributes to be fetched from the SQL DB store. The following figure shows an example of the **HTTP Filter Configure** page followed by parameter definition:

Figure 136: *HTTP Filter Configure Page*

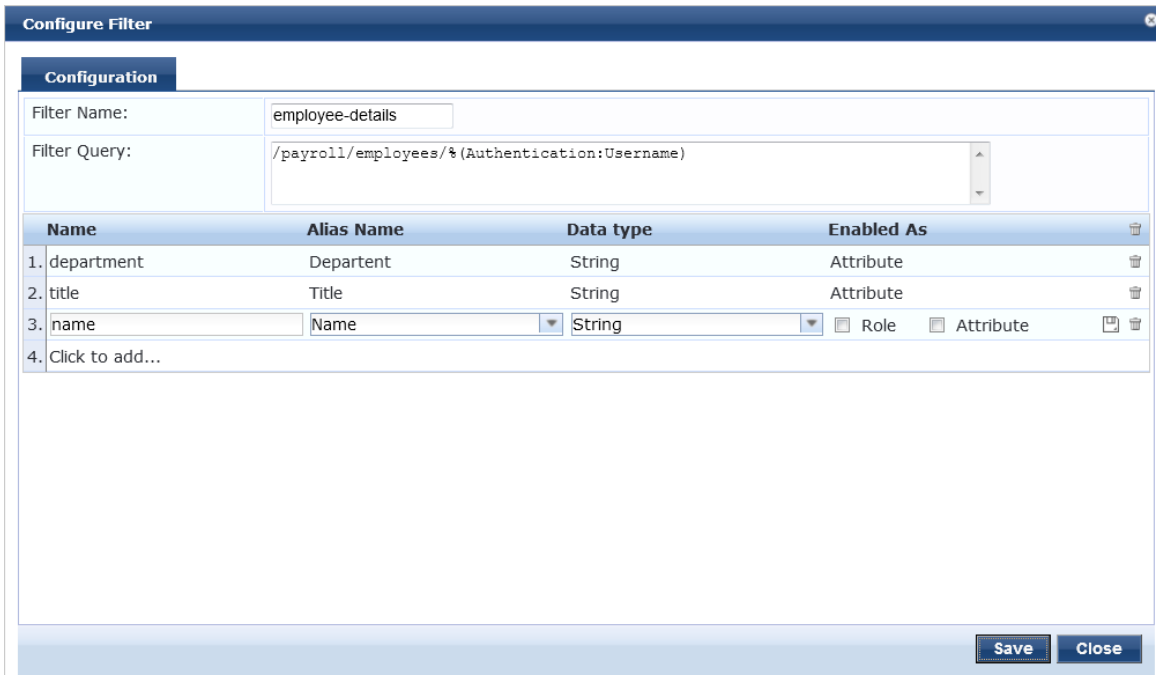


Table 95: *HTTP Configure Filter Page Parameters*

Parameter	Description
Filter Name	Displays the name of the selected filter.
Filter Query	Specifies the HTTP path (without the server name) to fetch the attributes from the HTTP server. For example, if the full path name to the filter is http server URL = http://<hostname or fqdn>:xxxx/abc/def/xyz, you enter /abc/def/xyz.
Name	Specifies the name of the attribute.
Alias Name	Specifies the alias name for the attribute. By default, this is the same as the attribute name.
Data Type	Specifies the data type for this attribute such as String, Integer, and Boolean,
Enabled As	Specify whether the value to be used directly as a role or attribute in an Enforcement Policy. This bypasses the step of assigning a role in Policy Manager through a Role Mapping Policy.

Summary Tab

You can use the **Summary** tab to view configured parameters.

Kerberos

Policy Manager can perform standard PAP/GTC or tunneled PAP/GTC (for example, EAP-PEAP[EAP-GTC]) authentication against any Kerberos 5 compliant server such as Microsoft Active Directory server. It is mandatory to pair this source type with an authorization source (identity store) containing user records.

You can configure Kerberos authentication sources on the following tabs:

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure shows an example of the **Kerberos - General** tab followed by parameter definition:

Figure 137: *Kerberos - General Tab*

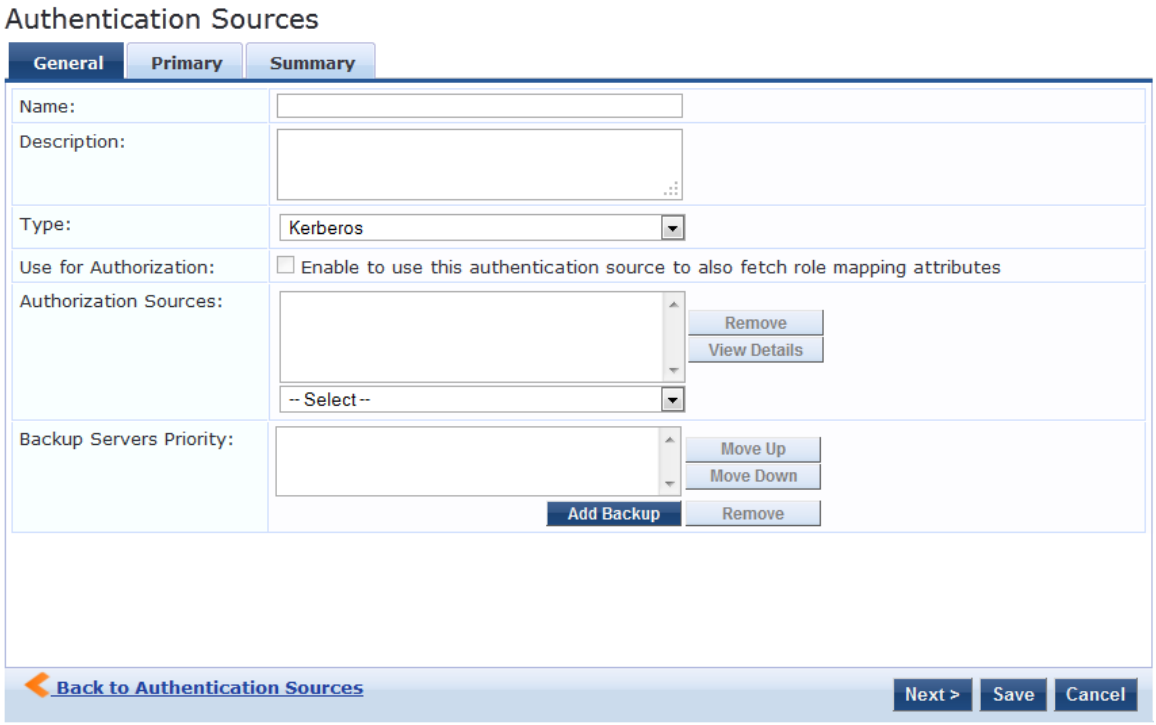


Table 96: *Kerberos - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select **Kerberos**.

Table 96: *Kerberos - General tab Parameters (Continued)*

Parameter	Description
Use for Authorization	Disable in this context.
Authorization Sources	Specify one or more authorization sources from which role mapping attributes to be fetched. Select a previously configured authentication source from the drop-down list and click **Add** to add it to the list of authorization sources. Click **Remove** to remove the selected authentication source from the list. **NOTE:** As described in Services on page 79, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes iirespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup kerberos server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields applicable for primary server specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure shows an example of the **Kerberos - Primary** tab followed by parameter definition:

Figure 138: *Kerberos - Primary Tab*

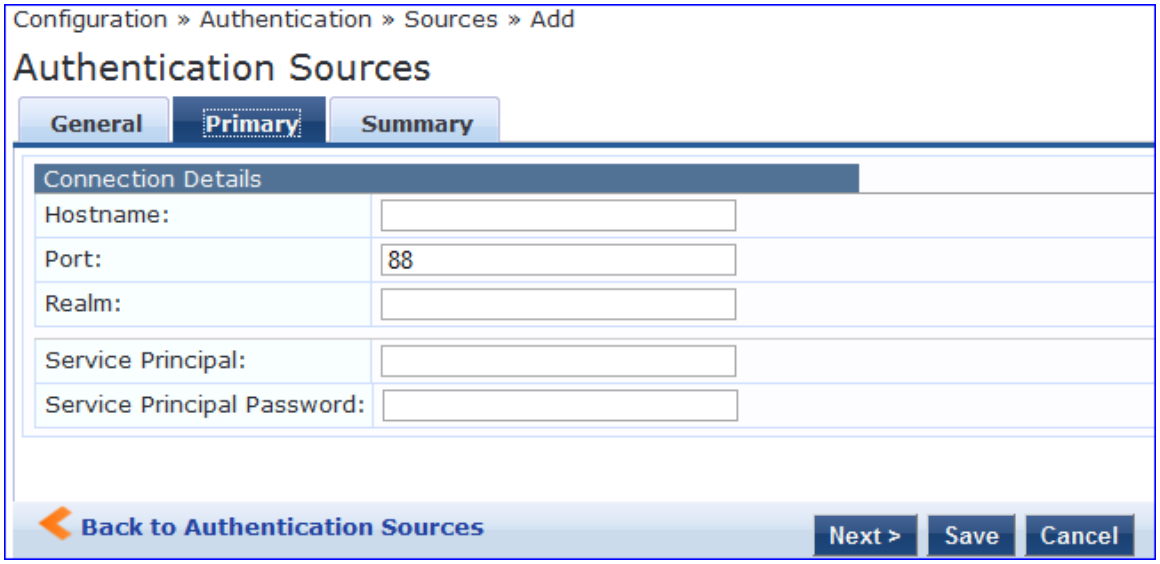


Table 97: *Kerberos - Primary tab Parameters*

Parameter	Description
Hostname	Specify the name of the host or the IP address of the kerberos server.
Port	Specify the port at which the token server listens for kerberos connections. The default port is 88.
Realm	Specify the domain of authentication. In the case, specify **Kerberos** domain.
Service Principal Name	Enter the identity of the service principal as configured in the Kerberos server.
Service Principal Password	Enter the password for the service principal.

Summary Tab

You can use the **Summary** tab to view configured parameters.

Okta

You can use Okta as an authentication source only for servers of the type Dell Application Authentication. Configure Okta authentication sources on the following tabs:

- General Tab on page 181
- Primary Tab on page 183
- Attributes Tab on page 183
- Summary Tab

Click the **Summary** tab to view configured parameters.

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure shows an example of the **Okta - General** tab followed by parameter definition:

Figure 139: *Okta - General Tab*

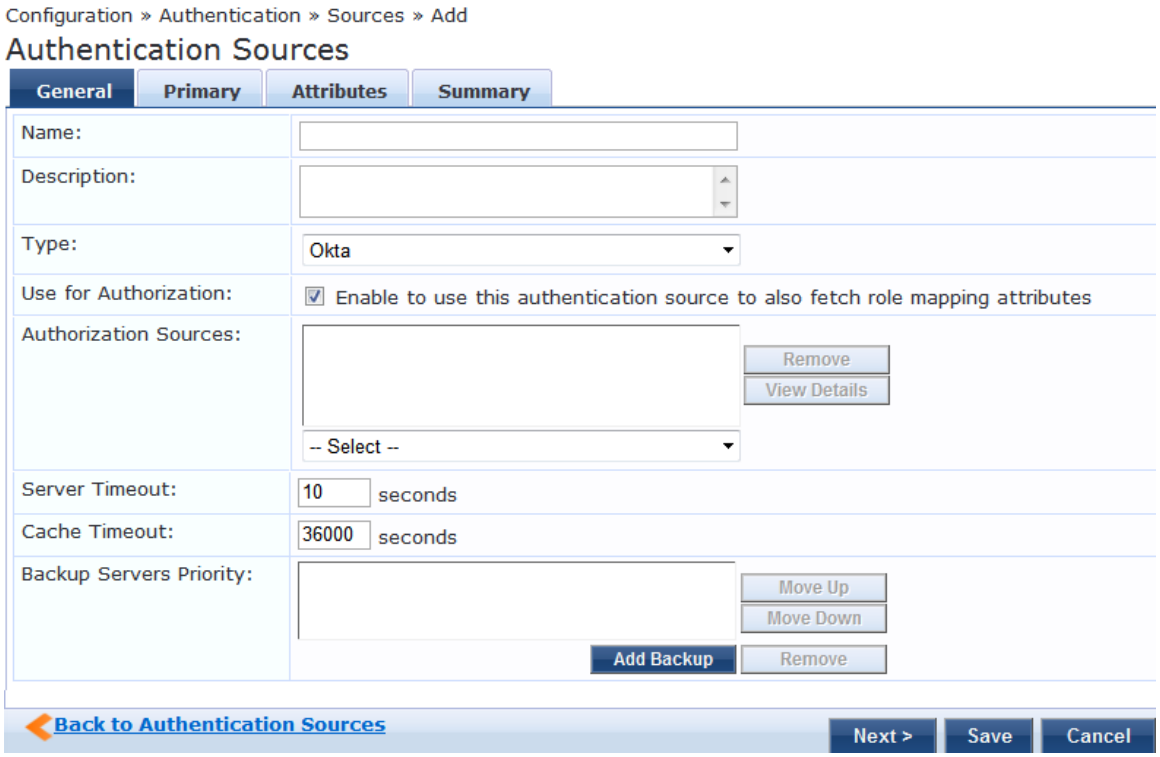


Table 98: *Okta - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select **Okta**.
Use for Authorization	Enable this check box to request Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This check box is enabled by default.

Table 98: *Okta - General tab Parameters (Continued)*

Parameter	Description
Server Timeout	Specify the duration in number of seconds that Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the duration in number of seconds that Policy Manager waits before attempting to fail over from the primary to the backup servers in the order in which they are configured.
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.
Backup Servers Priority	Click **Add Backup** to add a backup server. From the **Backup 1** tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure shows an example of the **Okta - Primary** tab followed by parameter definition:

Figure 140: *Okta - Primary Tab*

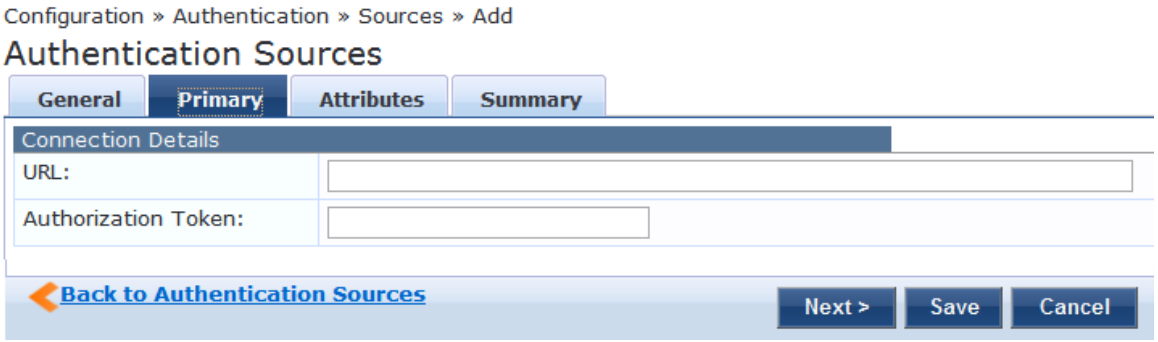


Table 99: *Okta - Primary tab Parameters*

Parameter	Description
Connection Details	
URL	Enter the address of the OKTA server.
Authorization Token	Enter the authorization token provided by Okta support.

Attributes Tab

The **Attributes** tab defines the Okta query filters and the attributes to be fetched by using those filters. The following figure shows an example of the **Okta - Attributes** tab followed by parameter definition:

Figure 141: *Okta - Attributes Tab*

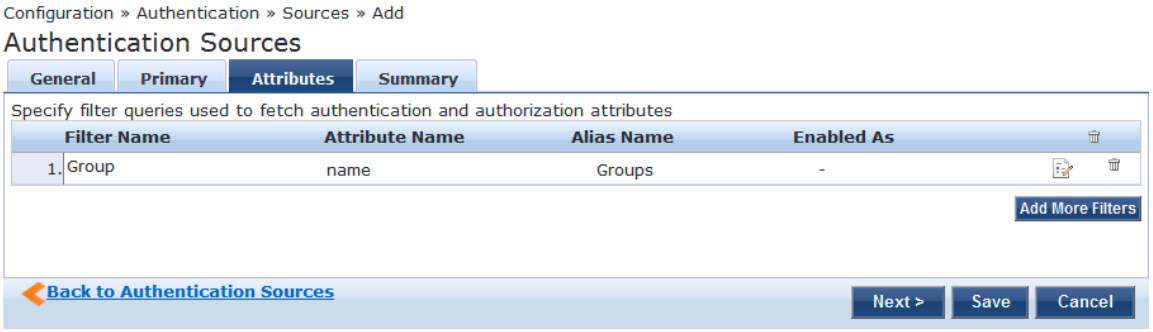


Table 100: *Okta - Attributes tab Parameters*

Tab	Parameter/Description
Filter Name	Displays the name of the filter. **NOTE:** You can configure only **Group** for Okta.
Attribute Name	Specifies the name of the LDAP/AD attributes defined for this filter.
Alias Name	Specifies the alias name for each attribute name selected for the filter.
Enable As	Specifies whether value is to be used directly as a role or attribute in an Enforcement Policy. This bypasses the step of assigning a role in Policy Manager through a Role Mapping Policy.
Add More Filters	Click this button to open the **Configure Filter** page. Refer to Add More Filters on page 184.

Add More Filters

The **Configure Filter** page defines a filter query and the related attributes to be fetched from the SQL DB store. The following figure shows an example of the **Okta - Configure Filter** page followed by parameter definition:

Figure 142: *Okta - Configure Filter Page*

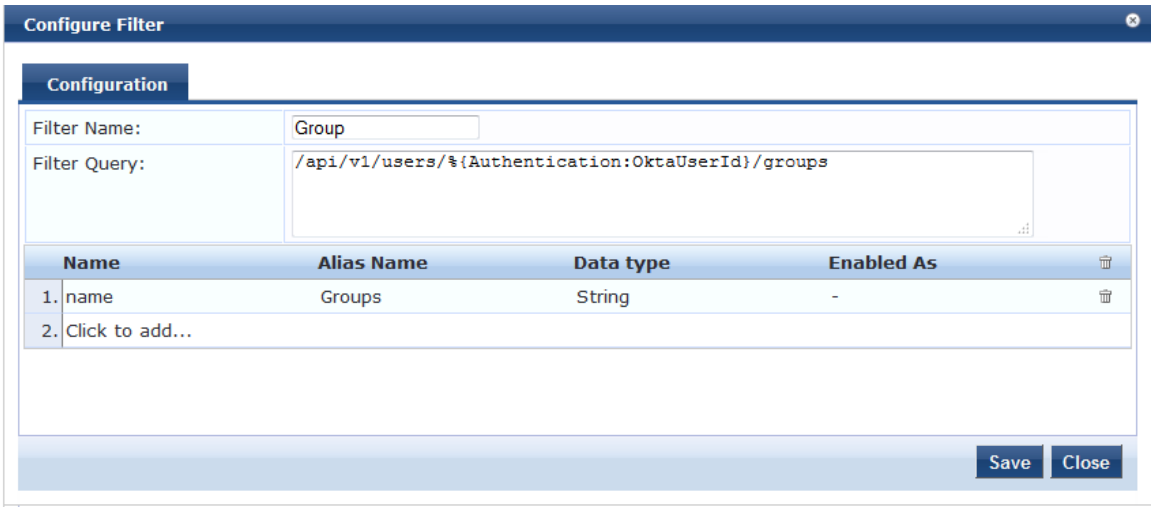


Table 101: *Okta Configure Filter Page*

Parameter	Description
Filter Name	Enter the name of the filter.
Filter Query	Specifies an SQL query to fetch attributes from the user or device record in DB.
Name	Displays the name of the attribute.
Alias Name	Specifies an alias name for the attribute. By default, this is the same as the attribute name.
Data Type	Specifies the data type for this attribute such as String, Integer, and Boolean.
Enabled As	Specify whether this value is to be used directly as a role or attribute in an Enforcement Policy. This bypasses the step of having to assign a role in Policy Manager through a Role Mapping Policy.

Summary Tab

You can use the **Summary** tab to view configured parameters.

Static Host List

An internal relational database stores the Policy Manager configuration data and locally configured user and device accounts. The following three pre-defined authentication sources represent the three databases used to store local users, guest users, and registered devices respectively:

- [Local User Repository]
- [Guest User Repository]
- [Guest Device Repository]

While regular users reside in an authentication source such as Active Directory (or in other LDAP-compliant stores), you can configure the temporary users including guest users in the Policy Manager local repositories. For a user account created in the local database, the role is statically assigned to that account. This means you do not need to specify a role mapping policy for user accounts in the local database. However, if new custom

attributes are assigned to a user (local or guest) account in the local database, these can be used in role mapping policies.

The local user database is pre-configured with a filter to retrieve the password and the expiry time for the account. Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against the local database.

You configure primary and backup servers, session details, and the list of static hosts for **Static Host List** authentication sources on the following tabs:

- General Tab on page 186
- Static Host Lists Tab on page 186
- Summary Tab

General Tab

The **General** tab labels the authentication source. The following figure shows an example of the **Static Host List - General** tab followed by parameter definition:

Figure 143: *Static Host List - General Tab*

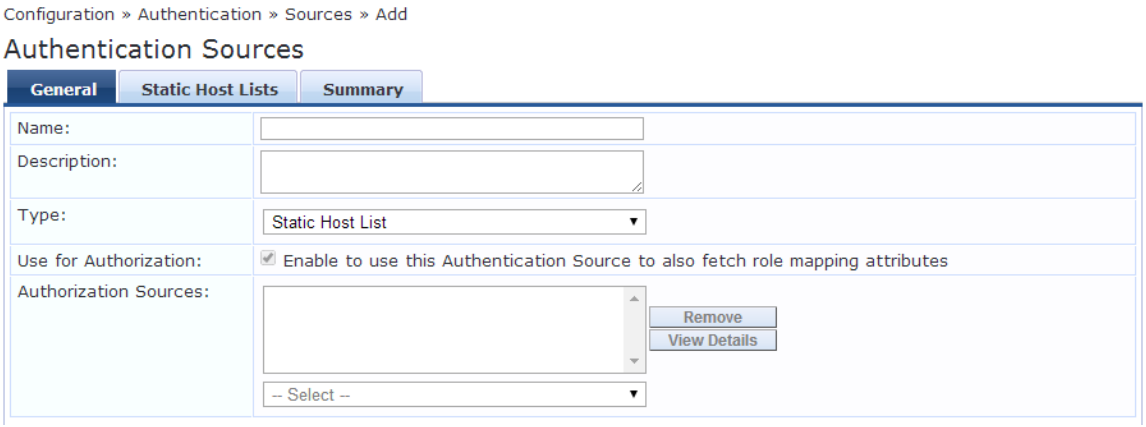


Table 102: *Static Host List - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of authentication. In this context, select **Static Host List**.
Use for Authorization	This option is not configurable.
Authorization Sources	This option is not configurable.

Static Host Lists Tab

The **Static Hosts List** tab defines the list of static hosts to be included as part of the authorization source. The following figure shows an example of the **Static Host List - Static Host Lists** tab followed by parameter definition:

Figure 144: *Static Host List - Static Host Lists Tab*

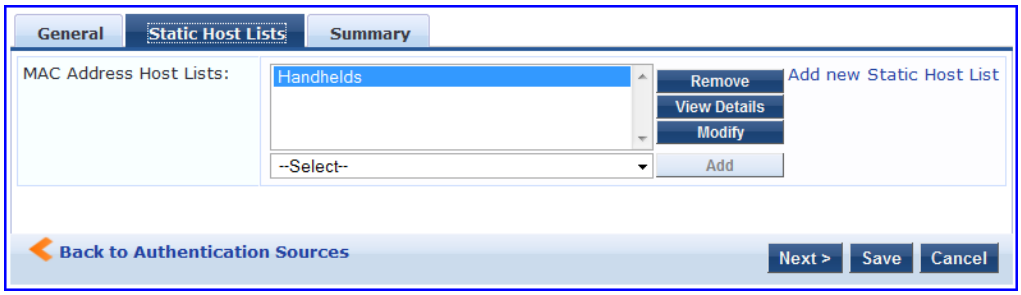


Table 103: *Static Hosts List - Static Host Lists tab Parameters*

Parameter	Description
MAC Address Host Lists	Select a Static Host List from the drop-down list and click **Add** to add it to the list. Click **Remove** to remove the selected static host list. Click on **View Details** to view the contents of the selected static host list. Click on **Modify** to modify the selected static host list.

Only Static Host Lists of type MAC Address List or MAC Address Regular Expression can be configured as authentication sources. Refer to Adding and Modifying Static Host Lists on page 200 for more information.

Summary Tab

You can use the **Summary** tab to view configured parameters.

Token Server

Policy Manager can perform GTC authentication against any token server than can authenticate users by acting as a RADIUS server (for example, RSA SecurID Token Server) and can authenticate users against a token server and fetch role mapping attributes from any other configured Authorization Source.

Pair this source type with an authorization source (identity store) containing user records. When using a token server as an authentication source, use the administrative interface to optionally configure a separate authorization server. Policy Manager can also use the RADIUS attributes returned from a token server to create role mapping policies. For more information, see Namespaces on page 513.

You configure primary and backup servers, session details, and the filter query and role mapping attributes to fetch for Token Server authentication sources on the following tabs:

- General Tab on page 187
- Primary Tab on page 189
- Attributes Tab on page 190

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure shows an example of the **Token Server - General** tab followed by parameter definition:

Figure 145: *Token Server - General Tab*

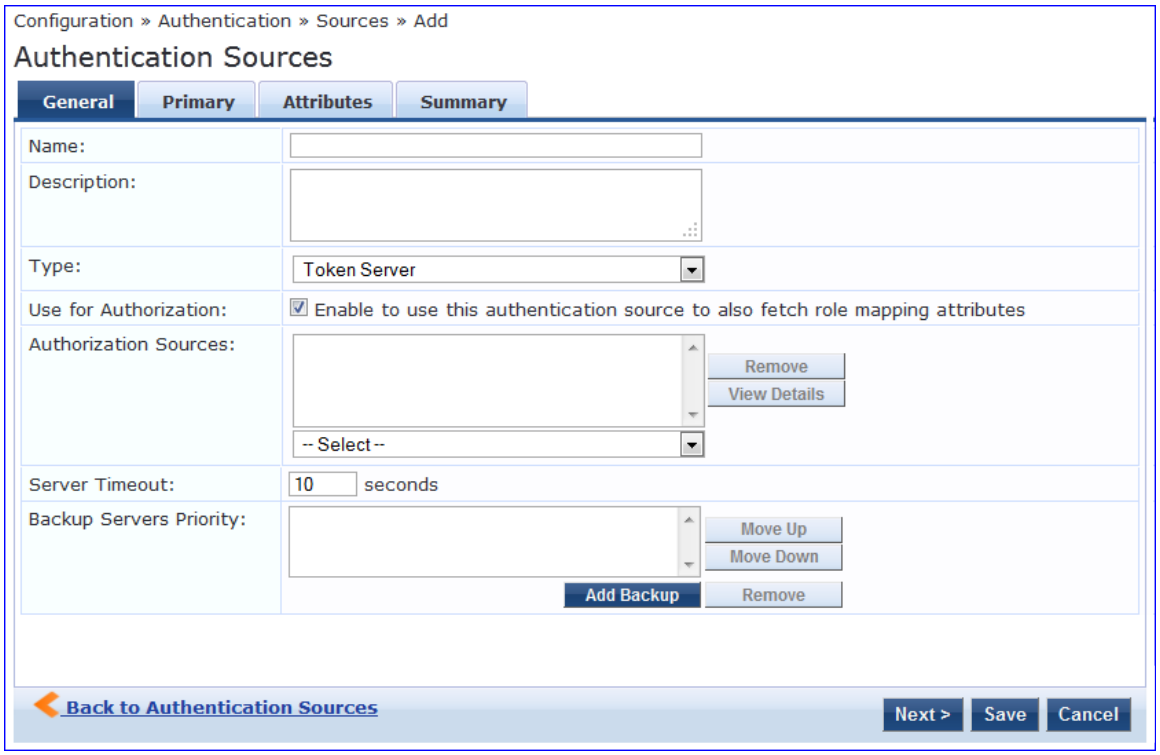


Table 104: *Token Server - General tab Parameters*

Parameter	Description
Name	Specify the label of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of authentication. In this context, select **Token Server**.
Use for Authorization	Enable this check box to instruct Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This check box is enabled by default

Table 104: *Token Server - General tab Parameters (Continued)*

Parameter	Description
Authorization Sources	Specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop-down list, and click **Add** to add it to the list of authorization sources. Click **Remove** to remove it from the list. If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources. **NOTE:** As described in Services on page 79, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Server Timeout	Specify the duration in seconds that Policy Manager waits before attempting to fail over from primary to the backup servers (in the order in which they are configured).
Backup Servers Priority	To add a backup server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** Tab defines the settings for the primary server. The following figure shows an example of the **Token Server - Primary** tab followed by parameter definition:

Figure 146: *Token Server - Primary Tab*

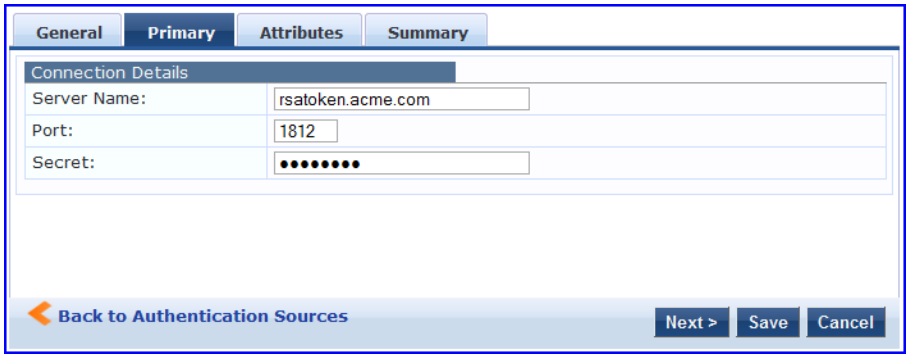


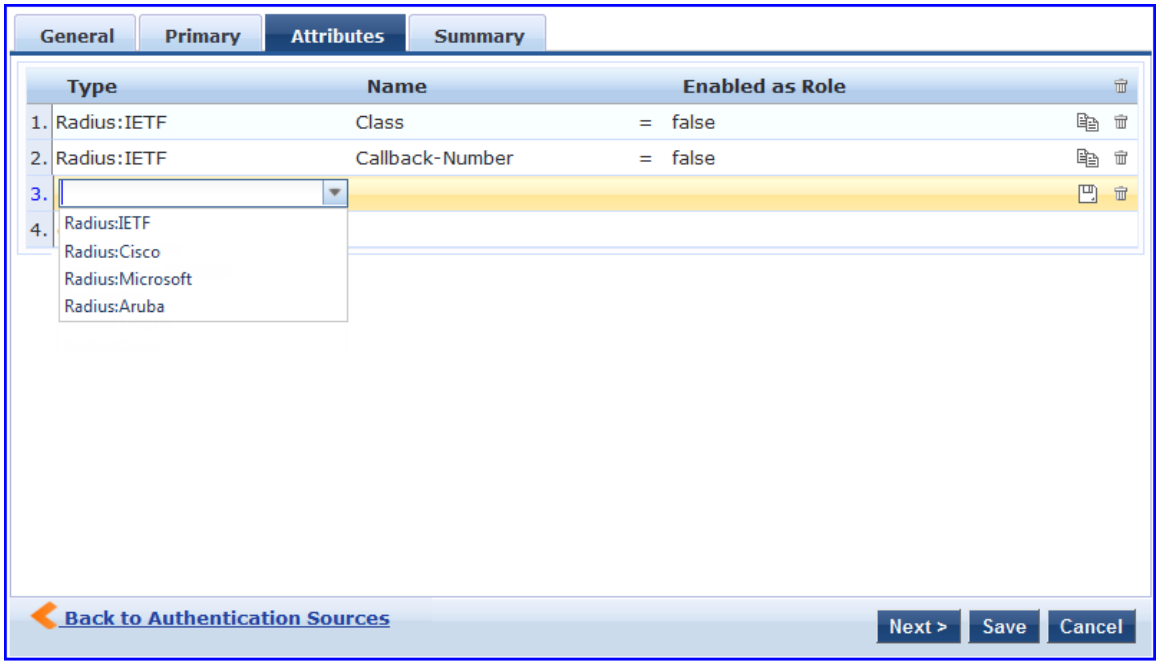
Table 105: *Token Server - Primary tab Parameters*

Parameter	Description
Server Name	Displays the host name or the IP address of the token server,
Port	Specifies the UDP port at which the token server listens for RADIUS connections. The default port is 1812.
Secret	Specify the RADIUS shared secret to connect to the token server.

Attributes Tab

The **Attributes** tab defines the RADIUS attributes to be fetched from the token server. These attributes can be used in role mapping policies. Policy Manager loads all RADIUS vendor dictionaries in the **Type** drop-down list to help select the attributes. The following figure shows an example of the **Token Server - Attributes** tab followed by parameter definition:

Figure 147: *Token Server - Attributes Tab*



See Configuring a Role and Role Mapping Policy on page 202 for more information.

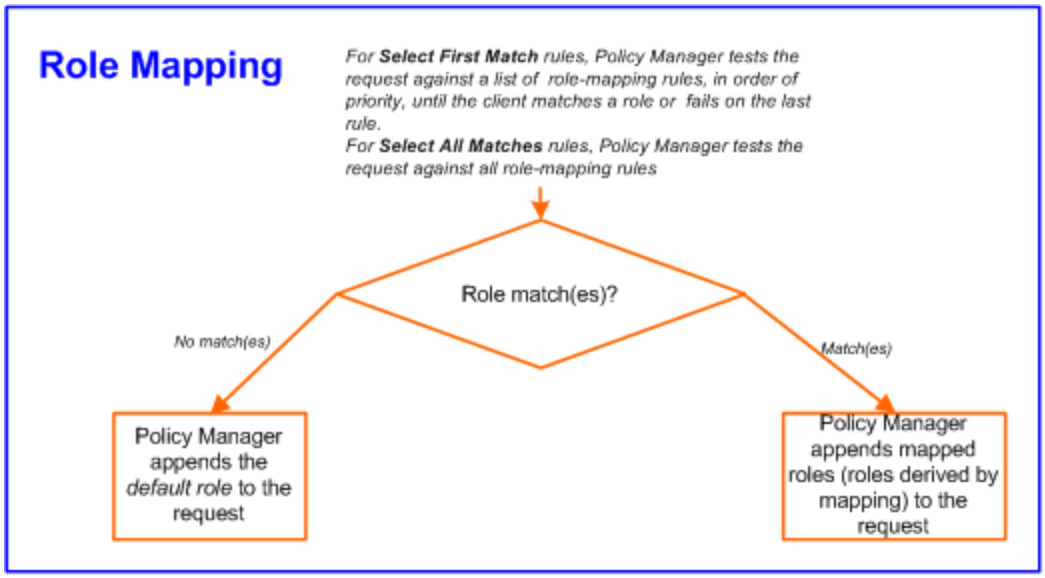
Table 106: *Token Server - Attribute tab Parameters*

Parameter	Description
Type	Select the type of authentication source from the drop-down list.
Name	Specifies the name of the Token Server attributes.
Enabled as Role	Specifies whether value is to be used directly as a role or attribute in an Enforcement Policy. This bypasses the step of assigning a role in Policy Manager through a Role Mapping Policy.

Roles can range in complexity from a simple user group (e.g., Finance, Engineering, or Human Resources) to a combination of a user group with some dynamic constraints (e.g., "San Jose Night Shift Worker"- An employee in the Engineering department who logs in through the San Jose network device between 8 PM and 5 AM on weekdays). It can also apply to a list of users.

A Role Mapping Policy reduces client (user or device) identity or attributes associated with the request to *Role(s)* for Enforcement Policy evaluation. The roles ultimately determine differentiated access.

Figure 148: *Role Mapping Process*



A role can be:

- Authenticated through predefined Single Sign-On rules.
- Associated directly with a user in the Policy Manager *local user* database.
- Authenticated based on predefined allowed endpoints.
- Associated directly with a *static host list*, again through *role mapping*.
- Discovered by Policy Manager through *role mapping*. Roles are typically discovered by Policy Manager by retrieving attributes from the *authentication source*. *Filter rules* associated with the authentication source tell Policy Manager where to retrieve these attributes.
- Assigned automatically when retrieving attributes from the *authentication source*. Any attribute in the authentication source can be mapped directly to a role.

For more information, see:

- Configuring Single Sign-On, Local Users, Endpoints, and Static Host Lists on page 192
- Configuring a Role and Role Mapping Policy on page 202

Configuring Single Sign-On, Local Users, Endpoints, and Static Host Lists

The internal Policy Manager database (*[Local User Repository]*, *[Guest User Repository]*) supports storage of user records, when a particular class of users is not present in a central user repository (e.g., neither *Active Directory* nor other database); by way of an example of such a class of users, guest or contractor records can be stored in the local user repository.

To authenticate local users from a particular service, include [Local User Repository] among the Authentication Sources.

The **Single Sign-On** page allows you to enable access for Insight, Guest, and/or Policy Manager using a trusted IdP certificate. The **Local Users** page configures role-based access for individual users. The **Endpoints** page lists the endpoints that have authenticated requests to Policy Manager. These entries are automatically populated from the 802.1X, MAC-based, and Web authentication and processed by Policy Manager. These can be further modified to add tags, known/unknown, disabled status. A **Static Host List** comprises of a list of MAC and IP addresses. These can be used as whitelists or blacklists to control access to the network. For more information, see:

- Configuring Single Sign-On on page 192
- Adding and Modifying Local Users on page 193
- Adding and Modifying Endpoints on page 195
- Adding and Modifying Static Host Lists on page 200

Configuring Single Sign-On

Single Sign-On (SSO) allows ClearPass users to access the Policy Manager, Guest, and Insight applications without re-authenticating after they have signed in to one of the applications. ClearPass provides SSO support through Security Assertion Markup Language (SAML). ClearPass allows you to create trusted relationships between Service Provider (SP) and Identity Provider (IdP).

Perform the following steps to configure and enable SSO.

1. Go to **Configuration > Identity > Single Sign-On**.
2. The Service **SAML SP Configuration** tab, enter the IdP Single sign-on URL.
3. In the **Enable SSO for** section, select the checkbox for the application(s) you want users to access with single sign-on.
4. To do a certificate comparison, select the IdP Certificate from the **Select Certificate** drop-down list. For example, the image below uses a trusted EMAILADDRESS certificate.

The list of IdP Certificates includes all of those that are enabled on the **Administration > Certificates > Trust List** page. Refer to Certificate Trust List on page 447 for more information.

5. Navigate to the **SAML IdP Configuration** tab.
6. To download IdP metadata for a specific IdP, enter the name of the IdP portal and then click the **Download** button.
7. To configure an SAML service provider, click the **Add SP metadata** button.
8. Specify the name of the service provider, browse to locate the metadata file, and click **Upload**.
9. Click **Save**.

Figure 149: *Single Sign-On - SAML SP Configuration tab*

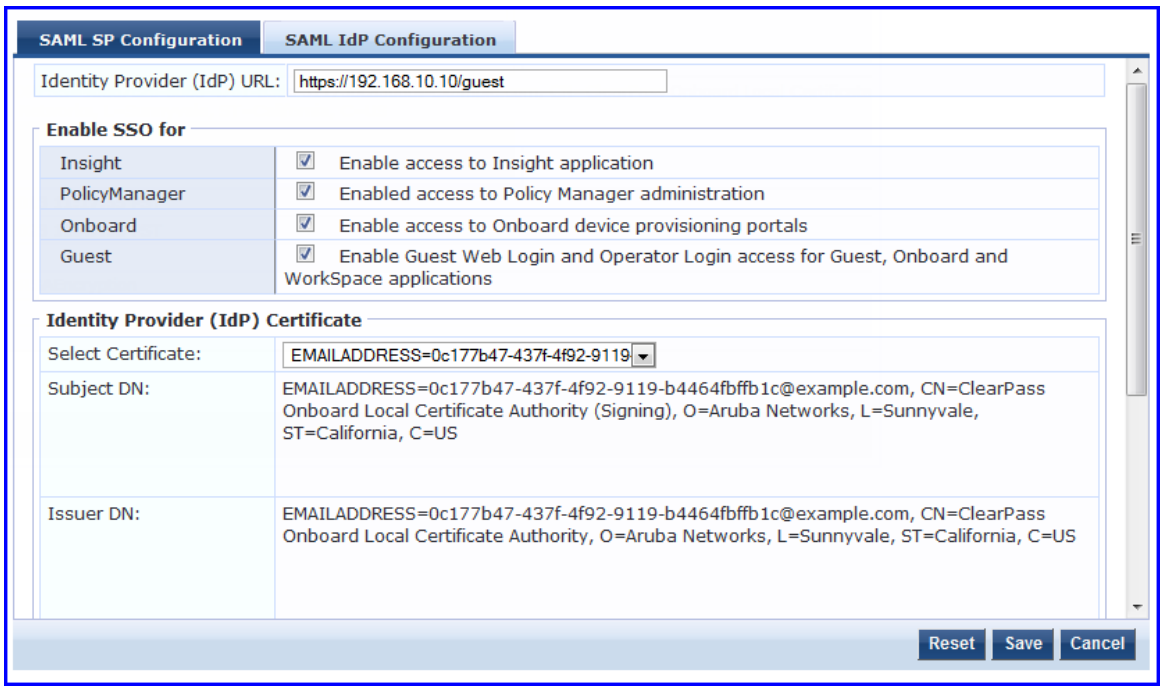
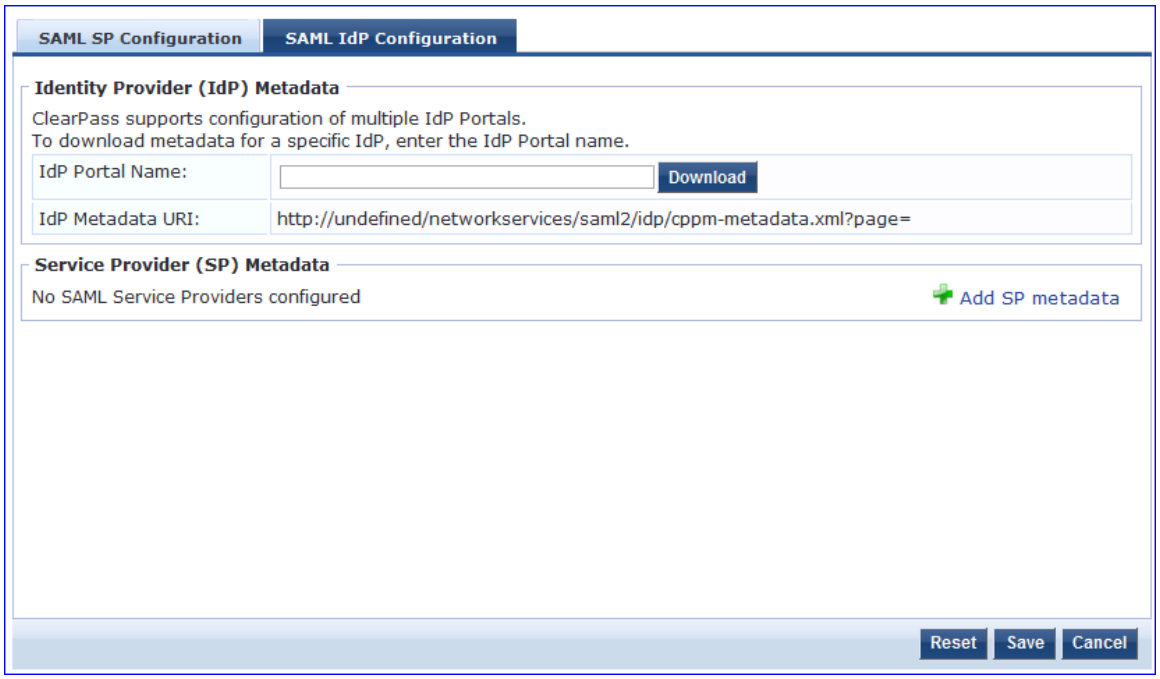


Figure 150: *Single Sign-On SAML IdP Configuration tab*



Adding and Modifying Local Users

Policy Manager lists all local users in the **Configuration > Identity > Local Users** page. To add a local user, click **Add** to display the **Add Local User** popup.

- To edit a local user, in the Local Users listing page, click on the name to display the **Edit Local User** popup.
- To delete a local user, in the Local Users listing page, select it (via the check box) and click **Delete**.
- To export a local user, in the Local Users listing page, select it (via the check box) and click **Export**.
- To export ALL local users, in the Local Users listing page, click **Export All**.

- To import local users, in the Local Users listing page, click **Import**.

For more information, see the following figures and parameter definition table.

Figure 151: *Local Users Listing*

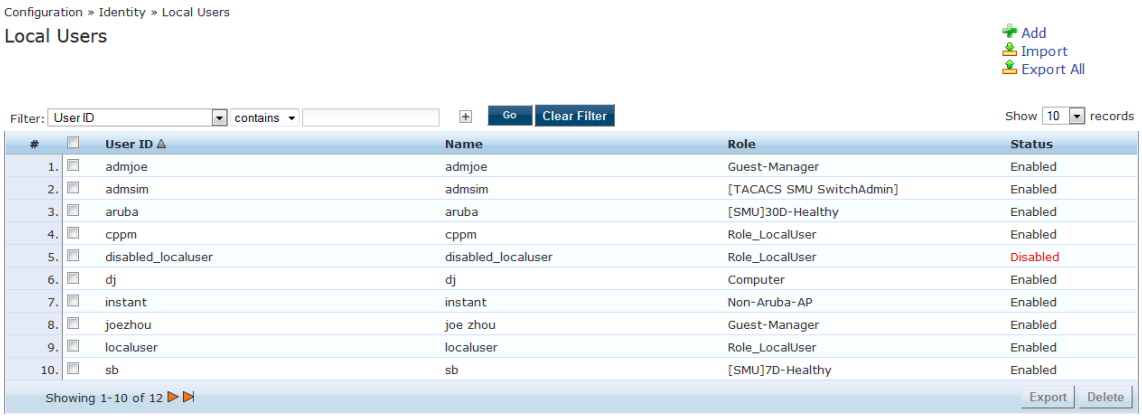


Figure 152: *Add Local User page*

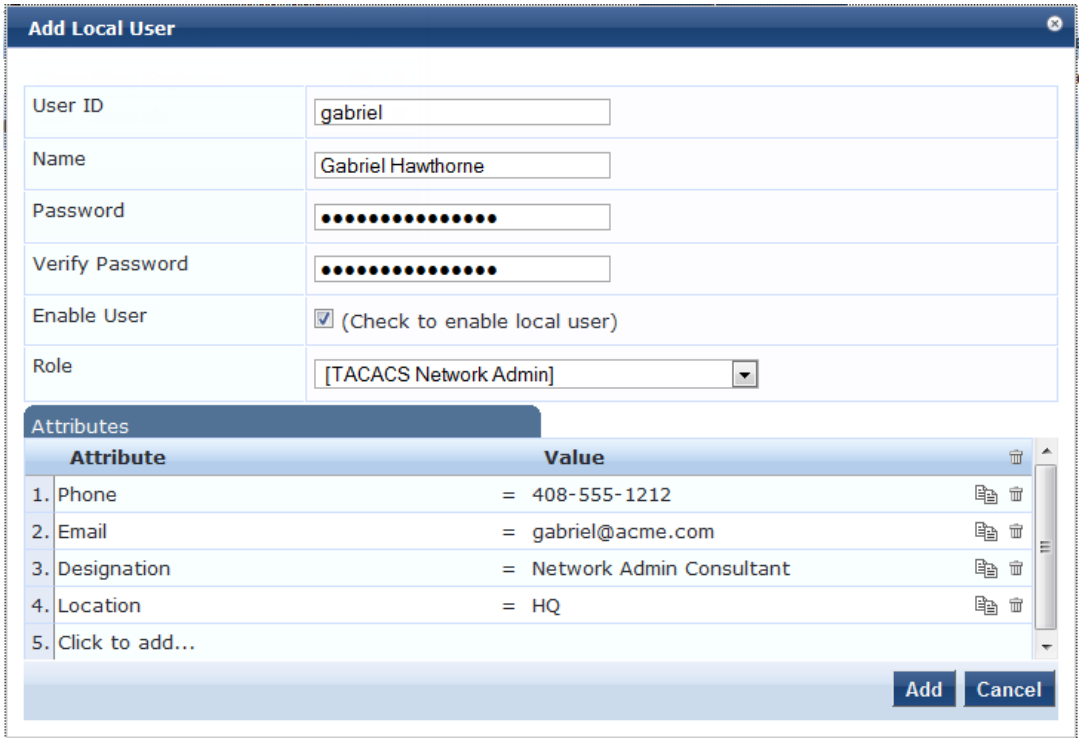


Table 107: *Add Local User Page Parameters*

Parameter	Description
User ID	Enter the user name of the local user.
Name	Enter the name of the local user.
Password	Enter the password of the local user.

Table 107: *Add Local User Page Parameters (Continued)*

Parameter	Description
Verify Password	Re-enter the password of the local user.
Enable User	Uncheck to disable this user account.
Role	Select a static role for this local user.
Attributes	Add custom attributes for this local user. Click on the **Click to add...** row to add custom attributes. By default, four custom attributes appear in the Attribute drop-down list: Phone, Email, Sponsor, Designation. You can enter any name in the attribute field. All attributes are of String datatype. The value field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in the Attribute drop-down list for all local users. **NOTE:** All attributes entered for a local user are available in the role mapping rules editor under the LocalUser namespace.

Adding and Modifying Endpoints

Policy Manager automatically lists all endpoints that are authenticated in the **Configuration > Identity > Endpoints** page. The following figure shows an example of the **Endpoints** page followed by parameter definition:

Figure 153: *Endpoints Listing*

Table 108: *Endpoint Page Parameters*

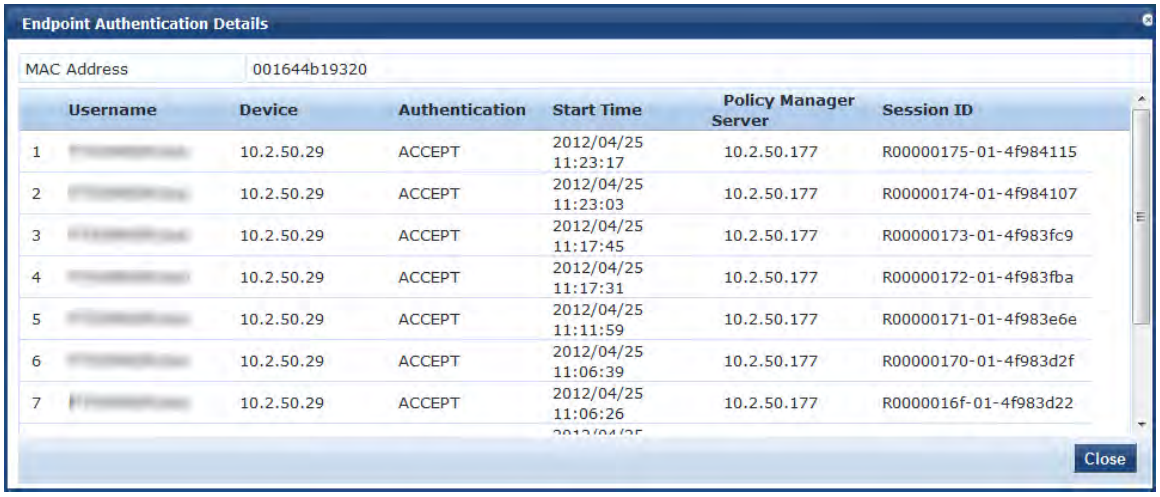
Parameter	Description
MAC Address	Displays the MAC address of the endpoint.
Hostname	Specifies the hostname of the policy server.
Device Category	Specifies the built-in category of the profiled device belongs to. For example, Smartdevices, Access Points, Computer, VOIP phone, and so on.

Table 108: *Endpoint Page Parameters (Continued)*

Parameter	Description
Device OS Family	Specifies the operating system that the device is configured with. For example, when the category is Computer, ClearPass Policy Manager shows a **Device OS Family** of Windows, Linux, or Mac OS X.
Status	Displays the status of the endpoint.
Profiled	Displays whether the device is profiled or not.

Select an endpoint by clicking the check box and click the **Authentication Records** button from the **Endpoints** page to view the authentication details of an endpoint. This displays the **Endpoint Authentication Details** page. The following figure shows an example of the **Endpoint Authentication Details** page:

Figure 154: *Endpoint Authentication Details*



Select an endpoint by clicking the check box and click the **Trigger Server Action** button from the **Endpoints** page to trigger actions that are performed on endpoints. For example, locking a device, triggering a remote, enterprise wipe, and so on. The following figure shows an example of the **Trigger Server Action** page followed by parameter definition:

Figure 155: *Endpoints - Trigger Server Action Page*

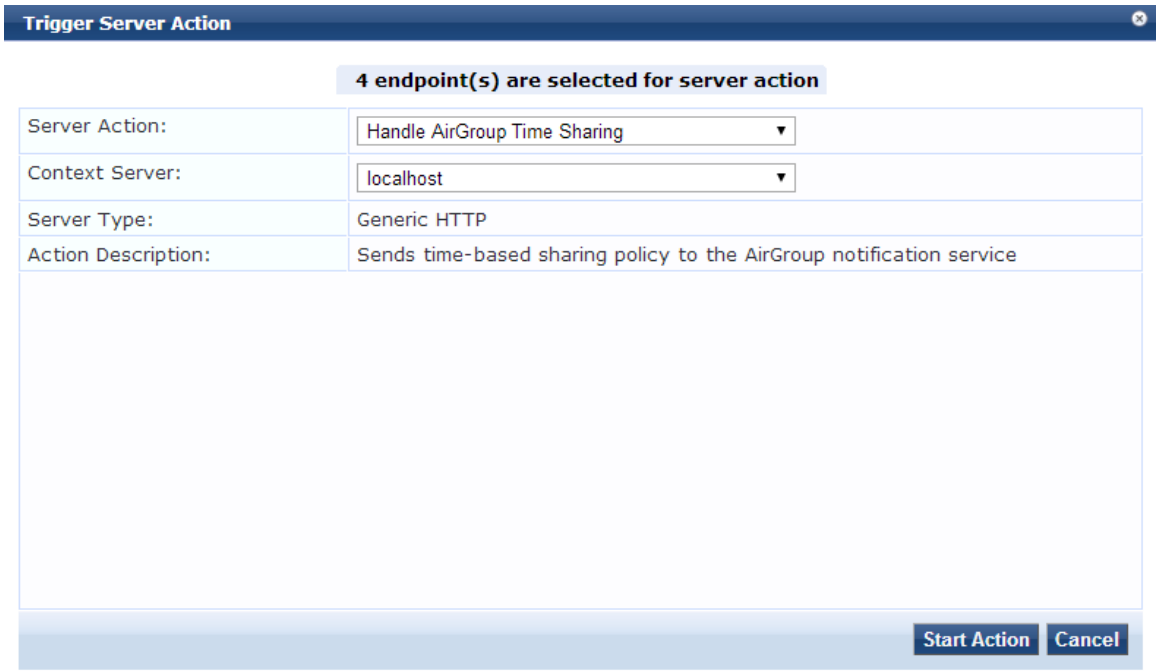


Table 109: *Trigger Server Action Page Parameters*

Parameter	Description
Server Action	Select the server action. For example, Send message, Lock Device, Remote Wipe, and so on.
Context Server	Enter a valid server name. You can enter an IP address or domain name.
Server Type	Specifies the server type configured when the server action was configured.
Action Description	Specifies the description of the action. For example, the description can be "Delete all information stored" if the configured action is **Remote Wipe**.

Select an endpoint by clicking the check box and click the **Update Fingerprint** button from the **Endpoints** page to update device fingerprints from a hosted portal. The following figure shows an example of the **Update Device Fingerprint** page followed by parameter definition:

Figure 156: *Update Device Fingerprint*

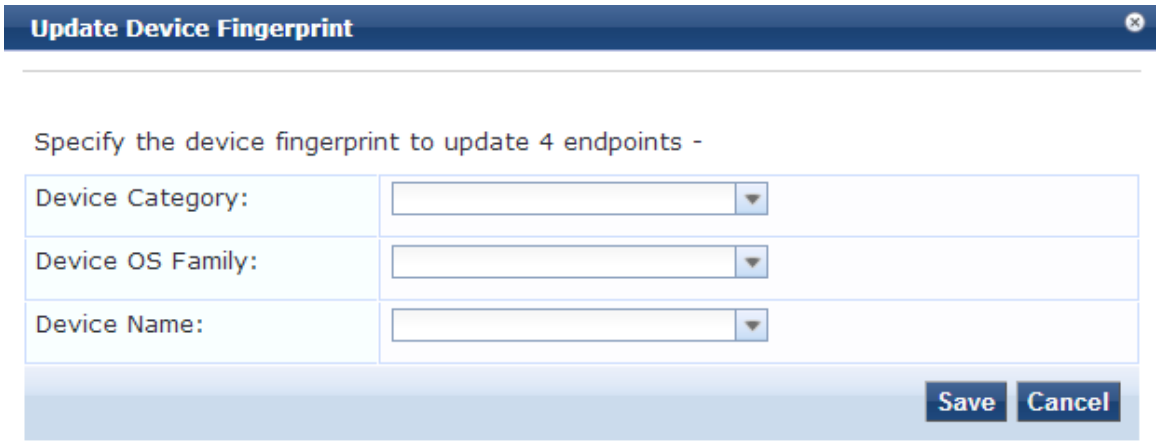


Table 110: *Update Device Fingerprint parameters*

Parameter	Description
Device Category	Select the built-in category of the profiled device belongs to. For example, Smartdevices, Access Points, Computer, VOIP phone, and so on.
Device OS Family	Select the operating system configured on the device. For example, when the category is Computer, you can select Windows, Linux, or Mac OS X.
Device Name	Enter the name of the device. You can select the name of the device from the built-in list.

Click **Add** to view the **Add Endpoint** page to manually add an endpoint. The following figure shows an example of the **Add Endpoint** page followed by parameter definition:

Figure 157: *Add Endpoint Page*

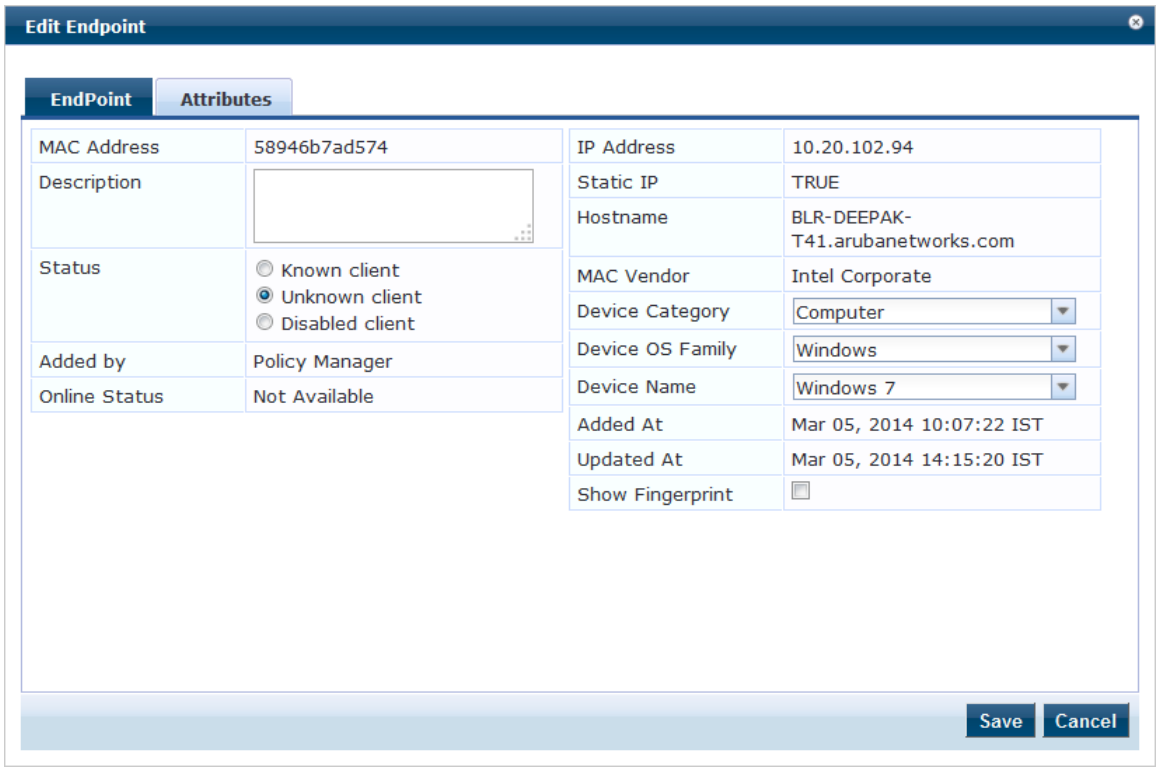


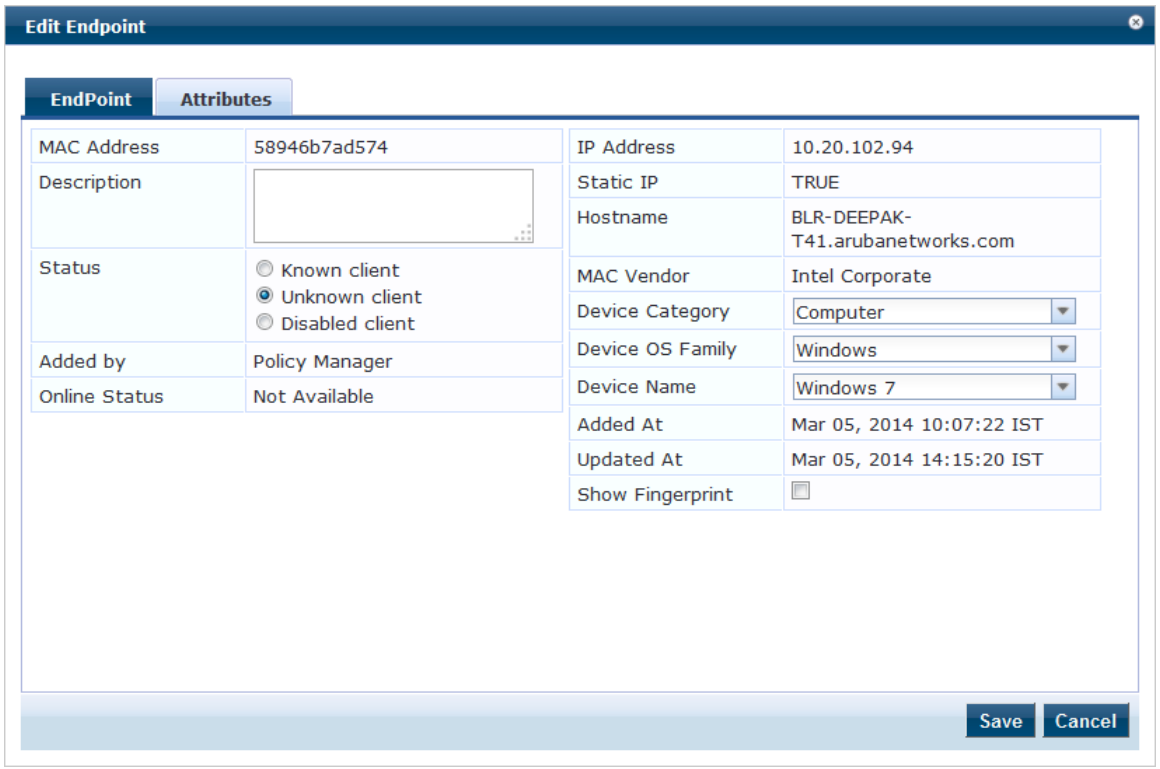
Table 111: *Add Endpoint Page Parameters*

Parameter	Description
MAC Address	Specifies the MAC address of the endpoint.
Description	Specifies the description that provides additional information about the endpoint.
Status	Mark the status as Known, Unknown, or Disabled client. The **Known** and **Unknown** status can be used in role mapping rules using the Authentication:MacAuth attribute. You can use the **Disabled** status to block access to a specific endpoint. This status is automatically set when an endpoint is blocked from the **Endpoint Activity** table (in the **Live Monitoring** section).
Attributes	Add custom attributes for this endpoint. Click on the **Click to add...** row to add custom attributes. You can enter any name in the attribute field. All attributes are of String datatype. The **Value** field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in the **Attribute** drop-down list for all endpoints. **NOTE:** All attributes entered for an endpoint are available in the role mapping rules editor under the Endpoint namespace.

To edit an endpoint in the **Endpoints** page, click an endpoint from the list of endpoints to display the **Edit Endpoint** page.

Notice that the **Policy Cache Values** section lists the role(s) assigned to the user and the posture status. Policy Manager can use these cached values in authentication requests from this endpoint. **Clear Cache** clears the computed policy results (roles and posture).

Figure 158: *Edit Endpoint Page*



Additional Available Tasks

- To delete an endpoint, in the **Endpoints** page, select an endpoint (using check box) and click the **Delete** button.
- To export an endpoint, in the **Endpoints** page, select an endpoint (using check box) and click the **Export** button.
- To export all endpoints, in the **Endpoints** page, click the **Export All** link in the upper right corner of the page.
- To import endpoints, in the **Endpoints** page, click the **Import** link in the upper right corner of the page.

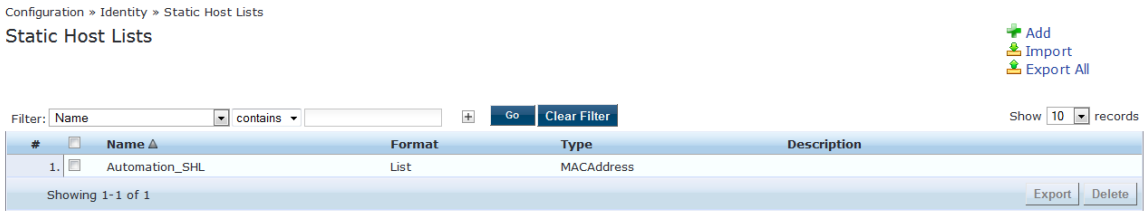
Adding and Modifying Static Host Lists

A static host list comprises a named list of MAC or IP addresses, which can be invoked the following ways:

- In Service and Role-mapping rules as a component.
- For non-responsive services on the network (for example, printers or scanners), as an Authentication Source.

Only static host lists of type MAC address are available as authentication sources. A static host list often functions, in the context of the service, as a whitelist or a blacklist. Therefore, they are configured independently at the global level.

Figure 159: *Static Host Lists Page*



To add a Static Host List, go to **Configuration > Identity > Static Host Lists** page and click the **Add** link. The **Add Static Host List** popup opens. For more information, see the following figure and parameter definition table.

Figure 160: *Add Static Host List Page*

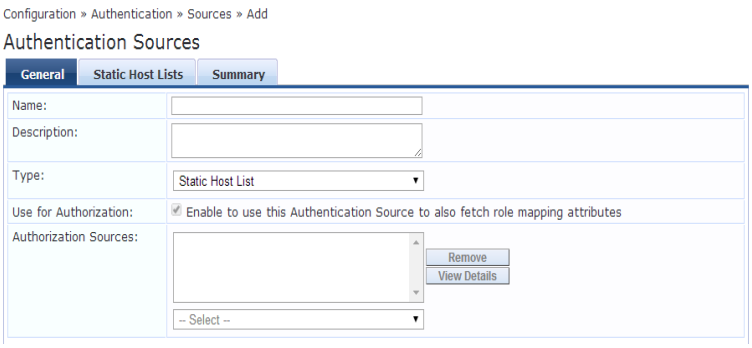


Table 112: *Add Static Host List Page Parameters*

Parameter	Description
Name	Enter the name of the static host list.
Description	Specify the description of the static host list.
Host Format	Select a format for expression of the address: **subnet, IP address** or **regular expression**.
Host Type	Select a host type: **IP Address** or **MAC Address** (radio buttons).
List	Use the **Add Host** and **Remove Host** widgets to maintain membership in the current Static Host List.

Additional Available Tasks

- To edit a Static Host List from the Static Host Lists listing page, click on the name to display the **Edit Static Host List** popup.
- To delete a Static Host List from the Static Host Lists listing page, select a Static Host List (via check box) and click the **Delete** button.
- To export a Static Host List, in the Static Host Lists listing page, select a Static Host List (via check box) and click the **Export** button.
- To export all Static Host Lists, in the Static Host Lists listing page, click the **Export All** link.

- To import Static Host Lists, in the Static Host Lists listing page, click the **Import** link

Configuring a Role and Role Mapping Policy

After authenticating a request, a Policy Manager *Service* invokes its *Role Mapping Policy,* resulting in assignment of a role(s) to the client. This role becomes the identity component of **Enforcement Policy** decisions.

A service can be configured without a Role Mapping Policy, but only one Role Mapping Policy can be configured for each service.

Policy Manager ships a number of preconfigured roles, including the following:

- [Contractor] - Default role for a Contractor
- [Employee] - Default role for an Employee
- [Guest] - Default role for guest access
- [Other] - Default role for other user or device
- [TACACS API Admin] -API administrator role for Policy Manager admin
- [TACACS Help Desk] - Policy Manager Admin Role, limited to views of the Monitoring screens
- [TACACS Network Admin] - Policy Manager Admin Role, limited to Configuration and Monitoring UI screens
- [TACACS Read-only Admin] - Read-only administrator role for Policy Manager Admin
- [TACACS Receptionist] - Policy Manager Guest Provisioning Role
- [TACACS Super Admin] - Policy Manager Admin Role with unlimited access to all UI screens

Additional roles are available with AirGroup and Onboard licenses.

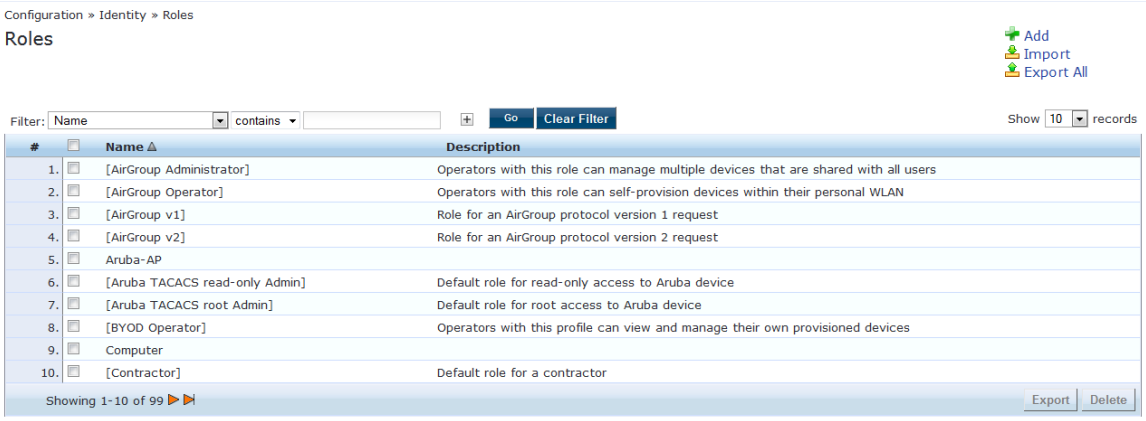
For more information, see:

- Adding and Modifying Roles on page 202
- Adding and Modifying Role Mapping Policies on page 203

Adding and Modifying Roles

Policy Manager lists all available roles in the **Configuration > Identity > Roles** page.

Figure 161: *Roles Page*



You can configure a role from within a Role Mapping Policy (**Add New Role**), or independently from the menu **Configuration > Identity > Roles > Add**. In either case, roles exist independently of an individual service and can be accessed globally through the Role Mapping Policy of any service.

When you click **Add** roles from any of these locations, Policy Manager displays the **Add New Role** popup. For more information, see the following figures and parameter definition table.

Figure 162: *Add New Role Page*

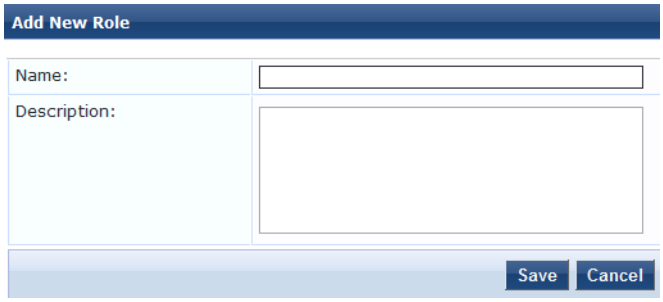


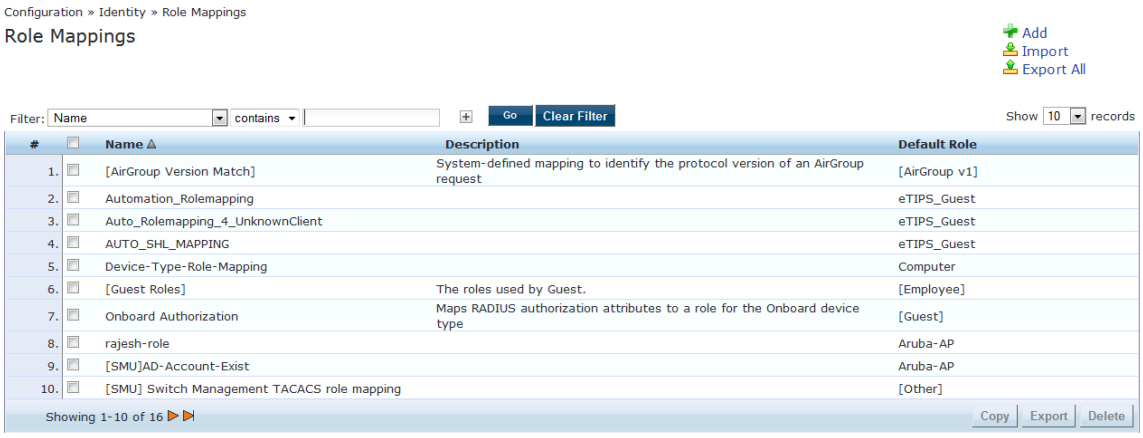
Table 113: *Add New Role Page Parameters*

Parameter	Description
Name	Enter the name of the role.
Description	Specify the description of the new role.

Adding and Modifying Role Mapping Policies

From the **Configuration > Services** page, you can configure role mapping for a new service (as part of the flow of the **Add Service** wizard), or modify an existing role mapping policy directly from the **Configuration > Identity > Role Mappings** page.

Figure 163: *Role Mappings Page*



When you click **Add** role mapping from any of these locations, Policy Manager displays the **Role Mappings** page, which contains the following three tabs:

- Policy
- Mapping Rules
- Summary

Policy Tab

The **Policy** tab labels the method and defines the Default Role (the role to which Policy Manager defaults if the mapping policy does not produce a match for a given request).

Figure 164: *Role Mappings (Policy Tab)*

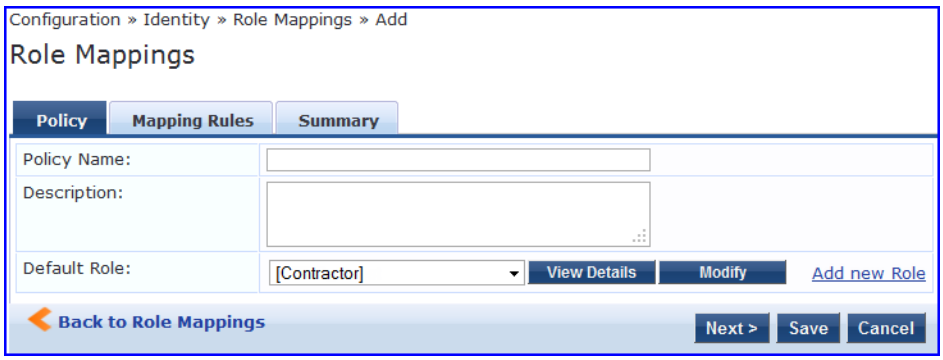


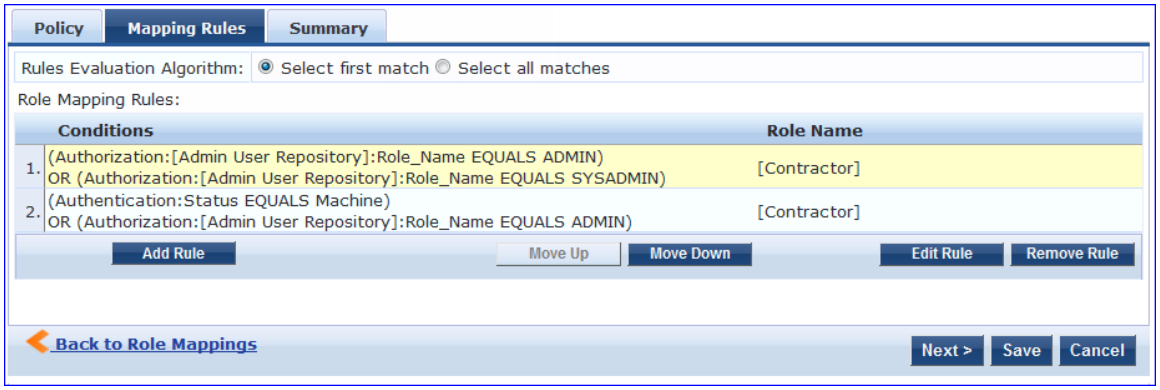
Table 114: *Role Mappings (Policy tab) Parameters*

Parameter	Description
Policy Name	Enter the name of the role mapping policy.
Description	Specify the description of the role mapping policy.
Default Role	Select the role to which Policy Manager will default when the role mapping policy does not produce a match.
View Details / Modify / Add new Role	Click on **View Details** to view the details of the default role.
Modify	Click on **Modify** to modify the default role.
Add new Role	Click on **Add new Role** to add a new role.

Mapping Rules Tab

The **Mapping Rules** tab selects the evaluation algorithm, add/edit/remove rules, and reorder rules. On the **Mapping Rules** tab, click the **Add Rule** button to create a new rule, or select an existing rule (by clicking on the row) and then click the **Edit Rule** button or **Remove Rule** button.

Figure 165: *Role Mapping (Mapping Rules Tab)*



When you select **Add Rule** or **Edit Rule**, Policy Manager displays the **Rules Editor** popup.

Figure 166: *Rules Editor Page*

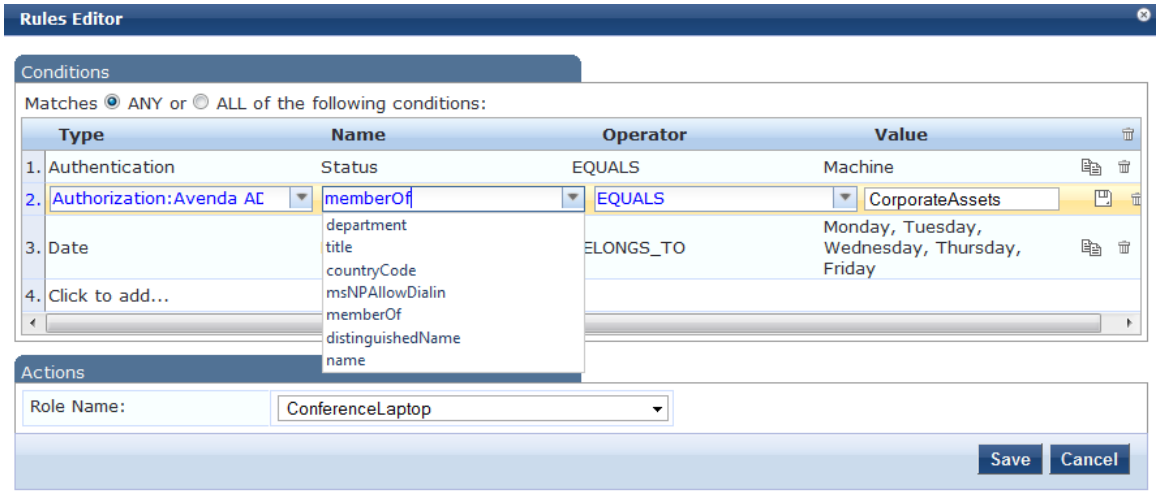


Table 115: *Role Mappings Page (Rules Editor) Page Parameters*

Parameter	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to Namespaces on page 513.) In the role mapping context, Policy Manager allows attributes from following namespaces: • Application • Application:ClearPass • Authentication • Authorization • Authorization:<authorization_source_instance> - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (See Adding and Modifying Authentication Sources on page 154). Only those attributes that have been configured to be fetched are shown in the attributes drop-down list. • Certificate • Connection • Date • Device • Endpoint • GuestUser • Host • LocalUser • Onboard • TACACS • RADIUS - All enabled RADIUS vendor dictionaries.
Name	Drop-down list of attributes present in the selected namespace.
Operator	Drop-down list of context-appropriate (with respect to the attribute data type) operators.

Table 115: *Role Mappings Page (Rules Editor) Page Parameters (Continued)*

Parameter	Description
	Operators have their obvious meaning; for stated definitions of operator meaning, refer to Operators on page 524.
Value	Depending on attribute data type, this may be a free-form (one or many line) edit box, a drop-down list, or a time/date widget.

The Operator values that display for each Type and Name are based on the data type specified for the Authentication Source (from the **Configuration > Authentication > Sources** page). If, for example, you modify the UserDN Data type on the Authentication Sources page to be an Integer rather than a string, then the list of Operator values here will populate with values that are specific to Integers.

After you save your Role Mapping configuration, it appears in the **Mapping Rules** list. In this interface, you can select a rule, and then use the various widgets to Move Up, Move Down, Edit the rule, or Remove the rule.

Policy Manager provides several *posture* methods to evaluate the health of the clients that request access. These methods all return *Posture Tokens* (E.g., Healthy, Quarantine for use by Policy Manager for input into *Enforcement Policy*. One or more posture methods can be associated with a *Service*.

For more information, see:

- Posture Architecture and Flow on page 207
- Configuring Posture on page 209
- Adding a Posture Policy on page 210
- Adding and Modifying Posture Servers on page 247

Posture Architecture and Flow

Policy Manager supports three types of posture checking.

Posture Policy

Policy Manager supports four pre-configured posture plugins for Windows, one plugin for Linux® and one plugin for Mac OS® X, against which administrators can configure rules that test for specific attributes of client health and correlate the results to return Application Posture Tokens for processing by Enforcement Policies.

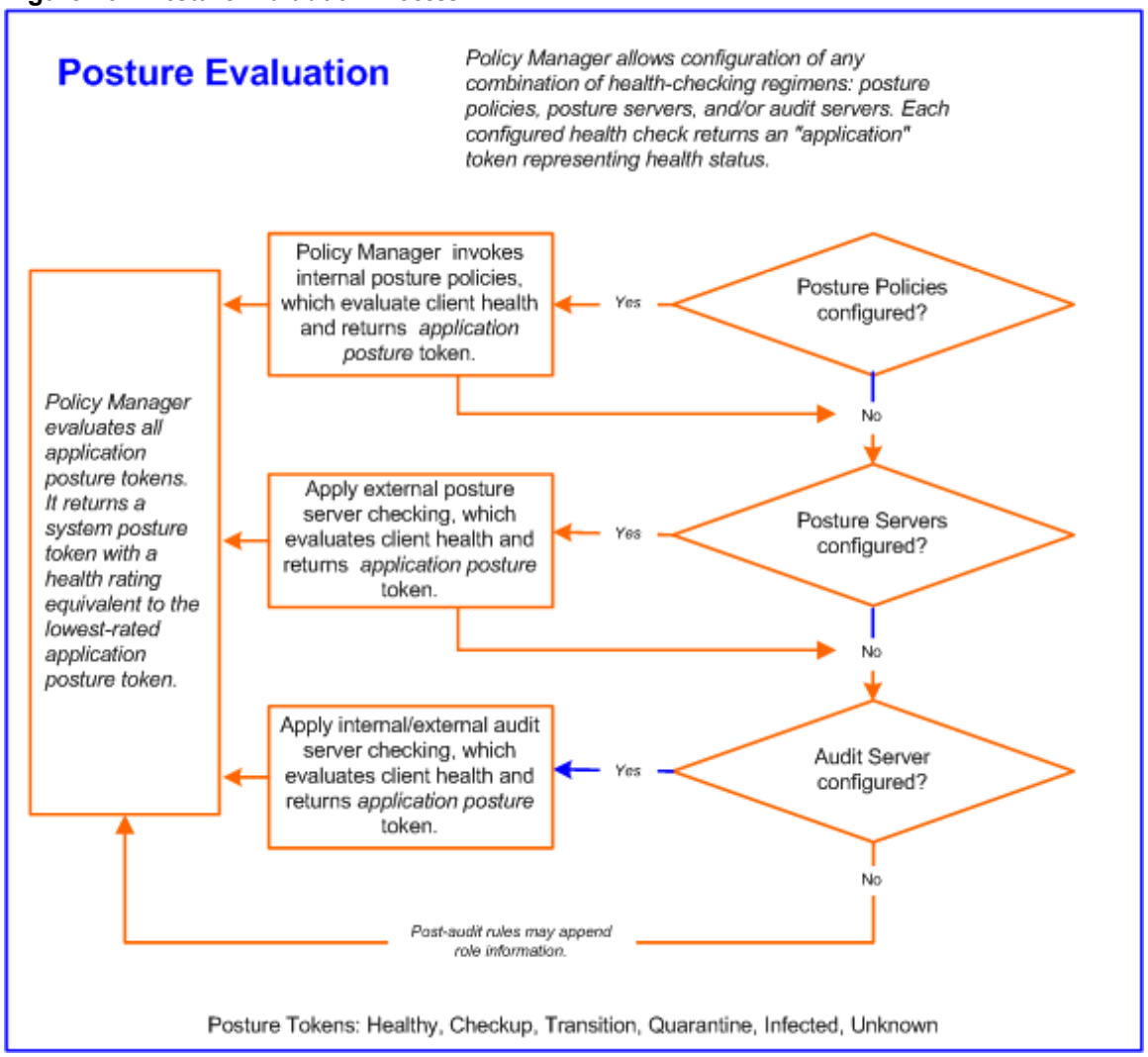
Posture Server

Policy Manager can forward all or part of the posture data received from the client to a Posture Server. The Posture Server evaluates the posture data and returns Application Posture Tokens. Policy Manager supports the Microsoft NPS Server for Microsoft NAP integration.

Audit Server

Audit Servers provide posture checking for unmanageable devices, such as devices lacking adequate posture agents or supplicants. In the case of such clients, the audit server's post-audit rules map clients to roles. Policy Manager supports two types of audit servers: The NMAP audit server, which is primarily used to derive roles from post-audit rules, and the NESSUS audit server, primarily used for vulnerability scans (and, optionally, post-audit rules).

Figure 167: *Posture Evaluation Process*



Policy Manager uses posture evaluation to assess client consistency with enterprise endpoint health policies, specifically with respect to:

- Operating system version/type
- Registry keys/services present (or absent)
- Antivirus/antispyware/firewall configuration
- Patch level of different software components
- Peer to Peer application checks
- Services to be running or not running
- Processes to be running or not running

Each configured health check returns an *application token* representing health:

- **Healthy.** Client is compliant: there are no restrictions on network access.
- **Checkup.** Client is compliant; however, there is an update available. This can be used to proactively remediate to healthy state.
- **Transient.** Client evaluation is in progress; typically associated with auditing a client. The network access granted is interim.

- **Quarantine.** Client is out of compliance; restrict network access, so the client only has access to the remediation servers.
- **Infected.** Client is infected and is a threat to other systems in the network; network access should be denied or severely restricted.
- **Unknown.** The posture token of the client is unknown.

Upon completion of all configured posture checks, Policy Manager evaluates all *application tokens* and calculates a *system token,* equivalent to the most restrictive rating for all returned application tokens. The *system token* provides the health posture component for input to the Enforcement Policy.

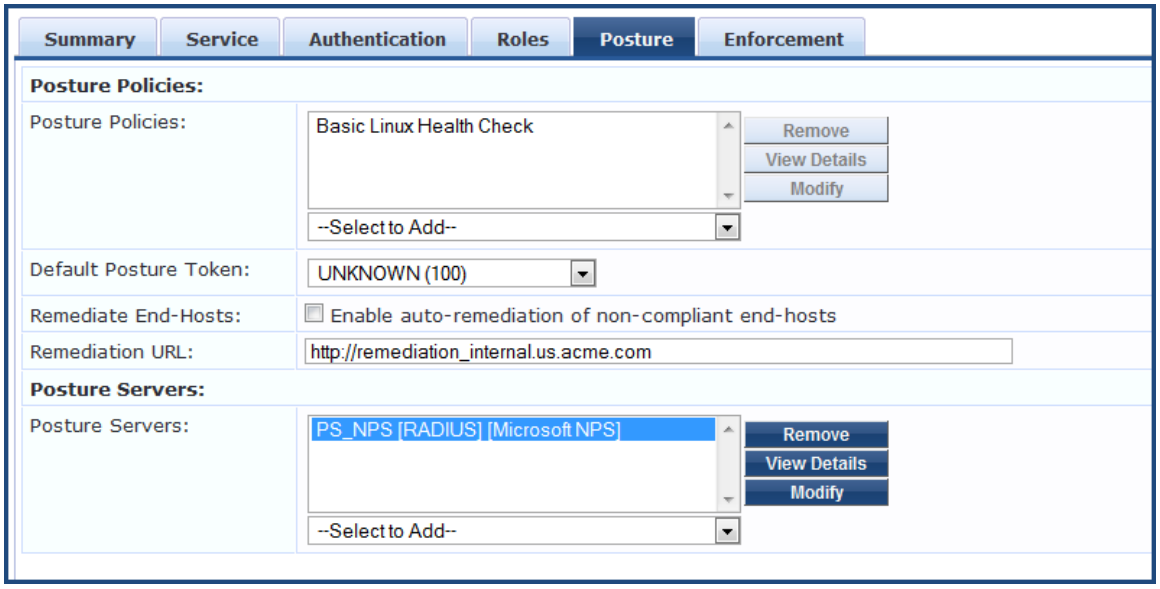
A Service can also be configured without any Posture policy.

Configuring Posture

The following image displays how to configure Posture at the Service level.

The Posture Compliance check box must be selected on the Service tab in order for Posture to be enabled.

Figure 168: *Posture Features at the Service Level*



You can configure the following features of posture:

Table 116: *Posture Features at the Service Level*

Configurable Component	How to Configure
Sequence of Posture Policies	Select a Policy, then select **Move Up**, **Move Down**, **Remove**, or **View Details**. • To add a previously configured Policy, select from the **Select** drop-down list, then click **Add**. • To configure a new Policy, click the **Add New Policy** link and refer to Adding a Posture Policy on page 210. • To edit the selected posture policy, click **Modify** and refer to Adding a Posture Policy on page 210.
Default Posture Token	The default posture token is UNKNOWN (100).
Remediation End-Hosts	Select this check box to enable auto-remediation action on non-compliant endpoints.
Remediation URL	This URL defines where to send additional remediation information to endpoints.
Sequence of Posture Servers	Select a Posture Server, then select **Move Up**, **Move Down**, **Remove**, or **View Details**. • To add a previously configured Posture Server, select from the **Select** drop-down list, then click **Add.** • To configure a new Posture Server, click **Add New Posture Server** (link) and refer to Adding and Modifying Posture Servers on page 247. • To edit the selected posture server, click **Modify** and refer to Adding and Modifying Posture Servers on page 247.
Enable auto-remediation of non-compliant end-hosts	Select the **Enable auto-remediation of non-compliant end-hosts** check box to enable the specified remediation server to enable auto-Remediation. Remediation server is optional. A popup appears on the client box, with the URL of the Remediation server.

Adding a Posture Policy

Adding a posture policy consists of four steps:

1. Configure the Policy.
2. Configure the Posture Plugins.
3. Configure the Rules.
4. Review the configuration summary page.

NAP Agent

If you select the **Posture Agent: NAP Agent** on the Policy tab, you can configure the following Posture Plugins.

Table 117: *NAP Agent Posture Plugins for Windows Operating Systems*

		Operating System Versions					
Plugin Name	Description	Windows 8	Windows 7	Windows Vista	Windows XP Service Pack 3	Windows Server 2008	Windows Server 2008R2
Windows System Health Validator	The Windows System Health Validator parameters permit or deny client computers to connect to your network, and to restrict client access to computers that have a Service Pack less than Service Pack *x*.	yes	yes	yes	yes	yes	yes
Windows Security Health Validator	The Windows Security Health Validator parameters permit or deny client computers access to your network, subject to checks of the client's system for Firewall, Virus Protection, Spyware Protection, Automatic Updates, and Security Updates*.	yes	yes	yes	yes	no	no
* If you configure the Windows Security Health Validator Posture Plugin for Windows XP, spyware protection is disabled.							

Table 118: *NAP Agent Posture Plugins for Linux Operating Systems*

		LINUX Operating Systems			
Plugin Name	Description	CentOS	Fedora	RedHat Enterprise Linux	SUSE Linux Enterprise Desktop
ClearPassWindows Universal System Health Validator	Services, which allows you to enable or disable health checks, set auto remediation checks, select or insert available services, and set which services to run and which to stop.	yes	yes	yes	yes
AntiVirus	Enable or disable AntiVirus check, configure auto remediation and user notification, add product-specific checks.	yes	yes	yes	yes
Firewall	Enable or disable Firewall check, configure remediation checks, configure which UDP and TCP ports to open, and which TCP and UDP ports to block or open.	yes	yes	yes	yes

OnGuard Agent (Persistent or Dissolvable)

Select the Posture Agent: On Guard Agent (Persistent or Dissolvable for use in the following scenarios:

- An environment that does not support 802.1X based authentication, such some legacy Microsoft Windows operating systems, or legacy network devices.
- An environment configured with an operating system that provides native support for 802.1X natively, but does not have a built-in health agent. The MAC OS X is an example of this type of environment.

If you select the **Posture Agent: OnGuard Agent (Persistent or Dissolvable)** on the Policy tab, you can configure the following Posture Plugins:

Table 119: *OnGuard Agent Validator Supported Windows Operating Systems*

			Supported Operating System Versions					
Posture Plugin Name	Description	Windows 2003	Windows 8	Windows 7	Windows Vista	Windows XP Service Pack 3	Windows Server 2008	Windows Server 2008R2
ClearPassWindows Universal System Health Validator	The configurable parameter categories for this validator are Services, Processes, Registry Keys, AntiVirus, AntiSpyware, Firewall, Peer To Peer, Patch Management, Windows HotFixes, USB Devices, Virtual Machines, Network Connections, Disk Encryption, and Installed Applications.	yes	yes	yes	yes	yes	yes	yes
Windows System Health Validator	The configurable parameter categories for this validator allow you to configure which client computers can connect to your network, and which clients are restricted from your network. Access is determined by a check of the service pack level. You	yes	yes	yes	yes	yes	yes	yes

Table 119: *OnGuard Agent Validator Supported Windows Operating Systems (Continued)*

			Supported Operating System Versions					
	determine the service pack level.							
Windows Security Health Validator	The configurable parameter categories for this validator allow you to configure parameters that permit or deny client computers access to your network, subject to checks of the client's system for Firewall, Virus Protection, Spyware Protection, Automatic Updates, and Security Updates*.	no	yes	yes	yes	yes	no	no
* If you configure the Posture Plugin for Windows XP, spyware protection is disabled.								

ClearPass Mac OS X

The configurable parameter categories for this validator are Services, Processes, AntiVirus, AntiSpyware, Firewall, Patch Management, Peer To Peer, USB Devices, Virtual Machines, Network Connections, Disk Encryption, and Installed Applications.

Select the **Posture Agent: OnGuard Agent (Persistent or Dissolvable)** for use in the following scenarios:

Table 120: *OnGuard Agent (Persistent or Dissolvable) Posture Plugins for Mac OS X*

Name of the Plugin	Description
ClearPassMac OS X Universal System Health Validator	The configurable parameter categories for this validator are: • Services • Processes • AntiVirus • AntiSpyware • Firewall • Patch Management • Peer To Peer • USB Devices • Virtual Machines • Network Connections • Disk Encryption • Installed Applications.

ClearPass Windows Universal System Health Validator - NAP Agent

The **ClearPass Windows Universal System Health Validator - NAP Agent** page popup appears in response to actions in the **Posture Plugins** page of the **Posture** configuration page if you select **Windows** and **NAP Agent**.

The OnGuard Agent version of the ClearPass Windows Universal System Health Validator supports all the features supported by the OnGuard Agent validator.

The configuration options and steps described under the ClearPass Windows Universal System Health Validator - OnGuard Agent on page 225 section also apply to the NAP Agent.

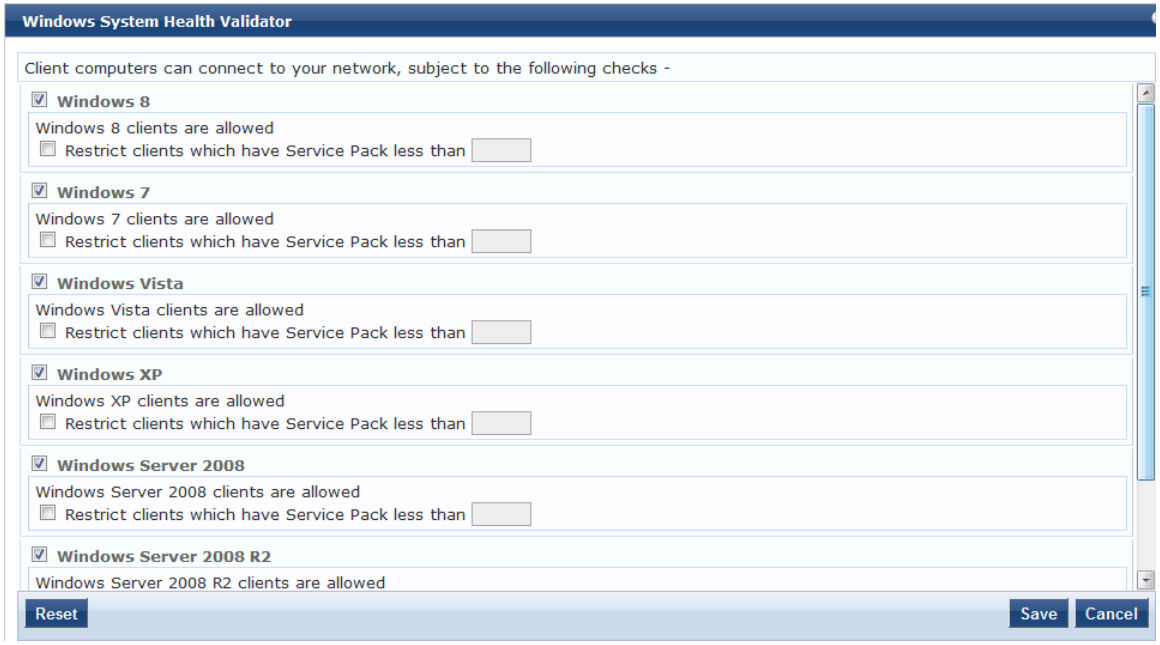
Even though the UI allows auto remediation configuration, the dissolvable OnGuard Agent does not support this feature.

Windows System Health Validator - NAP Agent

This validator checks for the level of Windows Service Packs.

1. Click a check box to enable support of specific operating systems.
2. Enter the minimum service pack level required on the client computer to connect to your network.
3. Click **Save**.

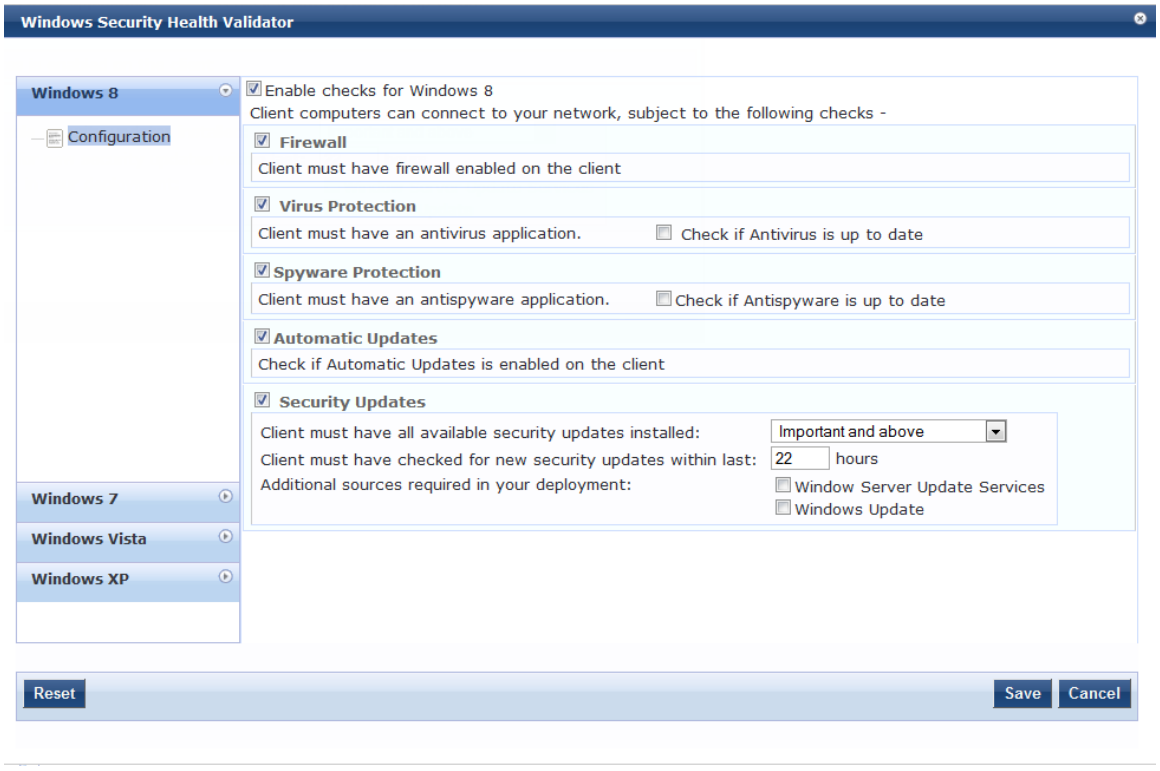
Figure 169: *Windows System Health Validator (Overview)*



Windows Security Health Validator - NAP Agent

This validator checks for the presence of specific types of security applications. An administrator can use the check boxes to restrict access based on the absence of the selected security application types.

Figure 170: *Windows Security Health Validator*



ClearPass Linux Universal System Health Validator - OnGuard Dissolvable Agent

The **ClearPass Linux Universal System Health Validator - OnGuard Dissolvable Agent** page pop up appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration (When you select **Linux** and **OnGuard Dissolvable Agent** from the **Posture Policy** page).

The OnGuard Dissolvable Agent version of the ClearPass Linux Universal System Health Validator supports the following features:

- AntiVirus
- Services

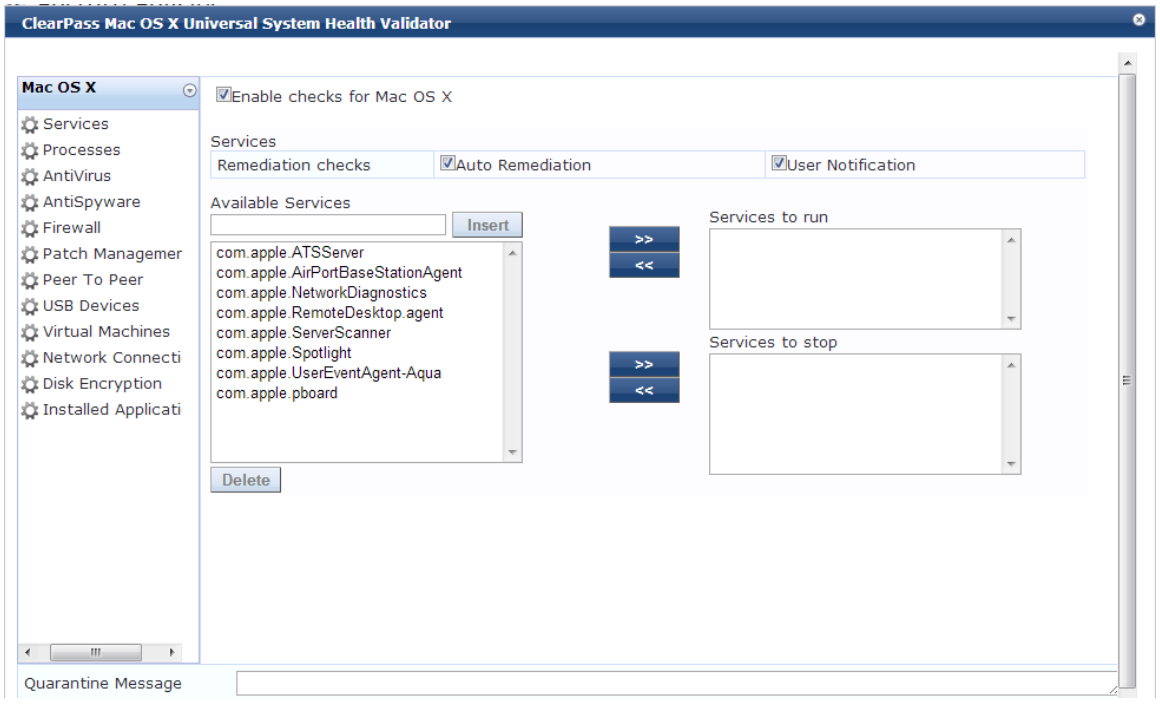
ClearPass Mac OS X Universal System Health Validator - OnGuard Agent

The **ClearPass Mac OS X Universal System Health Validator** page popup appears after you click **Configure** in the **Posture Plugins** tab of the **Posture** configuration.

Select a check box to enable checks for Mac OS X. Enabling these check boxes displays a corresponding set of configuration pages that are described in the following sections.

- Services on page 218
- Processes on page 218
- Antivirus on page 219
- AntiSpyware on page 220
- Firewall on page 220
- Patch Management on page 221
- USB Devices on page 222
- Virtual Machine on page 222
- Network Connections on page 222
- Disk Encryption on page 223
- Installed Applications on page 224

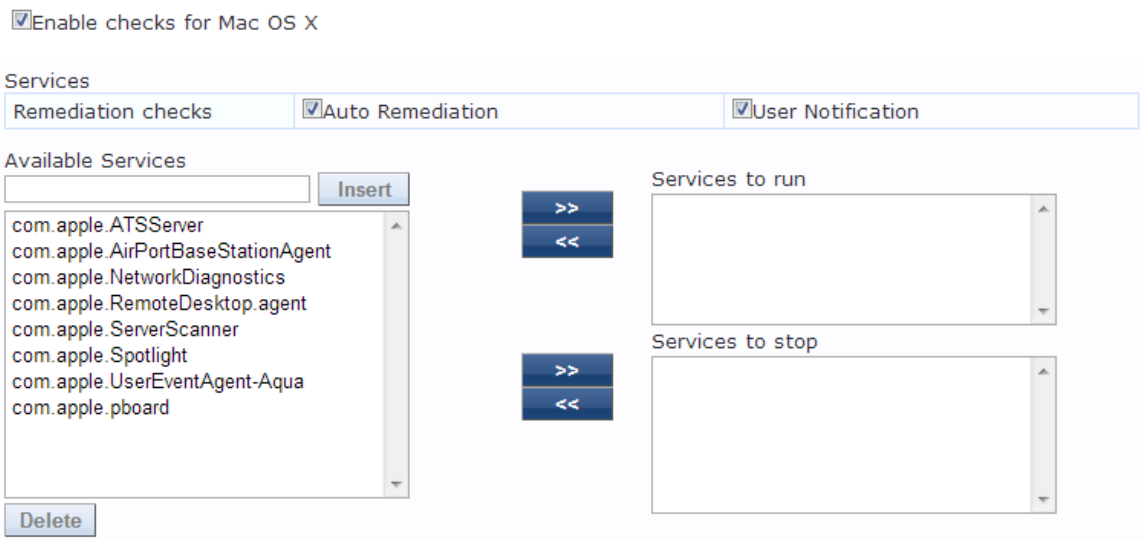
Figure 171: *ClearPass Mac OS X Universal System Health Validator - OnGuard Agent*



Services

Use the Services page to configure which services to run and which services to stop. See ClearPass Windows Universal System Health Validator - OnGuard Agent on page 225 for a description of the fields on this page.

Figure 172: *Services Configuration Page*



Processes

The **Processes** page provides a set of components for specifying specific processes to be explicitly present or absent on the system.

Figure 173: *Processes Page*

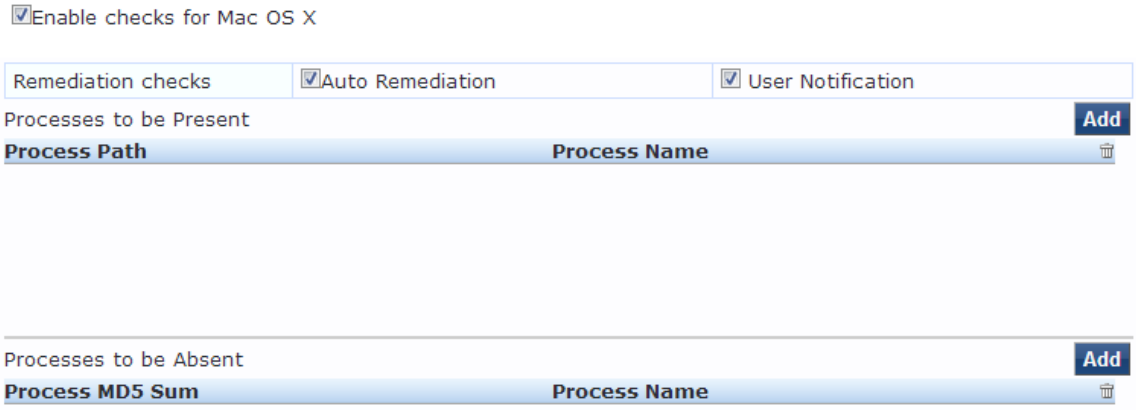
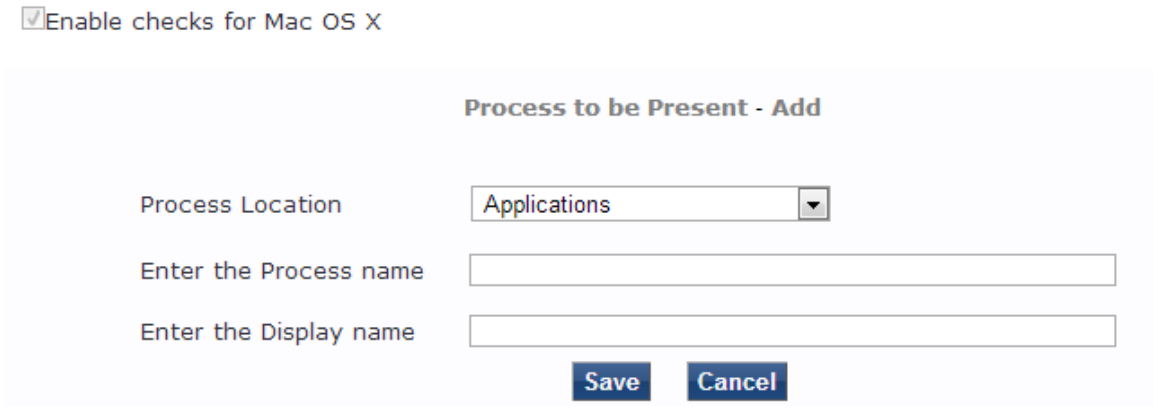


Figure 174: *Processes Add Page*

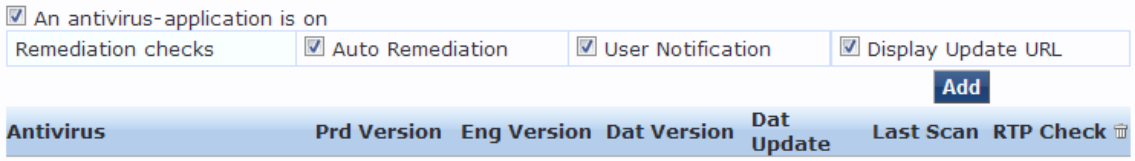


Antivirus

In the Antivirus page, you can specify that an Antivirus application must be on and allows drill-down to specify information about the Antivirus application. Click on **An Antivirus Application is On** to configure the Antivirus application information.

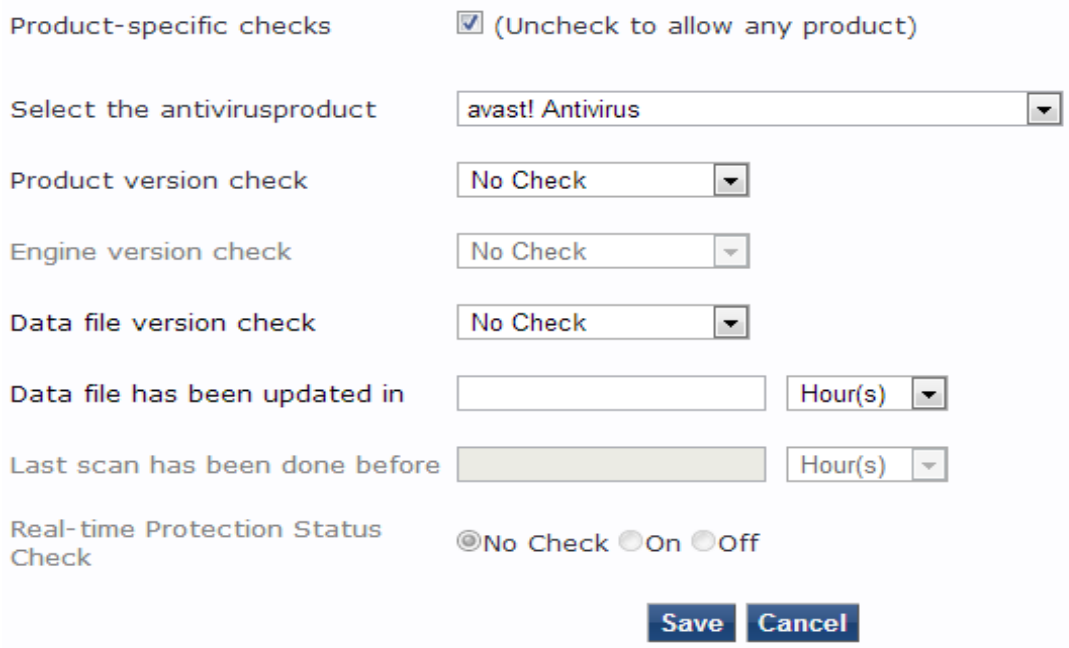
When enabled, the **Antivirus** detail page appears.

Figure 175: *Antivirus Page (Detail 1)*



Click **Add** to specify product and version check information.

Figure 176: *Antivirus Page (Detail 2)*



When you save your Antivirus configuration, it appears in the **Antivirus** page list. See ClearPass Windows Universal System Health Validator - OnGuard Agent on page 225 for antivirus page and field descriptions.

AntiSpyware

In the **AntiSpyware** page, an administrator can specify that an Antispyware application must be on and allows drill-down to specify information about the Antispyware application.

Figure 177: *AntiSpyware Page*

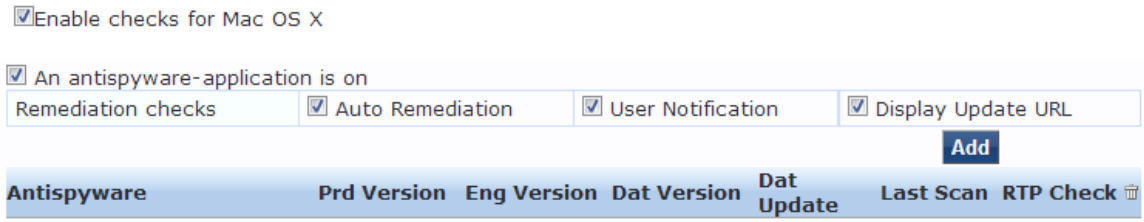
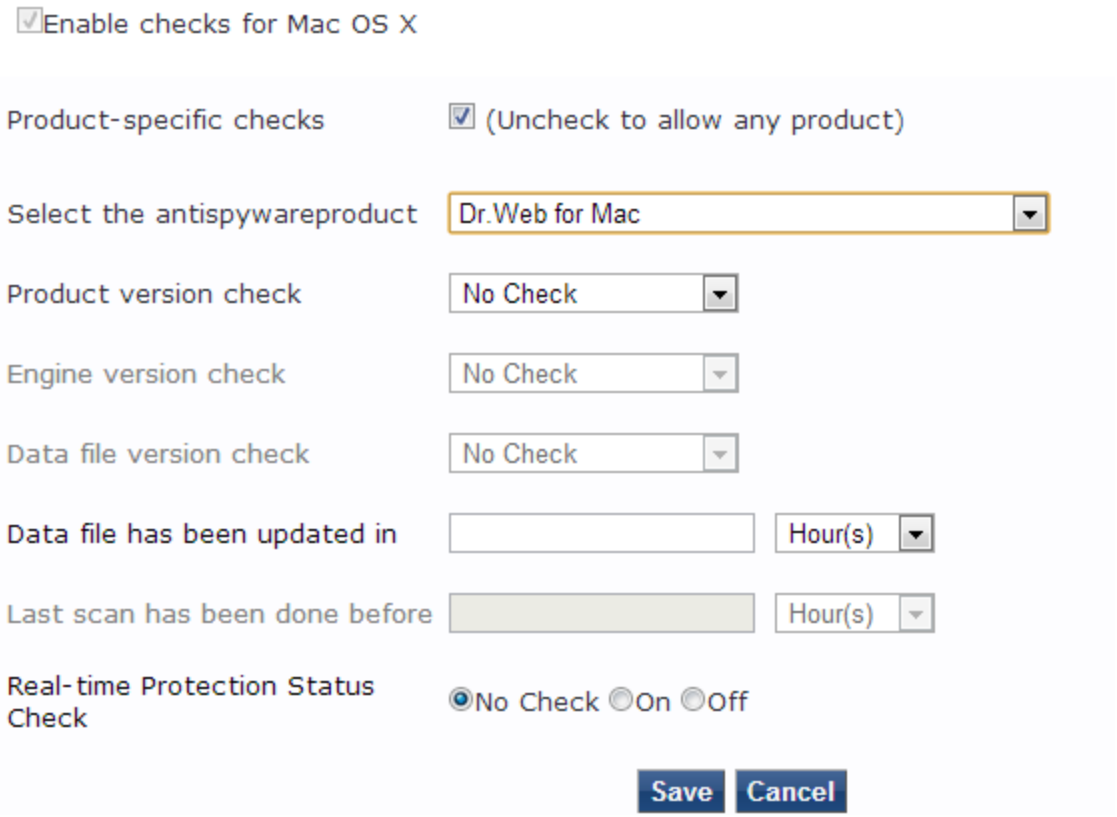


Figure 178: *AntiSpyware Add Page*



In the **Antispyware** page, click **An Antispyware Application is On** to configure the Antispyware application information. See Antivirus configuration details above for a description of the different configuration elements.

When you save your Antispyware configuration, it appears in the **Antispyware** page list.

The configuration elements are the same for anti-virus and antispyware products. Refer to the anti-virus configuration instructions above.

Firewall

In the **Firewall** page, you can specify that a Firewall application must be on and allows drill-down to specify information about the Firewall application.

In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

Figure 179: *Firewall Page*

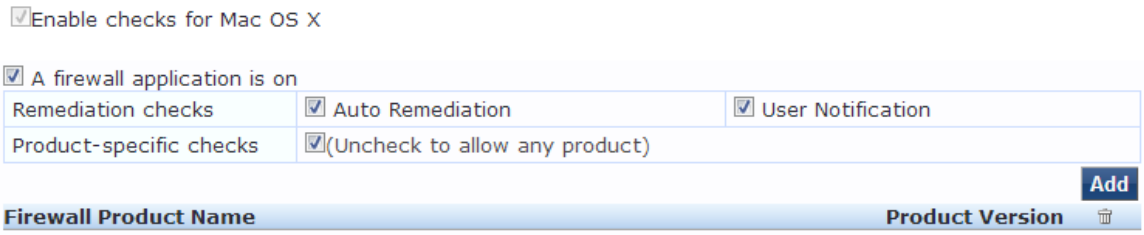
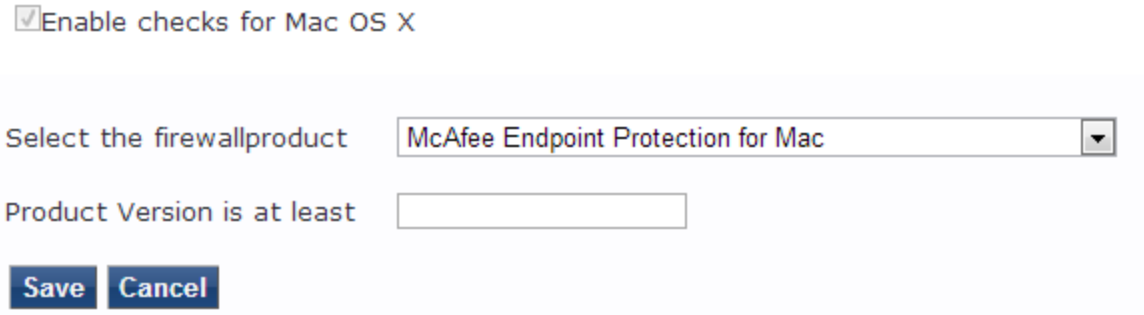


Figure 180: *Firewall Add Page*



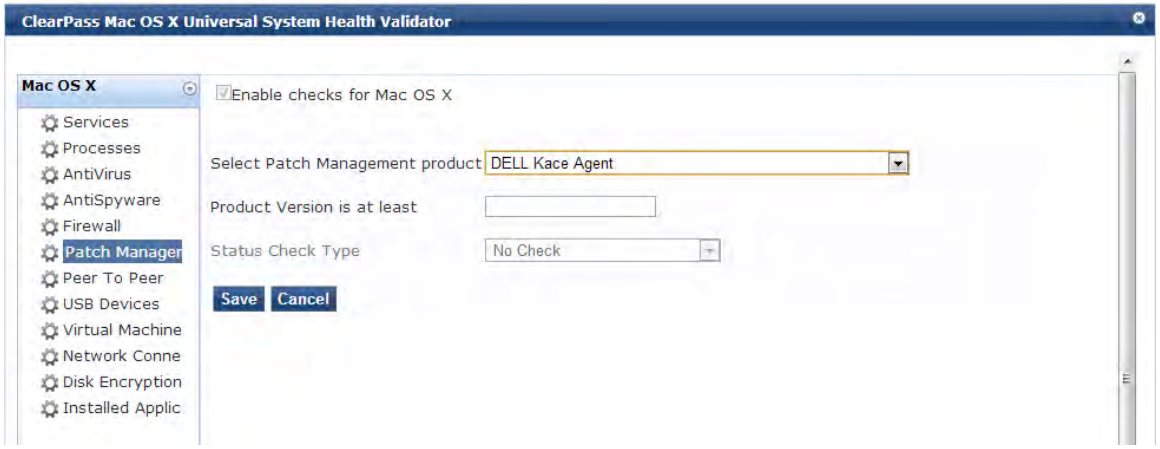
When enabled, the **Firewall** detail page appears. See ClearPass Windows Universal System Health Validator - OnGuard Agent on page 225 for firewall page and field descriptions.

Patch Management

In the Patch Management page, you can view or add the patch management product, and configure Auto Remediation and User Notification features.

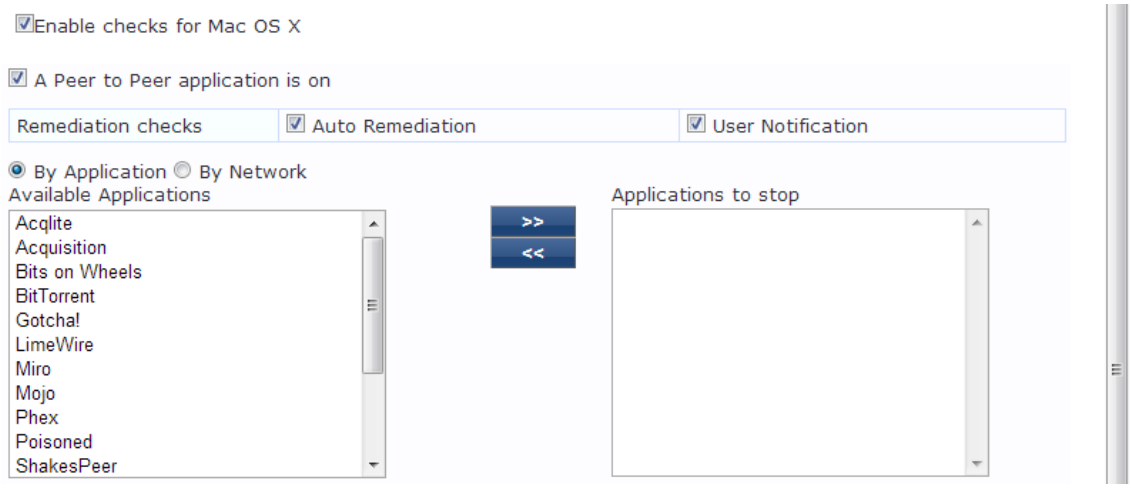
Figure 181: *Patch Management Overview*

Figure 182: *Patch Management Add Page*



Peer To Peer

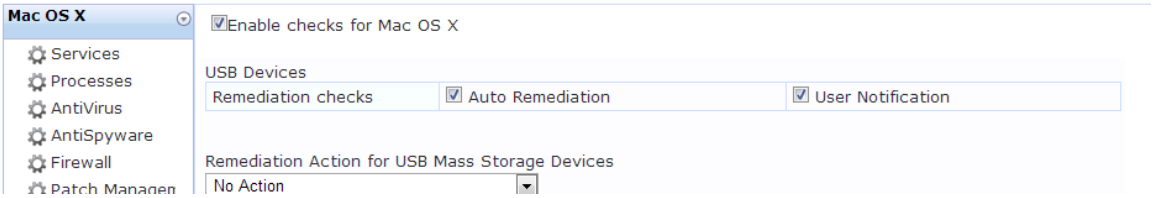
The **Peer To Peer** page provides a set of widgets for specifying specific peer to peer applications or networks to be explicitly stopped. When you select a peer to peer network, all applications that make use of that network are stopped.



USB Devices

Use this page to configure Auto Remediation and User Notification parameters, and whether or not to take action on Remediation Action for USB Mass Storage Devices or to remove USB Mass Storage Devices.

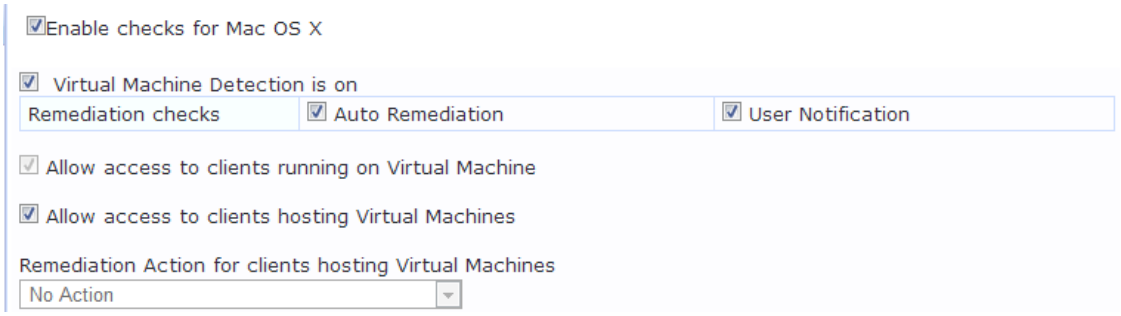
Figure 183: *USB Devices Page*



Virtual Machine

The **Virtual Machines** page provides configuration to Virtual Machines utilized by your network.

Figure 184: *Virtual Machine Page*



Network Connections

The **Network Connections** page provides configuration to control network connections based on connection type. Select the **Check for Network Connection Types** check box, and then click **Configure** to specify type of connection that you want to include.

Figure 185: *Network Connections Overview Page*

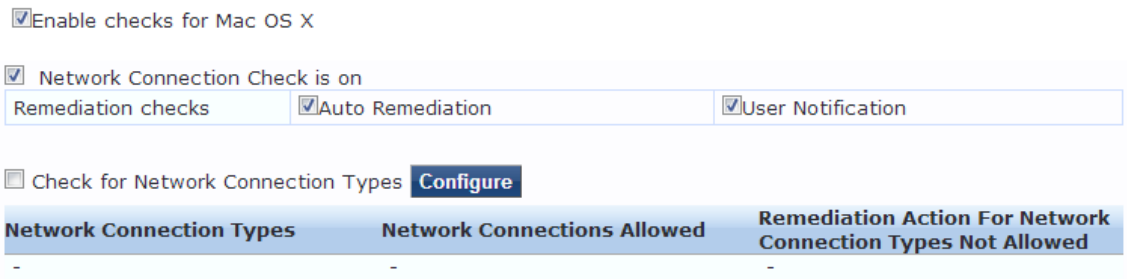
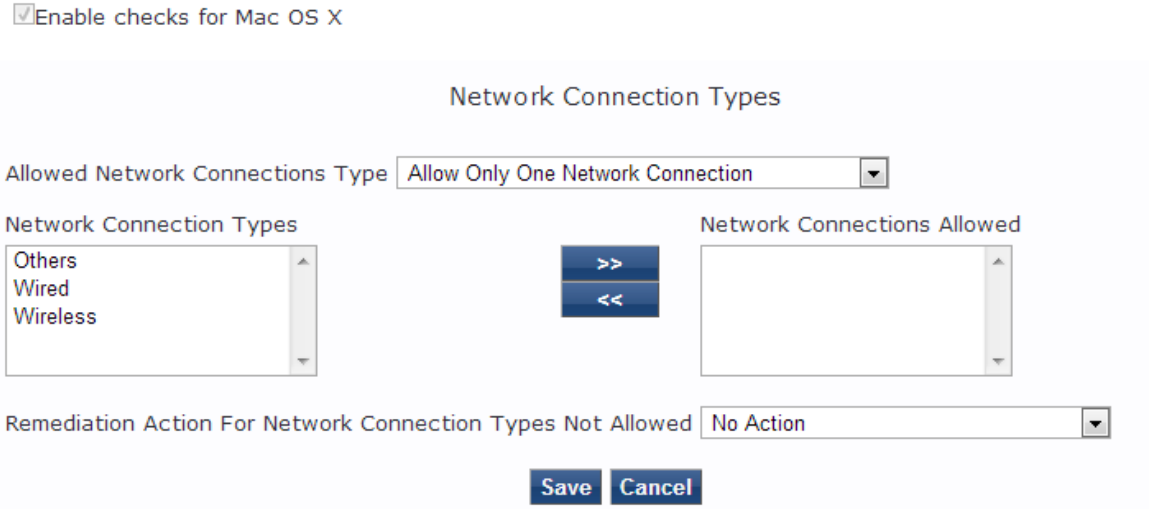


Figure 186: *Network Connections Configuration Page*



Disk Encryption

Disk encryption is a technology that protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

Figure 187: *Disk Encryption Page*

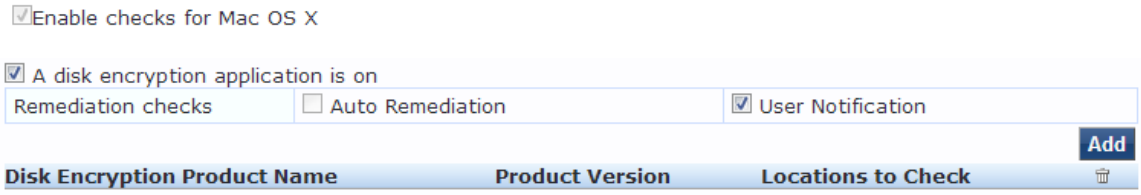
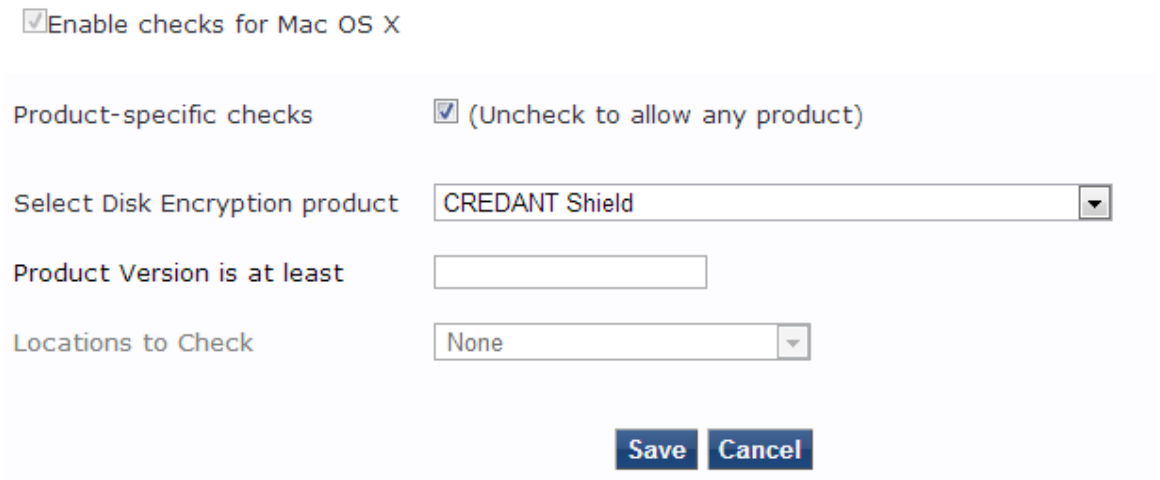


Figure 188: *Disk Encryption Add Page*



Installed Applications

The Installed applications category groups classes that represent software-related objects. In the Installed Applications page, you can turn on the installed applications check and specify information about which installed applications you want to monitor. You can take the following actions:

- Specify installed applications to monitor on a mandatory basis.
- Specify installed applications to be monitored on an optional basis.
- Specify installed applications that are never monitored.
- Specify that only the mandatory and optional applications are monitored.

Figure 189: *Installed Applications Page*

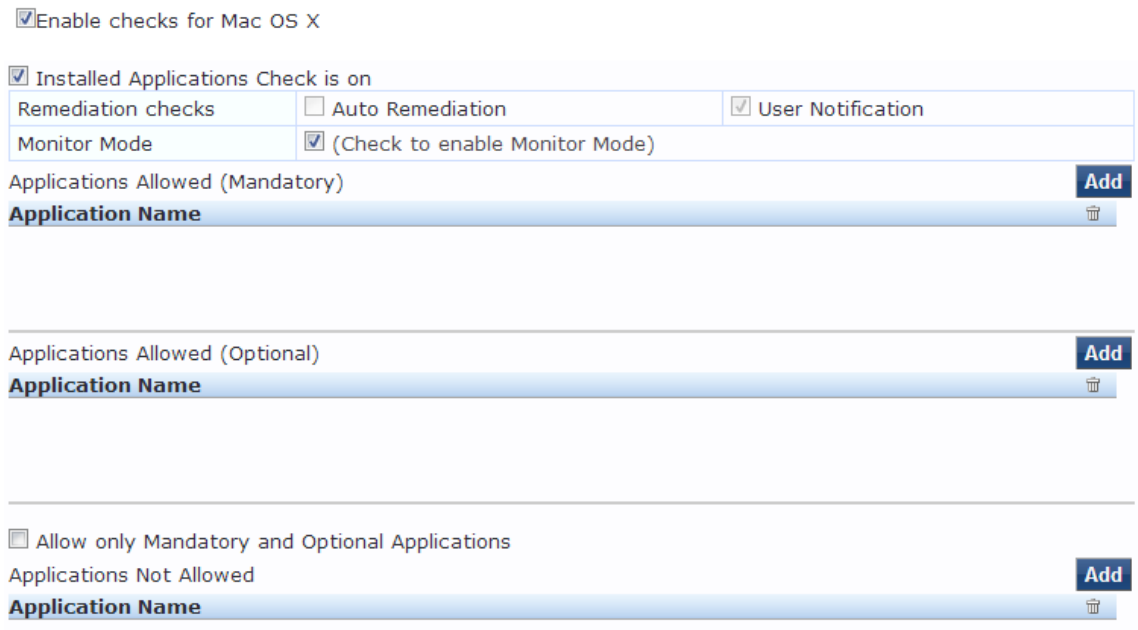
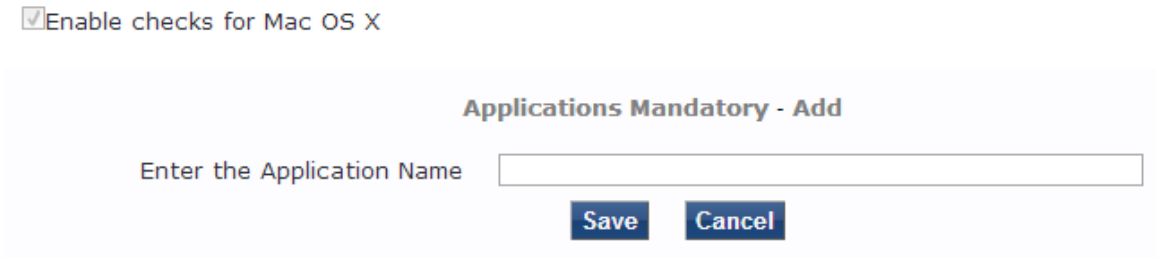


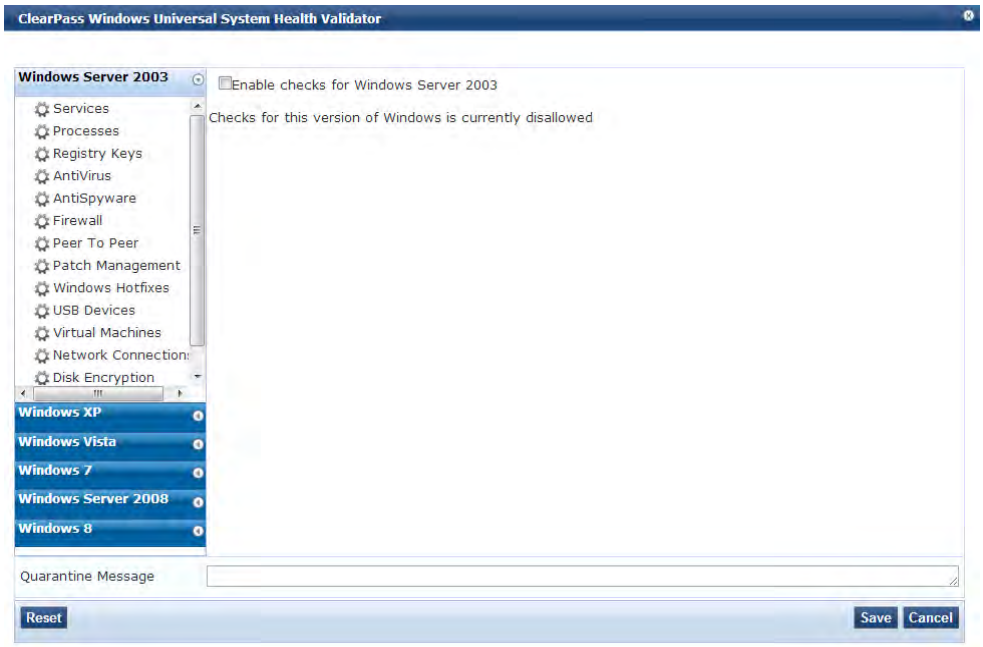
Figure 190: *Installed Applications Add Page*



ClearPass Windows Universal System Health Validator - OnGuard Agent

The **ClearPass Windows Universal System Health Validator** page is displayed after you configure the OnGuard agent and the Windows system in the **Posture Plugins** tab.

Figure 191: *ClearPass Windows Universal System Health Validator*



Select a version of Windows and click the check box to enable checks for that version. Enabling checks for a specific version displays the following set of configuration pages. These pages are explained in the following sections.

- Services on page 226
- Processes on page 226
- Registry Keys on page 229
- AntiVirus on page 232
- AntiSpyware on page 234
- Firewall on page 235
- Peer To Peer on page 236
- Patch Management on page 237
- Windows Hotfixes on page 239
- USB Devices on page 240
- Virtual Machines on page 241
- Network Connections on page 242

- Disk Encryption on page 243
- Installed Applications on page 244

Services

The **Services** page provides a set of widgets for specifying services to run or stop.

Figure 192: *Services Page*

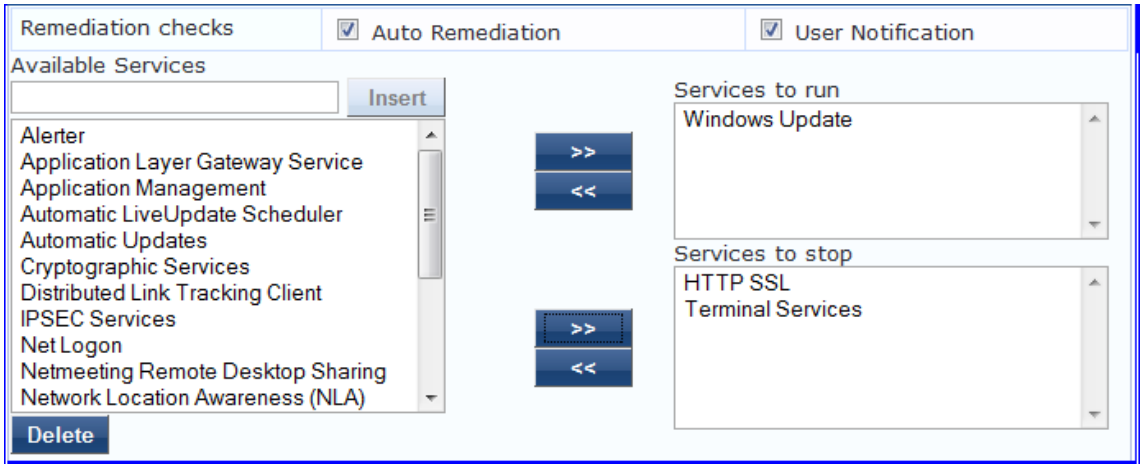


Table 121: *Services Page*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop or start services based on the entries in **Service to run** and **Services to stop** configuration).
User Notification	Enable to allow user notifications for service check policy violations.
Available Services	This scrolling list contains a list of services that you can select and move to the **Services to run** or **Services to stop** panels (using their associated widgets). This list varies depending on OS types. Click the **>>** or **<<** to add or remove, respectively, the services from the **Service to run** or **Services to stop** boxes.
Insert	To add a service to the list of available services, enter its name in the text box adjacent to this button, then click **Insert**.
Delete	To remove a service from the list of available services, select it and click **Delete**.

Processes

The **Processes** page provides a set of parameters to specify which processes to be explicitly present or absent on the system.

Figure 193: *Processes Page (Overview)*

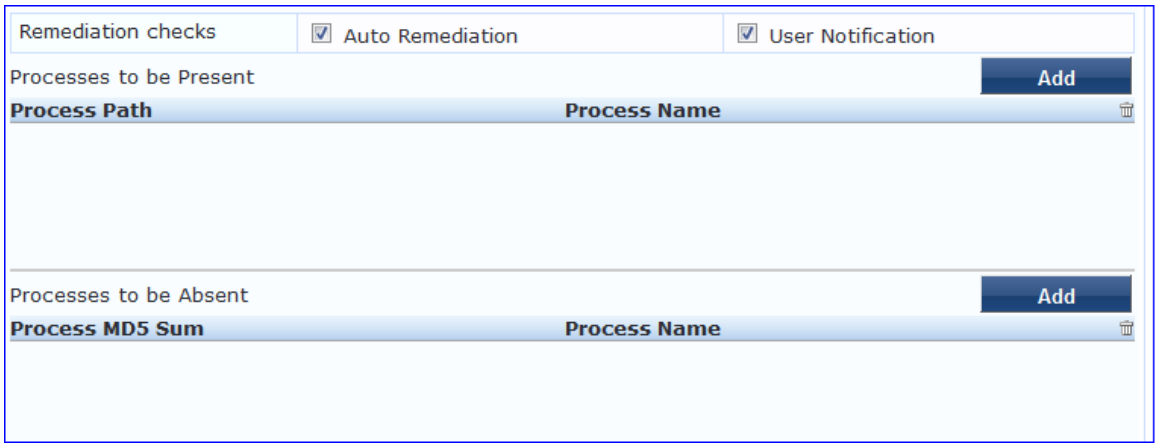


Table 122: *Process Page (Overview - Pre-Add)*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for registry checks (Automatically add or remove registry keys based on the entries in **Registry keys to be present** and **Registry keys to be absent** configuration).
User Notification	Enable to allow user notifications for registry check policy violations.
Processes to be present/absent	Click **Add** to specify a process to be added, either to the **Processes to be present** or **Processes to be absent** lists.

Click **Add** for Process to be Present to display the **Process** page detail.

Processes to be Present

Figure 194: *Process to be Present Page (Detail)*

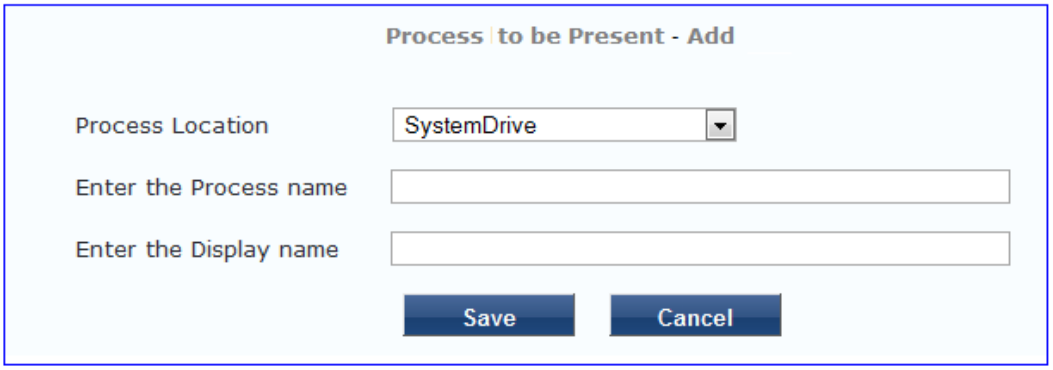


Table 123: *Process to be Present Page (Detail)*

Parameter	Description
Process Location	Choose from Applications, UserBin, UserLocalBin, UserSBin, or None
Enter the Process name	A pathname containing the process executable name.
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

After you save your Process details, the key information appears in the **Processes to be present** page list.

Processes to be Absent

Figure 195: *Process to be Absent Page (Detail)*

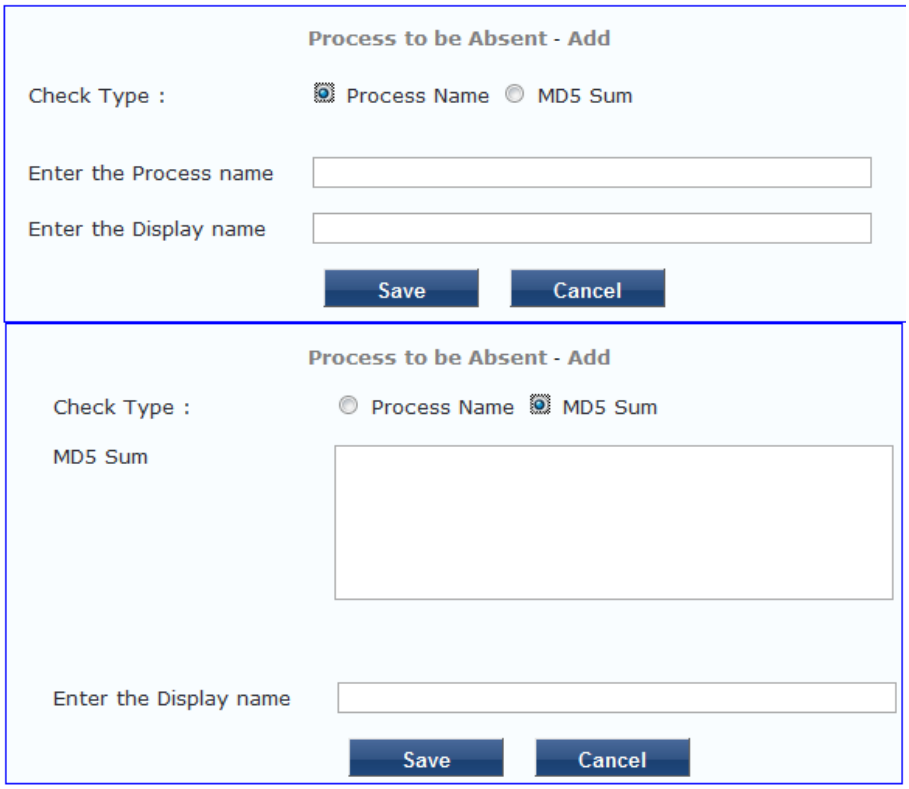
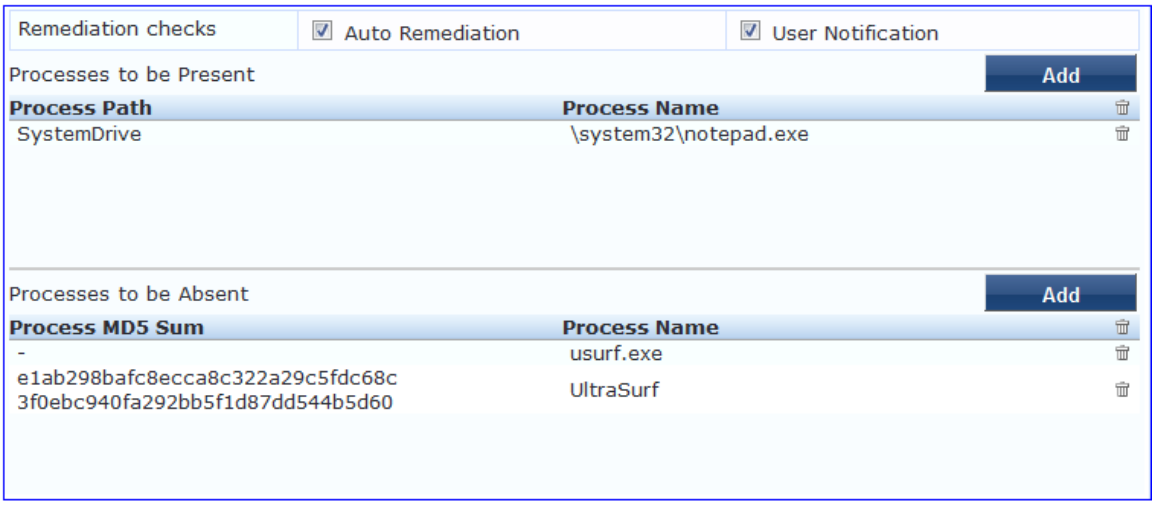


Table 124: *Process to be Absent Page (Detail)*

Parameter	Description
Check Type	Select the type of process check to perform. The agent can look for: • Process Name - The agent looks for all processes that matches with the given name. For example, if notepad.exe is specified, the agent kills all processes whose name matches, regardless of the location from which these processes were started. • MD5 Sum - This specifies one or more (comma separated) MD5 checksums of the process executable file. For example, if there are multiple versions of the process executable, you can specify the MD5 sums of all versions here. The agent enumerates all running processes on the system, computes the MD5 sum of the process executable file, and matches this with the specified list. One or more of the matching processes are then terminated.
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

Figure 196: *Process Page (Overview - Post Add)*



Registry Keys

The **Registry Keys** page allows you to specify which registry keys are to be explicitly present or absent.

Figure 197: *Registry Keys Page (Overview)*

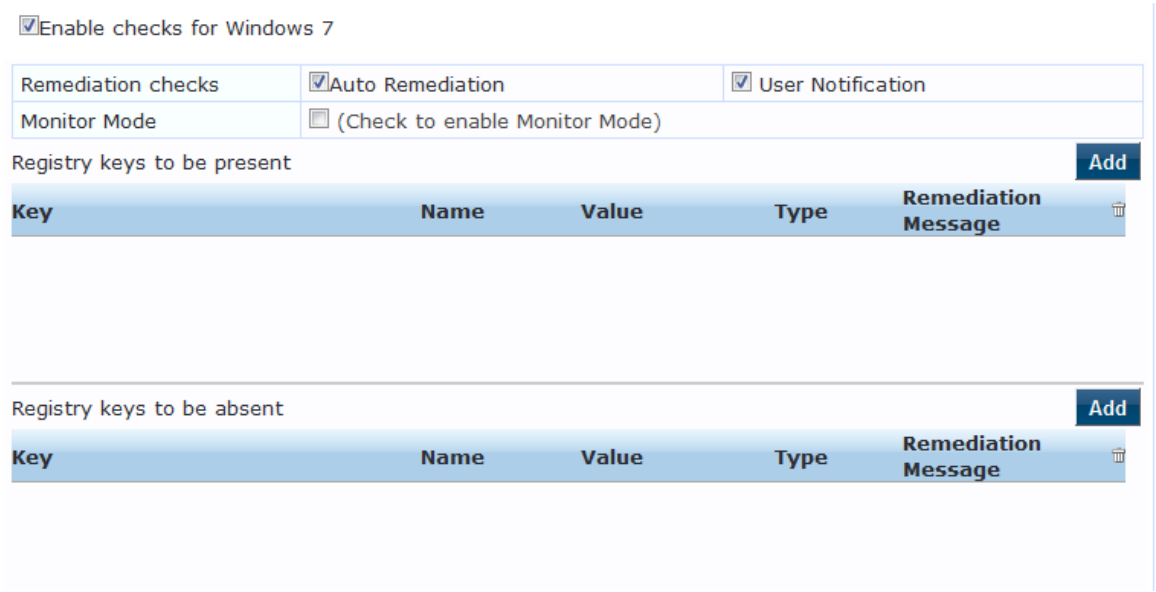


Table 125: *Registry Keys Page (Overview - Pre-Add)*

Parameter	Description
Auto Remediation	Enable auto remediation for registry checks. Use this page to automatically add or remove registry keys based on the entries in **Registry keys to be present** and **Registry keys to be absent** fields.
User Notification	Enable user notifications for registry check policy violations.
Monitor Mode	Enable this to set the health status of the **Registry Keys** health class healthy. This allows administrators to collect information related to missing registry keys without marking the clients as unhealthy even if some registry keys are missing.
Registry keys to be present	Click **Add** to specify a registry key to be added to the **Registry keys to be present** list. If the specified registry key is not present, the remediation message that is added in the **Registry Keys Page (Detail)** window is displayed on **OnGuard Agent**.
Registry keys to be absent	Click **Add** to add a registry key to the **Registry keys to be absent** list. If the specified registry key is not absent, the remediation message that is added in the **Registry Keys Page (Detail)** window is displayed on **OnGuard Agent**.

Click **Add** to display the **Registry** page detail.

Registry Keys to be Absent

Figure 198: *Registry Keys Page (Detail)*

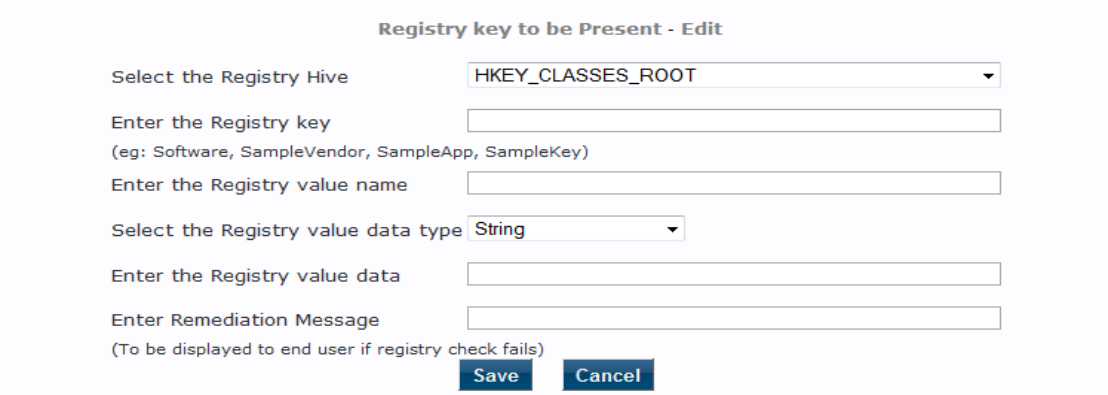
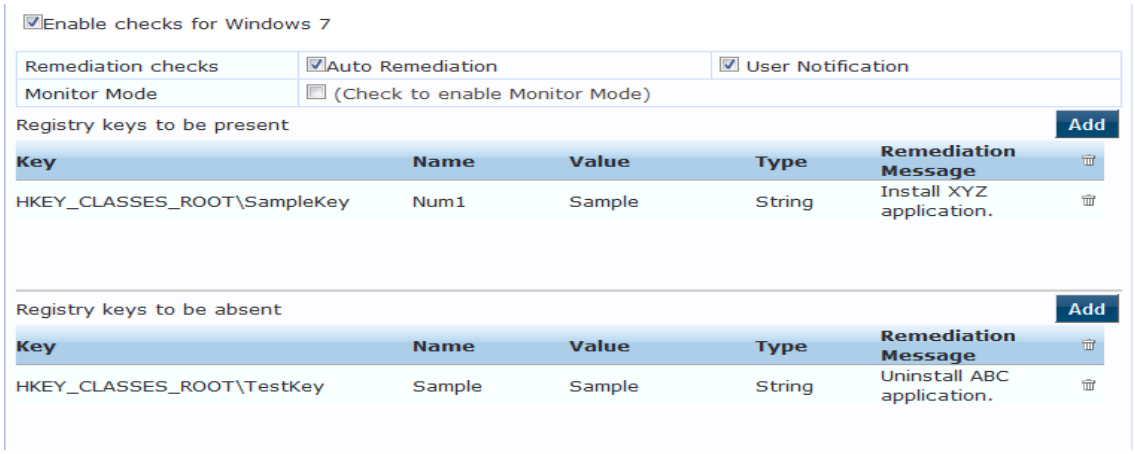


Table 126: *Registry Keys Page (Detail)*

Parameter	Description
Select the Registry Hive	Specify the registry hive from the following options: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS • HKEY_CURRENT_CONFIG
Enter the Registry key	Specify the registry key using the examples given in the GUI.
Enter the Registry value name	Specify the name of the registry value.
Select the Registry value data type	Specify the registry value data types. The data type can be any of the following: • Multi String • String • DWORD • QWORD • Expandable String
Enter the Registry value data	Specify the registry value.
Enter Remediation Message	Specify the custom remediation message to be displayed to end users if registry check is failed.

After you save the Registry details, the remediation message appears in the **Registry** page list.

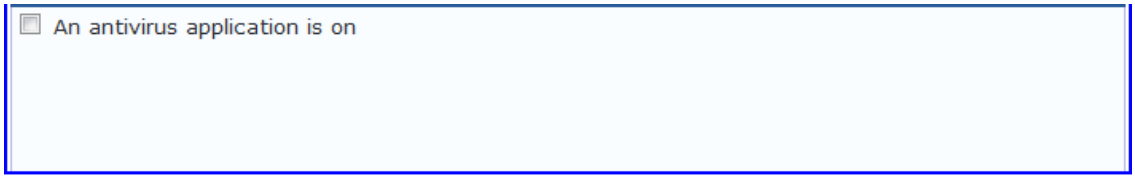
Figure 199: *Registry Keys Page (Overview - Post Add)*



AntiVirus

In the **Antivirus** page, you can turn on an Antivirus application.. Click **An anti-virus application is on** to configure the Antivirus application information.

Figure 200: *Antivirus Page (Overview - Before)*

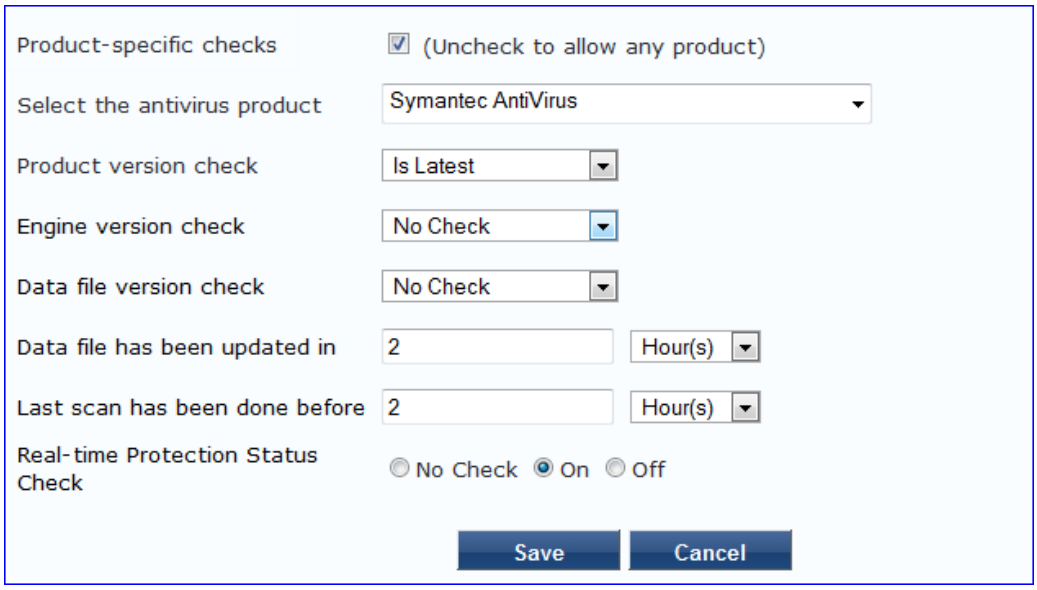


When enabled, the **Antivirus** detail page appears.

Figure 201: *Antivirus Page (Detail 1)*

Click **Add** to specify product, and version check information.

Figure 202: *Antivirus Page (Detail 2)*



After you save your Antivirus configuration, it appears in the **Antivirus** page list.

Figure 203: *Antivirus Page (Overview - After)*

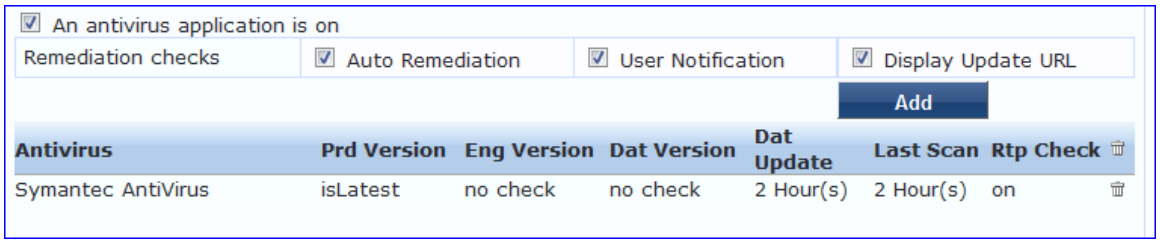


Table 127: *Antivirus Page*

Interface	Parameter	Description
Antivirus Page	• An Antivirus Application is On • Auto Remediation • User Notification • Display Update URL	• Click **Antivirus application is on** to enable testing of health data for configured Antivirus application(s). • Check the **Auto Remediation** check box to enable auto remediation of anti-virus status. • Check the **User Notification** check box to enable user notification of policy violation of anti-virus status. • Check the **Display Update URL** check box to show the origination URL of the update.
Antivirus Page (Detail 1)	• Add	• To configure Antivirus application attributes for testing against health data, click **Add**.
Antivirus Page (Detail 2)	• Product-specific checks • Select the antivirus product • Product version check • Engine version check	Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on

Table 127: *Antivirus Page (Continued)*

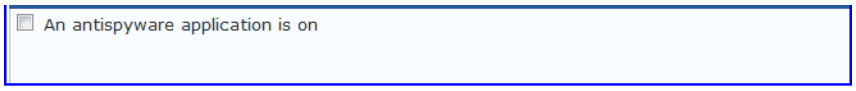
Interface	Parameter	Description

	• Engine version check
	• Datafile version check
	• Data file has been updated in
	• Last scan has been done before
	• Real-time Protection Status Check
		the UI.
		• Select the antivirus product - Select a vendor from the list.
		• Product version check - No Check, Is Latest (requires registration with ClearPass portal), At Least, In Last N Updates (requires registration with ClearPass Portal).
		• Engine version check - Same choices as product version check.
		• Data file version check - Same choices as product version check.
		• Data file has been updated in - Specify the interval in hours, days, weeks, or months.
		• Last scan has been done before - Specify the interval in hours, days, weeks, or months.
		• Real-time Protection Status Check
		  ▪ No Check - Dell Networking W-ClearPass Policy Manager does not use RTP Status value for health evaluation. This means that the client is treated as **healthy** irrespective of the value of RTP.
		  ▪ On - Client is marked as **healthy** only if the value of RTP status is On.
		  ▪ Off - Client is marked as **healthy** only if the value of RTP status is Off.

AntiSpyware

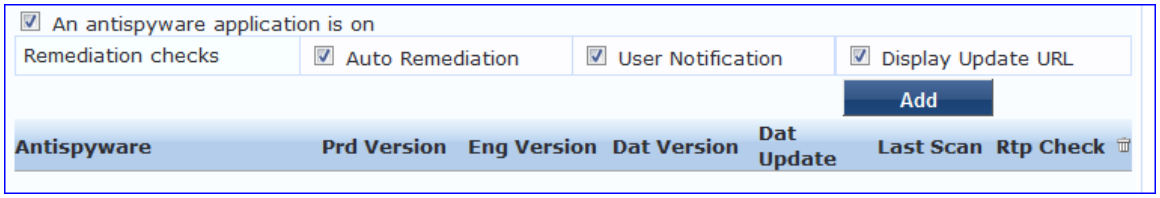
In the **AntiSpyware** page, an administrator can specify that an AntiSpyware application must be on and allows drill-down to specify information about the AntiSpyware application. Click **An Antipyware Application is On** to configure the AntiSpyware application information.

Figure 204: *AntiSpyware Page (Overview Before)*



When enabled, the **AntiSpyware** detail page appears.

Figure 205: *AntiSpyware Page (Detail 1)*



Click **Add** to specify product, and version check information.

Figure 206: *AntiSpyware Page (Detail 2)*

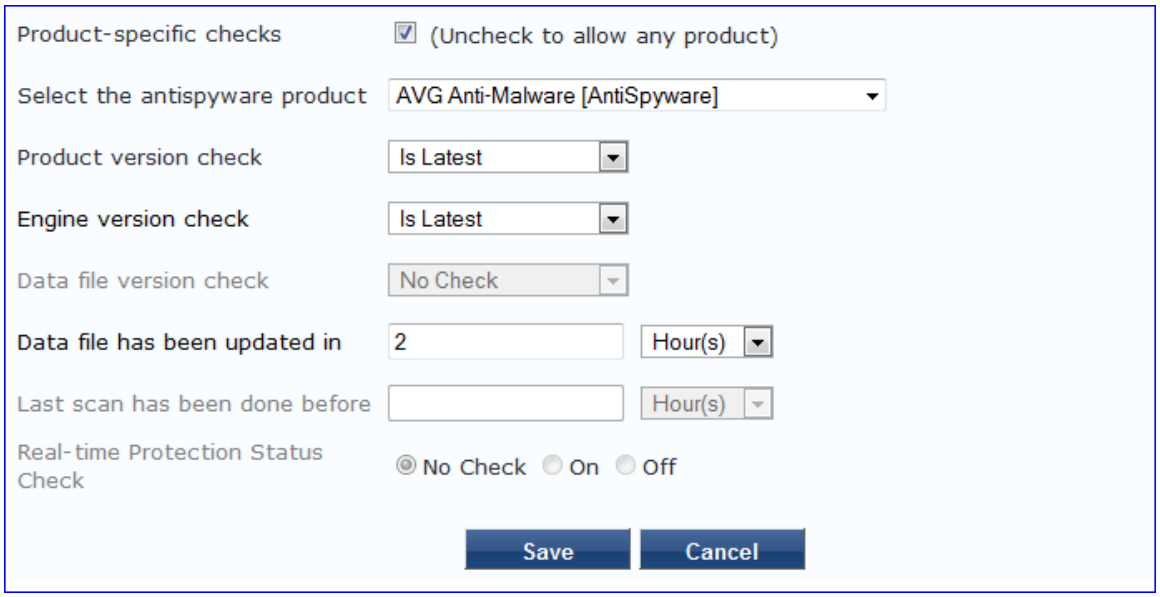


Figure 207: *AntiSpyware Page (Overview After)*

When you save your AntiSpyware configuration, it appears in the **AntiSpyware** page list.

The configuration elements are the same for antivirus and antispyware products. Refer to the previous AntiSpyware configuration instructions.

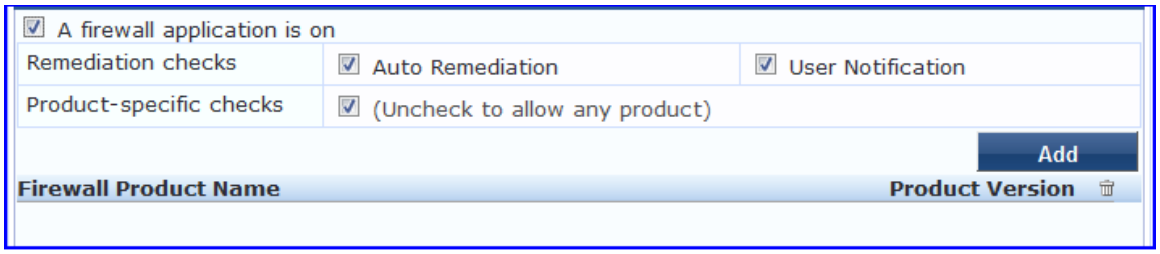
Firewall

In the **Firewall** page, you can specify that a Firewall application must be on and specify information about the Firewall application.

Figure 208: *Firewall Page (Overview Before)*

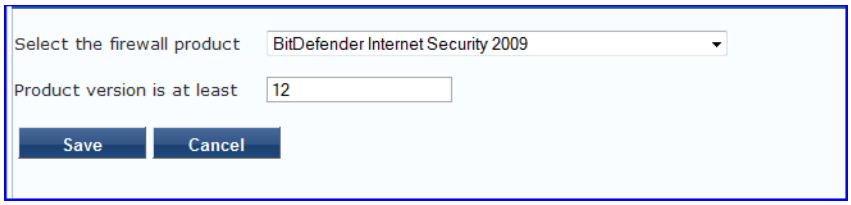
In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

Figure 209: *Firewall Page (Detail 1)*



When enabled, the **Firewall** detail page appears.

Figure 210: *Firewall Page (Detail 2)*



When you save your Firewall configuration, it appears in the **Firewall** page list.

Figure 211: *Firewall Page (Overview After)*

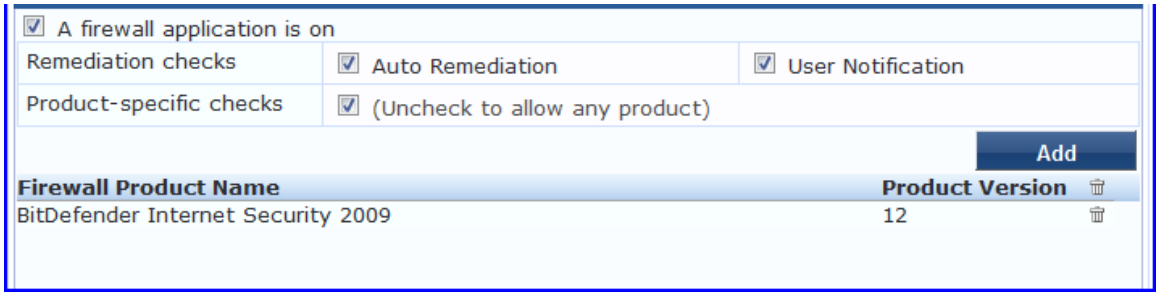


Table 128: *Firewall Page*

Interface	Parameter	Description
Firewall Page	• A Firewall Application is On • Auto Remediation • User Notification • Uncheck to allow any product	• Check the **Firewall Application is On** check box to enable testing of health data for configured firewall application(s). • Check the **Auto Remediation** check box to enable auto remediation of firewall status. • Check the **User Notification** check box to enable user notification of policy violation of firewall status. • Uncheck the **Uncheck to allow any product** check box to check whether any firewall application (any vendor) is running on the end host.
Firewall Page (Detail 1)	• Add • Trashcan icon	• To configure firewall application attributes for testing against health data, click **Add**. • To remove configured firewall application attributes from the list, click the **trashcan icon** in that row.
Firewall Page (Detail 2)	Product/Version	Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on the UI. • Select the firewall product - Select a vendor from the list • Product version is at least - Enter the version of the product.

Peer To Peer

The **Peer To Peer** page provides a set of widgets for specifying specific peer to peer applications or networks to be explicitly stopped. When you select a peer to peer network, all applications that make use of that network are stopped.

Figure 212: *Peer to Peer Page*

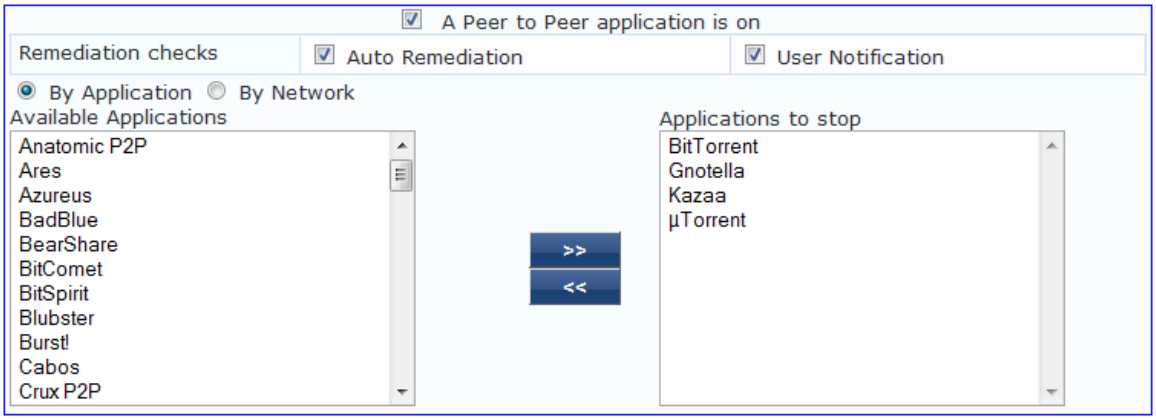


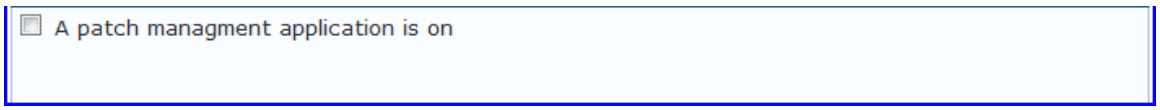
Table 129: *Peer to Peer Page*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop peer to peer applications based on the entries in **Applications to stop** configuration).
User Notification	Enable to allow user notifications for peer to peer application/network check policy violations.
By Application / By Network	Select the appropriate radio button to select individual peer to peer applications or a group of applications that use specific p2p networks.
Available Applications	This scrolling list contains a list of applications or networks that you can select and move to the **Applications to stop** panel. Click the **>>** or **<<** to add or remove, respectively, the applications or networks from the **Applications to stop** box.

Patch Management

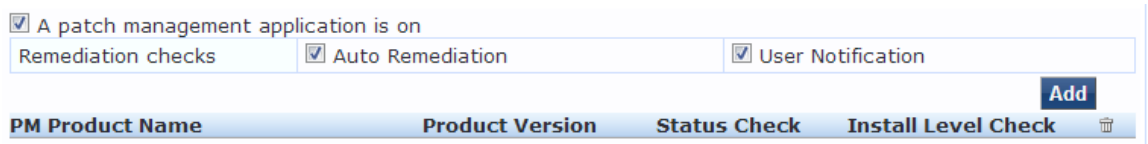
In the **Patch Management** page, you can specify that a patch management application must be on and allows drill-down to specify information about the patch management application. Click **A patch management application is On** to configure the patch management application information.

Figure 213: *Patch Management Page (Overview - Before)*



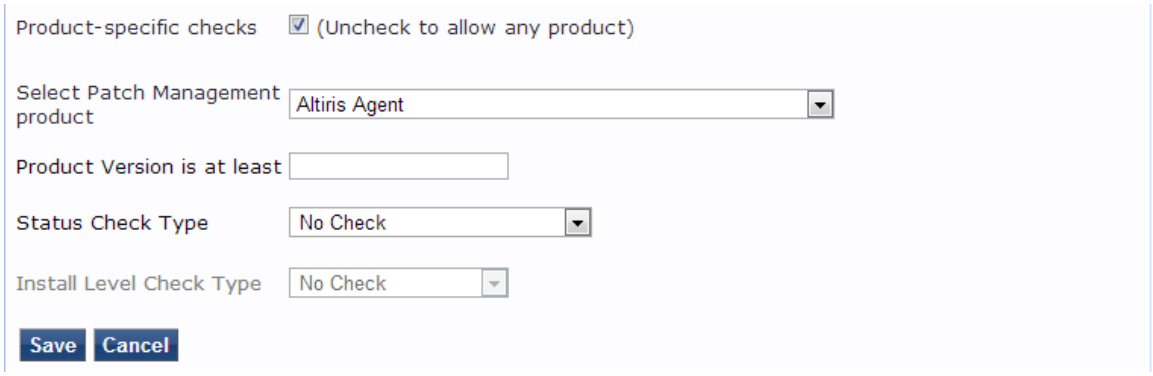
When enabled, the **Patch Management** detail page appears.

Figure 214: *Patch Management Page (Detail 1)*



Click **Add** to specify PM Product Name, Product Version, Status Check and Install Level Check information.

Figure 215: *Patch Management Page (Detail 2)*



When you save your patches configuration, it appears in the **Patch Management** page list.

Figure 216: *Patch Management Page (Overview - After)*

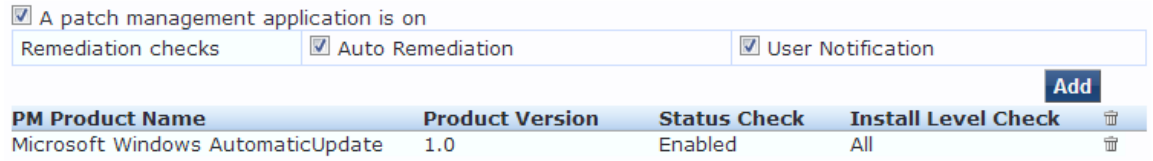


Table 130: *Patch Management Page*

Interface	Parameter	Description
Patch Management Page	• A patch management application is on • Auto Remediation • User Notification • Uncheck to allow any product	• Check the **A patch management application is on** to enable testing of health data for configured Antivirus application(s). • Check the **Auto Remediation** check box to enable auto remediation of patch management status. • Check the **User Notification** check box to enable user notification of policy violation of patch management status. • Clear **Uncheck to allow any product** check box to check whether any patch management application (any vendor) is running on the end host.
Patch Management Page (Detail 1)	• Add • Trashcan icon	• To configure patch management application attributes for testing against health data, click **Add**. • To remove configured patch management application attributes from the list, click the **trashcan icon** in that row.
Patch Management Page (Detail 2)	Product/Version	Configure settings for which to test against health data. All checks might not be available for some products. Where checks are not available, they are shown in disabled state on the UI. • **Select Patch Management product:** Select a vendor. This option is *only* enabled if the Product-specific checks check box is checked. • **Product version is at least:** Enter version number. This option is *only* enabled if the Product-specific checks check box is checked.

Table 130: *Patch Management Page (Continued)*

Interface	Parameter	Description
		• **Status Check Type:** Select this field to check whether Patch Agent is enabled or not. Dell Networking W-ClearPass Policy Manager server compares the Patch Agent Status sent by OnGuard Agent with the configured value. If the Patch Agent Status value is different from configured value, then client is treated as unhealthy. If Auto-remediation is enabled, then OnGuard Agent changes the Patch Agent Status on client to the configured value. Select any of the following options: ▪ **No Check** - Dell Networking W-ClearPass Policy Manager server ignores Patch Agent Status value. This means it will not check status of Patch Agent application on client. ▪ **Enabled** - Patch Agent is turned on and automatically update the client. ▪ **Disabled** - Patch Agent is disabled and it will not check for missing patches and update the client. ▪ **Notify Before Download** - Patch Agent is turned on and will notify user before downloading updates. ▪ **Notify Before Install** - Patch Agent is turned on and will notify user before installing updates. **NOTE:** The values specific to the selected product are displayed in the **Status Check Type** field. For example, all the 5 values are displayed for **Microsoft Windows AutomaticUpdate**. For **SCCM**, only **No Check**, **Disabled**, and **Notify Before Install** are displayed. • **Install Level Check:** Select No Check, All, Selected on Server, or Security. This option is *only* enabled if the Product-specific check box is checked. For Microsoft SCCM, selecting All, Selected on Server, or Security will return the full list of all missing patches. ▪ **All**: Check for all missing patches, and search for all available patches. ▪ **Selected on Server**: Check only for the patches pre-selected on the server. Some Patch Management products can push the patches to the endpoint device. This option provides the ability to check for only the pre-selected patches. ▪ **Security**: Check only for security updates. Some of the products can install only security-related patches. **NOTE:** If you select the Microsoft Windows Update Agent from the Select Patch Management product list and you select an option from the Install Level Check list, the results are listed below: ▪ **All**: Returns the full list of missing patches. ▪ **Selected on Server**: Returns a list of missing patches that are pre-selected on the server site. ▪ **Security**: Returns a list of missing patches that Microsoft classifies as Security Updates.

Windows Hotfixes

The **Windows Hotfixes** page provides a set of widgets for checking if specific Windows hotfixes are installed on the endpoint.

Figure 217: *Windows Hotfixes Page*

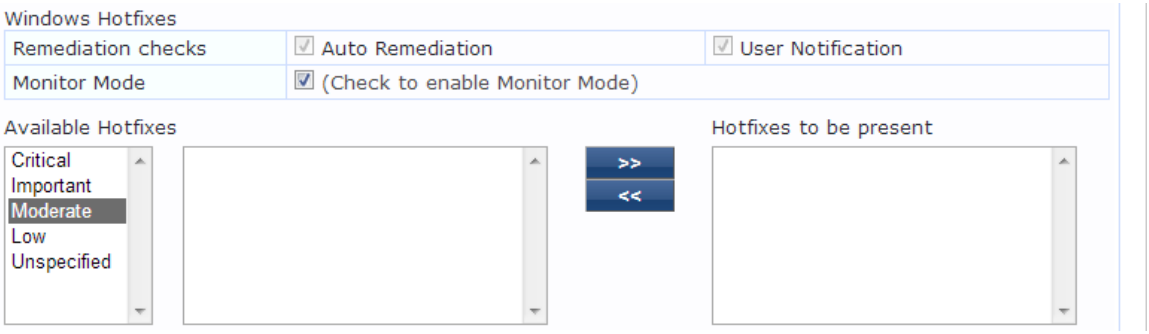


Table 131: *Windows Hotfixes*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for hotfixes checks (Automatically trigger updates of the specified hotfixes).
User Notification	Enable to allow user notifications for hotfixes check policy violations.
Monitor Mode	Click to enable Monitor Mode.
Available Hotfixes	The first scrolling list lets you select the criticality of the hotfixes. Based on this selection, the second scrolling list contains a list of hotfixes that you can select and move to the **Hotfixes to be present** panel (using their associated widgets). Click the **>>** or **<<** to add or remove, respectively, the hotfixes from the **Hotfixes to run** boxes.

USB Devices

The **USB Devices** page provides configuration to control USB mass storage devices attached to an endpoint.

Figure 218: *USB Devices*

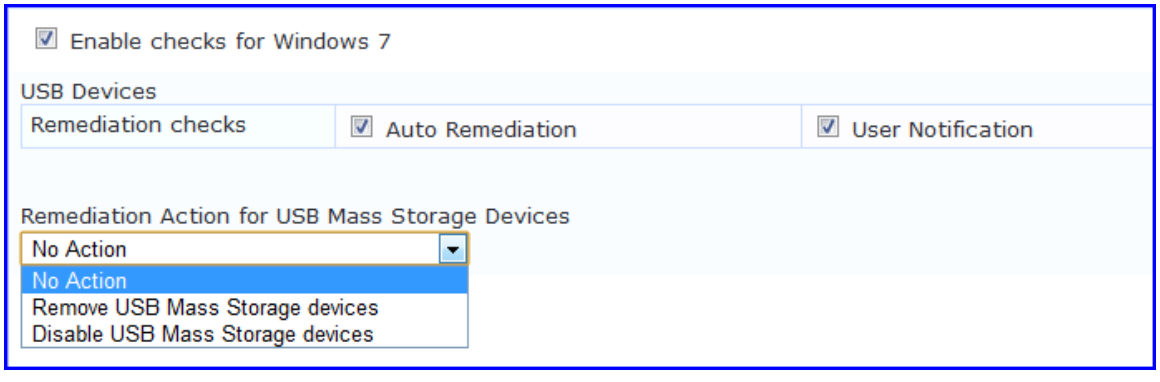


Table 132: *USB Devices*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for USB mass storage devices attached to the endpoint (Automatically stop or eject the drive).
User Notification	Enable to allow user notifications for USB devices policy violations.
Remediation Action for USB Mass Storage Devices	• No Action - Take no action; do not eject or disable the attached devices. • Remove USB Mass Storage Devices - Eject the attached devices. • Remove USB Mass Storage Devices - Stop the attached devices.

Virtual Machines

The **Virtual Machines** page provides configuration to Virtual Machines utilized by your network.

Figure 219: *Virtual Machines*

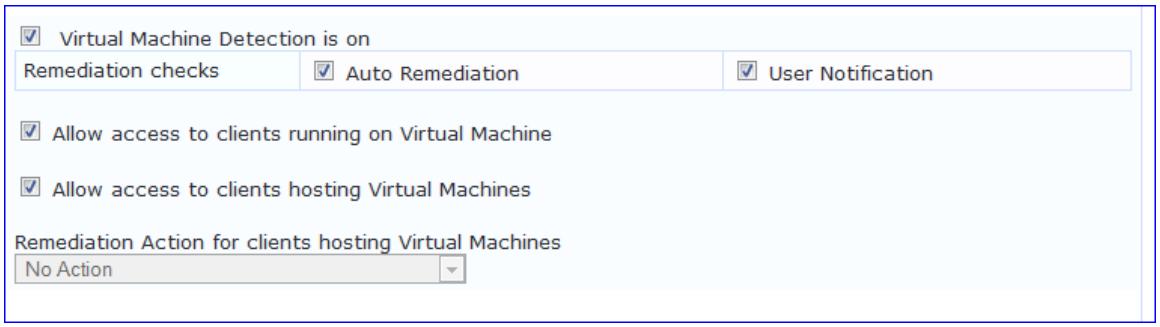


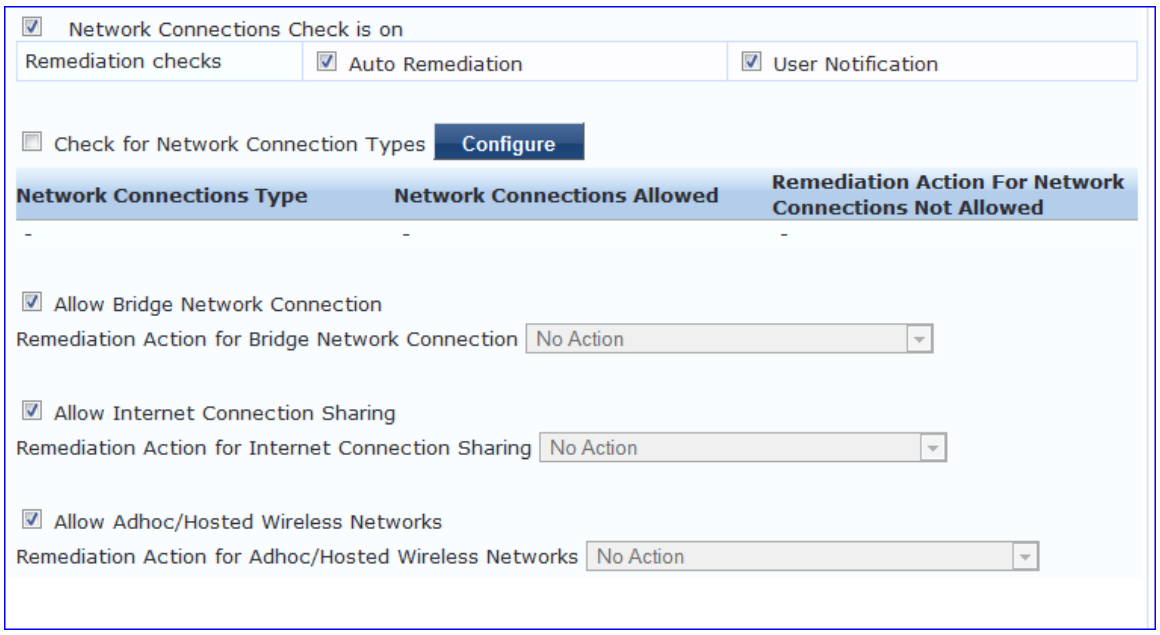
Table 133: *Virtual Machines*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for virtual machines connected to the endpoint.
User Notification	Enable to allow user notifications for virtual machine policy violations.
Allow access to clients running on Virtual Machine	Enable to allow clients that running a VM to be accessed and validated.
Allow access to clients hosting Virtual Machine	Enable to allow clients that hosting a VM to be accessed and validated.
Remediation Action for clients hosting Virtual Machines	• No Action - Take no action; do not stop or pause virtual machines. • Stop all Virtual Machines running on Host - Stop the VM clients that are running on Host. • Pause all Virtual Machines running on Host - Pause the VM clients that are running on Host.

Network Connections

The **Network Connections** page provides configuration to control network connections based on connection type.

Figure 220: *Network Connections*



Select the **Check for Network Connection Types** check box, and then click **Configure** to specify the type of connection that you want to include.

Configure Network Connection Type

Figure 221: *Network Connection Type Configuration*

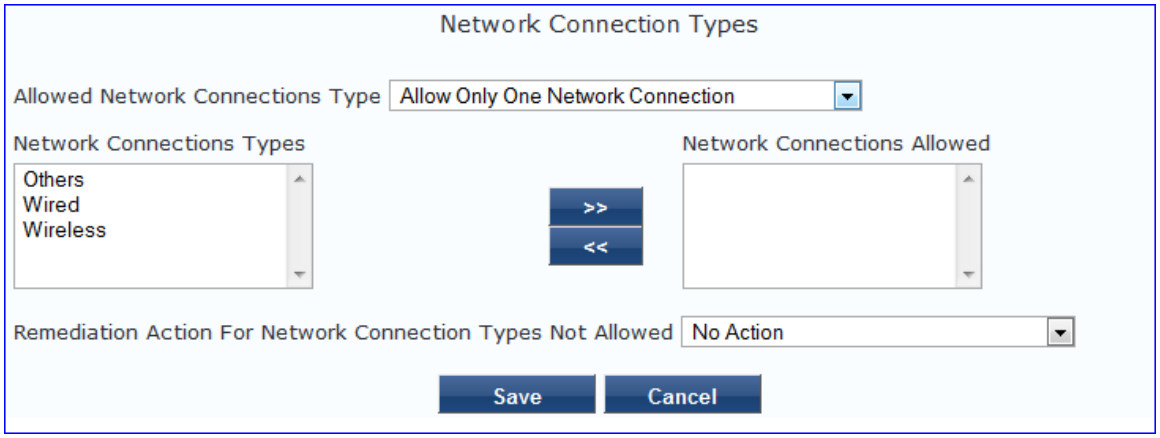


Table 134: *Network Connection Type Configuration Page*

Parameter	Description
Allow Network Connections Type	• Allow Only One Network Connection • Allow One Network Connection with VPN • Allow Multiple Network Connections
Network Connection Types	Click the **>>** or **<<** to add or remove Others, Wired, and Wireless connection types.
Remediation Action for USB Mass Storage Devices	• No Action - Take no action; do not eject or disable the attached devices. • Disable Network Connections - Disable network connections for the configured network type.

Click **Save** after you finish. This returns you to the Network Connections Configuration page. The remaining fields on this page are described below.

Table 135: *Network Connections Configuration*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for network connections.
User Notification	Enable to allow user notifications network connection policy violations.
Remediation Action for Bridge Network Connection	If **Allow Bridge Network Connection** is disabled, then specify whether to take no action when a bridge network connection exists or to disable all bridge network connections.
Remediation Action for Internet Connection Sharing	If **Allow Internet Connection Sharing** is disabled, then specify whether to take no action when Internet connection sharing exists or to disable Internet connection sharing.
Remediation Action for Adhoc/Hosted Wireless Networks	If **Allow Adhoc/Hosted Wireless Networks** is disabled, then specify whether to take no action when an adhoc wireless networks exists or to disable all adhoc/hosted wireless networks.

Disk Encryption

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

Figure 222: *Disk Encryption Configuration Page*

Table 136: *Disk Encryption Parameters*

Parameter	Description
User Notification	Enable to allow user notifications for virtual machine policy violations.
Product-specific checks	Clear to allow disk encryption on any product. The Select Disk Encryption product and Product Version is at least fields are disabled after you clear the checkbox.
Select Disk Encryption product	Select a specific disk encryption product.
Product Version is at least	Search for the production version of the selected product.
Locations to Check	Select location to check. The options are None, System Root Drive, All Drives, or Specific Locations.

Installed Applications

The Installed applications category groups classes that represent software-related objects. Access to these objects is supported by Windows Installer. Examples of objects in this category are installed products, file specifications, and registration actions.

In the **Installed Applications** page, you can turn on the installed applications check and specify information about which installed applications you want to monitor. You can take the following actions:

- Specify installed applications to monitor on a mandatory basis.
- Specify installed applications to be monitored on an optional basis.
- Specify installed applications that are never monitored.
- Specify that only the mandatory and optional applications are monitored.

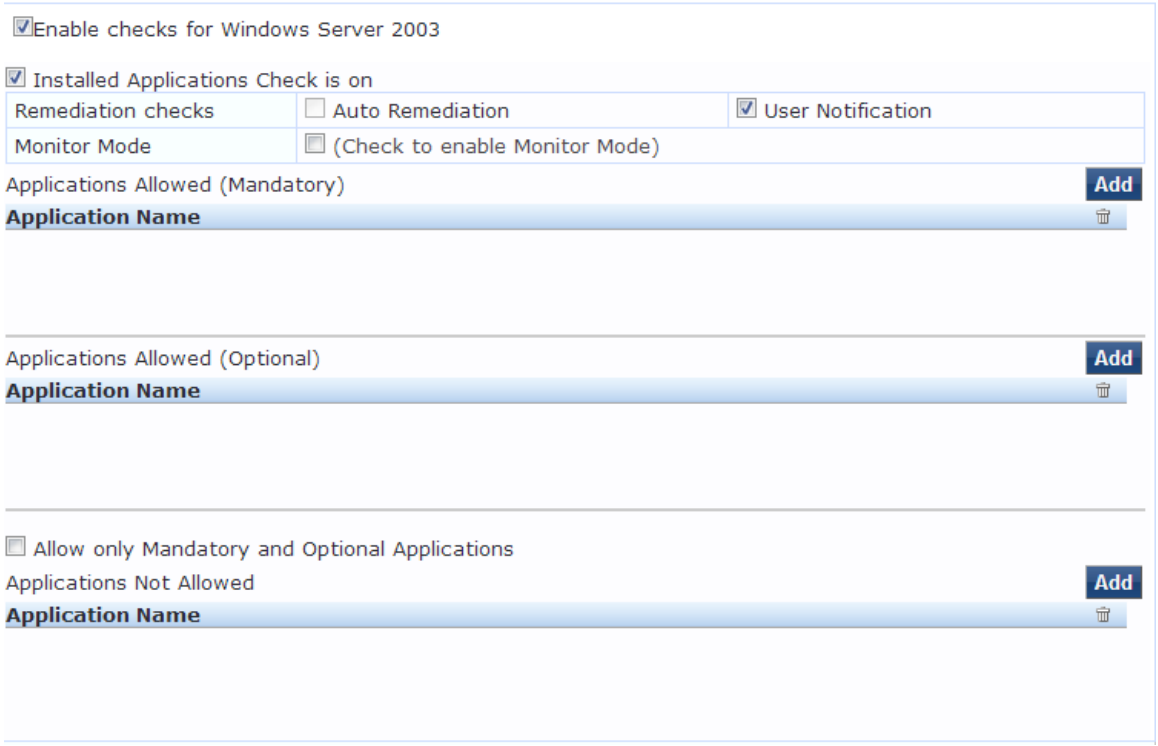


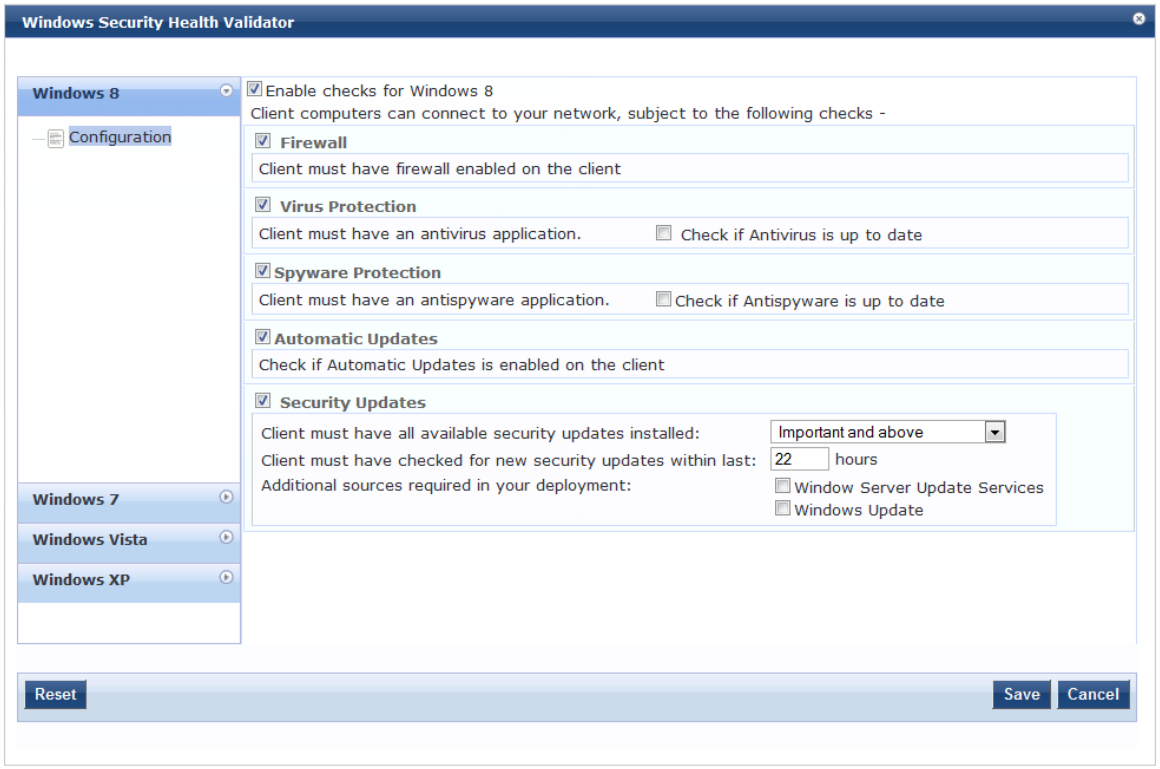
Table 137: *Installed Applications Configuration Page*

Parameter	Description
Remediation checks	Auto-remediation for Installed Applications health class is not supported.
User Notification	A Remediation message having a list of applications to install/uninstall will be displayed to end user.
Monitor Mode	Enable **Monitor Mode** to treat all the installed applications as always healthy.
Applications Allowed (Mandatory)	Enter the application name as it is shown in Add/Remove Programs.
Applications Allowed (Optional)	Enter the application name as it is shown in Add/Remove Programs.
Allow only Mandatory and Optional Applications	Check to allow only selected applications. All applications other than 'Allowed Applications, including both mandatory and optional' must be removed or uninstalled.

Windows Security Health Validator - OnGuard Agent

This validator checks for the presence of specific types of security applications. An administrator can use the check boxes to restrict access based on the absence of the selected security application types.

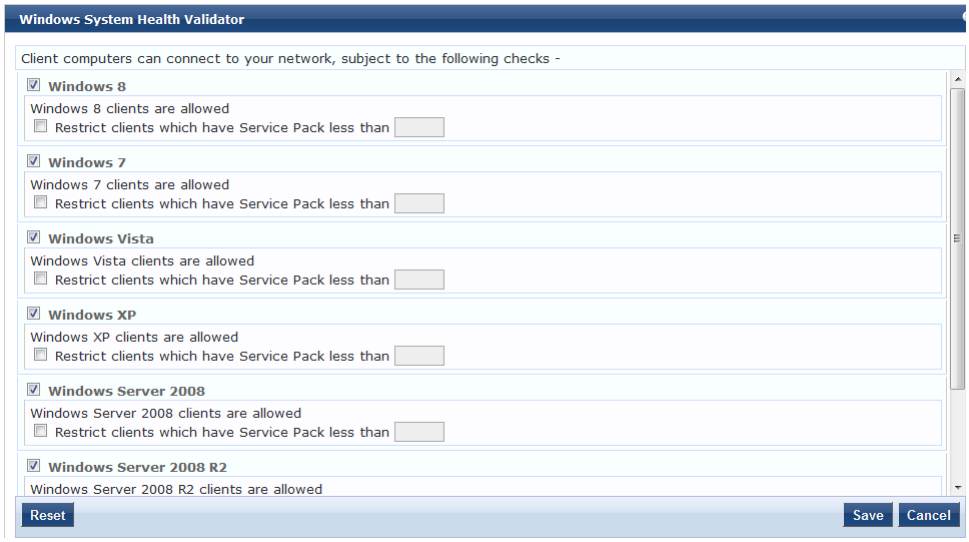
Figure 223: *Windows Security Health Validator*



Windows System Health Validator - OnGuard Agent

This validator checks for current Windows Service Packs. The OnGuard Agent also supports legacy Windows operating systems such as and Windows Server 2003. An administrator can use the check boxes to enable support of specific operating systems and to restrict access based on service pack level.

Figure 224: *Windows System Health Validator - OnGuard Agent (Overview)*



Adding and Modifying Posture Servers

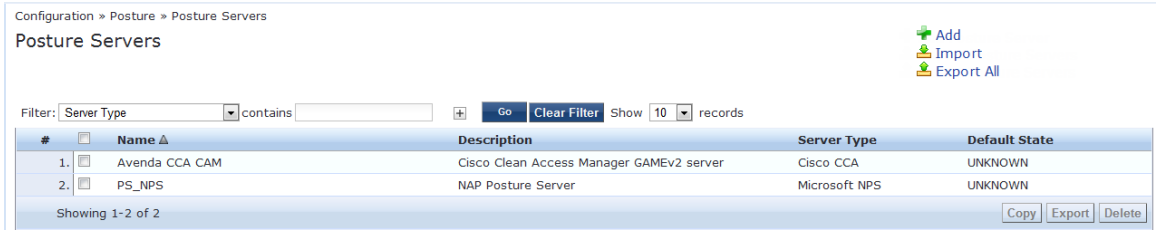
Policy Manager can forward all or part of the posture data received from the client to Posture Servers. The Posture Server evaluates the posture data and returns Application Posture Tokens.

From the **Services** page (**Configuration > Service**), you can configure a posture server for a new service (as part of the flow of the **Add Service** wizard), or modify an existing posture server directly (**Configuration > Posture > Posture Servers**, then click on its name in the **Posture Servers** listing).

Depending on the **Protocol** and **Requested Credentials**, different tabs and fields appear.

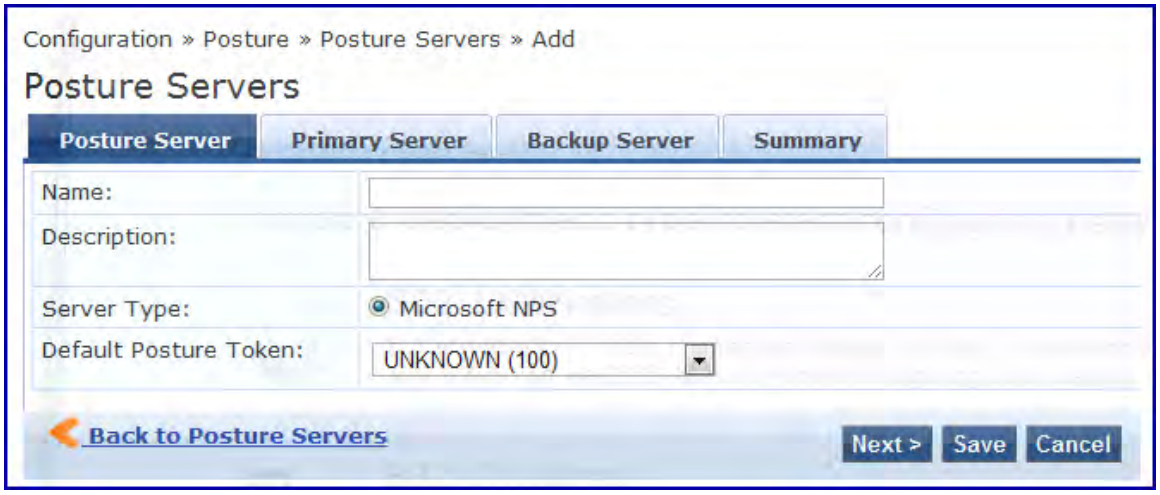
For more information, see Microsoft NPS on page 247.

Figure 225: *Posture Servers Listing Page*



When you click **Add Posture Server** from any of these locations, Policy Manager displays the **Posture Servers** configuration page.

Figure 226: *Add Posture Server Page*



Microsoft NPS

Use the Microsoft NPS server when you want Policy Manager to have health - NAP Statement of Health (SoH) credentials - evaluated by the Microsoft NPS Server.

Table 138: *Microsoft NPSSettings (Posture Server tab)*

Parameter	Description
Name/Description:	Freeform label and description.
Server Type:	Always **Microsoft NPS**.
Default Posture Token:	Posture token assigned if the server is unreachable or if there is a posture check failure. Select a status from the drop-down list.

Figure 227: *Microsoft NPS Settings (Primary and Backup Server tabs)*

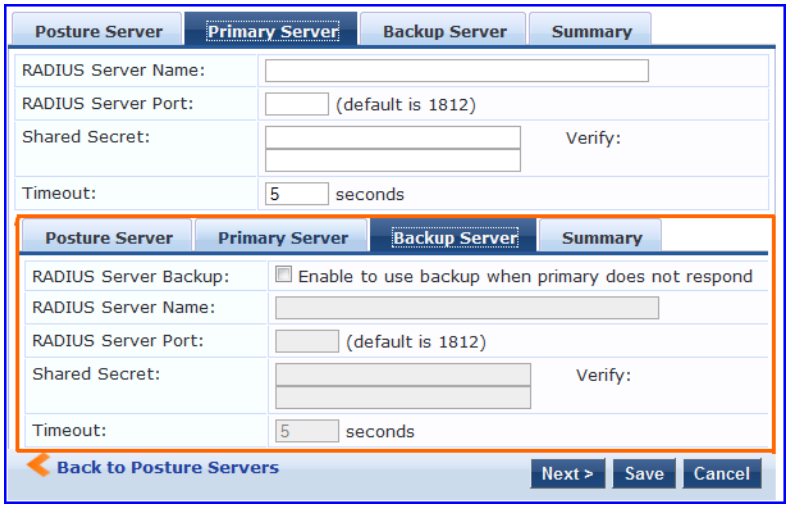


Table 139: *Microsoft NPS Settings (Primary and Backup Server tabs)*

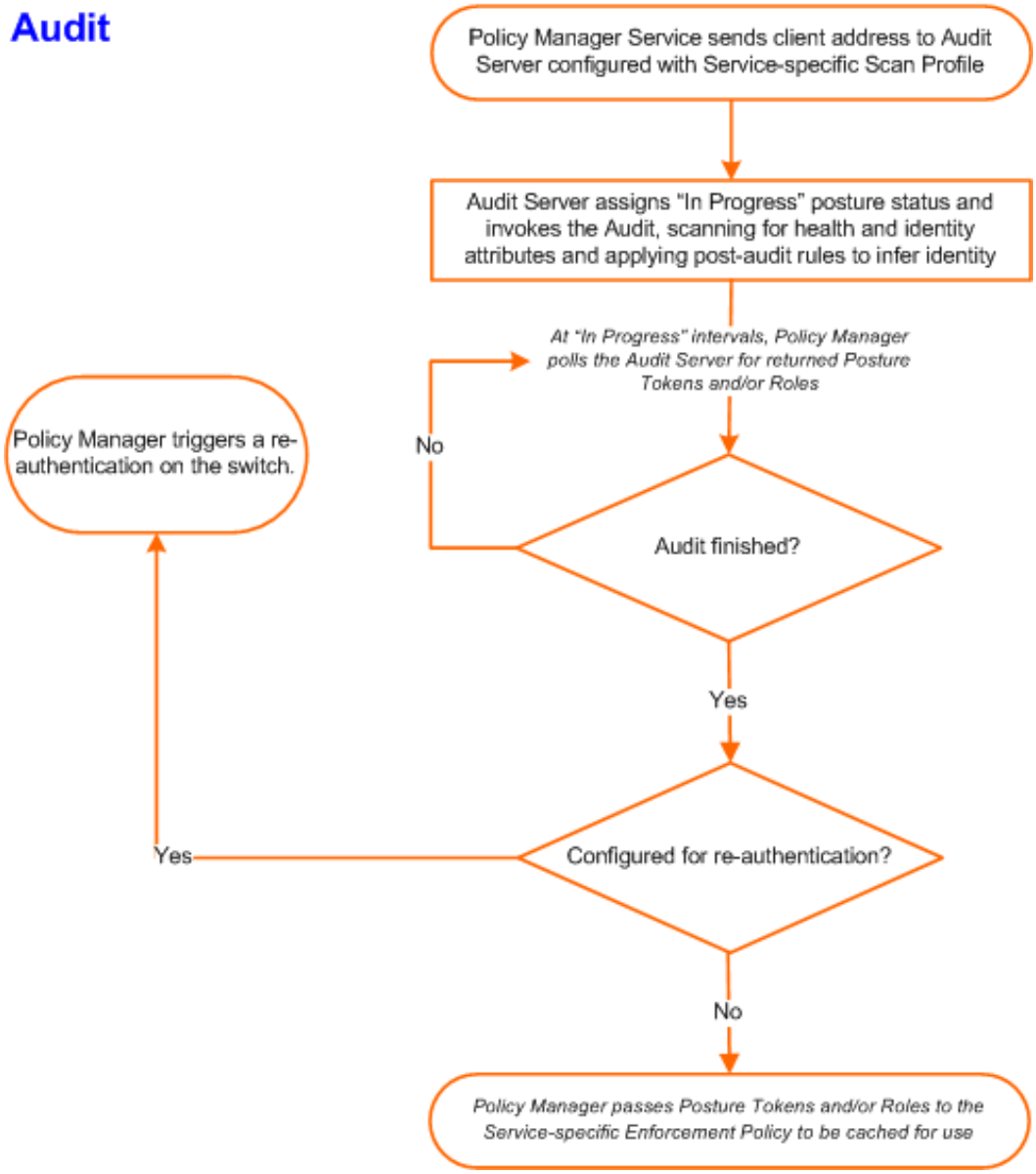
Parameter	Description
RADIUS Server Name/Port	Hostname or IP address and RADIUS server UDP port.
Shared Secret	Enter the shared secret for RADIUS message exchange; the same secret has to be entered on the RADIUS server (Microsoft NPS) side.
Timeout	How many seconds to wait before deeming the connection dead; if a backup is configured, Policy Manager will attempt to connect to the backup server after this timeout. For the backup server to be invoked on primary server failover, check the **Enable to use backup when primary does not respond** check box.

Audit Servers evaluate posture, role, or both, for unmanaged or unmanageable clients. One example could be clients that lack an adequate posture agent or 802.1X supplicant. For example, printers, PDAs, or guest users might not be able to send posture credentials or identify themselves. A Policy Manager Service can trigger an audit by sending a client ID to a pre-configured audit server, and the server returns attributes for role mapping and posture evaluation.

Audit servers are configured at a global level. Only one audit server can be associated with a service. The flow-of-control of the audit process is shown in the figure.

For more information, see Configuring Audit Servers on page 250.

Figure 228: *Flow of Control of Policy Manager Auditing*



Configuring Audit Servers

The Policy Manager server contains built-in Nessus (version 2.X) and NMAP servers. For enterprises with existing audit server infrastructure, or otherwise preferring external audit servers, Policy Manager supports these servers externally.

For more information, see:

- Built-In Audit Servers on page 250
- Custom Audit Servers on page 252
- Post-Audit Rules on page 260

Built-In Audit Servers

When configuring an audit as part of an Policy Manager Service, you can select the default Nessus (*[Nessus Server]*) or NMAP (*[Nmap Audit]*) configuration.

Add Auditing to a Policy Manager Service

1. Navigate to the **Audit** tab from one of the following locations:
   - To configure an audit server for a new service (as part of the flow of the Add Service wizard), navigate to **Configuration > Services**. Select the **Add Services** link. In the **Add Services** form, select the **Audit** tab.

You must select the **Audit End-hosts** check box on the **Services** tab in order for the **Audit** tab to display.

   - To modify an existing audit server, navigate to **Configuration > Posture > Audit Servers**, then select an audit server from the list.
2. Configure auditing. Complete the fields in the **Audit** tab as follows:

Figure 229: *Audit Tab*

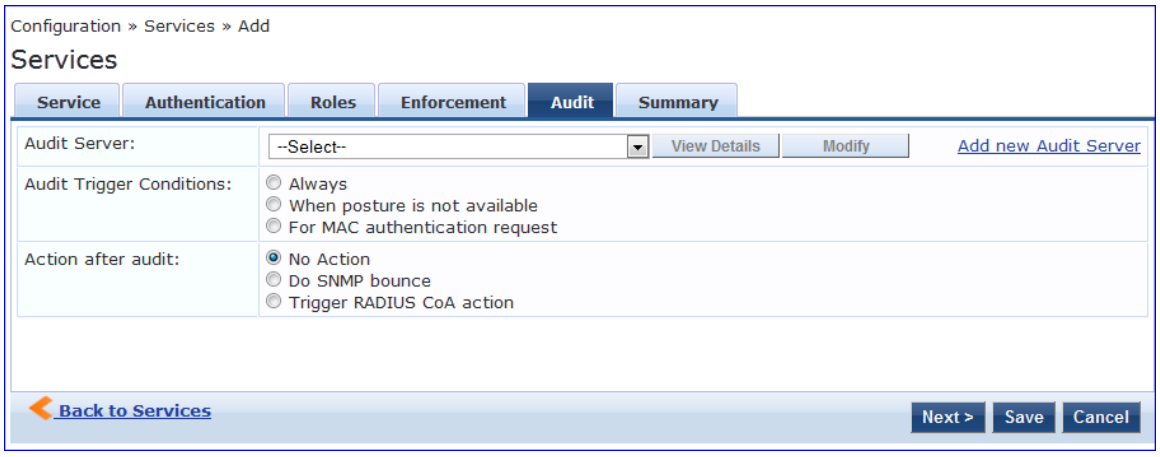


Table 140: *Audit tab*

Parameter	Description
Audit Server/Add new Audit Server	Select a built-in server profile from the list: • The *[Nessus Server]* performs vulnerability scanning. It returns a Healthy/Quarantine result. • The *[Nmap Audit]* performs network port scans. The health evaluation always returns **Healthy**. The port scan gathers attributes that allow determination of Role (s) through post-audit rules. **NOTE:** For Policy Manager to trigger an audit on an end-host, it needs to get the IP address of this end-host. The IP address of the end-host is not available at the time of initial authentication, in the case of 802.1X and MAC authentication requests. Policy Manager has a built-in DHCP snooping service that can examine DHCP request and response packets to derive the IP address of the end-host. For this to work, you need to use this service, Policy Manager must be configured as a DHCP "IP Helper" on your router/switch (in addition to your main DHCP server). Refer to your switch documentation for "IP Helper" configuration. To audit devices that have a static IP address assigned, it is recommended that a static binding between the MAC and IP address of the endpoint be created in your DHCP server. Refer to your DHCP Server documentation for configuring such static bindings. **NOTE:** Policy Manager does not issue the IP address; it just examines the DHCP traffic in order to derive the IP address of the end-host.

Audit Trigger Conditions	• **Always**: Always perform an audit.
	• **When posture is not available**: Perform audit only when posture credentials are not available in the request.
	• **For MAC Authentication Request,** If you select this option, then Policy Manager presents three additional settings:
	  ▪ **For known end-hosts only.** For example, when you want to reject unknown end-hosts, but audit known clients for. Known end-hosts are defined as those clients that are found in the authentication source(s) associated with this service.
	  ▪ **For unknown end-hosts only.** For example, when known end-hosts are assumed to be healthy, but you want to establish the identity of unknown end-hosts and assign roles. Unknown end-hosts are those end-hosts that are not found in any of the authentication sources associated with this service.
	  ▪ **For all end-hosts.** For both known and unknown end-hosts.

Re-authenticate client	Check the check box for Force re-authentication of the client after audit to bounce the switch port or to force an 802.1X reauthentication (both done via SNMP). **NOTE:** Bouncing the port triggers a new 802.1X/MAC authentication request by the client. If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager.

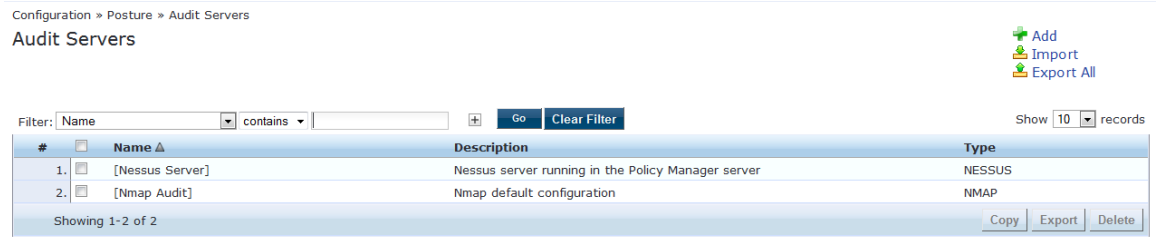
Modifying Built-In Audit Servers

To reconfigure a default Policy Manager Audit Servers:

1. Open the audit server profile.

   Navigate to **Configuration > Posture > Audit Servers**, then select an Audit Server from the list of available servers.

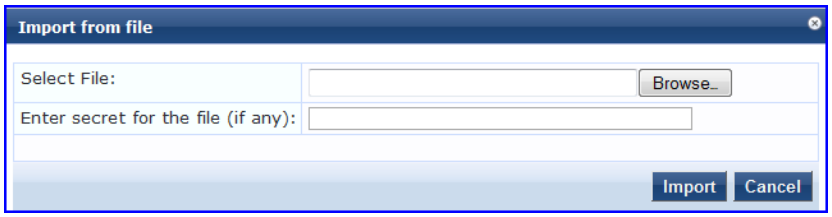
Figure 230: *Audit Servers Listing*



2. Modify the profile, plugins, and/or preferences.
   - In the **Audit** tab, you can modify the **In Progress Posture Status** and **Default Posture Status**.
   - If you selected a NESSUS Server, then the **Primary/Backup Server** tabs allow you to specify a scan profile. In addition, when you add a new scan profile, you can select plugins and preferences for the profile. Refer to Nessus Scan Profiles on page 254 for more information.

     The built-in Policy Manager Nessus Audit Server ships with approximately 1000 of the most commonly used Nessus plugins. You can download others from http://www.tenablesecurity.com, in the form *all-2.0.tar.gz*. To upload them to the built-in Policy Manager Audit Server, navigate to **Administration > Server Manager > Server Configuration**, select **Upload Nessus Plugins**, and then select the downloaded file.

Figure 231: *Upload Nessus Plugins Popup*



   - In the **Rules** tab, you can create post-audit rules for determining Role based on identity attributes discovered by the audit. Refer to Post-Audit Rules on page 260.

Custom Audit Servers

For enterprises with existing audit server infrastructure, or otherwise preferring custom audit servers, Policy Manager supports NESSUS (2.x and 3.x) (and NMAP scans using the NMAP plug-in on these external Nessus Servers).

To configure a custom Audit Server:

1. Open the Audit page.
   - To configure an audit server for a new service (as part of the flow of the Add Service wizard), navigate to **Configuration > Posture > Audit Servers**, then click **Add Audit Server**.
   - To modify an existing audit server, navigate to **Configuration > Posture > Audit Server**, and select an audit server.
2. Add a custom audit server

   When you click **Add Audit Server**, Policy Manager displays the **Add Audit Server** page. Configuration settings vary depending on audit server type:
   - Nessus Audit Server on page 253
   - NMAP Audit Server on page 258

Nessus Audit Server

Policy Manager uses the Nessus Audit Server interface primarily to perform vulnerability scanning. It returns a Healthy/Quarantine result.

The **Audit** tab identifies the server and defines configuration details.

Figure 232: *Nessus Audit Server (Audit Tab)*

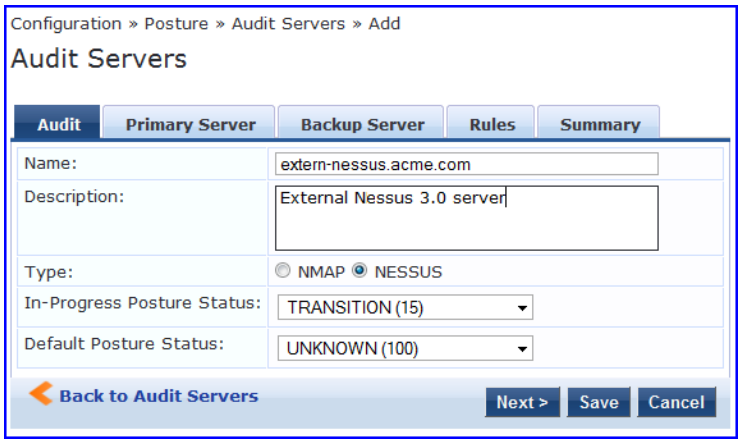


Table 141: *Nessus Audit Server (Audit tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	For purposes of an NESSUS-type Audit Server, always NESSUS.
In Progress Posture Status	Posture status during audit. Select a status from the drop-down list.
Default Posture Status	Posture status if evaluation does not return a condition/action match. Select a status from the drop-down list.

The **Primary Server**and **Backup Server** tabs specify connection information for the NESSUS audit server.

Figure 233: *Nessus Audit Server (Primary & Backup Tabs)*

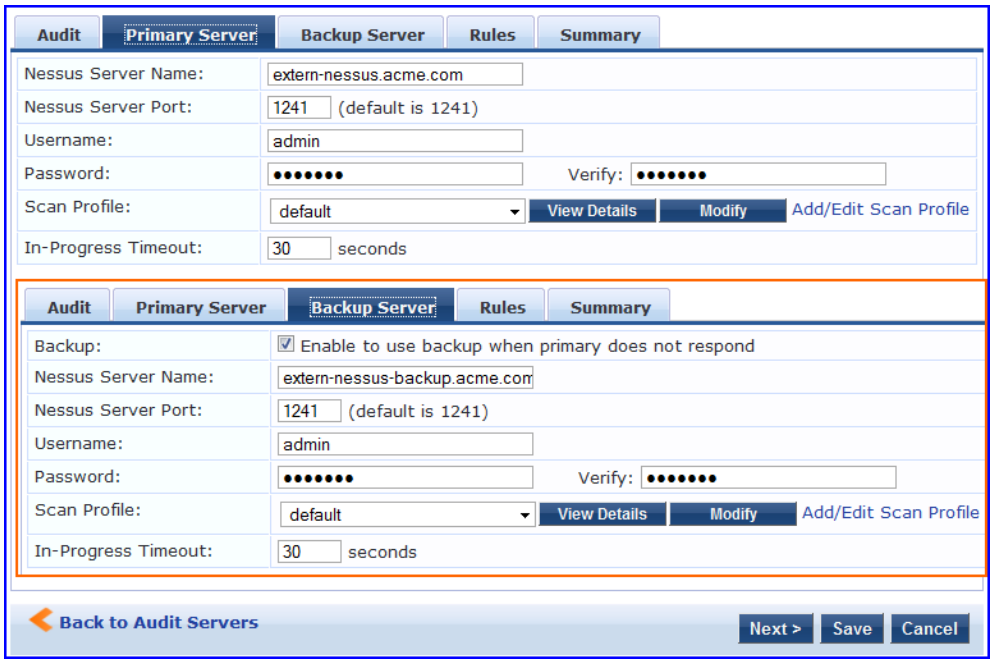


Table 142: *Nessus Audit Server - Primary and Backup Server tabs*

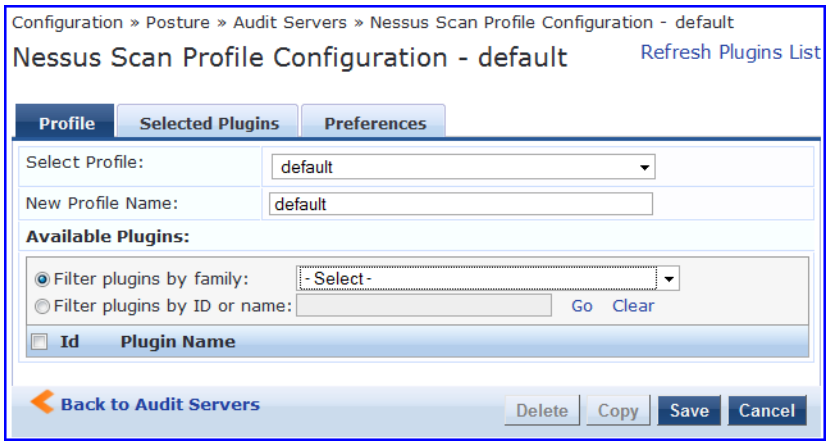
Parameter	Description
Server Name and Port/ Username/ Password	Standard NESSUS server configuration fields. **NOTE:** For the backup server to be invoked on primary server failover, check the **Enable to use backup when primary does not respond** check box.
Scan Profile	You can accept the default Scan Profile or select **Add/Edit Scan Profile** to create other profiles and add them to the Scan Profile list. Refer to Nessus Scan Profiles on page 254.

The **Rules** tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to Post-Audit Rules on page 260.

Nessus Scan Profiles

A scan profile contains a set of scripts (plugins) that perform specific audit functions. To Add/Edit Scan Profiles, select **Add/Edit Scan Profile** (link) from the **Primary Server** tab of the Nessus Audit Server configuration. The **Nessus Scan Profile Configuration** page displays.

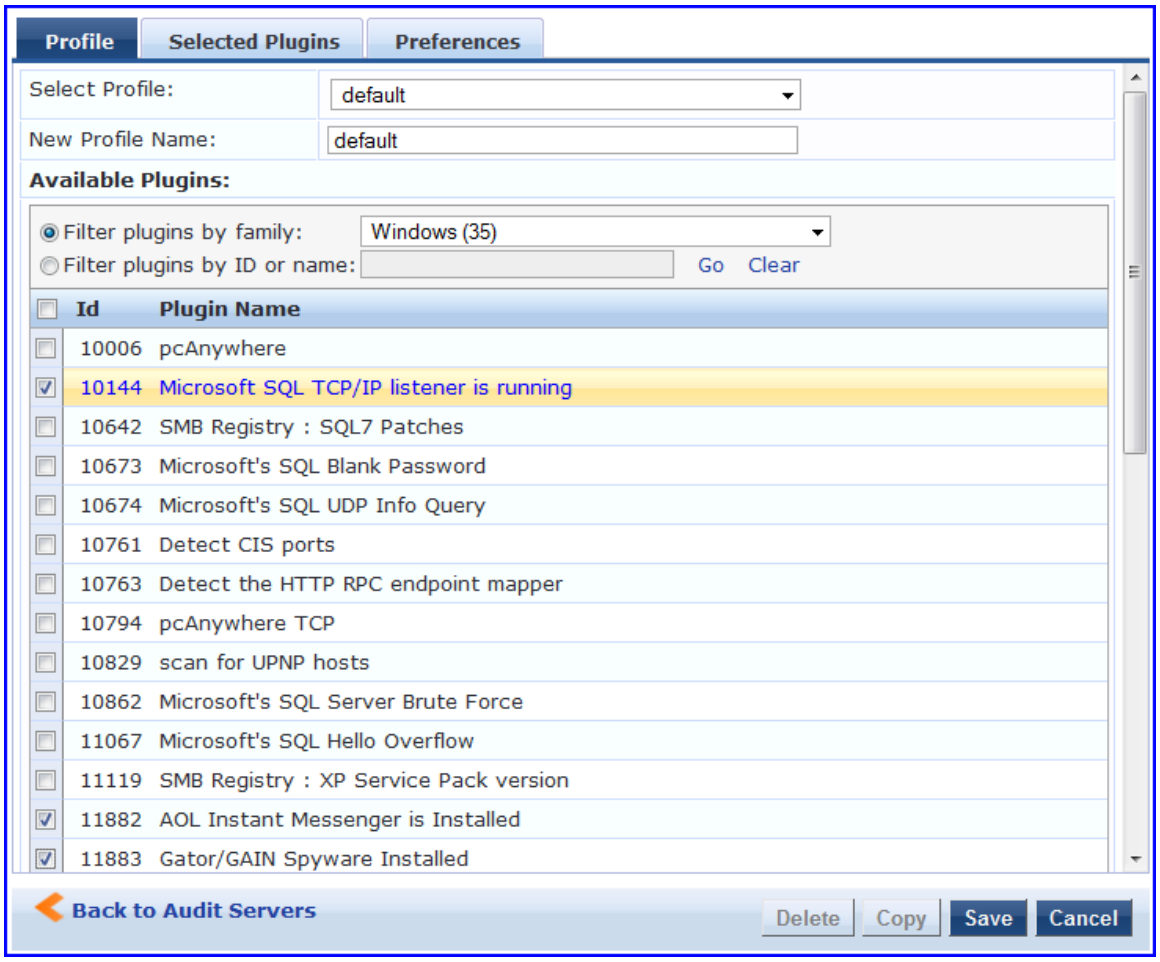
Figure 234: *Nessus Scan Profile Configuration Page*



You can refresh the plugins list (after uploading plugins into Policy Manager, or after refreshing the plugins on your external Nessus server) by clicking Refresh Plugins List. The Nessus Scan Profile Configuration page provides three views for scan profile configuration:

- The **Profile** tab identifies the profile and provides a mechanism for selection of plugins:
  - From the **Filter plugins by family** drop-down list, select a family to display all available member plugins in the list below. You may also enter the name of a plugin in **Filter plugins by ID** or name text box.
  - Select one or more plugins by enabling their corresponding check boxes (at left). Policy Manager will remember selections as you select other plugins from other plugin families.
  - When finished, click the **Selected Plugins** tab.

Figure 235: *Nessus Scan Profile Configuration (Profile Tab)*



- The **Selected Plugins** tab displays all selected plugins, plus any dependencies.
  To display a synopsis of any listed plugin, click on its row.

Figure 236: *Nessus Scan Profile Configuration (Profile Tab) - Plugin Synopsis*

NOTE

Of special interest is the section of the synopsis entitled **Risks**. To delete any listed plugin, click on its corresponding trashcan icon. To change the vulnerability level of any listed plugin, click on the link to change the level to one of HOLE, WARN, or INFO. This action tells Policy Manager the vulnerability level that is considered to be assigned QUARANTINE status.

Figure 237: *Nessus Scan Profile Configuration (Selected Plugins Tab)*

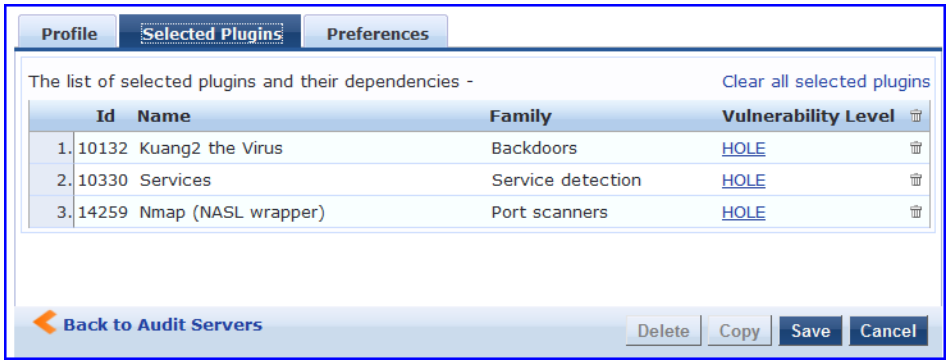


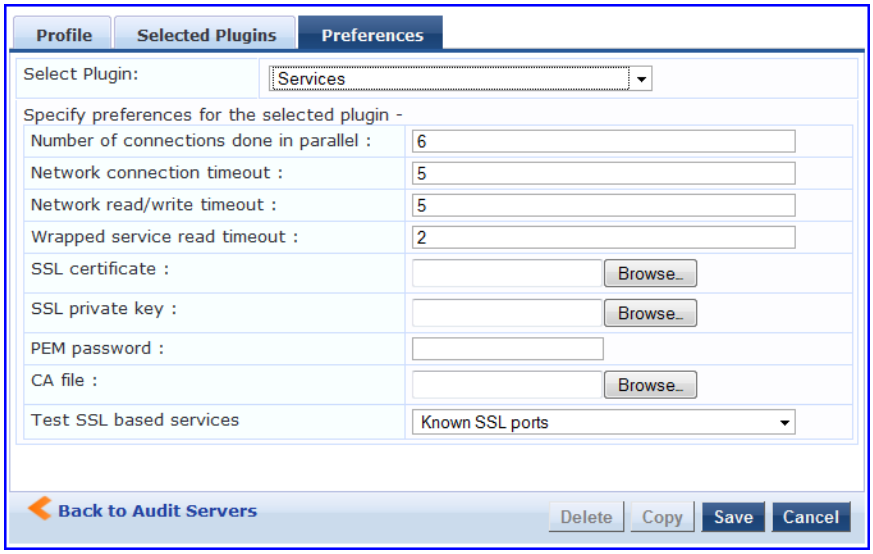
Figure 238: *Nessus Scan Profile Configuration (Selected Plugins Tab) - Vulnerability Level*

For each selected plugin, the Preferences tab contains a list of fields that require entries.

In many cases, these fields will be pre-populated. In other cases, you must provide information required for the operation of the plugin.

By way of example of how plugins use this information, consider a plugin that must access a particular service, in order to determine some aspect of the client's status; in such cases, login information might be among the preference fields.

Figure 239: *Nessus Scan Profile Configuration (Preferences Tab)*



After saving the profile, plugin, and preference information for your new (or modified) plugin, you can go to the **Primary/Backup Servers** tabs and select it from the **Scan Profile** drop-down list.

NMAP Audit Server

Policy Manager uses the NMAP Audit Server interface exclusively for network port scans. The health evaluation always returns **Healthy**. The port scan gathers attributes that allow determination of Role(s) through post-audit rules.

The **Audit** tab labels the Server and defines configuration details.

Figure 240: *Audit Tab (NMAP)*

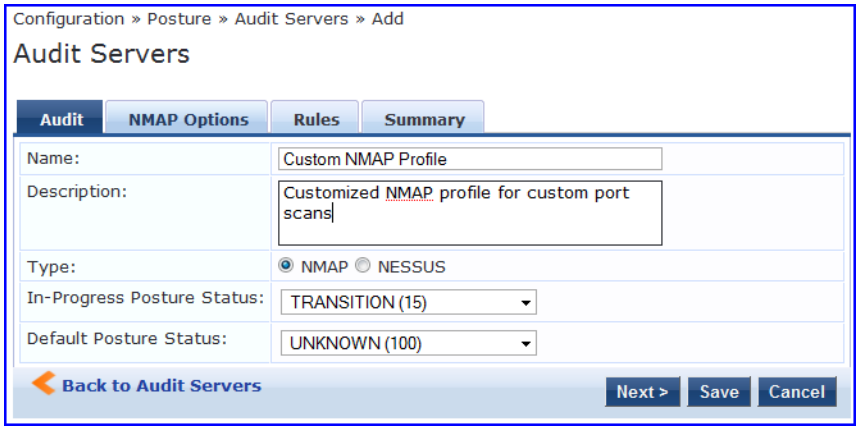


Table 143: *Audit Tab (NMAP)*

Parameter	Description
Name/Description	Freeform label and description.
Type	For purposes of an NMAP-type Audit Server, always **NMAP**.
In Progress Posture Status	Posture status during audit. Select a status from the drop-down list.
Default Posture Status	Posture status if evaluation does not return a condition/action match. Select a status from the drop-down list.

The **NMAP Options** tab specifies scan configuration.

Figure 241: *Options Tab (NMAP)*

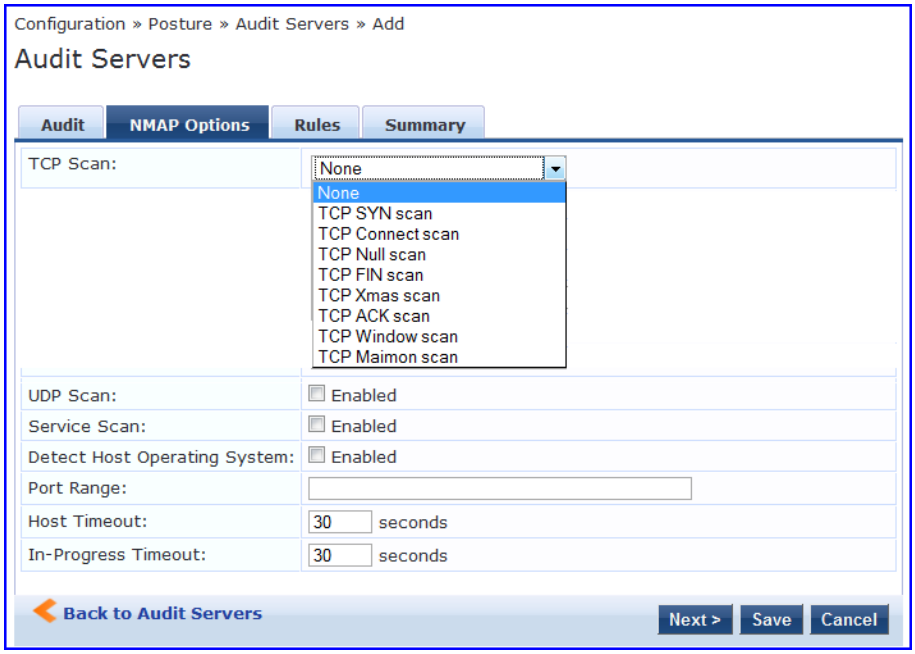


Table 144: *Options Tab (NMAP)*

Parameter	Description
TCP Scan	To specify a TCP scan, select from the **TCP Scan** drop-down list. Refer to NMAP documentation for more information on these options. NMAP option --scanflags.
UDP Scan	To enable, check the **UDP Scan** check box. NMAP option -sU.
Service Scan	To enable, check the **Service Scan** check box. NMAP option -sV.

Parameter	Description
Detect Host Operating System	To enable, check the **Detect Host Operating System** check box. NMAP option -A.
Port Range/ Host Timeout/ In Progress Timeout	• Port Range - Range of ports to scan. NMAP option -p. • Host Timeout - Give up on target host after this long. NMAP option --host-timeout • In Progress Timeout - How long to wait before polling for NMAP results.

The **Rules** tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to Post-Audit Rules on page 260.

Post-Audit Rules

The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role.

Figure 242: *All Audit Server Configurations (Rules Tab)*

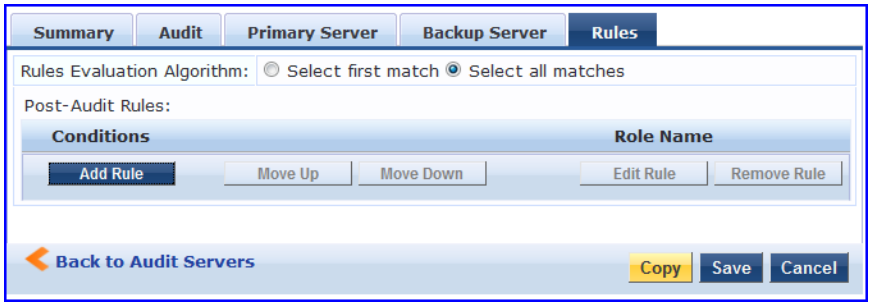


Table 145: *All Audit Server Configurations (Rules Tab)*

Parameter	Description
Rules Evaluation Algorithm	**Select first matched** rule and return the role or **Select all matched** rules and return a set of roles.
Add Rule	Add a rule. Brings up the rules editor. See below.
Move Up/Down	Reorder the rules.
Edit Rule	Brings up the selected rule in edit mode.
Remove Rule	Remove the selected rule.

Figure 243: *All Audit Server Configurations (Rules Editor)*

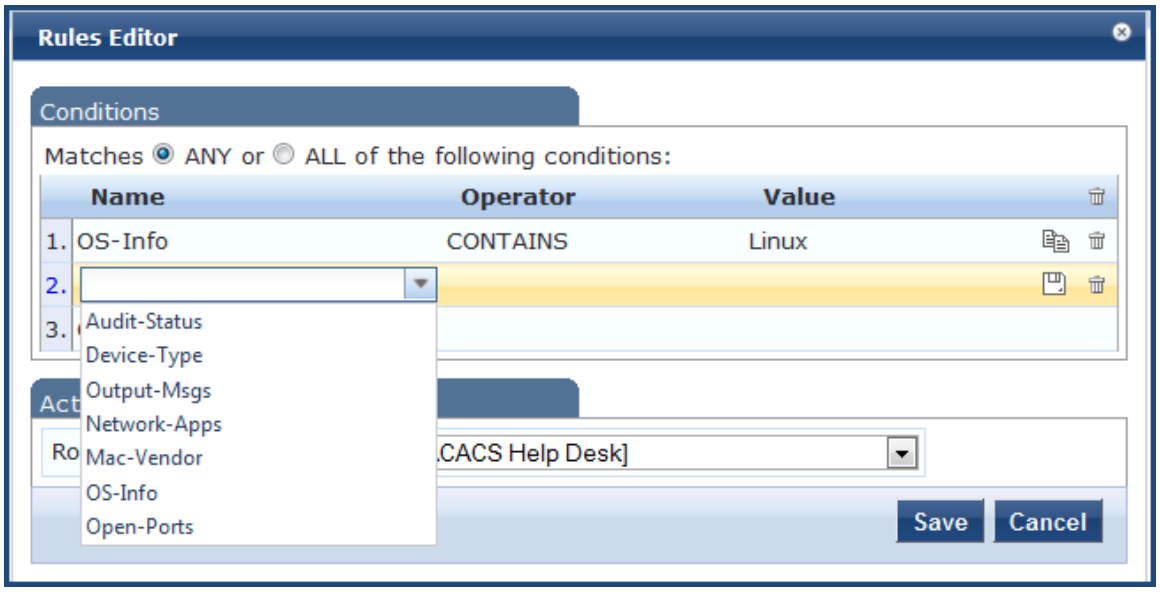


Table 146: *All Audit Server Configurations (Rules Editor)*

Parameter	Description
Conditions	The **Conditions** list includes five dictionaries: Audit-Status, Device-Type, Output-Msgs, Mac-Vendor, Network-Apps, Open-Ports, and OS-Info. Refer to Namespaces on page 513.
Actions	The **Actions** list includes the names of the roles configured in Policy Manager.
Save	To commit a Condition/Action pairing, click **Save**.

Policy Manager controls network access by sending a set of access-control attributes to the request-originating Network Access Device (NAD).

Policy Manager sends these attributes by evaluating an *Enforcement Policy* associated with the service. The evaluation of Enforcement Policy results in one or more *Enforcement Profiles*; each Enforcement Profile wraps the access control attributes sent to the Network Access Device. For example, for RADIUS requests, commonly used Enforcement Profiles include attributes for VLAN, Filter ID, Downloadable ACL, and Proxy ACL.

For more information, see:

- Enforcement Architecture and Flow on page 263
- Configuring Enforcement Profiles on page 264
- Configuring Enforcement Policies on page 298

Enforcement Architecture and Flow

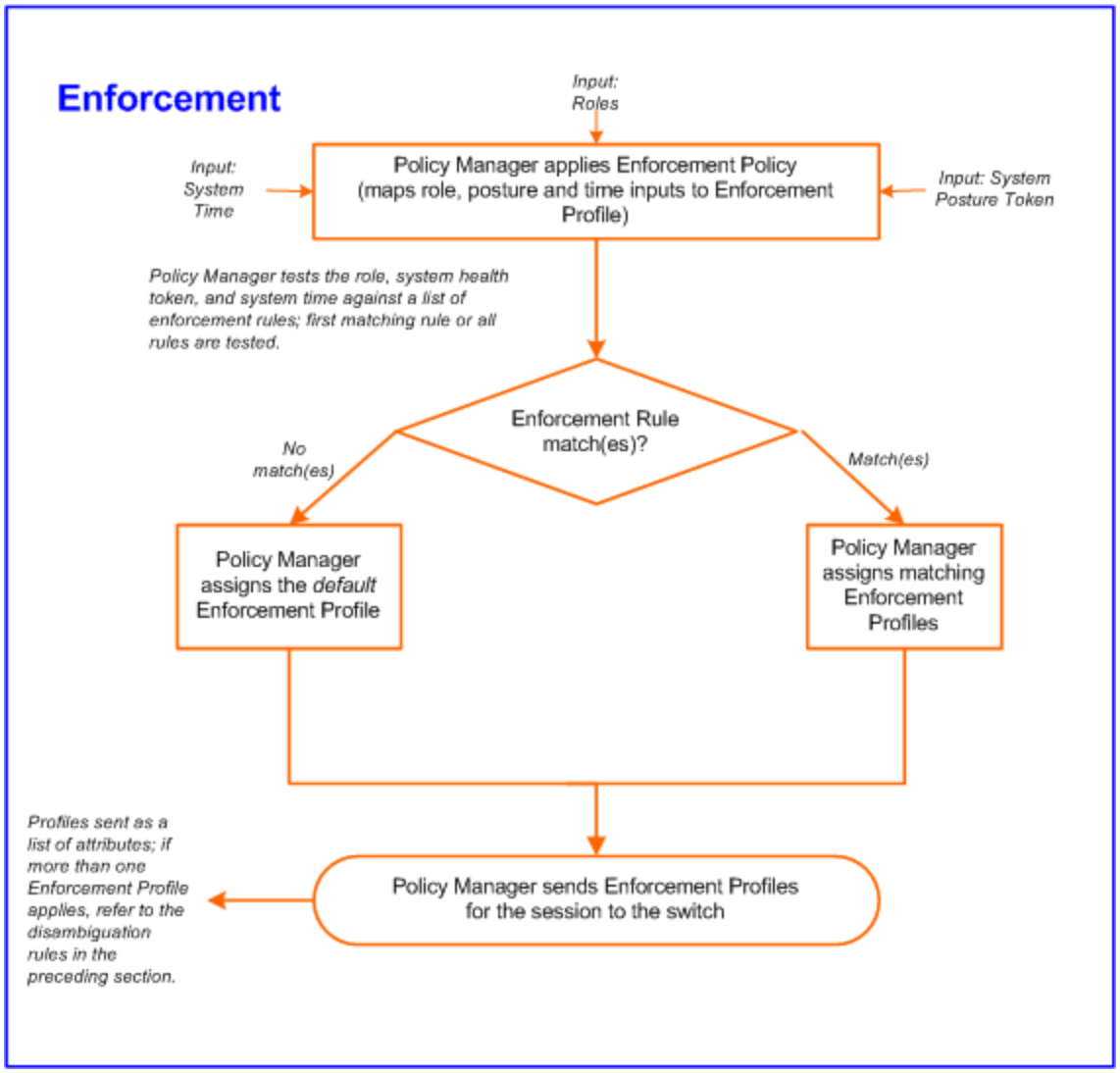
To evaluate a request, a Policy Manager Application assembles the request's client roles, client posture (system posture token), and system time. The calculation that matches these components to a pre-defined Enforcement Profile occurs inside of a black box called an Enforcement Policy.

Each Enforcement Policy contains a rule or set of rules for matching Conditions (role, posture and time) to Actions (Enforcement Profiles). For each request, it yields one or more matches, in the form of Enforcement Profiles, from which Policy Manager assembles access-control attributes for return to the originating NAD, subject to the following disambiguation rules:

- If an attribute occurs only once within an Enforcement Profile, transmit as is.
- If an attribute occurs multiple times within the same Enforcement Profile, transmit as a multi-valued attribute.
- If an attribute occurs in more than one Enforcement Profile, only transmit the value from the first Enforcement Profile in priority order.

Optionally, each Enforcement Profile can have an associated group of NADs; when this occurs, Enforcement Profiles are only sent if the request is received from one of the NADs in the group. For example, you can have the same rule for VPN, LAN and WLAN access, with enforcement profiles associated with device groups for each type of access. If a device group is not associated with the enforcement profile, attributes in that profile are sent regardless of where the request originated.

Figure 244: *Flow of Control of Policy Manager Enforcement*



Configuring Enforcement Profiles

You configure Policy Manager Enforcement Profiles globally, but they must be referenced in an enforcement policy that is associated with a Service.

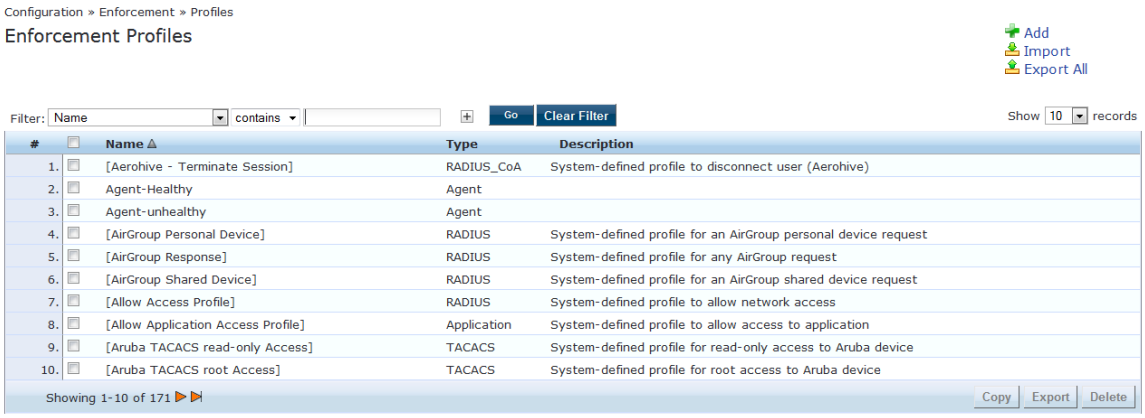
From the **Enforcement Policies** page (**Configuration > Enforcement > Policies**), you can configure an Enforcement Profile for a new enforcement policy (as part of the flow of the **Add Enforcement Policy** wizard), or modify an existing Enforcement Profile directly (**Configuration > Enforcement > Profiles**, then click on its name in the **Enforcement Profile** listing).

For information about configuring individual Enforcement Profiles, see:

- Agent Enforcement on page 266
- Aruba Downloadable Role Enforcement on page 268
- Aruba RADIUS Enforcement on page 277
- Cisco Downloadable ACL Enforcement on page 278
- Cisco Web Authentication Enforcement on page 279

- ClearPass Entity Update Enforcement on page 281
- CLI Based Enforcement on page 282
- Filter ID Based Enforcement on page 284
- Generic Application Enforcement on page 285
- HTTP Based Enforcement on page 287
- RADIUS Based Enforcement on page 288
- RADIUS Change of Authorization (CoA) on page 289
- Session Restrictions Enforcement on page 292
- SNMP Based Enforcement on page 294
- TACACS+ Based Enforcement on page 295
- VLAN Enforcement on page 297

Figure 245: *Enforcement Profiles Page*



Policy Manager comes pre-packaged with the default profiles described in Table 147:

Table 147: *Default Enforcement Profiles*

Profile	Available for the following Enforcement Types
[Aerohive - Terminate Session]	RADIUS_CoA
[AirGroup Personal Device]	RADIUS
[AirGroup Response]	RADIUS
[AirGroup Shared Device]	RADIUS
[Allow Access Profile]	RADIUS
[Allow Application Access Profile]	Application
[Aruba TACACS read-only Access]	TACACS
[Aruba TACACS root Access]	TACACS
[Aruba Terminate Session]	RADIUS_CoA

Table 147: *Default Enforcement Profiles (Continued)*

Profile	Available for the following Enforcement Types
[Cisco - Bounce-Host-Port]	RADIUS_CoA
[Cisco - Disable Host-Port]	RADIUS_CoA
[Cisco - Reauthenticate-Session]	RADIUS_CoA
[Cisco - Terminate-Session]	RADIUS_CoA
[Deny Access Profile]	RADIUS
[Deny Application Access Profile]	Application
[Drop Access Profile]	RADIUS
[Handle AirGroup Time Sharing]	HTTP
[HP - Terminate Session]	RADIUS_CoA
[Juniper Terminate Session]	RADIUS_CoA
[Motorola - Terminate Session]	RADIUS_CoA
[Operator Login - Admin Users]	Application
[Operator Login - Local Users]	Application
[TACACS API Admin]	TACACS
[TACACS Deny Profile]	TACACS
[TACACS Help Desk]	TACACS
[TACACS Network Admin]	TACACS
[TACACS Read-only Admin]	TACACS
[TACACS Receptionist]	TACACS
[TACACS Super Admin]	TACACS
[Trapeze - Terminate Session]	RADIUS_CoA
[Update Endpoint Known]	Post-Authentication

Agent Enforcement

Use this page to configure profile and attribute parameters for the Agent Enforcement Profile.

Profile tab

Figure 246: *Agent Enforcement Profile tab*

Table 148: *Add Agent Enforcement Profile tab Parameters*

Parameter	Description
Template	Agent Enforcement
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	Agent. The value field is populated automatically.
Action	Disabled. Enabled only when RADIUS type is selected. Click to Accept, Deny or Drop to define the action taken on the request.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 247: *Agent Enforcement Attributes tab*

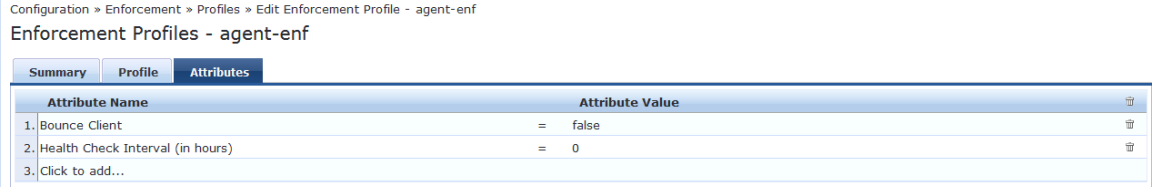


Table 149: *Agent Enforcement Attributes tab Parameters*

Attribute	Parameter
Attribute Name	Select one of the following attribute names: • **Bounce Client -** Set the value to **true** by checking the box to terminate the network connection. • **Message -** Enter the message that needs to be notified on the endpoint. • **Enable to hide Retry button** - Set the value to **true** to hide the **Retry** button in the OnGuard Agent. • **Enable to hide Logout button** - Set the value to **true** to hide the **Logout** button in the OnGuard Agent. • **Health Check Interval (in hours)** - Specify the health check interval value in hours for different Agent Enforcement Profiles for different users. The allowed range is of 0 – 1000 hours. For example, you can create Student-Enforcement-Profile with a value of 8 hours and Staff-Enforcement-Profile with a value of 48 hours. The value configured in the **Health Check Quiet Period (in hours)** field in the **Agent Enforcement Attribute** tab takes precedence over the value configured in the **Global Agent Settings** field. If both the values are configured, then the **Agent Enforcement Attribute** value is used by OnGuard Agent. The value of the **Policy result cache timeout** (path: Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General tab) field must be greater than the highest value of all the **Health Check Interval (in hours)** field values. For example, if you have created the profiles Student-Enforcement-Profile and Staff-Enforcement-Profile with health check interval configured, then the value of the **Policy result cache timeout** field must be greater than the highest value of **Health Check Quiet Period (in hours)** configured in the following fields: ▪ Global Agent Settings ▪ Student-Enforcement-Profile ▪ Staff-Enforcement-Profile Note the following information when you set the **OnGuard Health Check Interval** parameter: ▪ You can set this parameter if OnGuard mode is set to health only. ▪ This parameter is valid only for wired and wireless interface types. ▪ This parameter is not applicable for the OnGuard Dissolvable Agent, VPN, and other interface types. • **Session Timeout (in seconds) -** Configure the agent session timeout interval to re-evaluate the system health again. OnGuard triggers auto-remediation using this value to enable or disable AV-RTP status check on endpoint. Agent re-authentication is determined based on session-time out value. You can specify the session timeout interval from 60 – 600 seconds. Setting the lower value for session timeout interval results numerous authentication requests in **Access Tracker** page. The default value is 0.
Attribute Value	Set the value depends on the selected **Attribute Name**.

Aruba Downloadable Role Enforcement

Use this page to configure profile and role configuration attributes for the **Aruba Downloadable Role Enforcement** profile.

Profile tab

Figure 248: *Aruba Downloadable Role Enforcement Profile tab*

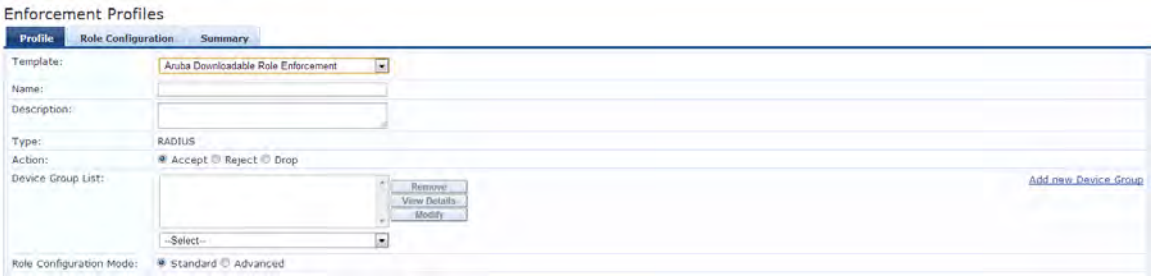


Table 150: *Aruba Downloadable Role Enforcement Profile tab Parameters*

Parameter	Description
Template	Select Aruba Downloadable Role Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. This description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	Specifies the type of authentication. In this context, RADIUS. This field is automatically populated.
Action	Click **Accept**, **Reject**, or **Drop** to define the action taken on the request. The default action is **Accept**.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups)** page. After adding one or more device group(s), you can select a group and perform one of the following actions: • Click **Remove** to delete the selected device group list entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new device group, click the **Add new Device Group** link and see Adding and Modifying Device Groups on page 309.

Role Configuration tab

The fields on the **Role Configuration** tab require that you select a link to launch a new page where you set role configuration attributes. For example, adding a Captive Portal profile. The following figure shows an example of the **Aruba Downloadable Role Enforcement Role Configuration** tab followed by parameter definition:

Figure 249: *Aruba Downloadable Role Enforcement Role Configuration tab*

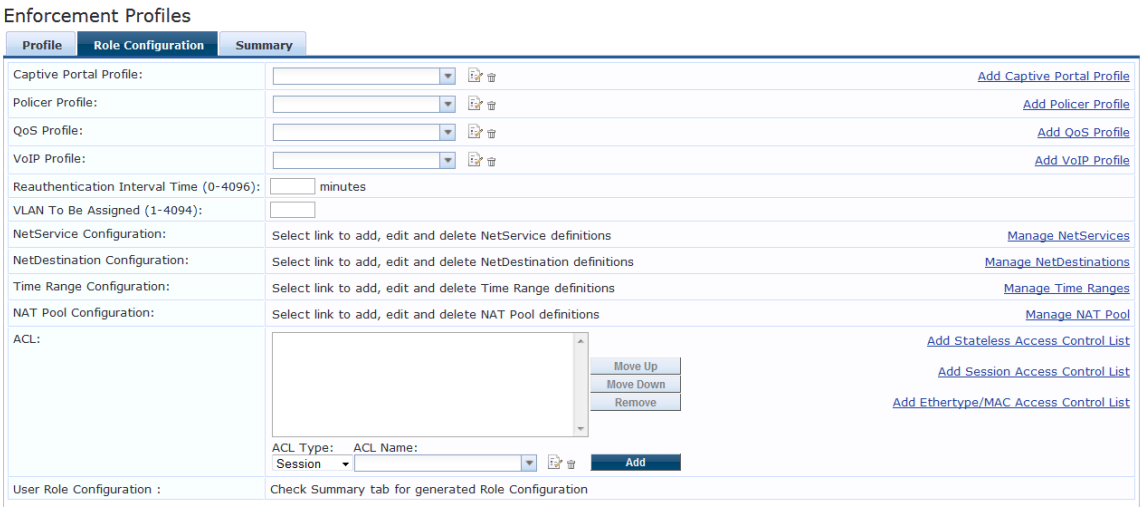


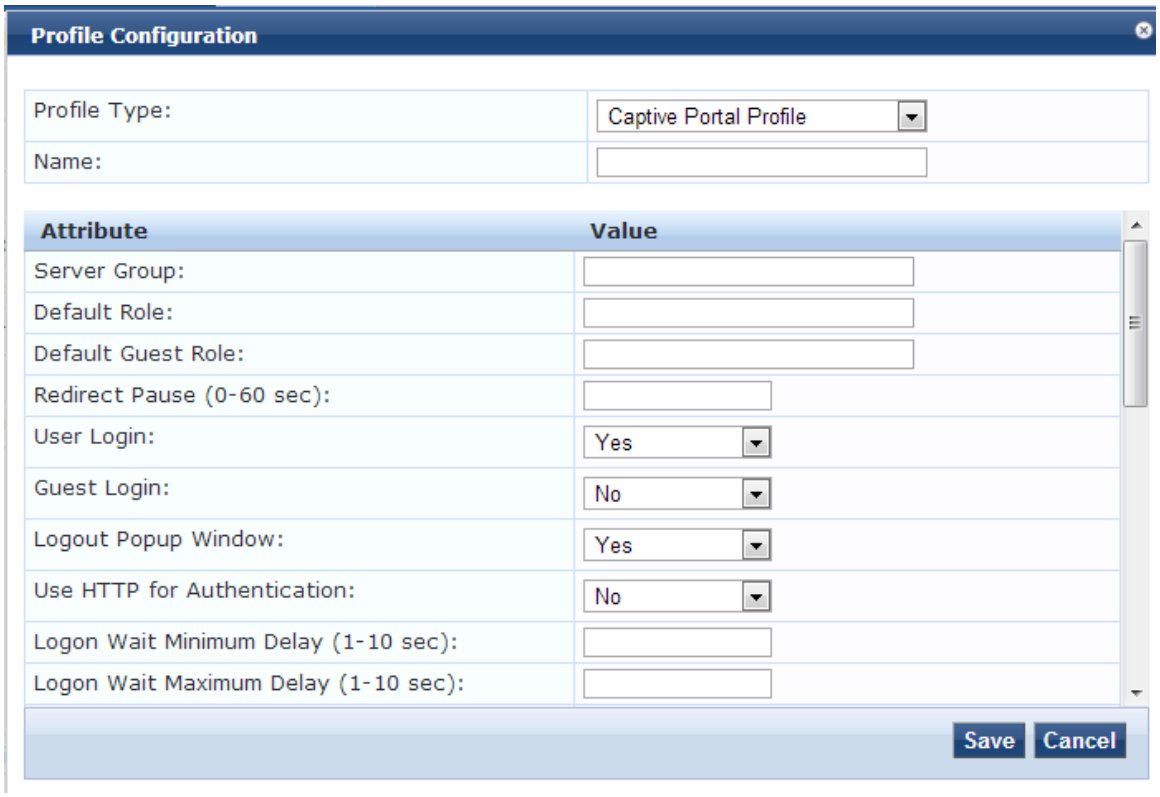
Table 151: *Role Configuration Attributes Page Parameters*

Role Configuration	Parameter
Reauthentication Interval Time (0-4096)	Enter the number of minutes between reauthentication intervals. You can select the range between 0 to 4096 minutes.
VLAN To Be Assigned (1-4904)	Enter a number between 1 and 4094 that defines when the VLAN is to be assigned.
	Click to modify profiles and parameters on the page.
ACL Type	Select from the following ACL types: • Ethertype • MAC • Session • Stateless
ACL Name	Click the name of the ACL type. Click **Add** to move the **ACL Name** to the **ACL** field. Click **Move Up**, **Move Down**, or **Remove** to modify the names in the ACL list.

Captive Portal Profile

Click the **Add Captive Portal Profile** link. Enter a name for the profile. Configure the required attributes and click **Save** or **Cancel.**

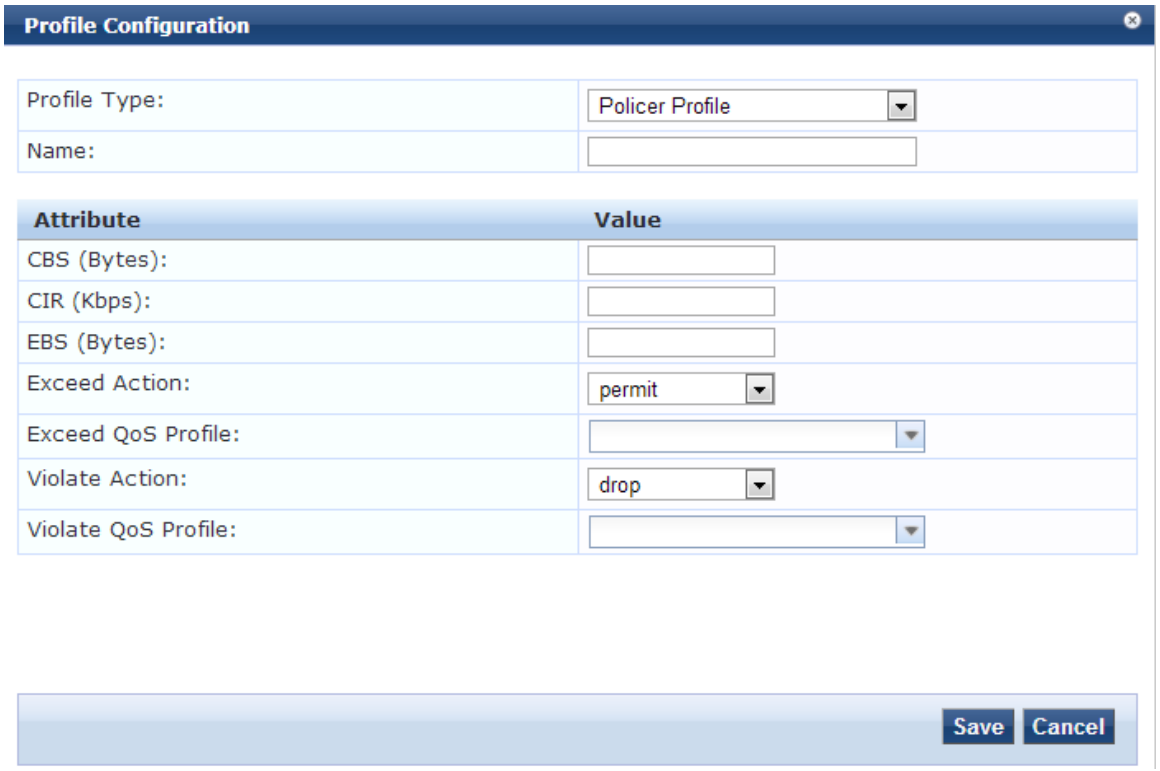
Figure 250: *Add Captive Portal Profile Attributes Page*



Policer Profile

Click the **Add Policer Profile** link. Enter a name for the profile. Configure the required attributes and click **Save** or **Cancel**.

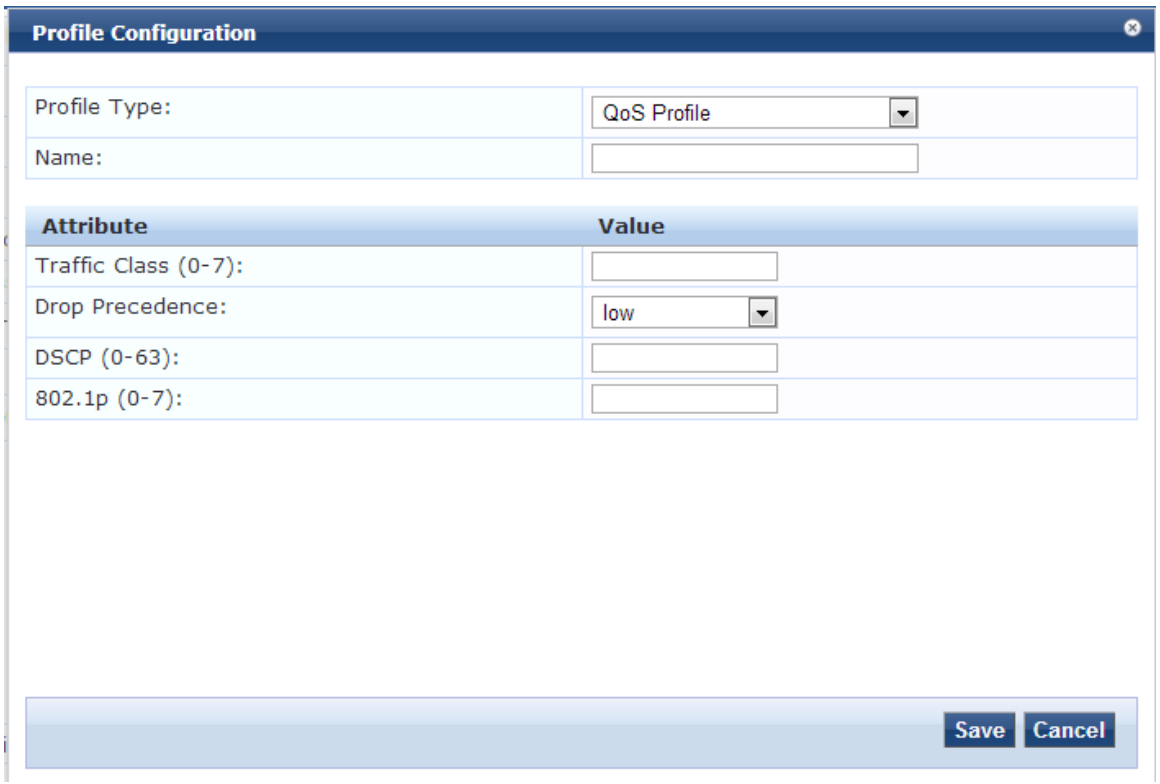
Figure 251: *Add Policer Profile Attributes Page*



QOs Profile

Click the **Add QoS Profile** link. Enter a name for the profile. Configure the required attributes and click **Save** or **Cancel**.

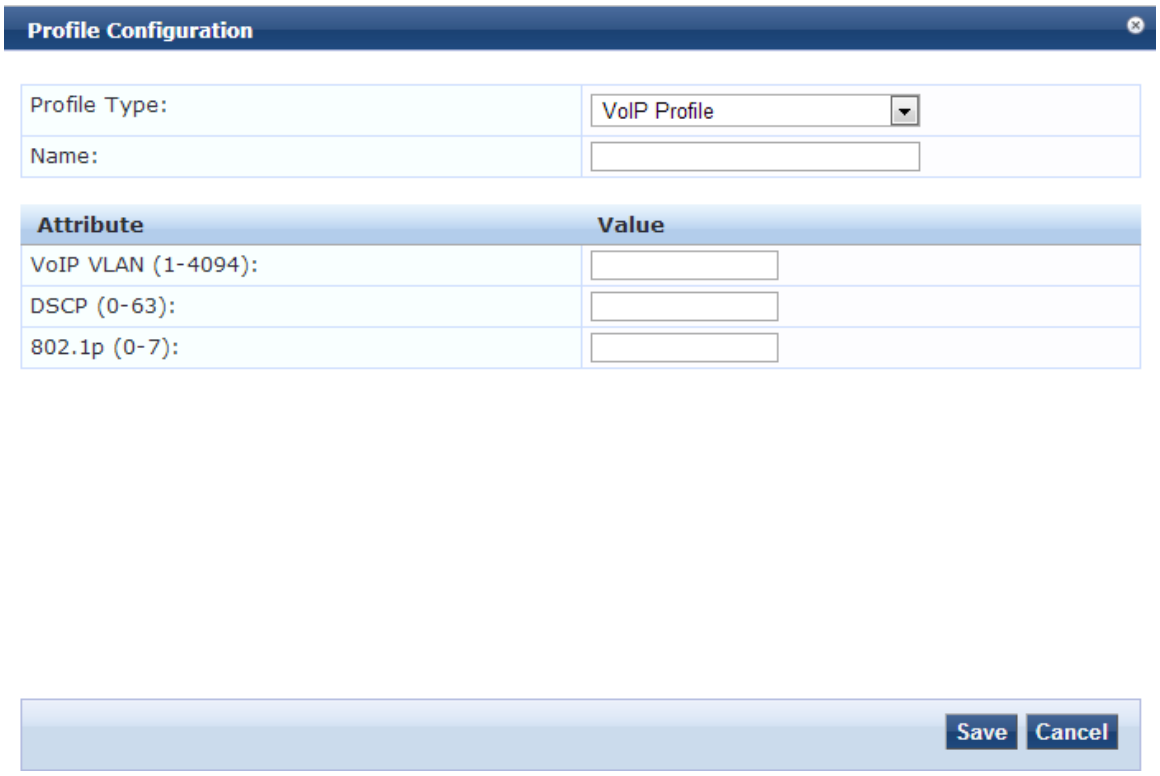
Figure 252: *Add QosProfle Attributes Page*



VoIP Profile

Click the **Add VoIP Profile** link. Enter a name for the profile. Configure the required attributes and click **Save** or **Cancel**.

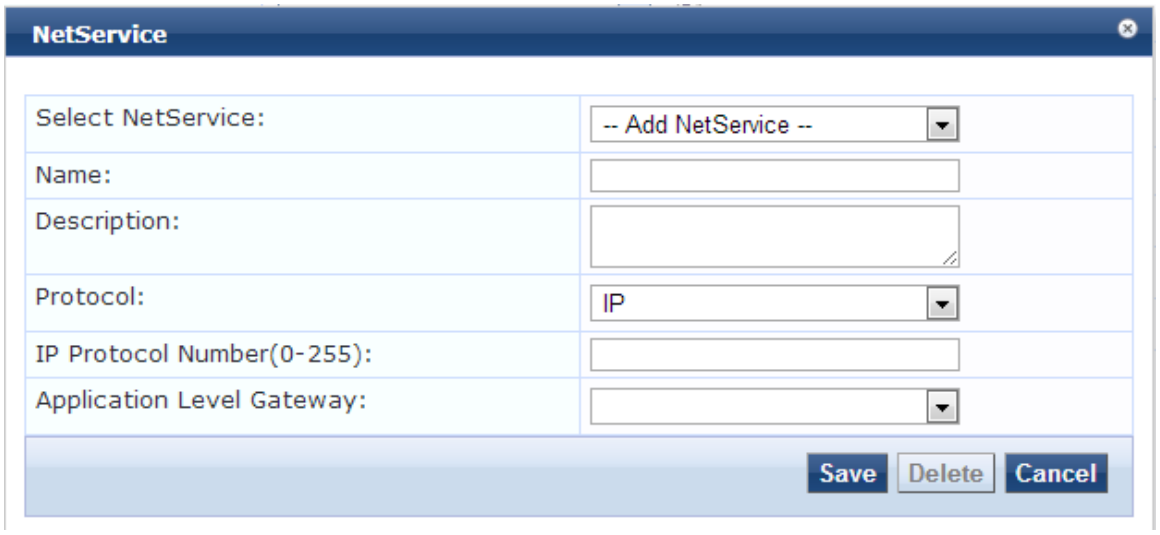
Figure 253: *Add VoIP Profile Attributes Page*



NetService Configuration

Click the **Manage NetServices** link. Configure the required attributes and click **Save, Delete**, or **Cancel**.

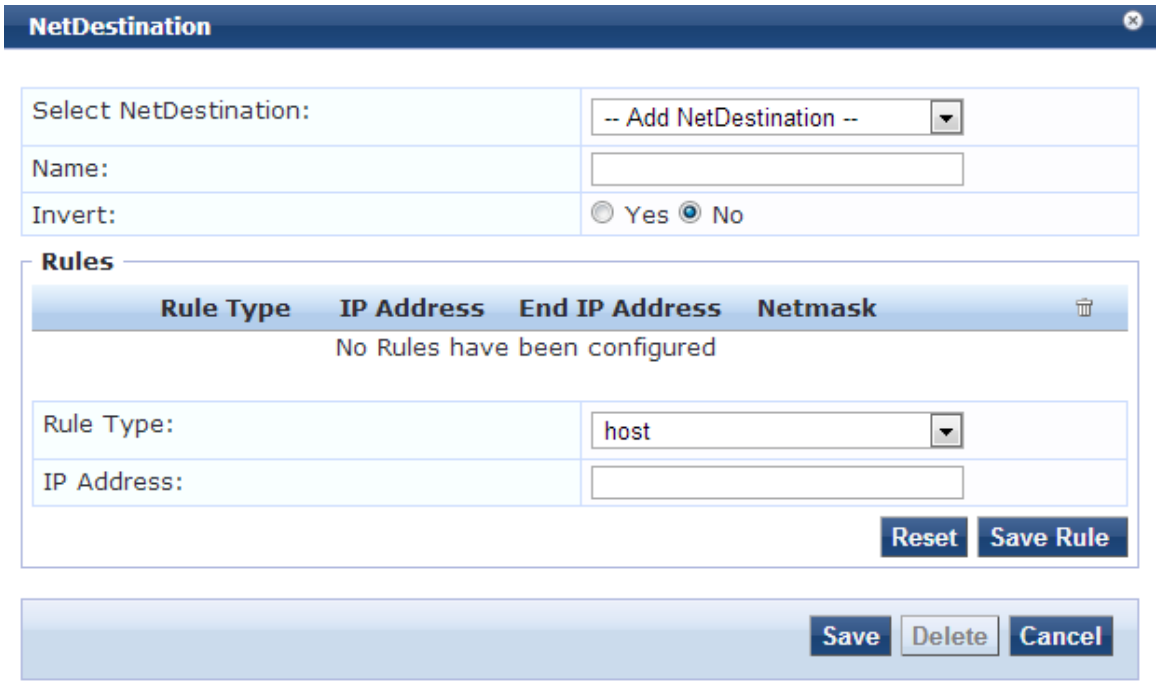
Figure 254: *Manage NetServices Attributes Page*



NetDestination Configuration

Click the **Manage NetDestinations** link. Configure the required attributes. Click **Reset** or **Save Rule**. Then click **Save**, **Delete**, **Reset**, or **Cancel**.

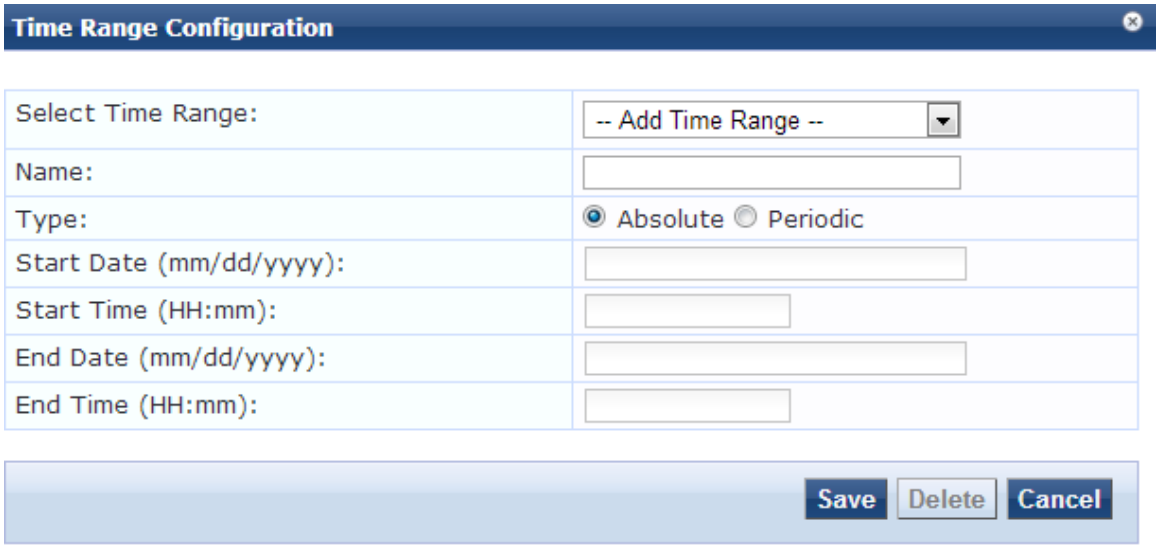
Figure 255: *Manage NetDestinations Attributes Page*



Time Range Configuration

Click the **Manage Time Ranges** link. Configure the required attributes and click **Save**, **Delete** or **Cancel**.

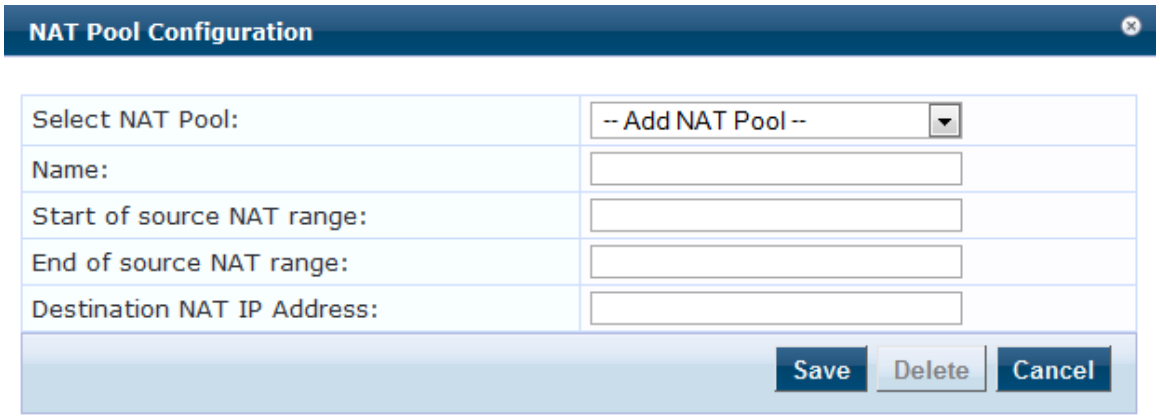
Figure 256: *Time Range Configuration Attributes page*



NAT Pool Configuration

Use the **NAT Pool Configuration** page to configure the start and end of the source NAT range and associate them with session ACLs.

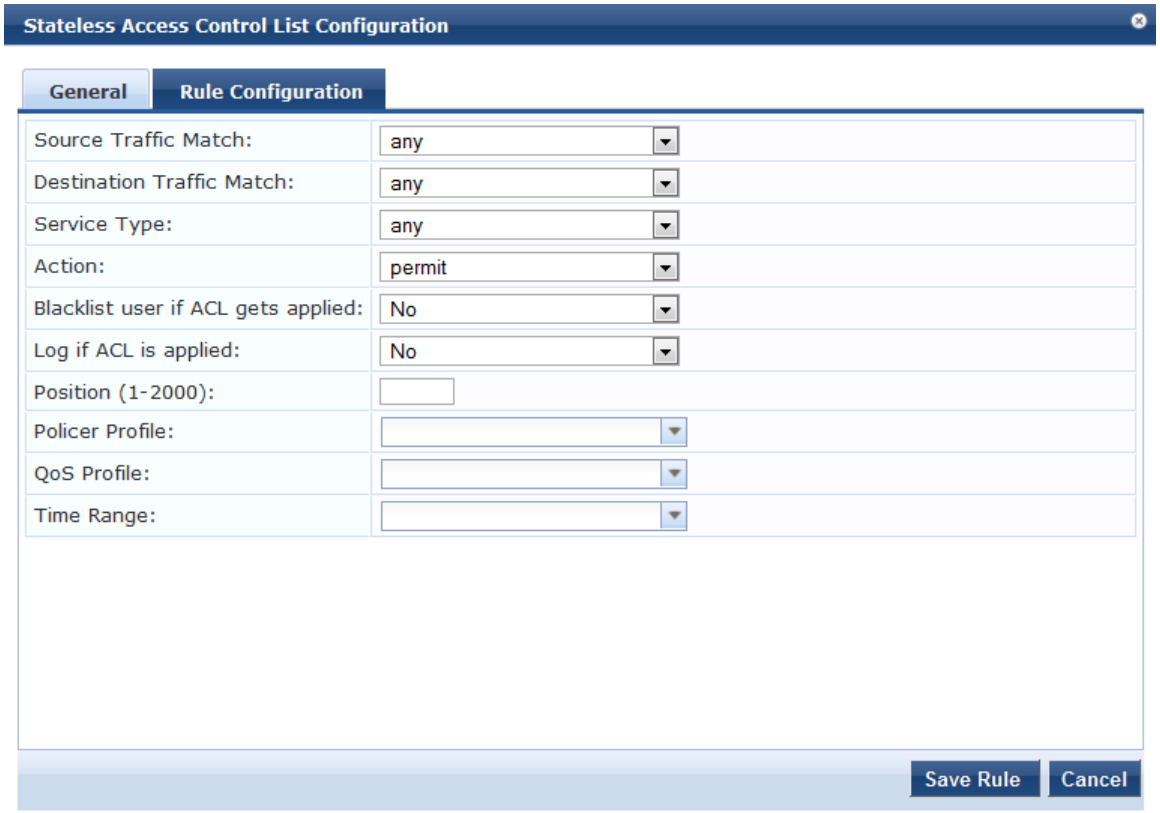
Figure 257: *NAT Pool Configuration Page*



ACL

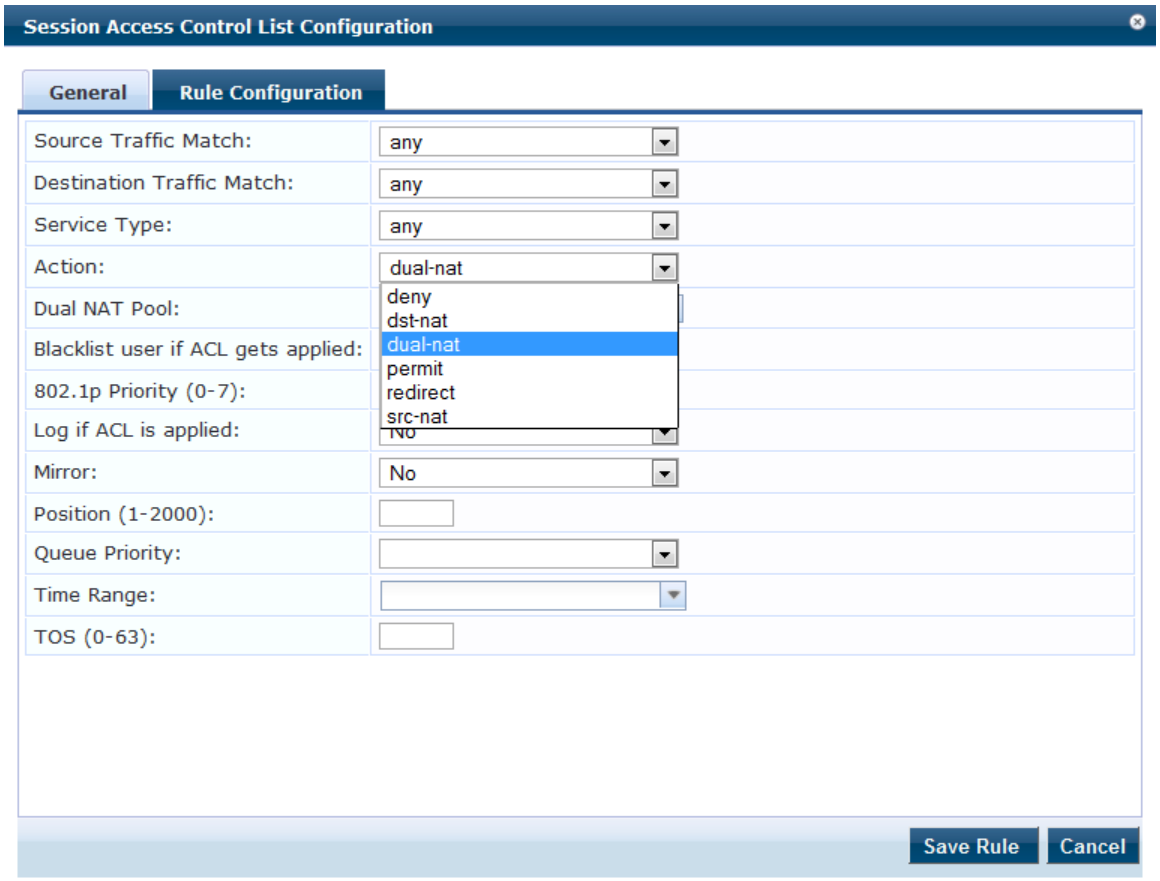
Click the **Add Stateless Access Control List** link. Enter a name for the Stateless ACL. Click the **Add Rule** link on the **General** tab. Enter the required attributes in the **Rule Configuration** tab and click **Save Rule** or **Cancel**.

Figure 258: *Stateless Access Control List Configuration Attributes Page*



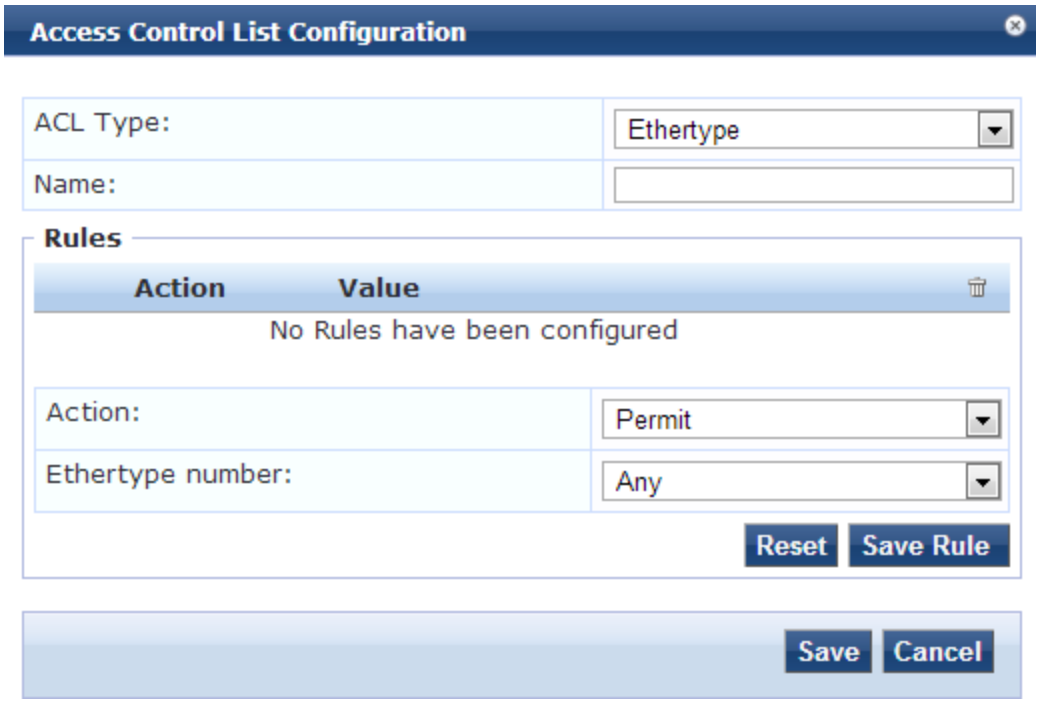
Click the **Add Session Access Control List** link and enter the name for the Session ACL. Click the **Add Rule** link on the **General** tab. You can view different fields depends on the **Action** type you choose from the drop-down list. For example, if you select the dual-nat action type, you can view the **Dual NAT Pool** field additionally to specify the action. Enter the required attributes in the **Rule Configuration** tab and click **Save Rule** or **Cancel**.

Figure 259: *Session Access Control List Attributes Page*



Click the **Add Ethernet/MAC Access Control List** link. Enter a name for the Ethernet/MAC ACL. Enter the required attributes in the **Rules** section of the page and click **Reset**, **Save Rule**. Then click **Save** or **Cancel**.

Figure 260: *Ethernet/MAC Access Control List Attributes Page*



Aruba RADIUS Enforcement

Use this page to configure profile and attribute parameters for the Aruba RADIUS Enforcement Profile.

Profile tab

Figure 261: *Aruba RADIUS Enforcement Profile tab*

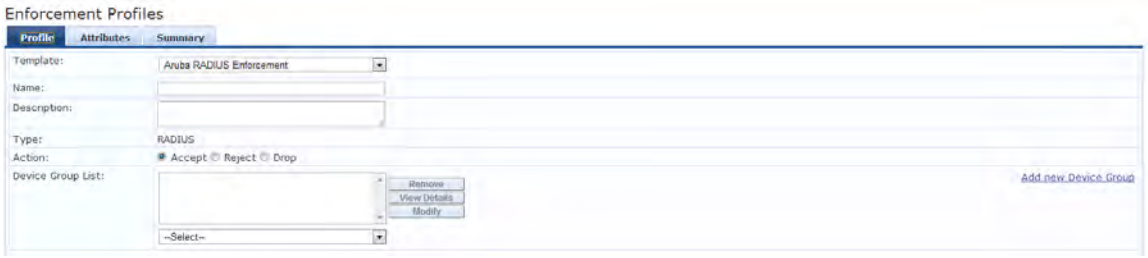


Table 152: *Aruba RADIUS Enforcement Profile tab Parameters*

Parameter	Description
Template	Aruba RADIUS Enforcement
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject or Drop to define the action taken on the request.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 262: *Aruba RADIUS Enforcement Attributes tab*

Table 153: *Aruba RADIUS Enforcement Attributes tab Parameters*

Attribute	Description
Type:	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Cisco Downloadable ACL Enforcement

Use this page to configure profile and attribute parameters for the Cisco Downloadable ACL Enforcement Profile.

Profile tab

Figure 263: *Cisco Downloadable ACL Enforcement Profile tab*

Table 154: *Cisco Downloadable ACL Enforcement Profile tab Parameters*

Parameter	Description
Template:	Cisco Downloadable ACL Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	RADIUS. The field is populated automatically.
Action:	Enabled. Click Accept, Reject, or Drop to define the action taken on the

Table 154: *Cisco Downloadable ACL Enforcement Profile tab Parameters (Continued)*

Parameter	Description
	request.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 264: *Cisco Downloadable ACL Enforcement Attributes tab*

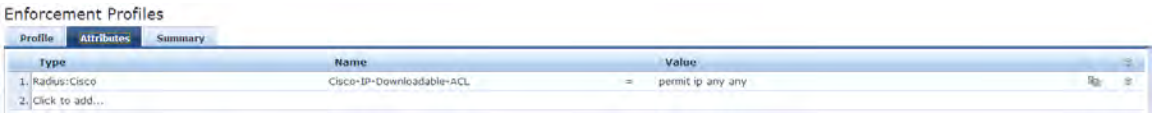


Table 155: *Cisco Downloadable ACL Enforcement Attributes tab Parameters*

Parameter	Description
Type:	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Cisco Web Authentication Enforcement

Use this page to configure profile and attribute parameters for the Cisco Web Authentication Enforcement Profile.

Profile tab

Figure 265: *Cisco Web Authentication Enforcement Profile tab*

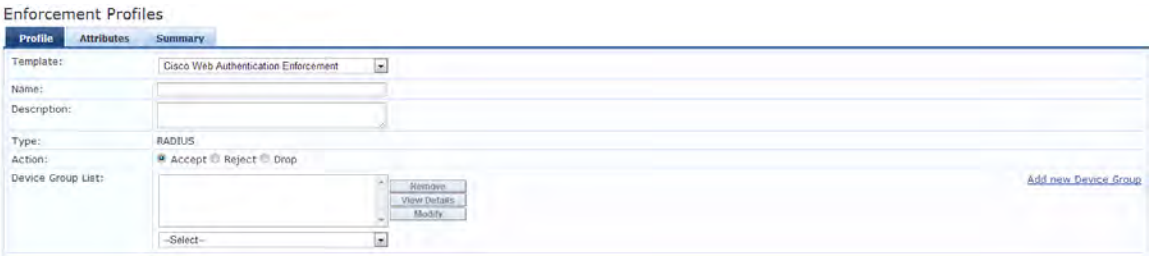


Table 156: *Cisco Web Authentication Enforcement Parameters*

Parameter	Description
Template	Cisco Web Authentication Enforcement
Name	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

After you complete setting the attributes, click **Save**. Click **Next** to open the Summary tab.

Figure 266: *Cisco Web Authentication Enforcement Attributes tab*

Table 157: *Cisco Web Authentication Enforcement Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

ClearPass Entity Update Enforcement

Use this page to configure profile and attribute parameters for the ClearPass Entity Update Enforcement Profile.

Profile tab

Figure 267: *ClearPass Entity Update Enforcement Profile tab*

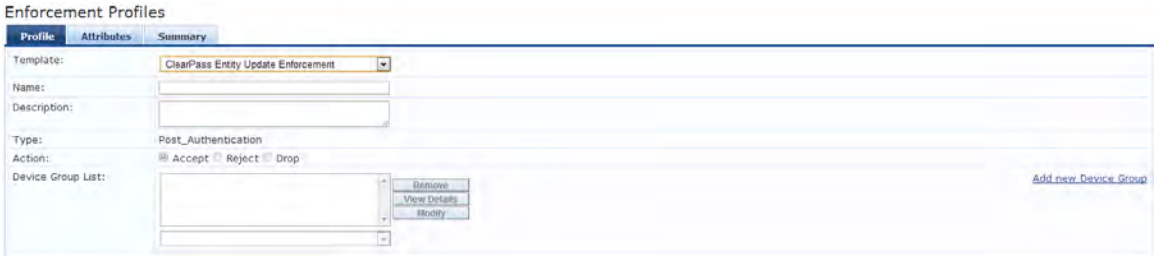


Table 158: *ClearPass Entity Update Enforcement Profile tab Parameters*

Parameter	Description
Template:	ClearPass Entity Update Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	Post_Authentication. The field is populated automatically.

Table 158: *ClearPass Entity Update Enforcement Profile tab Parameters (Continued)*

Parameter	Description
Action:	Disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 268: *ClearPass Entity Update Enforcement Attributes tab*

Table 159: *ClearPass Entity Update Enforcement Attributes tab Parameters*

Attribute	Description
Type:	• Endpoint • Expire-Time-Update • GuestUser • Status-Update
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

CLI Based Enforcement

Use this page to configure profile and attribute parameters for the CLI Based Enforcement Profile.

Profile tab

Figure 269: *CLI Based Enforcement Profile tab*

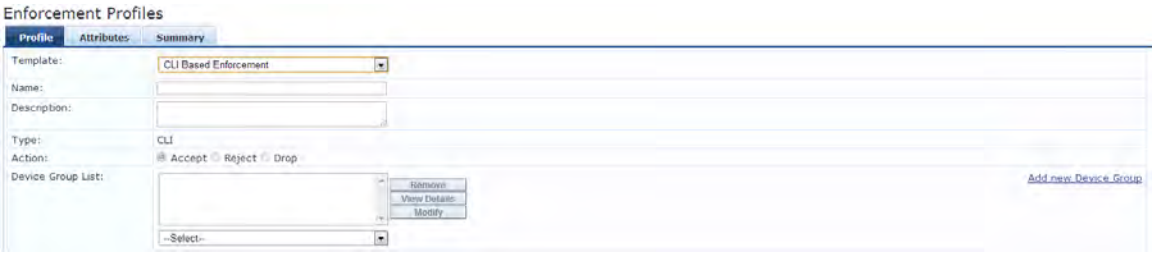


Table 160: *CLI Based Enforcement Profile tab Parameters*

Parameter	Description
Template:	CLI Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	CLI
Action:	Disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed on the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 270: *CLI Based Enforcement Attributes tab*

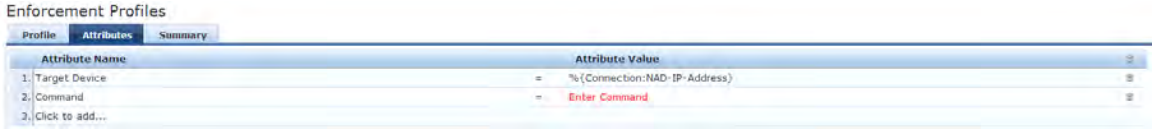


Table 161: *CLI Based Enforcement Attributes tab Parameters*

Attribute	Parameter
Attribute Name	Select Command or Target Device.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

Filter ID Based Enforcement

Use this page to configure profile and attribute parameters for the Filter ID Based Enforcement Profile.

Profile tab

Figure 271: *Filter ID Based Enforcement Profile tab*

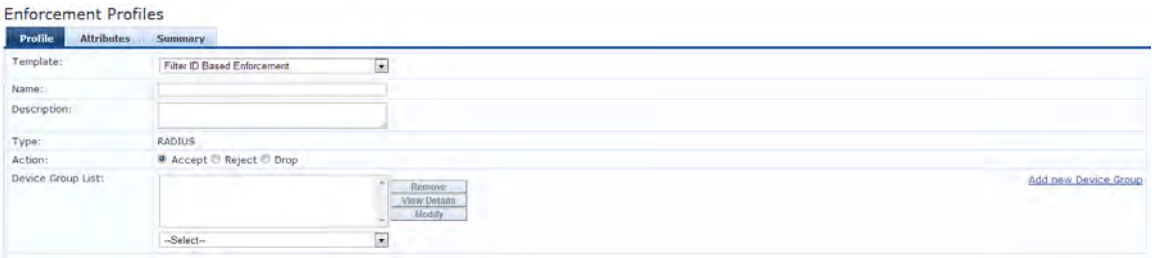


Table 162: *Filter ID Based Enforcement Profile tab Parameters*

Parameter	Description
Template:	Filter ID Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	RADIUS. The field is populated automatically.

Parameter	Description
Action:	Enabled. Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group:	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 272: *Filter ID Based Enforcement Profile Attributes tab*

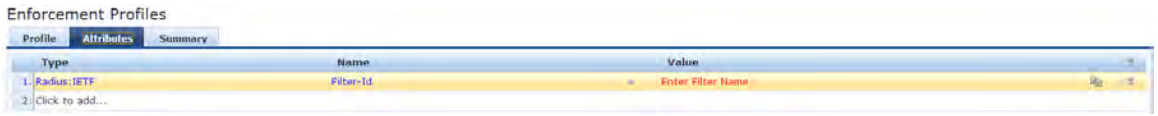


Table 163: *Filter ID Based Enforcement Profile Attributes tab Parameters*

Parameter	Description
Type:	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Generic Application Enforcement

Use this page to configure profile and attribute parameters for the Generic Application Enforcement Profile.

Profile tab

Figure 273: *Generic Application Enforcement Profile tab*

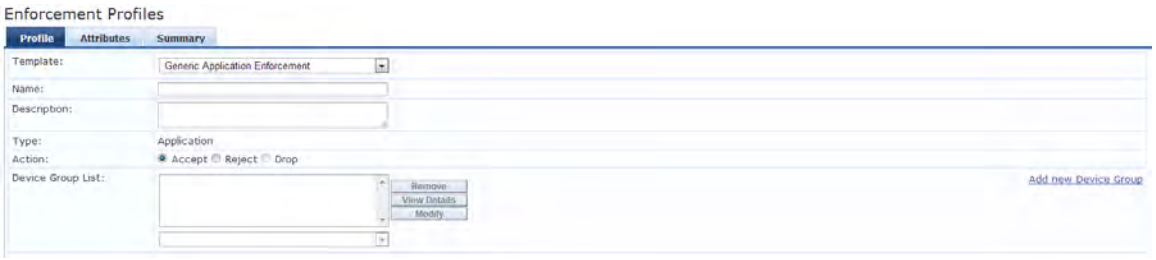


Table 164: *Generic Application Enforcement Profile tab Parameters*

Parameter	Description
Template:	Generic Application Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	Application. The field is populated automatically.
Action:	Enabled. Click Accept or Reject to define the action taken on the request. The Drop button is disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 274: *Generic Application Enforcement Attributes tab*

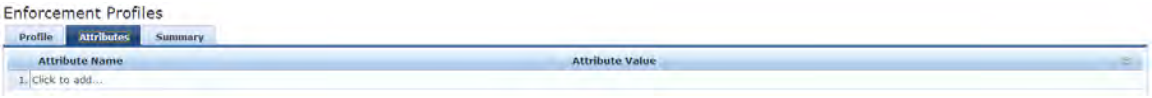


Table 165: *Generic Application Enforcement Attributes tab Parameters*

Parameter	Description
Attribute Name	Select an attribute name from the list. The list has multiple pages.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

HTTP Based Enforcement

Use this page to configure profile and attribute parameters for the HTTP Based Enforcement Profile.

Profile tab

Figure 275: *HTTP Based Enforcement Profile tab*

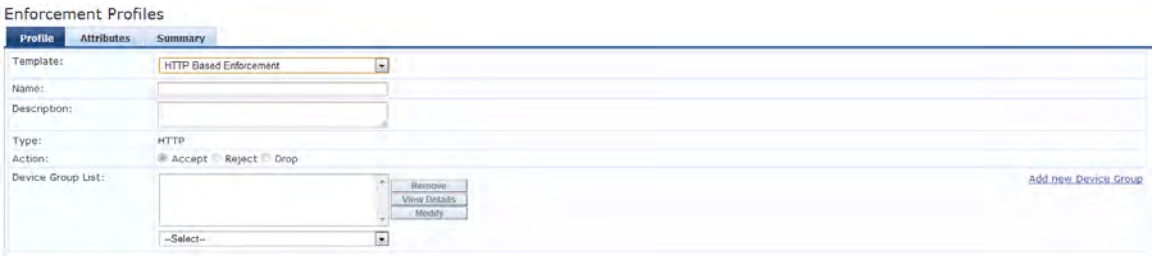


Table 166: *HTTP Based Enforcement Profile tab Parameters*

Parameter	Description
Template:	HTTP Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	HTTP. The field is populated automatically.
Action:	Disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 276: *HTTP Based Enforcement Attributes tab*

Table 167: *HTTP Based Enforcement Attributes tab Parameters*

Parameter	Description
Attribute Name	Select Target Server or Action.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

RADIUS Based Enforcement

Use this page to configure profile and attribute parameters for the RADIUS Based Enforcement Profiles.

Profile tab

Figure 277: *RADIUS Based Enforcement Profile tab*

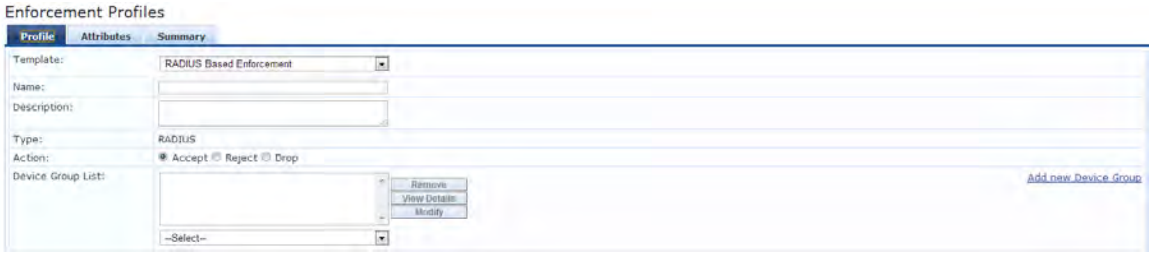


Table 168: *RADIUS Based Enforcement Profile tab Parameters*

Parameter	Description
Template	RADIUS Based Enforcement
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	RADIUS. The field is populated automatically.

Table 168: *RADIUS Based Enforcement Profile tab Parameters (Continued)*

Parameter	Description
Action	Enabled. Click Accept, Reject or Drop to define the action taken on the request.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry • Click **View Details** to see the device group parameters • Click **Modify** to change the parameters of the selected device group
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 278: *RADIUS Based Enforcement Attributes tab*

Table 169: *RADIUS Based Enforcement Attributes tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

RADIUS Change of Authorization (CoA)

Use this page to configure profile and attribute parameters for the RADIUS Change of Authorization (CoA) Enforcement Profile.

Profile tab

Figure 279: *Radius Change of Authorization (CoA) Profile tab*

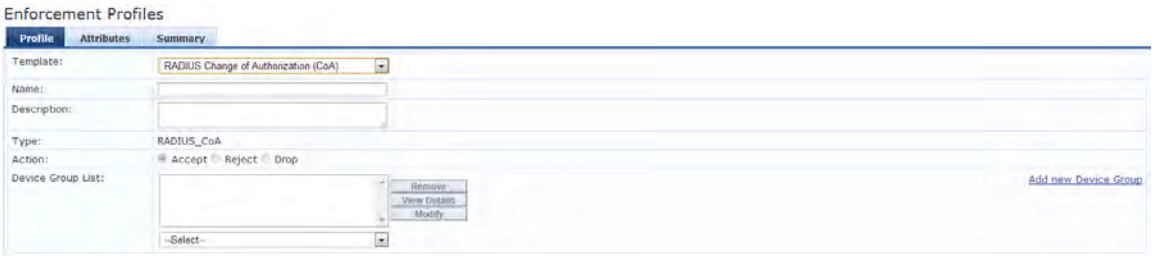


Table 170: *Radius Change of Authorization (CoA) Profile tab Parameters*

Parameter	Description
Template:	Select from: • Cisco-Disable-Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate-Session • HP - Change-VLAN • HP - Generic-CoA • Aruba - Change-User-Role • IETF - Terminate-Session-IETF • Aruba - Change-VPN-User-Role • IETF- Generic-CoA-IETF
Type:	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the RADIUS CoA Template selected and the Type Attribute that were selected.
Value:	The options displayed for the Value Attribute depend on the RADIUS CoA Template selected and the Type Attribute that were selected.
Type:	RADIUS_CoA. The field is populated automatically.

Table 170: *Radius Change of Authorization (CoA) Profile tab Parameters (Continued)*

Parameter	Description
Action:	Disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed on the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 280: *Radius Change of Authorization (CoA) Attributes tab*

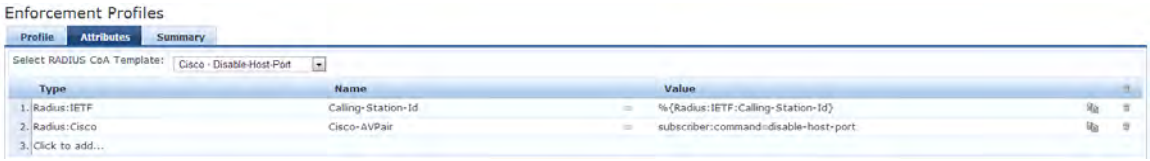


Table 171: *Radius Change of Authorization (CoA) Attributes tab Parameters*

Parameter	Description
RADIUS CoA Template:	Select from: • Cisco-Disable-Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate-Session • HP - Change-VLAN • HP - Generic-CoA • Aruba - Change-User-Role • IETF - Terminate-Session-IETF • Aruba - Change-VPN-User-Role • IETF- Generic-CoA-IETF
Type:	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Template and Type Attribute that were selected.
Value:	The options displayed for the Value Attribute depend on the Template, Type Attribute and Name Attribute that were selected.

Session Restrictions Enforcement

Use this page to configure profile and attribute parameters for Session Restrictions Enforcement Profile.

Profile tab

Figure 281: *Session Restrictions Enforcement Profile tab*

Table 172: *Session Restrictions Enforcement Profile tab Parameters*

Parameter	Description
Template:	Session Restrictions Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	Post_Authentication. The field is populated automatically.
Action:	Disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 282: *Session Restrictions Enforcement Attributes tab*

Table 173: *Session Restrictions Enforcement Attributes tab*

Parameter	Description

Type	Select from:
	• Bandwidth-Check
	• Expire-Check
	• Post-Auth-Check
	• Session-Check
	NOTE: Palo Alto integration is extended to Guest MAC Caching use cases. Configure:
	`Session-Check::IP-Address-Change-Notify = <ip-address>`
	`Session-Check::Username = %{Endpoint:Username}`
	Post Auth sends the Guest username instead of the MAC Address in the user id updates.

Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

SNMP Based Enforcement

Use this page to configure profile and attribute parameters for the SNMP Based Enforcement Profile.

Profile tab

Figure 283: *SNMP Based Enforcement Profile tab*

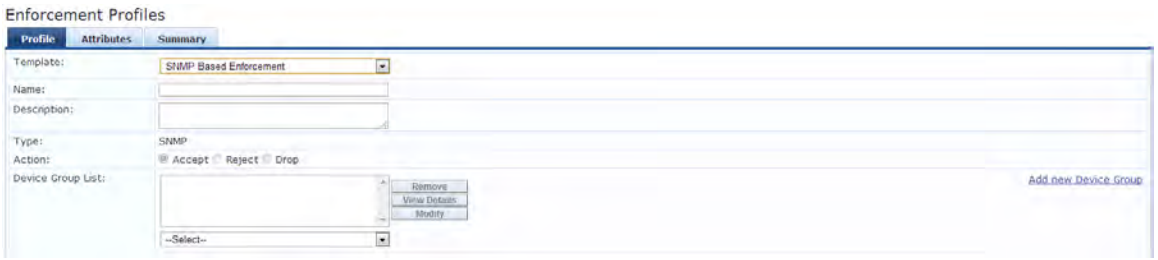


Table 174: *SNMP Based Enforcement Profile tab Parameters*

Parameter	Description
Template:	SNMP Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.

Table 174: *SNMP Based Enforcement Profile tab Parameters (Continued)*

Parameter	Description
Type:	SNMP. The field is populated automatically.
Action:	Disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 284: *SNMP Based Enforcement Attributes tab*

Table 175: *SNMP Based Enforcement Attributes tab Parameters*

Parameter	Description
Attribute Name:	Select from: • VLAN ID • Session Timeout (in seconds) • Reset Connection (after the settings are applied)
Attribute Value:	The options displayed for the Attribute Value depend on Attribute Name that was selected.

TACACS+ Based Enforcement

Use this page to configure profile, service, and attribute parameters for the TACACS+ Based Enforcement Profile.

Profile tab

Figure 285: *TACACS+ Based Enforcement Profile tab*

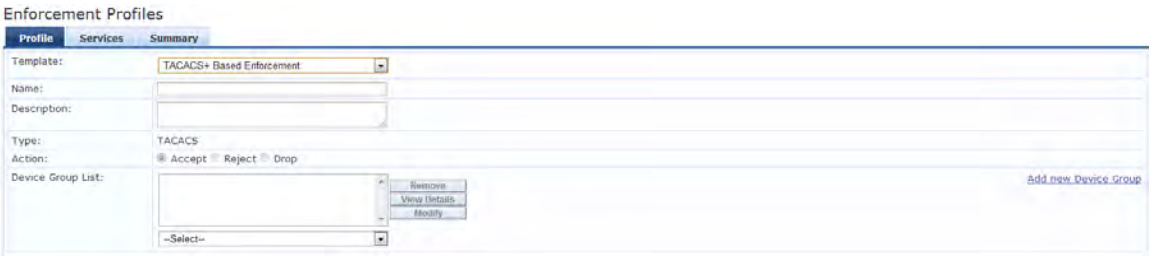


Table 176: *TACACS+ Based Enforcement Profile tab Parameters*

Parameter	Description
Template:	TACACS+ Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	TACACS. The field is populated automatically.
Action:	Disabled.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Services tab

Figure 286: *TACACS+ Based Enforcement Services tab*

Table 177: *TACACS+ Based Enforcement Services tab Parameters*

Parameter	Description
Privilege Level:	Select a level between 0 and 15.
Selected Services	Select a service from the list and add it to the Selected Services: field. Click **Remove** to remove a service from the field.
Export All	Click this link to download the TACACS+ Services dictionary is downloaded to the local computer.
Custom Services:	To add new TACACS+ services / attributes, upload the modified dictionary xml click the Update TACACS+ Services Dictionary.
Type:	Select a Service Attribute parameter from the list.
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

VLAN Enforcement

Use this page to configure profile and attribute parameters for the VLAN Enforcement Profile.

Profile tab

Figure 287: *VLAN Enforcement Profile tab*

Table 178: *VLAN Enforcement Profile tab Parameters*

Parameter	Description
Template:	VLAN Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	RADIUS. The field is populated automatically.

Table 178: *VLAN Enforcement Profile tab Parameters (Continued)*

Parameter	Description
Action:	Enabled. Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List:	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 309.

Attributes tab

Figure 288: *VLAN Enforcement Attributes tab*

Table 179: *VLAN Enforcement Attributes tab Parameters*

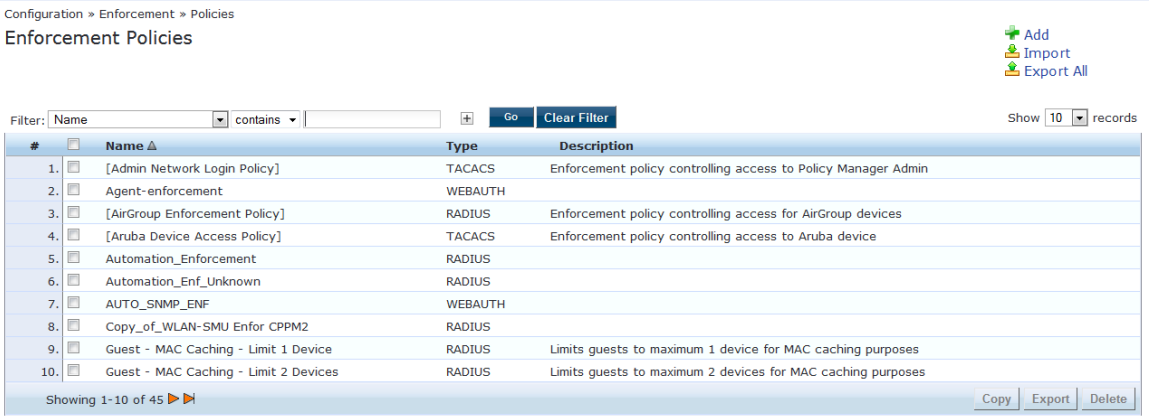
Parameter	Description
Type:	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Configuring Enforcement Policies

One and only one Enforcement Policy can be associated with each Service. Enforcement policies can be added in one of two ways:

- From the **Configuration > Enforcement > Enforcement Policies**.
- From the **Configuration > Services** page as part of the flow of the **Add Service** wizard.

Figure 289: *Enforcement Policies Listing Page*



Click **Add Enforcement Policy** to open the **Add Enforcement Policy** wizard:

Figure 290: *Add Enforcement Policy (Enforcement tab)*

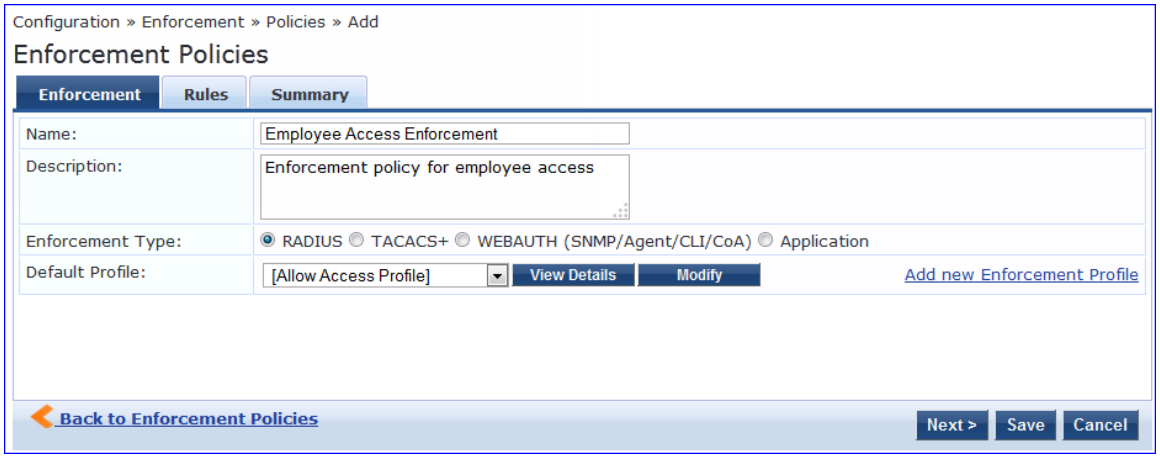


Table 180: *Add Enforcement Policy (Enforcement tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	Select: **RADIUS, TACACS+, WebAuth (SNMP/CLI)/CoA** or **Application**. Based on this selection, the Default Profile list shows the right type of enforcement profiles in the drop-down list (See Below). **NOTE:** Web-based Authentication or WebAuth (HTTPS) is the mechanism used by authentications performed via a browser, and authentications performed via Dell W-OnGuard. Both SNMP and CLI (SSH/Telnet) based Enforcement Profiles can be sent to the network device based on the type of device and the use case.
Default Profile	An Enforcement Policy applies Conditions (roles, health and time attributes) against specific

Table 180: *Add Enforcement Policy (Enforcement tab) (Continued)*

Parameter	Description
	values associated with those attributes to determine the Enforcement Profile. If none of the rules matches, Policy Manager applies the Default Profile. Click **Add new Enforcement Profile** to add a new profile (This is integrated into the flow. After you are done creating the profile, Policy Manager brings you back to the current page/tab.)

In the **Rules** tab, click **New Rule** to display the **Rules Editor**:

Figure 291: *Add Enforcement Policy (Rules Tab)*

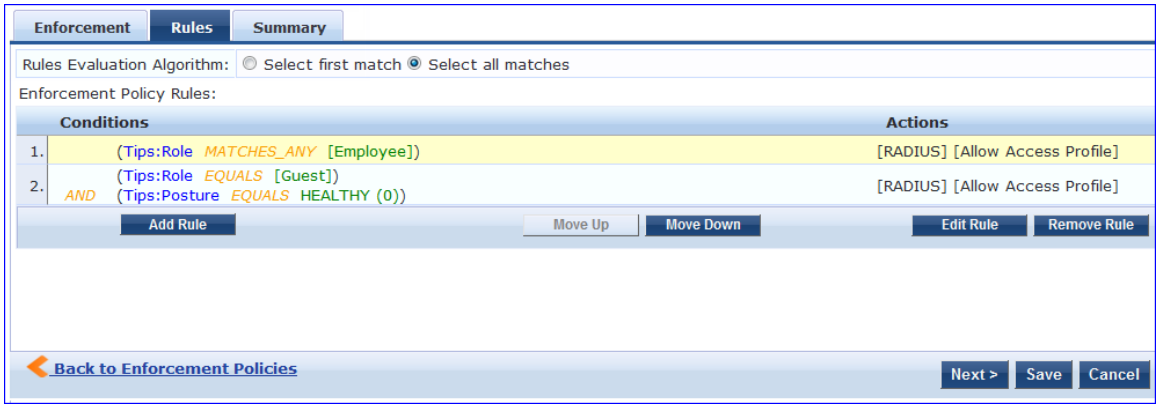


Table 181: *Add Enforcement Policy (Rules tab)*

Field	Description
Add/Edit Rule	Bring up the rules editor to add/edit a rule.
Move Up/Down	Reorder the rules in the enforcement policy.
Remove Rule	Remove a rule.

Table 182: *Add Enforcement Policy (Rules Editor)*

Field	Description
Conditions/Enforcement Profiles	Select conditions for this rule. For each condition, select a matching action (Enforcement Profile). **NOTE:** A condition in an Enforcement Policy rule can contain attributes from the following namespaces: Tips:Role, Tips:Posture, and Date. **NOTE:** The value field for the Tips:Role attribute can be a role defined in Policy Manager, or a role fetched from the authorization source. (Refer to see how Enable as Role can be turned on for a fetched attribute). Role names fetched from the authorization source can be entered freeform in value field. To commit the rule, click **Save**.
Enforcement Profiles	If the rule conditions match, attributes from the selected enforcement profiles are sent to Network Access Device. If a rule matches and there are multiple enforcement profiles, the enforcement profile disambiguation rules apply. Refer to Configuring Enforcement Profiles on page 264 for a list of the default profiles.

A Policy Manager Device represents a Network Access Device (NAD) that sends network access requests to Policy Manager using the supported RADIUS, TACACS+, or SNMP protocol.

For more information, see:

- Adding and Modifying Devices on page 303
- Adding and Modifying Device Groups on page 309
- Adding and Modifying Proxy Targets on page 311

Adding and Modifying Devices

To connect with Policy Manager using the supported protocols, a NAD must belong to the global list of devices in the Policy Manager database.

Policy Manager lists all configured devices in the **Devices** page: **Configuration > Network > Devices**. From this interface:

Figure 292: *Network Devices page*

For more information, see:

- Adding a Device on page 303
- Additional Available Tasks on page 309

Adding a Device

To add a device, click the **Add** link, and then complete the fields in the **Add Device** popup. The following figure shows an example of the **Device** tab followed by parameter definition:

Figure 293: *Device Tab*

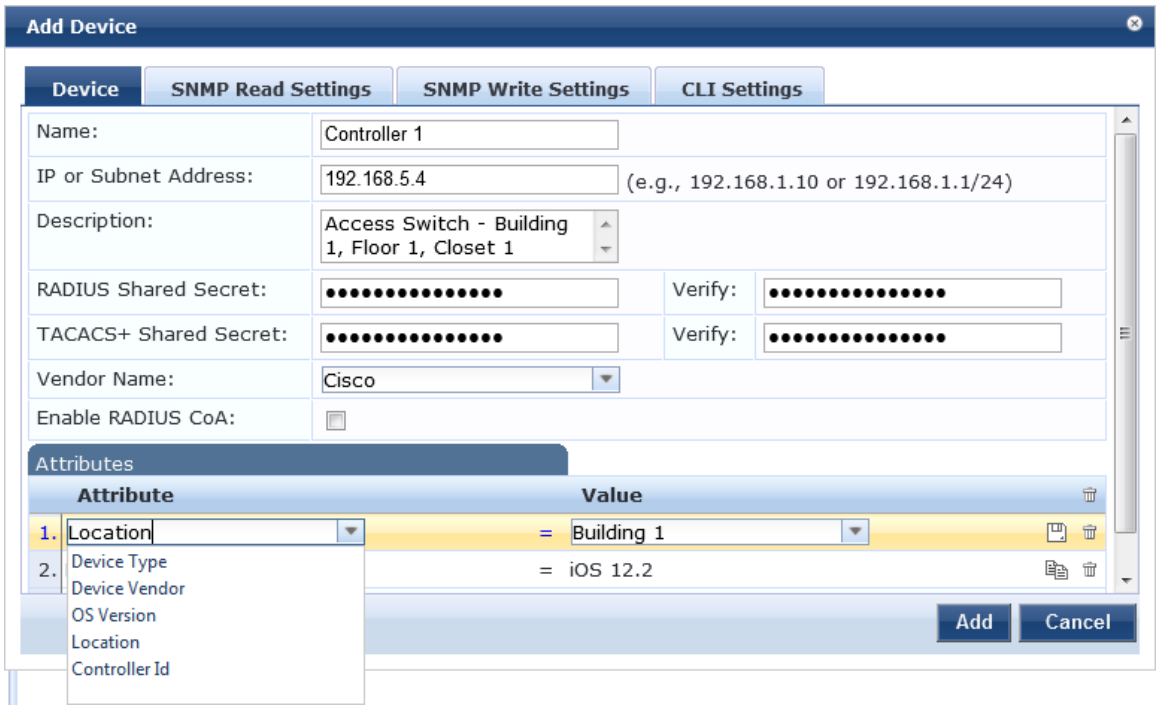


Table 183: *Device tab Parameters*

Parameter	Description
Name	Specify the identity of the device.
Description	Provide the additional information that helps to identify the device.
IP Address or Subnet	Specify the IP address or the subnet of the device. For example, 192.168.5.0/24.
RADIUS/TACACS+ Shared Secret	Enter and confirm a Shared Secret for each of the two supported request protocols.

Table 183: *Device tab Parameters (Continued)*

Parameter	Description
Vendor	Specify the dictionary to be loaded for this device. This field is optional. **NOTE:** RADIUS:IETF, the dictionary containing the standard set of RADIUS attributes, is always loaded. When you specify a vendor here, the RADIUS dictionary associated with this vendor is automatically enabled.
Enable RADIUS CoA RADIUS CoA Port	Enable RADIUS CoA (RFC 3576/5176) for this device. Set the UDP port on the device to send CoA actions. The default value is 3799.
Attributes	Add custom attributes for this device. Click on the "Click to add..." row to add custom attributes. By default, four custom attributes appear in the **Attribute** drop down: Location, OS-Version, Device-Type, and Device-Vendor. You can enter any name in the **Attribute** field. All attributes are of string datatype. The value field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in the **Attribute** drop down for all devices. **NOTE:** All attributes entered for a device are available in the role mapping rules editor under the Device namespace.

The following figures show the examples of **SNMP Read/Write Settings** tabs followed by parameter definition:

Figure 294: *SNMP Read/Write Settings tabs*

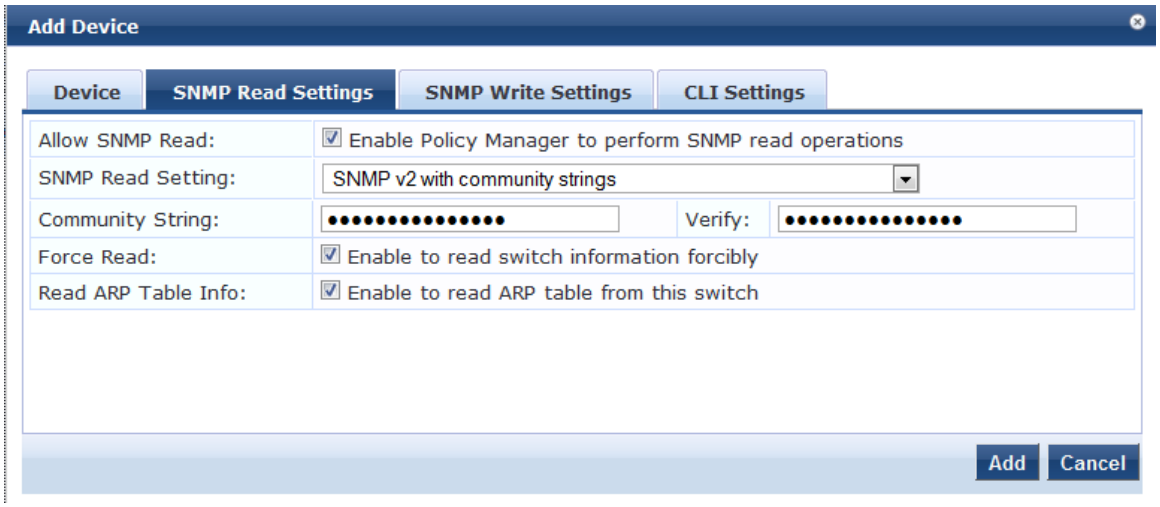


Figure 295: *SNMP Read/Write Settings tabs - SNMP v3 Details*

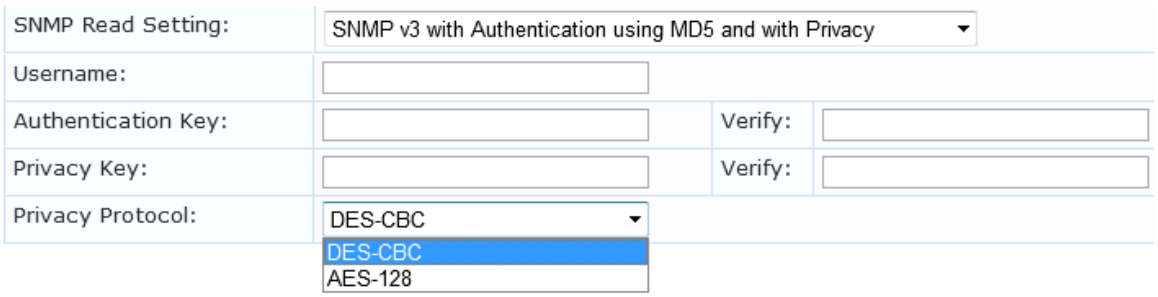


Table 184: *SNMP Read/Write Settings tabs Parameters*

Parameter	Description
Allow SNMP Read/Write	Toggle to enable or disable SNMP Read/Write.
Default VLAN (SNMP Write only)	Specify the VLAN port setting after SNMP-enforced session expires.
SNMP Read Setting	Specify the SNMP Read settings for the device. You can set any of the following options: • SNMP v1 with community strings • SNMP v2 with community strings • SNMP v3 with no Authentication • SNMP v3 with Authentication using MD5 and no Privacy • SNMP v3 with Authentication using MD5 and with Privacy • SNMP v3 with Authentication using SHA and no Privacy • SNMP v3 with Authentication using SHA and with Privacy **NOTE:** The MD5 authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.
SNMP Write Settings	Specify the SNMP Write settings for the device. You can set any of the following options: • SNMP v1 with community strings • SNMP v2 with community strings • SNMP v3 with no Authentication • SNMP v3 with Authentication using MD5 and no Privacy • SNMP v3 with Authentication using MD5 and with Privacy • SNMP v3 with Authentication using SHA and no Privacy • SNMP v3 with Authentication using SHA and with Privacy **NOTE:** The MD5 authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.
Community String (SNMP v2 only)	Enter the community string for sending the traps.
Verify	Re-enter the community string for sending the traps.

Table 184: *SNMP Read/Write Settings tabs Parameters (Continued)*

Parameter	Description
Force Read (SNMP v1 and v2 only)	Enable this setting to ensure that all Dell Networking W-ClearPass Policy Manager nodes in the cluster read SNMP information from this device regardless of the trap configuration on the device. This option is useful when demonstrating static IP-based device profiling because this does not require any trap configuration on the network device.
Read ARP Table Info	Enable this setting, if this is a Layer 3 device and you intend to use the ARP table on this device to discover endpoints in the network. Static IP endpoints discovered this way are further probed using SNMP to profile the device.
Username (SNMP v3 only)	Specify the Admin user name to use for SNMP read/write operations.
Authentication Key (SNMP v3 only)	Specify the SNMP v3 with authentication option (SHA or MD5). **NOTE:** The **EAP-MD5** authentication type is not supported if you run Dell Networking W-ClearPass Policy Manager in the FIPS mode.
Privacy Key (SNMP v3 only)	Specify the SNMP v3 with privacy option.
Privacy Protocol (SNMP v3 w/ privacy only)	Choose one of the available privacy protocols: • DES-CBC • AES-128

In a large or geographically spread cluster deployments, you do not want all CPPM nodes to probe all SNMP configured devices. The default behavior is for a CPPM node in the cluster to read network device information only for devices configured to send traps to that CPPM node.

Figure 296: *CLI Settings Tab*

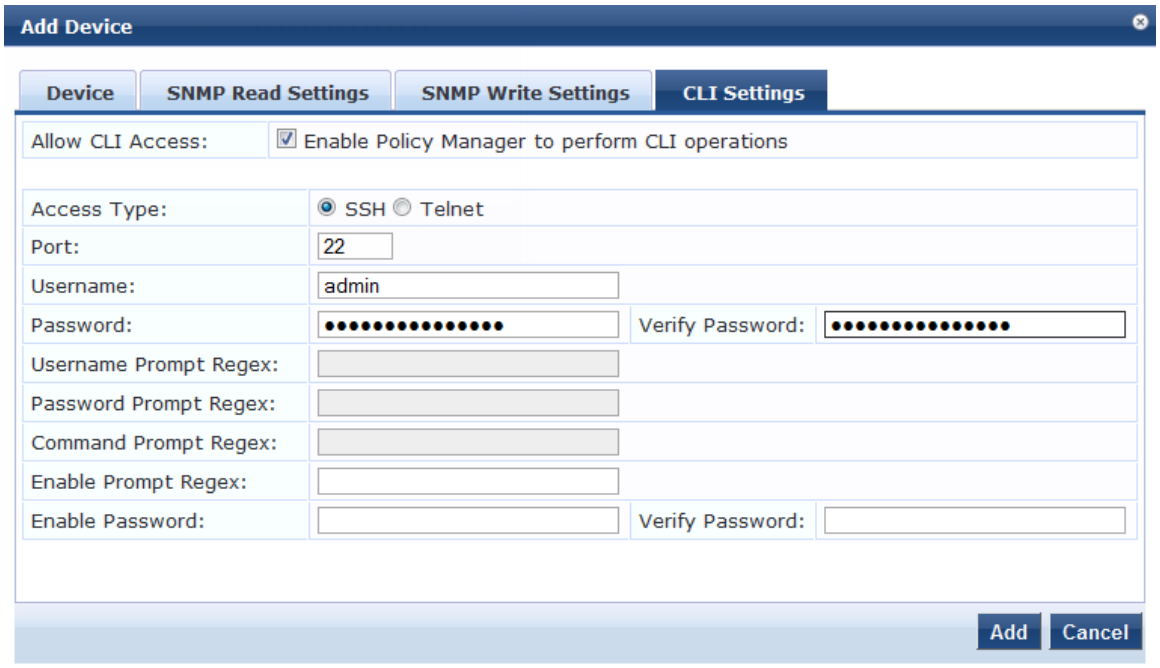


Table 185: *CLI Settings tab Parameters*

Parameter	Description
Allow CLI Access	Toggle to enable or disable CLI access.
Access Type	Select SSH or Telnet. Policy Manager uses the selected access method to log into the device CLI.
Port	Specify the SSH or Telnet TCP port number.
Username/Password	Enter the credentials to log into the CLI.
Username Prompt Regex	Specify the regular expression for the username prompt. Policy Manager looks for this pattern to recognize the telnet username prompt.
Password Prompt Regex	Specify the regular expression for the password prompt. Policy Manager looks for this pattern to recognize the telnet password prompt.
Command Prompt Regex	Specify the regular expression for the command line prompt. Policy Manager looks for this pattern to recognize the telnet command line prompt.
Enable Prompt Regex	Specify the regular expression for the command line in the **enable** prompt. Policy Manager looks for this pattern to recognize the telnet command line prompt.
Enable Password	Enter and re-enter the credentials for **Enable** in the CLI.

Additional Available Tasks

- To import a device, click **Import Devices**. In the **Import from File** popup, browse to select a file, and then click **Import**. If you entered a secret key to encrypt the exported file, enter the same secret key to import the device back.
- To export all devices from the configuration, click **Export Devices**. In the **Export to File** popup, specify a file path, and then click **Export**. In the Export to File popup, you can choose to encrypt the exported data with a key. This protects data such as shared secret from being visible in the exported file. To import it back, you specify the same key with which you exported.
- To export a single device from the configuration, select it (via the check box on the left), and then click **Export**. In the **Save As** popup, specify a file path, and then click **Export**.
- To delete a single device from the configuration, select it (via the check box on the left), and then click **Delete**. Commit the deletion by selecting **Yes**; dismiss the popup by selecting **No.**

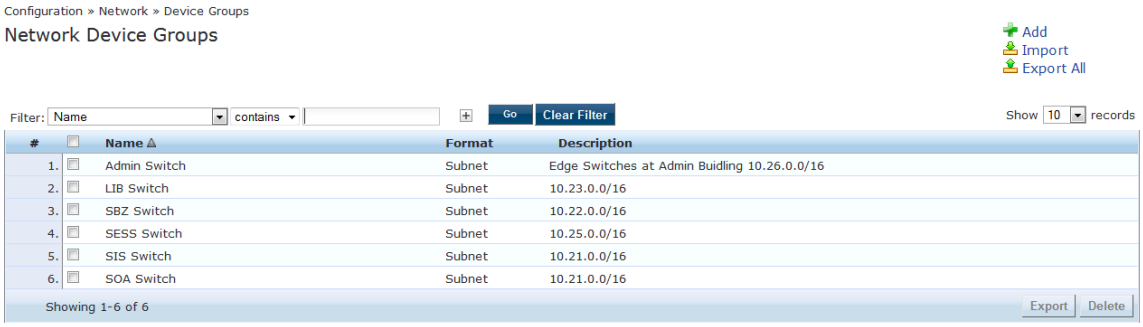
Adding and Modifying Device Groups

Policy Manager groups devices into *Device Groups,* which function as a component in Service and Role Mapping rules. Device Groups can also be associated with Enforcement Profiles; Policy Manager sends the attributes associated with these profiles only if the request originated from a device belonging to the device groups.

Administrators configure Device Groups at the global level. They can contain the members of the IP address of a specified subnet (or regular expression-based variation), or devices previously configured in the Policy Manager database.

Policy Manager lists all configured device groups in the **Device Groups** page: **Configuration > Network > Device Groups**.

Figure 297: *Device Groups Page*



To add a Device Group, click **Add**. Complete the fields in the **Add New Device Group** popup:

Figure 298: *Add New Device Group Popup*

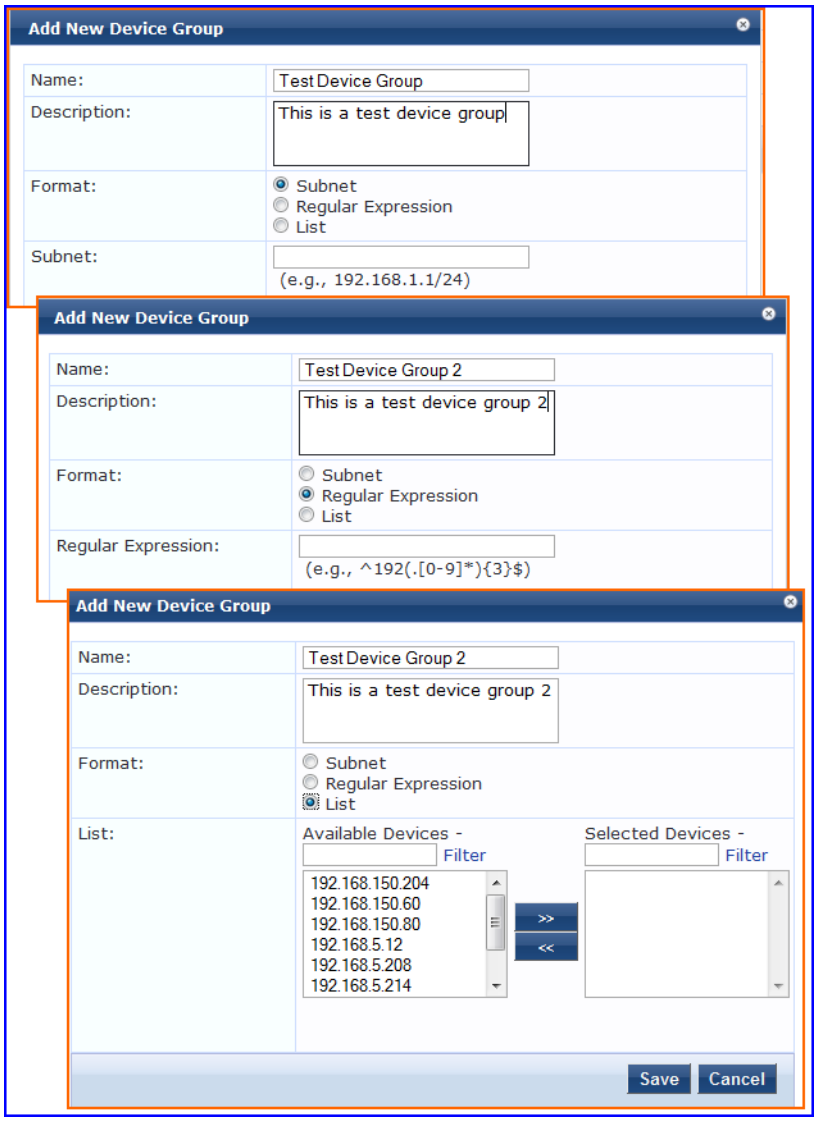


Table 186: *Add New Device Group popup*

Parameter	Description
Name/ Description/ Format	Specify identity of the device.
Subnet	Enter a subnet consisting of network address and the network suffix (CIDR notation); for example, 192.168.5.0/24
Regular Expression	Specify a regular expression that represents all IPv4 addresses matching that expression; for example, ^192(.[0-9]*){3}$

Table 186: *Add New Device Group popup (Continued)*

Parameter	Description
List: Available/Selected Devices	Use the widgets to move device identifiers between Available and Selected. Click **Filter** to filter the list based on the text in the associated text box.
Save/Cancel	Click **Save** to commit or **Cancel** to dismiss the popup.

For SNMP enforcement on the network device, one or more of the following traps have to be configured on the device: Link Up trap, Link Down trap, MAC Notification trap. In addition, one or more of the following SNMP MIBs must be supported by the device: RFC-1213 MIB, IF-MIB, BRIDGE-MIB, ENTITY-MIB, Q-BRIDGE-MIB, CISCO-VLAN-MEMBERSHIP-MIB, CISCO-STACK-MIB, CISCO-MAC-NOTIFICATION-MIB.
These traps and MIBs enable Policy Manager to correlate the MAC address, IP address, switch port, and switch information.

Additional Available Tasks

- To import a Device Group, click **Import** in the **Import from File** popup, browse to select a file, then click **Import**.
- To export all Device Groups from the configuration, click **Export All** in the **Export to File** popup, specify a file path, then click **Export**.
- To export a single Device Group from the configuration, select it (using the check box on the left), then click **Export**; in the **Save As** popup, specify a file path, then click **Export**.
- To delete a single Device Group from the configuration, select it (using the check box on the left), then click **Delete**; commit the deletion by selecting **Yes**. Dismiss the popup by selecting **No**.

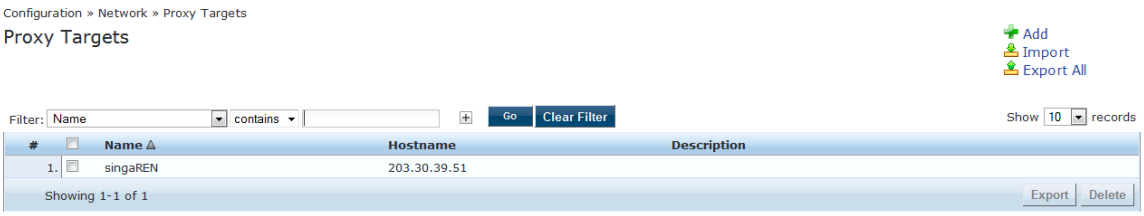
Adding and Modifying Proxy Targets

In Policy Manager, a proxy target represents a RADIUS server (Policy Manager or third party) that is the target of a proxied RADIUS request. For example, when a branch office employee visits a main office and logs into the network, Policy Manager assigns the request to the first Service in priority order that contains a Service Rule for RADIUS proxy Services and appending the *domain* to the Username.

Proxy targets are configured at a global level. They can then be used in configuring RADIUS proxy Services. (Refer to Policy Manager Service Types on page 98.)

Policy Manager lists all configured proxy servers in the **Proxy Servers** page: **Configuration > Network > Proxy Servers**.

Figure 299: *Proxy Targets Page*



Add a Proxy Target

To add a Proxy Target, click **Add** and complete the fields in the **Add Proxy Target** popup. You can also add a new proxy target from the **Services** page (**Configuration > Service** (as part of the flow of the Add **Service** wizard for a RADIUS Proxy Service Type).

Figure 300: *Add Proxy Target Popup*

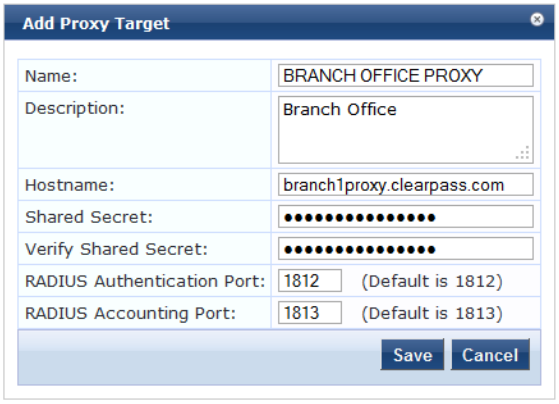


Table 187: *Add Proxy Target popup*

Parameter	Description
Name/Description	Freeform label and description.
Hostname/Shared Secret	RADIUS Hostname and Shared Secret. Use the same secret that you entered on the proxy target (refer to your RADIUS server configuration).
RADIUS Authentication Port	Enter the UDP port to send the RADIUS request. Default value for this port is 1812.
RADIUS Accounting Port	Enter the UDP port to send the RADIUS accounting request. Default value for this port is 1813.

Additional Available Tasks

Import a Proxy Target

Click **Import**. In the **Import from File** popup, browse to select a file and click **Import**.

Export all Proxy Targets

Click **Export All**. In the **Export to File** popup, specify a file path Click **Export**.

Export one Proxy Target

Click a checkbox to select the proxy target and then click **Export**. In the **Save As** popup, specify a file path, and then click **Export**.

Delete one Proxy Target

Click a checkbox to select the Proxy Target and then click **Delete**. Commit the deletion by selecting **Yes**. Dismiss the popup by selecting **No**.

Custom Admin Privileges

Dell Networking W-ClearPass Policy Manager ships with six read-only default administrator privilege XML files. You have the option to export one or more default files and modify the file to create a customized administrator privileges file. Customized administrator privileges are defined in a specifically formatted XML file and then imported into Policy Manager on the Admin Privileges page.

For more information, see:

- Administrator Privilege XML File Structure on page 348
- Administrator Privileges and IDs on page 348
- Creating Custom Administrator Privileges on page 351
- Sample Administrator Privilege XML File on page 352
- Data Filters on page 58

Figure 301: *Admin Privileges Page*

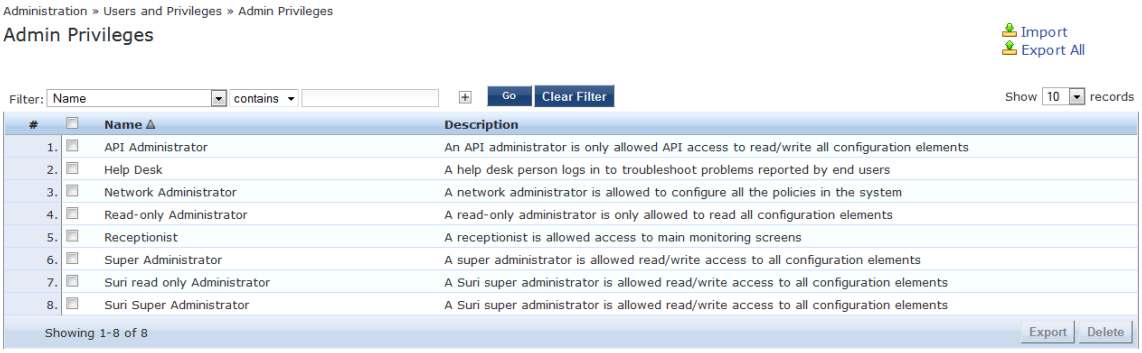


Table 188: *Admin Privileges Page Parameters*

Parameter	Description
Name/Description	Displays the names and descriptions of the six default custom administrator privilege XML files as well as any custom privilege files that have been imported,
Import	Click to navigate to and import a new or changed custom administrator privileges XML file.
Export All	Select a file and click this button to export an administrator privileges XML file to a local drive.

After the policies are final, you can use the **Configuration > Policy Simulation** utility to evaluate the policies before deployment. The Policy Simulation utility applies a set of request parameters as input against a given policy component and displays the outcome in the **Results** tab.

For more information, see:

- Active Directory Authentication on page 316
- Application Authentication on page 317
- Audit on page 318
- Chained Simulation on page 319
- Enforcement Policy on page 322
- RADIUS Authentication on page 325
- Role Mapping on page 330
- Service Categorization on page 333

The following figure shows an example of the **Policy Simulation** page followed by parameter definition:

Figure 302: *Policy Simulation page*

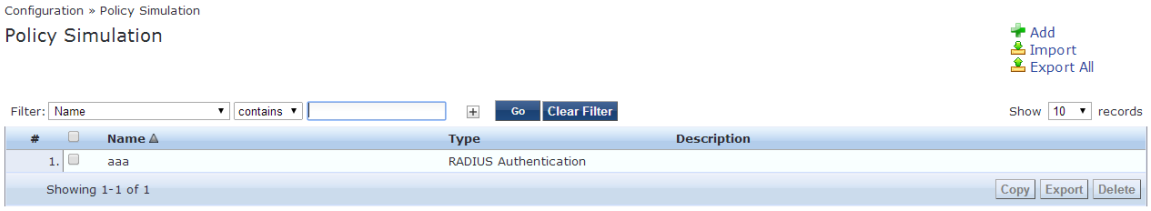


Table 189: *Policy Simulation Page Parameters*

Parameter	Description
Add	Opens the **Configuration** > **Policy Simulation** > **Add** page.
Import	Opens the **Import from file** popup.
Export All	Opens the **Export to file** popup.
Filter	Specify a filter by which to constrain the display of simulation data.
Copy	Make a copy of the selected policy simulation. The copied simulation is renamed with a prefix of *Copy_Of_*.
Export	Opens the **Export** popup.
Delete	Click to delete a selected (check box on left) Policy Simulation.

Active Directory Authentication

This simulation tests authentication against an Active Directory domain or trusted domain to verify that the CPPM domain membership is valid.

NOTE

The **Attributes** tab is not available for this simulation type.

Simulation tab

Figure 303: *Active Directory Authentication Simulation tab*

Table 190: *Active Directory Authentication Simulation tab Parameters*

Parameter	Description
Active Directory Domain	Select the domain(s) to which the node is joined.
Username	Enter the username to login to the domain.
Password	Enter the password to login to the domain.

Results tab

The Results tab for the Active Directory Authentication simulation displays a summary of the Authentication test and provides a status message.

Figure 304: *Active Directory Authentication Results tab*

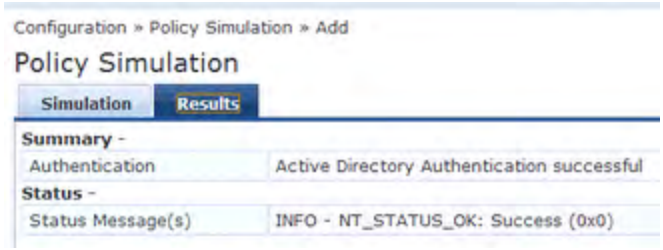


Table 191: *Active Directory Authentication Results tab Parameters*

Parameter	Description
Summary	Displays the results of the Active Directory Authentication simulation.
Status	Displays the status message.

Application Authentication

This simulation tests authentication requests generated from ClearPass Guest application.

Simulation tab

Figure 305: *Application Authentication Simulation tab*

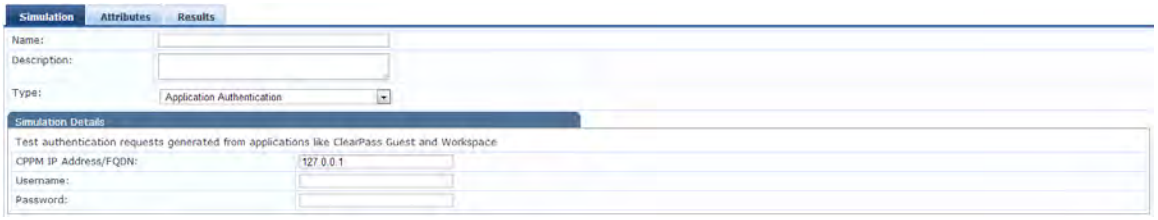


Table 192: *Application Authentication Simulation tab Parameters*

Parameter	Description
CPPM IP Address/FQDN:	Enter the IP Address or FQDN of the domain(s) to which the node is joined.
Username:	Enter the username.
Password:	Enter the password.

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 306: *Application Authentication Attributes tab*

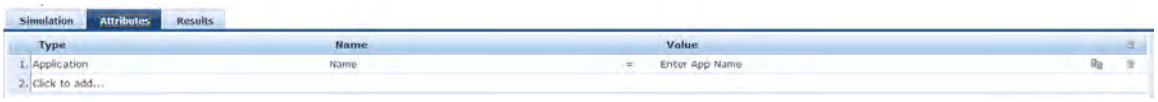


Table 193: *Application Authentication Attributes tab Parameters*

Attribute	Parameter
Type	Select Application or select Application:ClearPass. See Application Namespace on page 514
Name	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Results tab

The Results tab of the Application Authentication simulation displays the outcome of the Authentication Result and the Application Output Attributes.

Figure 307: *Application Authentication Results tab*

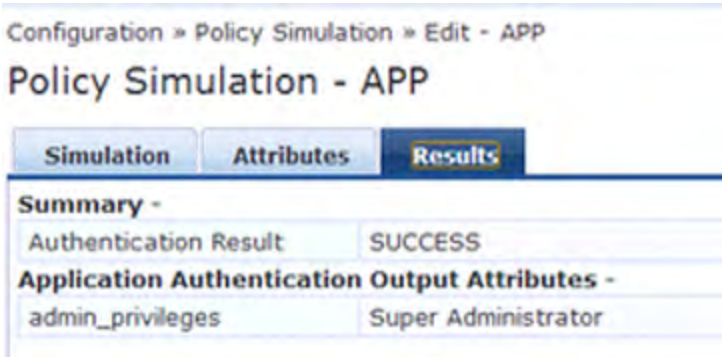


Table 194: *Application Authentication Results tab Parameters*

Parameter	Description
Summary	Displays the results of the Active Directory Authentication simulation.
Application Authentication Output Attributes	Displays the output attributes, such as Super Administrator.

Audit

This simulation allows you to specify an audit against a Nessus Server or Nmap Server, given its IP address.

NOTE

The Attributes tab is not available for this simulation type.

NOTE

Audit simulations can take more than 30 minutes. An AuditinProgress status message is displayed until the audit is completed.

Figure 308: *Audit Simulation tab*

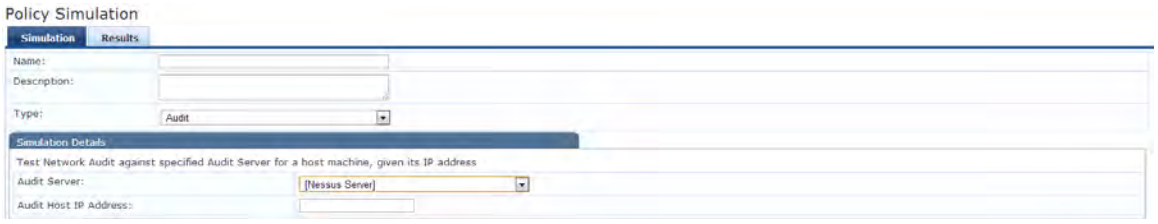


Table 195: *Audit Simulation tab Parameters*

Parameter	Description
Audit Server:	Select [Nessus Server] or [Nmap Audit].
Audit Host IP Address:	Enter the host IP address of the audit host.

Results tab

Figure 309: *Audit Simulation Results tab*

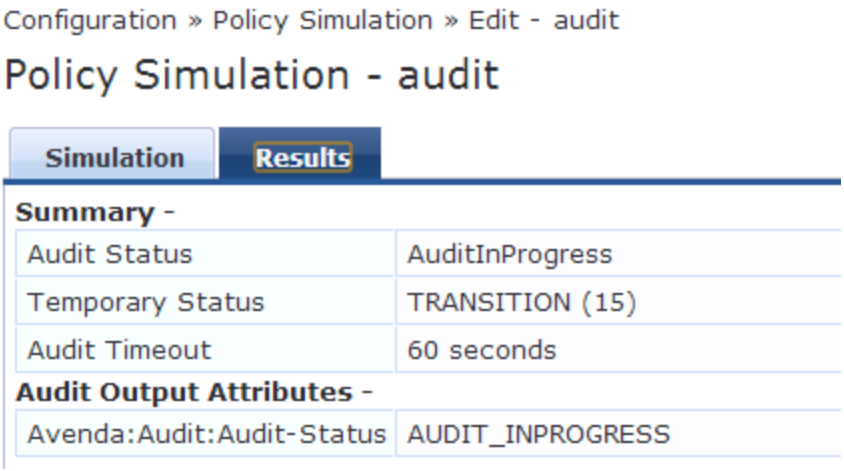


Table 196: *Audit Results tab Parameters*

Parameter	Description
Summary -	Displays information about the Audit Status, Temporary Status, and Audit Timeout.
Audit Output Attributes -	Displays the Audit-Status, such as AUDIT_INPROGRESS.

Chained Simulation

Given the service name, authentication source, user name, and an optional date and time, the chained simulation combines the results of role mapping, posture validation and enforcement policy simulations and displays the corresponding results.

Simulation tab

Figure 310: *Chained Simulation tab*

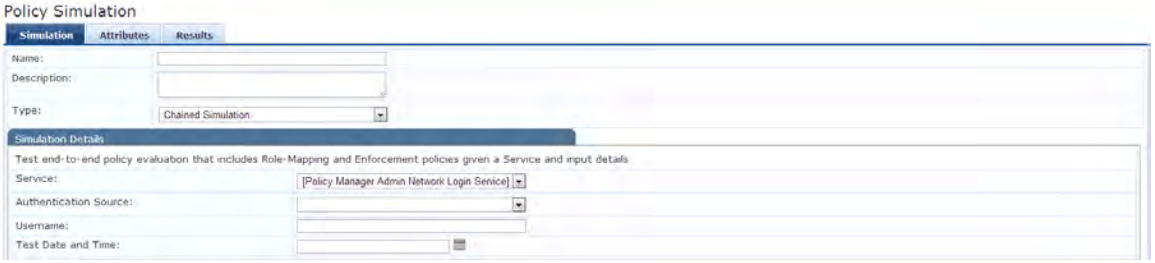


Table 197: *Chained Simulation tab Parameters*

Parameters	Description
Service:	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Authentication Source:	Default Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Default Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching Values = [Guest Device Repository] *or* [Local User Repository] if you select [Guest Operator Logins]
Username:	Enter the username.
Test Date and Time:	Click the calendar icon to select a start date and time for simulation test. For more information, see Date Namespaces on page 520

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 311: *Chained Simulation Attributes tab*

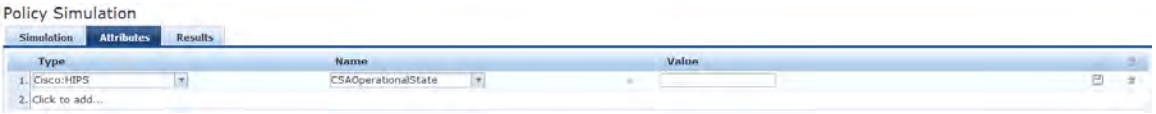


Table 198: *Chained Simulation Attributes tab Parameters*

Attribute	Parameter
Type:	
Host	See Host Namespaces on page 521
Authentication	See Authentication Namespaces on page 515
Connection	See Connection Namespaces on page 519

Attribute	Parameter
Application	See Application Namespace on page 514
Certificate	See Certificate Namespaces on page 518
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba • Trend:AV • Cisco: HIPS • Cisco:HOST • Cisco:PA • NAI:AV • Symantec:AV	See RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Results tab

Figure 312: *Chained Simulation Results tab*

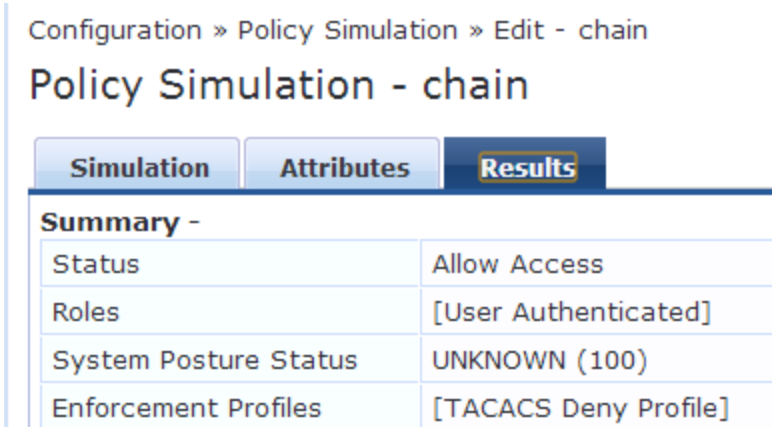


Table 199: *Chained Simulation Results tab Parameters*

Parameter	Description
Summary -	Provides the following information about the Chained Simulation: • Status • Roles • System Posture Status • Enforcement Profiles

Enforcement Policy

Given the service name (and the associated enforcement policy), a role or a set of roles, the system posture status, and an optional date and time, the enforcement policy simulation evaluates the rules in the enforcement policy and displays the resulting enforcement profiles and their contents.

Authentication Source and User Name inputs are used to derive dynamic values in the enforcement profile that are retrieved from the authorization source. These inputs are optional.

Dynamic Roles are attributes that are enabled as a role retrieved from the authorization source. For an example of enabling attributes as a role, see Generic LDAP and Active Directory on page 155.

Simulation tab

Figure 313: *Enforcement Policy Simulation tab*

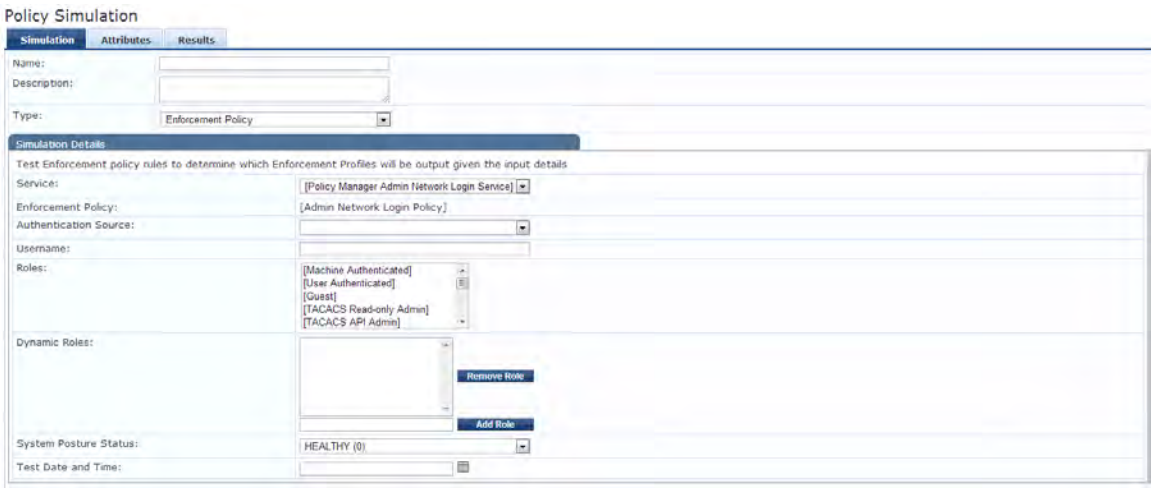


Table 200: *Enforcement Policy Simulation tab Parameters*

Parameter	Description
Service:	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Enforcement Policy:	Autofilled with **[Admin Network Login Policy]** if you select [Policy Manager Admin Network Login Service] Autofilled with **[AirGroup Enforcement Policy]** if you select [AirGroup Authorization Service] Autofilled with **[Aruba Device Access Policy]** if you select [Aruba Device Access Service] Autofilled with **[Guest Operator Logins]** if you select [Guest Operator Logins] service Autofilled with **Copy_of_Guest Access Policy** if you select Guest Access service Autofilled with **Guest Access With MAC Caching Policy** if you select Guest Access With MAC Caching
Authentication Source:	Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching Values = [Local User Repository] *or* [Guest Device Repository] if you select Guest Operator Logins
Username:	Enter username.
Roles:	Select from: • [Machine Authenticated] • [User Authenticated] • [Guest] • [TACACS Read-only Admin] • [TACACS API Admin] • [TACACS Help Desk] • [TACACS Receptionist] • [TACACS Network Admin] • [TACACS Super Admin] • [Contractor] • [Other] • [Employee] • [MAC Caching • [Onboard Android] • [Onboard Windows]

Table 200: *Enforcement Policy Simulation tab Parameters (Continued)*

Parameter	Description
	• [Onboard Mac OS X] • Onboard iOS] • [Aruba TACACS root Admin] • [Aruba TACACS read-only Admin] • [Device Registration] • [BYOD Operator] • [AirGroup V1] • [AirGroup v2]
Dynamic Roles:	Add Role: Enter the name of a dynamic role in the Add Role field and click the Add Role button to populate the Dynamic Roles list. Remove role: Highlight a dynamic role and click Remove Role button.
System Posture Status:	Select from: • HEALTHY (0) • CHECKUP (10) • TRANSITION (15) • QUARANTINE (20) • INFECTED (30) • UNKNOWN (100) See Posture Namespaces on page 522
Test Date and Time:	Click calendar icon to select start date and time for simulation test. See Date Namespaces on page 520

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 314: *Enforcement Policy Attributes tab*

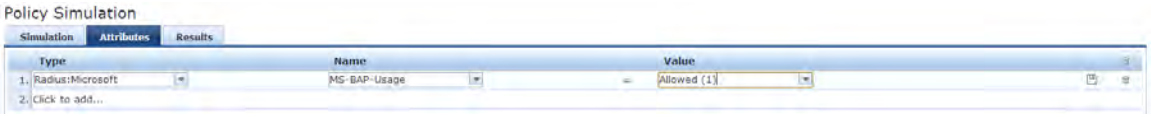


Table 201: *Enforcement Policy Attributes tab Parameters*

Attribute	Description
Type:	
Host:	See Host Namespaces on page 521
Authentication:	See Authentication Namespaces on page 515
Connection:	See Connection Namespaces on page 519
Application:	See Application Namespace on page 514

Table 201: *Enforcement Policy Attributes tab Parameters (Continued)*

Attribute	Description
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba	See RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Results tab

Figure 315: *Policy Simulation Results tab*

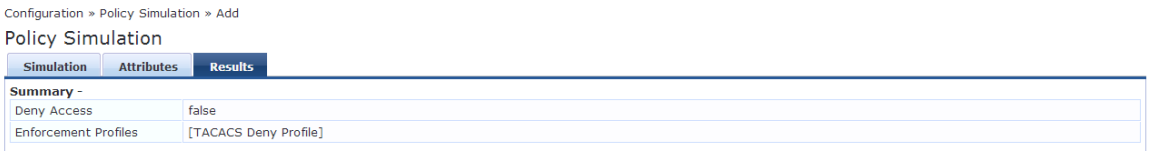


Table 202: *Enforcement Policy Results tab Parameters*

Parameter	Description
Deny Access-	Displays the output of the Deny Access test.
Enforcement Profile	Displays the name of the Enforcement Profile.

RADIUS Authentication

Dictionaries in the RADIUS namespace come pre-packaged with the product. The administration interface does provide a way to add dictionaries into the system (see RADIUS Dictionary on page 450 for more information). The RADIUS namespace uses the notation RADIUS:*Vendor*, where *Vendor* is the name of the Company that has defined attributes in the dictionary. Sometimes, the same vendor has multiple dictionaries, in which case the "Vendor" portion has the name suffixed by the name of the device or some other unique string.

Simulation tab

Figure 316: *RADIUS Authentication Simulation tab (Local Server selected)*

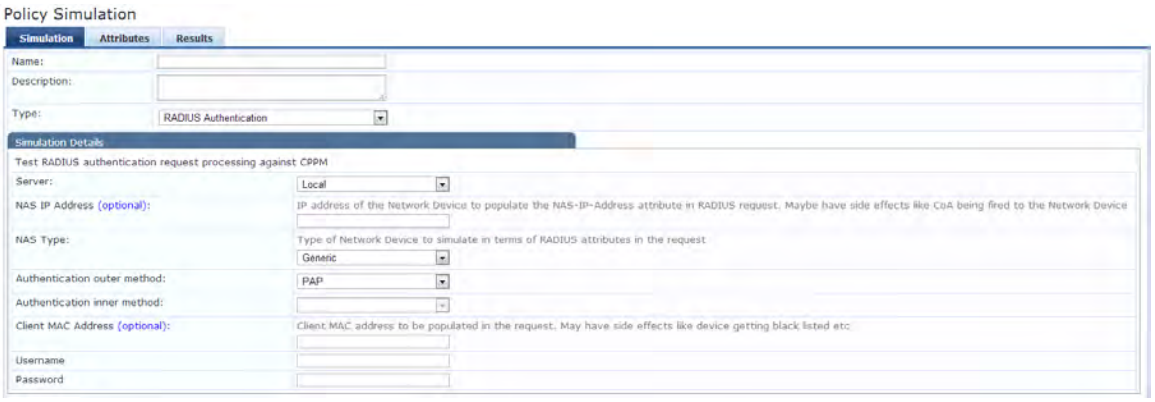


Figure 317: *RADIUS Authentication Simulation tab (Remote Server selected)*

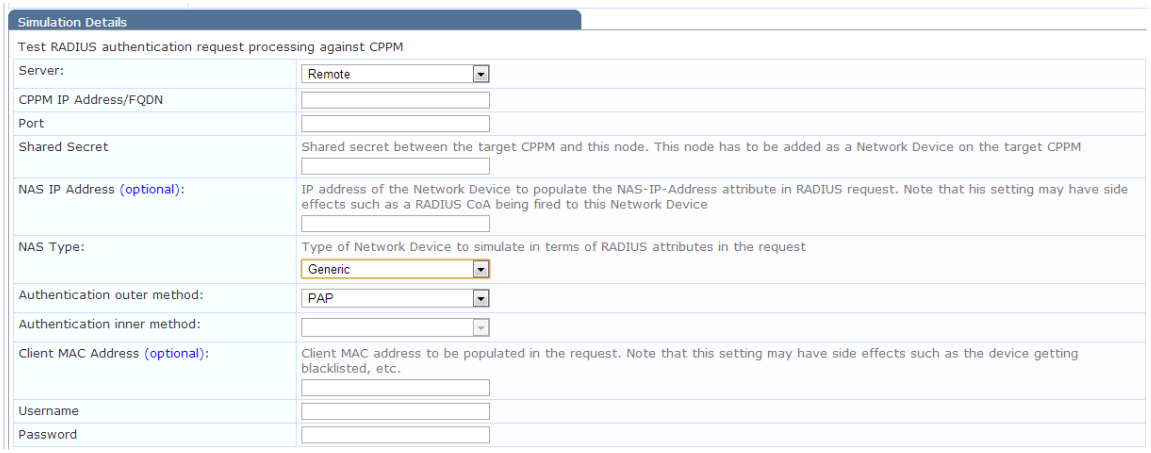


Table 203: *RADIUS Simulation tab Parameters*

Parameter	Description
Server:	Select Local or Remote.
CPPM IP Address or FQDN	**NOTE:** This field is only displayed if Remote Server is selected. Enter the IP Address or FQDN of the remote CPPM server.
Port:	**NOTE:** This field is only displayed if Remote Server is selected. Enter the port number of the remote CPPM server. The default port number is 1812.
Shared Secret:	**NOTE:** Only displayed if Remote Server is selected. Enter the shared secret between the target CPPM and this node. You must add the node as a Network Device on the target CPPM server.

Table 203: *RADIUS Simulation tab Parameters (Continued)*

Parameter	Description
Shared Secret	This field is only displayed if Remote Server is selected.
NAS IP Address (optional):	Enter the IP address of the network device to populate the NAS-IP-Address attribute in a RADIUS request.
NAS Type:	Select the type of network device to simulate in terms of RADIUS attributes in the request. The NAS types are: • Aruba Wireless Controller • Aruba Wired Switch • Cisco Wireless Controller • Generic

Authentication outer method:	• PAP - Authentication inner method: field is disabled.
	• CHAP - Authentication inner method field: is disabled.
	• MSCHAPv2 - Authentication inner method field: is disabled.
	• PEAP - Authentication inner method field: is enabled. The selections are:
	  ▪ EAP-MSCHAPv2
	  ▪ EAP-GTC
	  ▪ EAP-TLS*
	• TTLS -Authentication inner method field: is enabled. The selections are:
	  ▪ PAP
	  ▪ CHAP
	  ▪ MSCHAPv2
	  ▪ EAP-MSCHAPv2
	  ▪ EAP-GTC
	  ▪ EAP-TLS
	• TLS - Authentication inner method: field is disabled.
	
	For more information, see Authentication Namespaces on page 515

Client MAC Address (optional)	Enter the client MAC address to be populated in the request.
Username	Enter the username.
Password	Enter the password.
CA Certificate (optional):	1. Click **Choose File**. 2. Navigate to the optional Root CA certificate that is required to verify the RADIUS server's certificate. 3. Click **Open**. 4. Click **Upload**.

Table 203: *RADIUS Simulation tab Parameters (Continued)*

Parameter	Description
Client Certificate PKCS12 (PFX)*	1. Click **Choose File**. 2. Navigate to the client certificate that is used for TLS in PKCS12 - .pfx format, or .pfx or .p12 format. 3. Click **Open**. 4. Click **Upload**.
Passphrase for PFX file*	Enter the Passphrase for the selected PFX file.
* These fields are only displayed if you select TTLS *or* PEAP as the Authentication outer method: *and* you select EAP-TLS as the Authentication inner method.	

Attributes tab

Enter the attributes of the policy component to be tested.

NOTE

The attributes that you set depend on the NAS Type selected on the Simulation page.

NAS Type: Aruba Wireless Controller

Figure 318: *Aruba Wireless Controller Type Attributes tab*

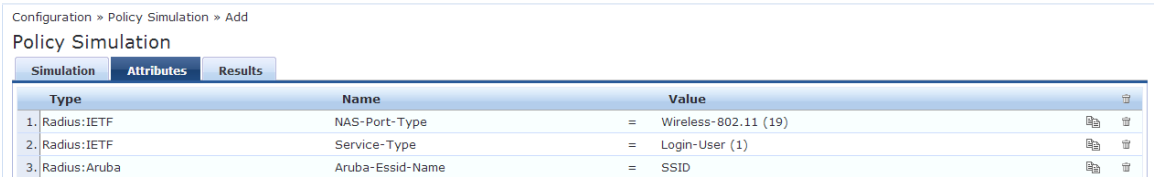


Table 204: *Aruba Wireless Controller Required Attribute Settings*

Attribute	Parameter
Line 1: • Type = Radius:IETF • Name = NAS-Port-Type • Value = Wireless-802.11 (19)	
Line 2: • Type = Radius:IETF • Name = Service-Type • Value = Login-User (1)	
Line 3: • Type = Radius:Aruba • Name = Aruba-Essid-Name • Value = SSID	

NAS Type: Aruba Wired Switch Controller

Figure 319: *NAS Type: Aruba Wired Switch Controller Attributes tab*

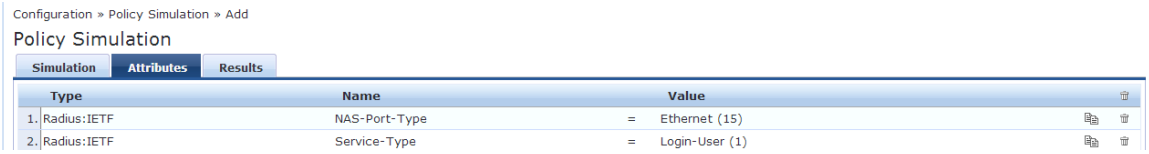


Table 205: *NAS Type: Aruba Wired Switch Controller Required Attribute Settings*

Attribute	
Line 1: • Type = Radius:IETF • Name = NAS-Port-Type • Value = Ethernet (15)	
Line 2: • Type = Radius:IETF • Name = Service-Type • Value = Login-User (1)	

NAS Type: Cisco Wireless Switch

Figure 320: *NAS Type: Cisco Wireless Switch Attributes tab*

Table 206: *[NAS Type: Cisco Wireless Switch Required Attribute Settings*

Attribute	
Line 1: • Type = Radius:IETF • Name = NAS-Port-Type • Value = 802.11(19)	
Line 2: • Type = Radius:IETF • Name = Service-Type • Value = Framed-User(2)	

Results tab

Figure 321: *Results tab*

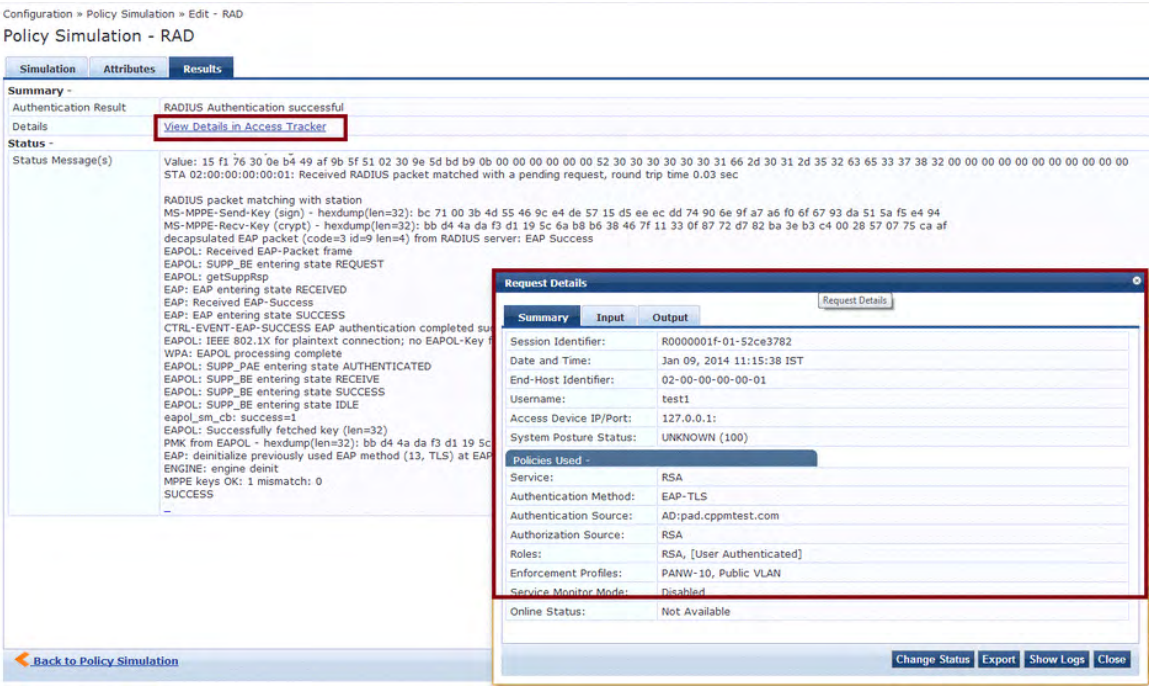


Table 207: *RADIUS Authentication Results tab Parameters*

Parameter	Description
Summary -	Displays a summary of the simulation.
Authentication Result	Displays the outcome of the Authentication test.
Details	Click this link to open a popup that provides details about the Authentication test. You can take the following actions: • Click the Summary, Input and Output tabs • Click the Change Status, Show Logs, Export or Close buttons.
Status Message(s)	Displays the status messages resulting from the test.

Role Mapping

The role mapping simulation tests Role-Mapping policy rules to determine which Roles will be output, given the service name (and associated role mapping policy), the authentication source and the user name.

You can also use role mapping simulation to test whether the specified authentication source is reachable.

Simulation tab

Figure 322: *Role Mapping Simulation tab*

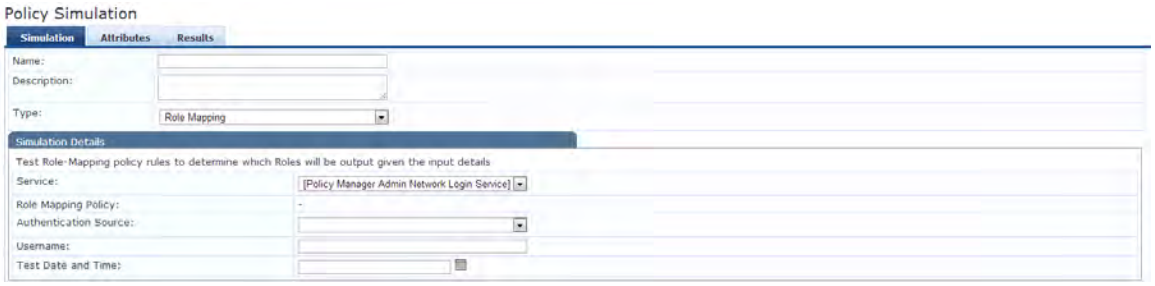


Table 208: *Role Mapping Simulation tab Parameters*

Parameter	Description
Service:	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Role Mapping Policy:	Field is disabled if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] • [Guest Operator Logins] Field is auto-filled with **[AirGroup Version Match]** if you select [AirGroup Authorization Service] Field is autofilled with **[Guest Roles]** if you select Guest Access Field is autofilled with **Guest MAC Authentication Role Mapping** if you select Guest Access With MAC Caching
Authentication Source:	Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access

Table 208: *Role Mapping Simulation tab Parameters (Continued)*

Parameter	Description
	• Guest Access With MAC Caching Values = [Guest Device Repository] *or* [Local User Repository] if you select [Guest Operator Logins]
Username:	Enter the user name.
Test Date and Time:	Click calendar icon to select start date and time for simulation test. For more information, see Date Namespaces on page 520

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 323: *Role Mapping Simulation Attributes tab*

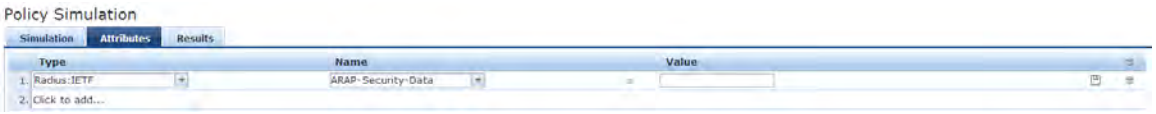


Table 209: *Role Mapping Simulation Attributes tab Parameters*

Attribute	Parameter
Type:	
Host	See Host Namespaces on page 521
Authentication	See Authentication Namespaces on page 515
Connection	See Connection Namespaces on page 519
Application	See Application Namespace on page 514
Certificate	See Certificate Namespaces on page 518

Table 209: *Role Mapping Simulation Attributes tab Parameters (Continued)*

Attribute	Parameter
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba	See RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Results tab

Figure 324: *Results tab*

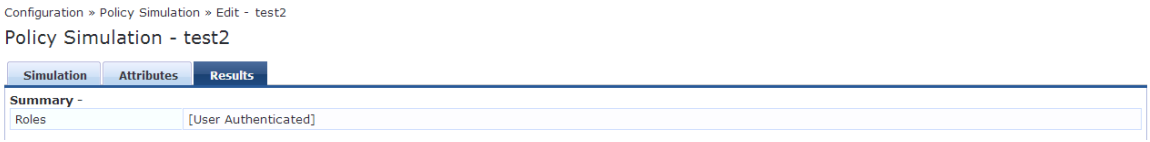


Table 210: *Role Mapping Results tab Parameters*

Parameter	Description
Summary -	Displays the results of the simulation.

Service Categorization

A service categorization simulation allows you to specify a set of attributes in the RADIUS or Connection namespace and test which configured service the request will be categorized into. The request attributes that you specify represent the attributes sent in the simulated request.

Simulation tab

Figure 325: *Service Categorization Simulation tab*

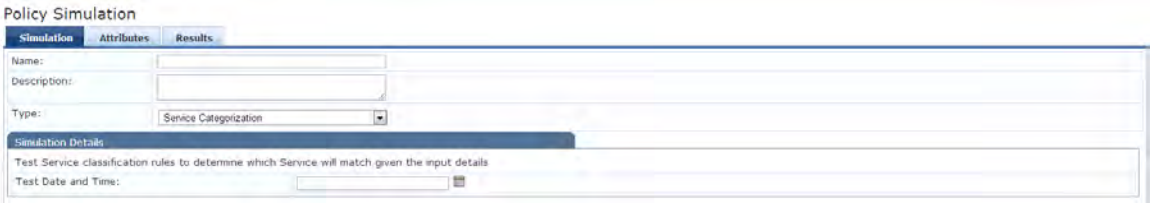


Table 211: *Service Categorization Simulation tab Parameter Description*

Parameter Type	Namespace Details
Test Date and Time:	Click calendar widget and select: • Test start date • Test start time

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 326: *Service Categorization Attributes tab*

Table 212: *Service Categorization Simulation Attributes tab Parameters*

Attribute	Parameter
Type:	
Host	See Host Namespaces on page 521
Authentication	See Authentication Namespaces on page 515
Connection	See Connection Namespaces on page 519
Application	See Application Namespace on page 514
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Aruba	See RADIUS Namespaces on page 522
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Results tab

Figure 327: *Results tab*

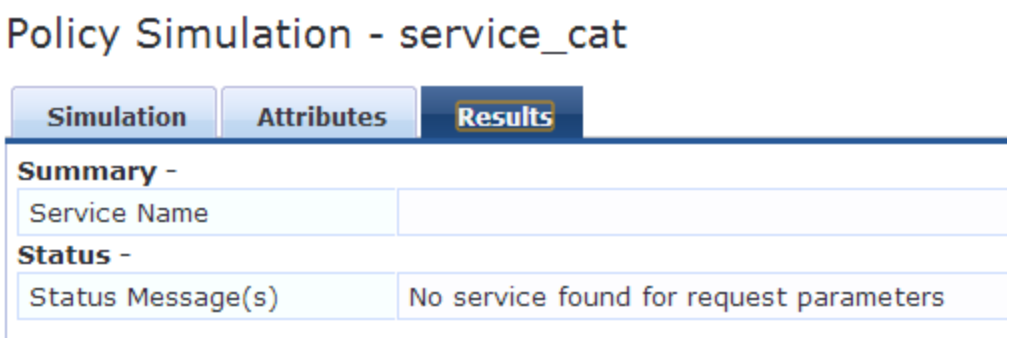


Table 213: *Service Configuration Results tab Parameters*

Parameter	Description
Summary -	Gives the name of the service.

Profile is a Dell Networking W-ClearPass Policy Manager module that automatically classifies endpoints using attributes obtained from software components called Collectors. You can use Profile to implement "Bring Your Own Device" (BYOD) flows, where access must be controlled, based on the type of the device and the identity of the user. While offering a more efficient and accurate way to differentiate access by endpoint type (laptop or tablet), ClearPass Profile associates an endpoint with a specific user or location and secures access for devices like printers and IP cameras. Profile can be set up in a network with a minimal amount of configuration.

For more information, see:

- Device Profile on page 337
- Collectors on page 337
- Fingerprint Dictionaries on page 342
- Profiling on page 340

Device Profile

A device profile is a hierarchical model consisting of 3 elements – DeviceCategory, DeviceFamily, and DeviceName – derived by Profile from endpoint attributes.

- DeviceCategory - This is the broadest classification of a device. It denotes the type of the device. Examples include Computer, Smartdevice, Printer, Access Point, etc.
- DeviceFamily - This element classifies devices into a category and is organized based on the type of operating system or vendor. For example, when the category is Computer, Dell Networking W-ClearPass Policy Manager could show a DeviceFamily of *Windows*, *Linux*, or *Mac OS X*, and when the Category is Computer, Dell Networking W-ClearPass Policy Manager could show a DeviceFamily of *Apple* or *Android*.
- DeviceName - Devices in a family are further organized based on more granular details, such as operating system version. For example, in a DeviceFamily of *Windows*, Dell Networking W-ClearPass Policy Manager could show a DeviceName of *Windows 7* or *Windows 2008 Server*.

This hierarchical model provides a structured view of all endpoints accessing the network.

In addition to these, Profile also collects and stores the following:

- IP Address
- Hostname
- MAC Vendor
- Timestamp when the device was first discovered
- Timestamp when the device was last seen

Collectors

Collectors are network elements that provide data to profile endpoints.

For more information, see:

- DHCP on page 338
- ClearPass Onboard on page 338
- HTTP User-Agent on page 338

- MAC OUI on page 338*
- ActiveSync Plugin on page 339
- CPPM OnGuard on page 339
- SNMP on page 339
- Subnet Scan on page 340

* Acquired via various authentication mechanisms such as 802.1X, MAC authentication, etc.

DHCP

DHCP attributes such as option55 (parameter request list), option60 (vendor class) and options list from DISCOVER and REQUEST packets can uniquely fingerprint most devices that use the DHCP mechanism to acquire an IP address on the network. Switches and controllers can be configured to forward DHCP packets such as DISCOVER, REQUEST and INFORM to CPPM. These DHCP packets are decoded by CPPM to arrive at the device category, family, and name. Apart from fingerprints, DHCP also provides hostname and IP address.

Sending DHCP Traffic to CPPM

Perform the following steps to configure your Dell W-Series Controller and Cisco Switch to send DHCP Traffic to CPPM.

```
interface <vlan_name>
ip address <ip_addr> <netmask>
ip helper-address <dhcp_server_ip>
ip helper-address <cppm_ip>end
end
```

Notice that multiple "`ip helper-address`" statements can be configured to send DHCP packets to servers other than the DHCP server.

ClearPass Onboard

ClearPass Onboard collects rich and authentic device information from all devices during the onboarding process. Onboard then posts this information to Profile via the Profile API. Because the information collected is definitive, Profile can directly classify these devices into their Category, Family, and Name without having to rely on any other fingerprinting information.

HTTP User-Agent

In some cases, DHCP fingerprint alone cannot fully classify a device. A common example is the Apple® family of smart devices; DHCP fingerprints cannot distinguish between an iPad® and an iPhone®. In these scenarios, User-Agent strings sent by browsers in the HTTP protocol are useful to further refine classification results.

User-Agent strings are collected from the following:

- ClearPass Guest (Amigopod)
- ClearPass Onboard
- Dell W-Series controller through IF-MAP interface

MAC OUI

MAC OUI can be useful in some cases to better classify endpoints. An example is Android™ devices where DHCP fingerprints can only classify a device as generic android, but it cannot provide more details regarding vendor. Combining this information with MAC OUI, profiler can classify a device as HTC™ Android, Samsung™ Android, Motorola® Android etc. MAC OUI is also useful to profile devices like printers that may be configured with static IP addresses.

ActiveSync Plugin

The ActiveSync plugin is to be installed on Microsoft Exchange servers. When a device communicates with exchange server using active sync protocol, it provides attributes like device-type and user-agent. These attributes are collected by the plugin software and are sent to the CPPM profiler. Profiler uses dictionaries to derive profiles from these attributes.

CPPM OnGuard

The ClearPass OnGuard agent performs advanced endpoint posture assessment. It can collect and send OS details from endpoints during authentication. The Policy Manager Profiler uses the os_type attribute from OnGuard to derive a profile.

SNMP

Endpoint information obtained by reading SNMP MIBs of network devices is used to discover and profile static IP devices in the network. The following information read via SNMP is used:

- sysDescr information from RFC1213 MIB is used to profile the device. This is used both for profiling switches/controllers/routers configured in CPPM, and for profiling printers and other static IP devices discovered through SNMP or subnet scans.
- cdpCacheTable information read from CDP (Cisco Discovery Protocol) capable devices is used to discover neighbor devices connected to switch/controller configured in CPPM
- lldpRemTable information read from LLDP (Link Layer Discovery Protocol) capable devices is used to discover and profile neighbor devices connected to switch/controller configured in CPPM
- ARPtable read from network devices is used as a means to discover endpoints in the network.

The SNMP based mechanism is only capable of profiling devices if they respond to SNMP, or if the device advertises its capability via LLDP. When performing SNMP reads for a device, CPPM uses SNMP Read credentials configured in Network Devices, or defaults to using SNMP v2c with "public" community string.

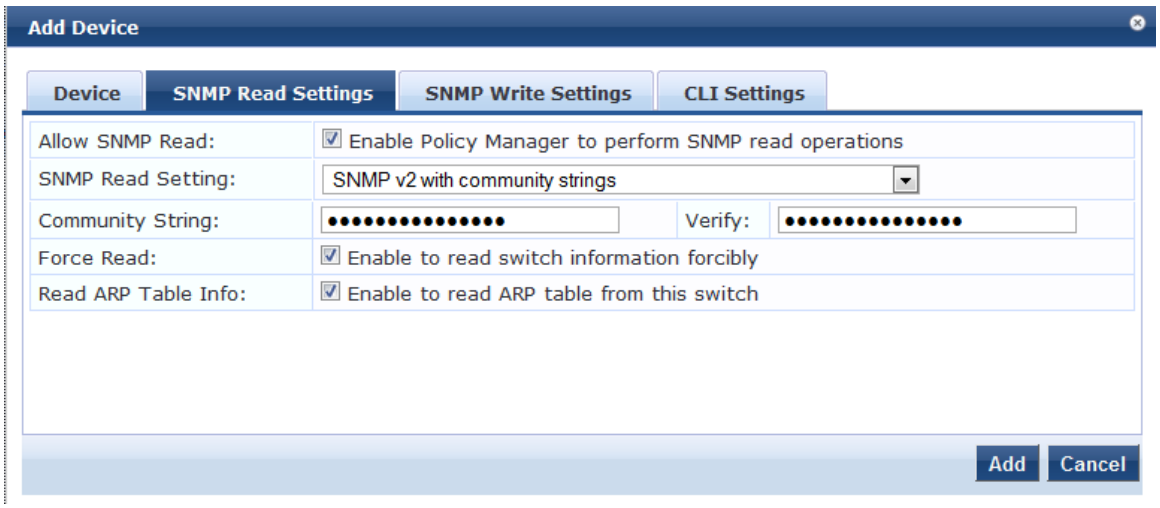
Note that the SNMP based mechanism is only capable of profiling devices if they respond to SNMP, or if the device advertises its capability via LLDP. When performing SNMP reads for a device, CPPM uses SNMP Read credentials configured in Network Devices, or defaults to using SNMP v2c with "public" community string.

Network Devices configured with SNMP Read enabled are polled periodically for updates based on the time interval configured in **Administration > Server Configuration > Service Parameters tab > ClearPass network services option > Device Info Poll Interval**.

The following additional settings are included with Profile support:

- Read ARP Table Info - Enable this setting if this is a Layer 3 device, and you want to use ARP table on this device as a way to discover endpoints in the network. Static IP endpoints discovered this way are further probed via SNMP to profile the device.
- Force Read - Enable this setting to ensure that all CPPM nodes in the cluster read SNMP information from this device regardless of trap configuration on the device. This option is especially useful when demonstrating static IP-based device profiling because this does not require any trap configuration on the network device.

Figure 328: *SNMP Read/Write Settings Tabs*



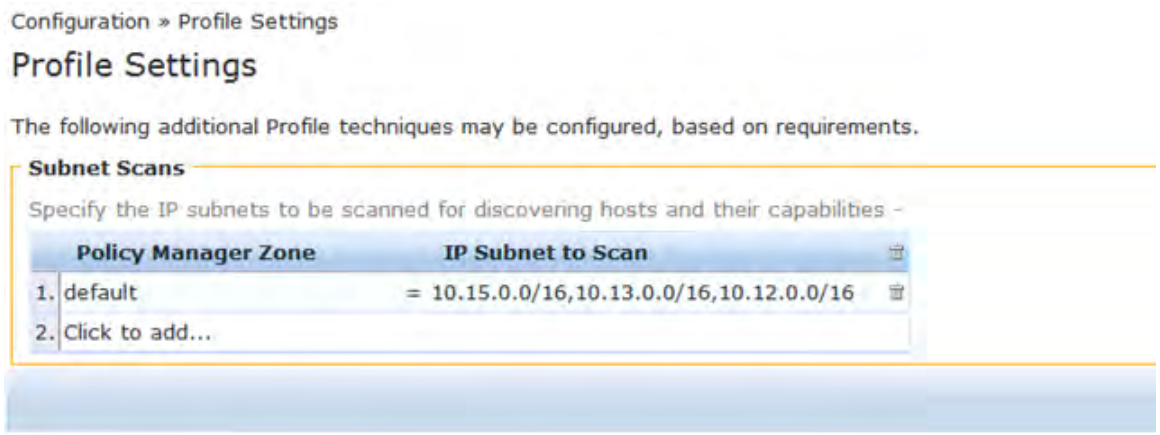
In large or geographically spread cluster deployments, you do not want all CPPM nodes to probe all SNMP configured devices. The default behavior is for a CPPM node in the cluster to read network device information only for devices configured to send traps to that CPPM node.

Subnet Scan

A network subnet scan is used to discover IP addresses of devices in the network. The devices discovered this way are further probed using SNMP to fingerprint and assign a Profile to the device. Network subnets to scan. Subnets to scan are configured per CPPM Zone. This is particularly useful in deployments that are geographically distributed. In such deployments, it is recommended that you assign the CPPM nodes in a cluster to multiple "Zones" (from Administration > Server Configuration > Manage Policy Manager Zones) depending on the geographical area served by that node, and enable Profile on at least one node per zone.

For more information, see Manage Policy Manager Zones on page 384.

Figure 329: *Subnet Scans page*



Profiling

The Profile module uses a two-stage approach to classify endpoints using input attributes.

Stage 1

Stage 1 tries to derive device profiles using static dictionary lookups. Based on the available attributes available, Stage 1 looks up DHCP, HTTP, ActiveSync, MAC OUI, and SNMP dictionaries and derives multiple matching profiles. After multiple matches are returned, the priority of the source that provided the attribute is used to select the appropriate profile. The following list shows the decreasing order of priority.

- OnGuard/ActiveSync plugin
- HTTP User-Agent
- SNMP
- DHCP
- MAC OUI

Stage 2

CPPM comes with a built-in set of rules that evaluates to a device-profile. Rules engine uses all input attributes and device profiles from Stage 1. The resulting rule evaluation may or may not result in a profile. Stage 2 is intended to refine the results of profiling.

Example

With DHCP options, Stage 1 can identify an Android device. Stage 2 uses rules to combine this with MAC OUI to further classify an Android device as Samsung Android, HTC Android, etc.

For more information, see:

- Post Profile Actions on page 341

The Profiler User Interface

CPPM provides interfaces pages that administrators can use to search and view profiled endpoints and also provides basic statistics about the profiled endpoints. The Cluster Status Dashboard widget shows basic distribution of device types.

The **Monitoring > Live Monitoring > Endpoint Profiler** page provides detailed device distribution information and a list of endpoints. From this page, you can search for endpoint profiles based on category, family, name, etc.

For more information, see:

- Endpoint Profiler on page 41
- Policy Manager Dashboard on page 11

Post Profile Actions

After profiling an endpoint, use the Profiler tab to configure parameters to perform CoA on the Network Device to which an endpoint is connected. Post profile configurations are configured under Service. The administrator can select a set of categories and a CoA profile to be applied when the profile matches one of the selected categories. CoA is triggered using the selected CoA profile. Any option from Endpoint Classification can be used to invoke CoA on a change of any one of the fields (category, family, and name).

Figure 330: *Profiler tab*

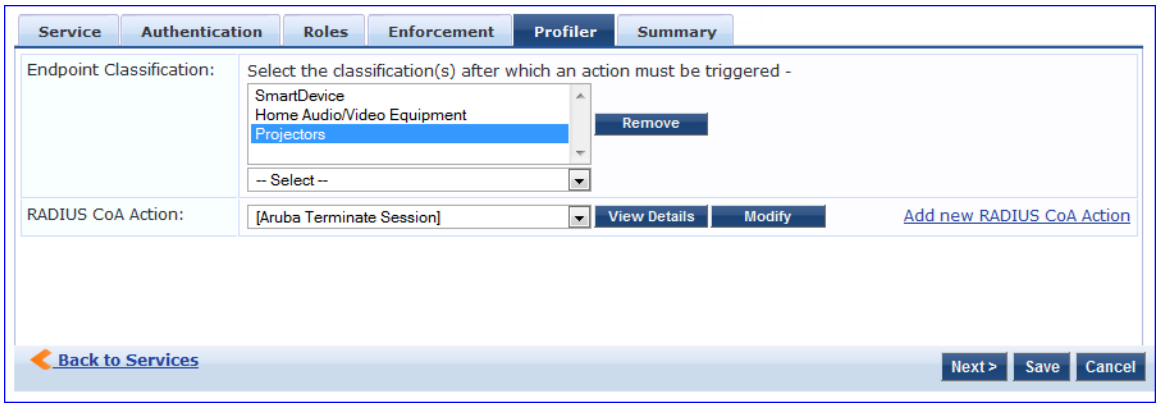


Table 214: *Profiler tab Parameters*

Parameter	Description
Endpoint Classification:	Select the classification after which an action must be triggered. You can select a new action, or remove a current action.
RADIUS CoA Action:	Select an action. Click **View Details** to view details about the selected action. Click **Modify**to change the values of the selected action.
Add new RADIUS CoA Action:	Click to add a RADIUS CoA action to the list.

Fingerprint Dictionaries

CPPM uses a set of dictionaries and built-in rules to perform device fingerprinting.

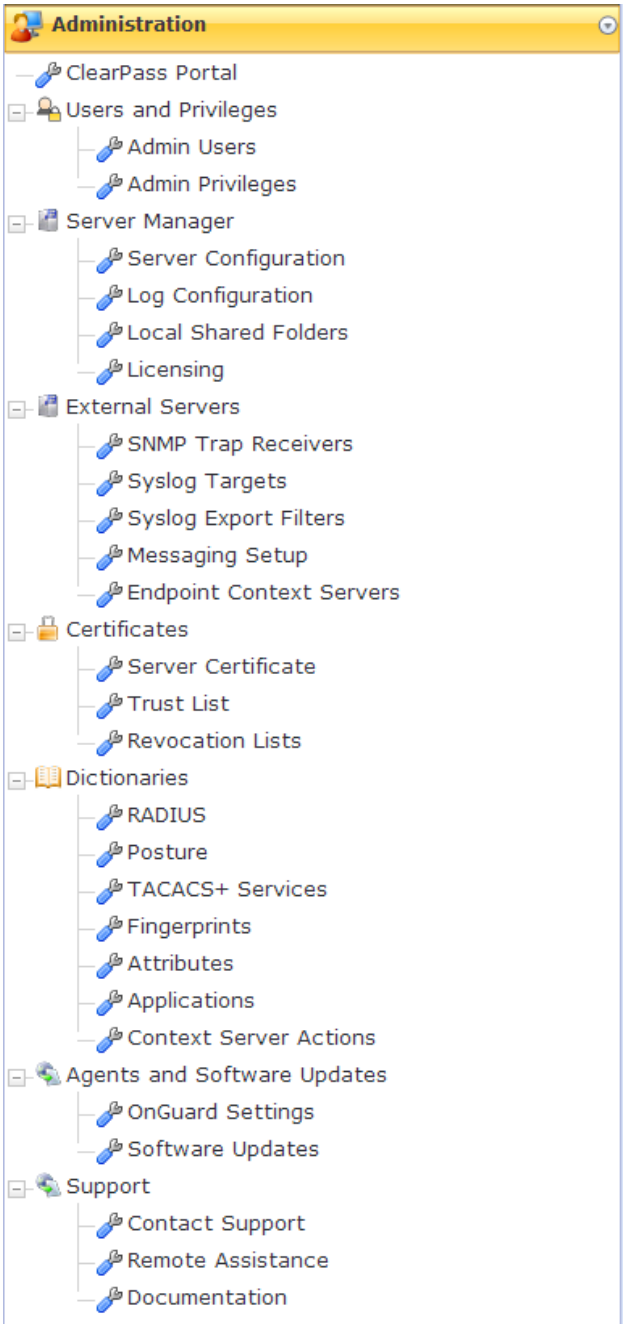
For more information, see Fingerprints Dictionary on page 454.

Because these dictionaries can change frequently, CPPM provides a way to automatically update fingerprints from a hosted portal. If external access is provided to CPPM, the fingerprints file can be downloaded and imported through CPPM admin.

For more information, see Software Updates on page 465.

Chapter 15
Administration

All administrative activities including server configuration, log management, certificate and dictionary maintenance, portal definitions, and administrator user account maintenance are done from the Administration menus. The Policy Manager Administration menu provides the following interfaces for configuration:



ClearPass Portal

Navigate to the **Administration > ClearPass Portal** page.

Click on any of the editable sections of this page to customize the content for your enterprise:

Figure 331: *ClearPass Portal*

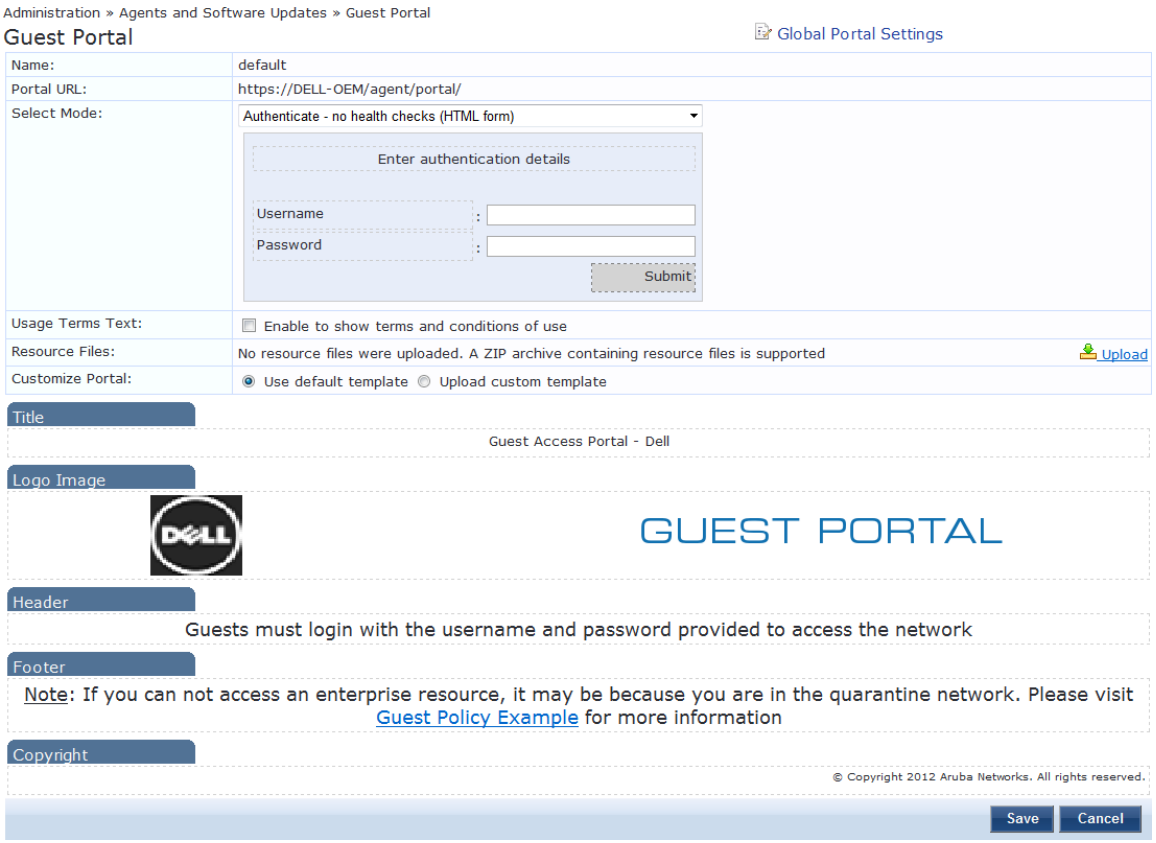


Table 215: *ClearPass Portal parameters*

Parameter	Description

Select Option	Select the page that the user sees when first logging in to ClearPass:
	• Default Landing Page
	• Application Login Page:
	  ▪ ClearPass Policy Manager
	  ▪ ClearPass Guest
	  ▪ ClearPass Insight
	  ▪ ClearPass Onboard
	• Guest Portal

Page Title	Click on the current title text to change the way the title appears.
Logo Image	Click on the logo image to browse and select an image for the banner.

Table 215: *ClearPass Portal parameters (Continued)*

Parameter	Description
Top section	Click to enter text that displays in the header.
Bottom section	Click to enter text that displays in the footer.
Copyright	Click to enter copyright text.

NOTE

Both HTTP and HTTPS protocols are supported for Guest Portal re-direction.

Admin Users

The Policy Manager Admin Users menu **Administration > Users and Privileges > Admin Users** provides the following interfaces for configuration:

- Add User on page 346
- Import Users on page 346
- Export Users on page 347
- Export on page 347

Figure 332: *Admin Users*

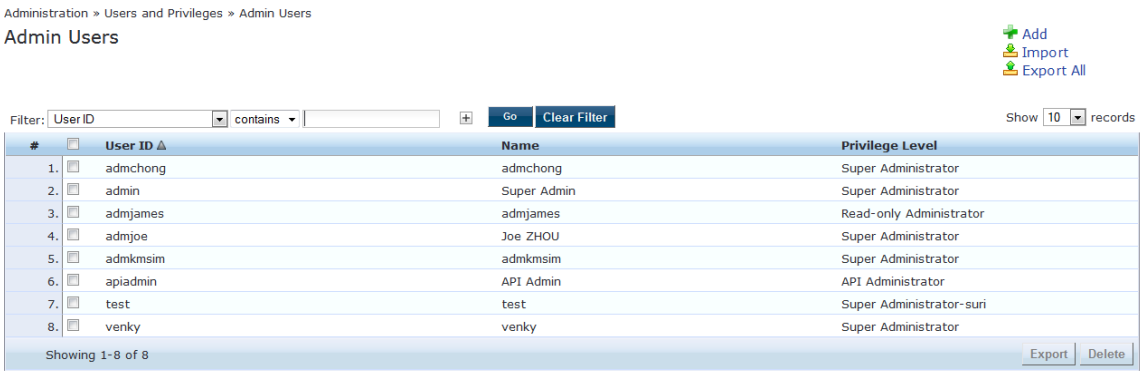


Table 216: *Admin Users*

Container	Description
Add	Opens the **Add User** popup form.
Import	Opens the **Import Users** popup form.
Export All	Exports all users to an XML file.

Table 216: *Admin Users (Continued)*

Container	Description
Export	Exports a selected to an XML file.
Delete	Deletes a selected User.

Add User

Select the **Add** link in the upper right portion of the page.

Figure 333: *Add Admin User*

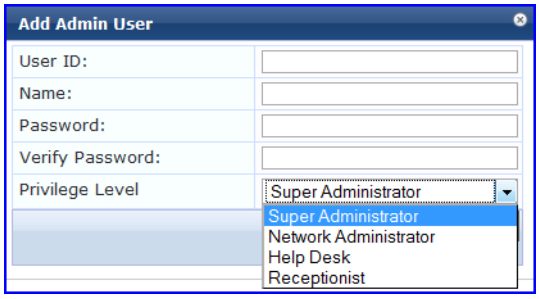


Table 217: *Add Admin User*

Container	Description
User ID	Specify the identity and password for a new admin user.
Name	
Password	
Verify Password	
Privilege Level	Select Privilege Level: Help Desk • Super Administrator • Network Administrator • Receptionist or any other custom privilege level
Add/Cancel	Add or dismiss changes.

Import Users

Select the **Import** link in the upper right portion of the page.

Figure 334: *Import (Admin) Users*

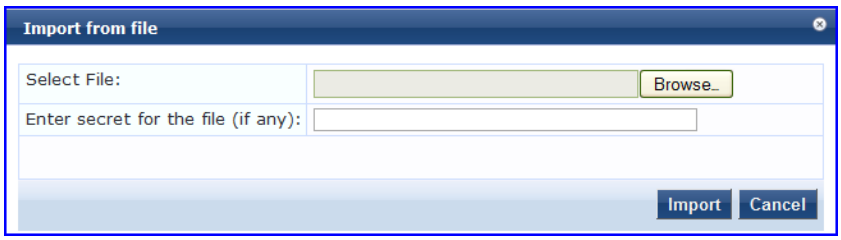


Table 218: *Import (Admin) Users*

Container	Description
Select file	Browse to select name of admin user import file.
Enter secret key for file (if any)	Enter the secret key used (while exporting) to protect the file.
Import/Cancel	Commit or dismiss import.

Export Users

Select the **Export All** link from the upper right portion of the page.

The **Export (Admin) Users** link exports all (admin) users. Click **Export.** Your browser displays its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Export

Select the **Export** button on the lower right portion of the page.

To export a user, select it (check box at left) and click **Export**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Admin Privileges

To view the available Admin Privileges, go to **Administration > Users and Privileges > Admin Privileges**.

Figure 335: *Admin Privileges*

See Custom Admin Privileges on page 313 to create additional administrator privileges and Exporting on page 2 to export the definition of one or more administrator privileges.

Administrator Privilege XML File Structure

Admin privilege files are XML files and have a very specific structure.

A header must be at the beginning of an admin privilege XML file and must be exactly:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

The root tag is `TipsContents`. It is a container for the data in the XML file and should look like this:

```
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
⋮
</TipsContents>
```

Following the `TipsContents` tag is an optional `TipsHeader` tag.

The actual admin privileges information is defined with the `AdminPrivilege` and `AdminTask` tags. You use one `AdminPrivilege` tag for each admin privilege you want to define. The `AdminPrivilege` tag contains two attributes: `name` and `description`. Inside the `AdminPrivilege` tag are one or more `AdminTask` tags, each one defining a lace within the Policy Manager application that a user with that privilege can view or change. The `AdminTask` tag contains one `taskid` attribute and a single `AdminTaskAction` tag. The `AdminTaskAction` tag has one attribute, type, and it can contain one of two values, `RO` (read only) or `RW` (read/write). The basic structure:

```
<AdminPrivileges>
  <AdminPrivilege name="" description="">
    <AdminTask taskid="">
      <AdminTaskAction type=""/>
    </AdminTask>
    <AdminTask taskid="">
      <AdminTaskAction type=""/>
    </AdminTask>
  </AdminPrivilege>
</AdminPrivileges>
```

Administrator Privileges and IDs

The following table provides the areas of the Policy Manager application and the associated taskid of each one. If you provide permission for an area, the same permission for all sub-areas is included by default. For example, if you give RW permissions for Enforcements (con.en), you grant permissions for its sub-areas, in this case, Policies (con.en.epo) and Profiles (con.en.epr), and you do not have to explicitly define the same permission for those sub-areas.

Table 219: *Administrator Privileges and IDs*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
Dashboard	dnd
Monitoring	mon
• Live Monitoring	mon.li
▪ Access Tracker	mon.li.ad
▪ Accounting	mon.li.ac

Table 219: *Administrator Privileges and IDs (Continued)*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
▪ Onguard Activity	mon.li.ag
▪ Analysis and Trending	mon.li.sp
▪ Endpoint Profiles	mon.li.ep
▪ System Monitor	mon.li.sy
• Audit Viewer	mon.av
• Blacklisted Users	mon.bl
• Event Viewer	mon.ev
• Data Filters	mon.df
Configuration	con
• Start Here (Services Wizard)	con.sh
• Services	con.se
• Service Templates	con.st
• Authentication	con.au
▪ Methods	con.au.am
▪ Sources	con.au.as
• Identity	con.id
▪ Single Sign-On	con.id.sso
▪ Local Users	con.id.lu
▪ Endpoints	con.id.ep
▪ Static Host Lists	con.id.sh
▪ Roles	con.id.rs
▪ Role Mappings	con.id.rm
• Posture	con.pv
▪ Posture Policies	con.pv.in
▪ Posture Servers	con.pv.ex

Table 219: *Administrator Privileges and IDs (Continued)*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
▪ Audit Servers	con.pv.au
• Enforcements	con.en
▪ Policies	con.en.epo
▪ Profiles	con.en.epr
• Network	con.nw
▪ Devices	con.nw.nd
▪ Device Groups	con.nw.ng
▪ Proxy Targets	con.nw.pr
Policy Simulation	con.ps
Profile Settings	con.prs
Administration	adm
• User and Privileges	adm.us
▪ ClearPass Portal	adm.po.cp
▪ Admin Users	adm.us.au
▪ Admin Privileges	adm.us.ap
• Server Manager	adm.mg
▪ Server Configuration	adm.mg.sc
▪ Log Configuration	adm.mg.ls
▪ Local Shared Folders	adm.mg.sf
▪ Licensing	adm.mg.li
• External Servers	adm.xs
▪ SNMP Trap Receivers	adm.xs.st
▪ Syslog Targets	adm.xs.es
▪ Syslog Export Filters	adm.xs.sx
▪ Messaging Setup	adm.xs.me

Table 219: *Administrator Privileges and IDs (Continued)*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
▪ Endpoint Context Servers	adm.xs.cs
▪ Context Server Actions	adm.di.csa
• Certificates	adm.cm
▪ Server Certificate	adm.cm.mc
▪ Trust List	adm.cm.ctl
▪ Revocation List	adm.cm.crl
• Dictionaries	adm.di
▪ RADIUS	adm.di.rd
▪ Posture	adm.di.pd
▪ TACACS+ Services	adm.di.td
▪ Fingerprints	adm.di.df
▪ Attributes	adm.di.at
▪ Applications	adm.di.ad
• Agents and Software Updates	adm.po
▪ Onguard Settings	adm.po.aas
▪ Software Updates	adm.po.es
• Support	adm.su
▪ Contact Support	adm.su.cs
▪ Remote Assistance	adm.su.ra
▪ Documentation	adm.su.doc

If you provide permission for an area, the same permission for all sub-areas is included by default. For example, if you give RW permissions for Enforcements (con.en), you grant permissions for its sub-areas, in this case, Policies (con.en.epo) and Profiles (con.en.epr), and you do not have to explicitly define the same permission for those sub-areas.

Creating Custom Administrator Privileges

You must use a plain text or XML editor, not a word processing application to create the custom admin privilege XML file. Applications such as Microsoft Word can introduce tags that will corrupt the XML file.

1. Create an XML file that defines a privilege.

2. Store the new file.
3. Go to **Administration > Users and Privileges > Admin Privileges**.
4. Click **Import Admin Privileges**.
5. Import the administrator privilege file you created in step 1. See Importing for details.

After you complete steps 1-5, the new administrator privileges document is displayed on the Admin Privileges page.

For more information, see:

- Administrator Privilege XML File Structure on page 348
- Administrator Privileges and IDs on page 348
- Sample Administrator Privilege XML File on page 352

Sample Administrator Privilege XML File

Read Only (RO) Privilege to all the sections (dnd, con, mon, adm)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Read-only Administrator" description="A read-only administrator is
only allowed to read all configuration elements">
      <AdminTask taskid="con"> //Refers to Configuration
        <AdminTaskAction type="RO"/>
      </AdminTask>
      <AdminTask taskid="dnd"> //Refers to DashBoard
        <AdminTaskAction type="RO"/>
      </AdminTask>
      <AdminTask taskid="mon"> //Refers to Monitoring
        <AdminTaskAction type="RO"/>
      </AdminTask>
      <AdminTask taskid="adm"> //Refers to Administration
        <AdminTaskAction type="RO"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

Only Read/Write access to Guest, Local and Endpoint Repository

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Read/Write Access to Guest, Local and Endpoint Repository"
description="A read-only administrator is only allowed to read all configuration elements">
      <AdminTask taskid="con.id.lu"> //Refers to Local Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.gu"> //Refers to Guest Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.ep"> //Refers to Endpoints Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

Read/Write permissions to DashBoard/ Monitoring and ReadOnly permissions to Server Configuration

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Limited access permission" description="A read-only administrator is
only allowed to read all configuration elements">
      <AdminTask taskid="dnd"> //Refers to DashBoard
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="mon"> //Refers to Monitoring
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="adm.mg.sc"> //Refers to Server Configuration
        <AdminTaskAction type="RO"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

Log Configuration

Use The Policy Manager Log Configuration menu to set parameters for the Service Log and for the System Level:

Figure 336: *Log Configuration (Service Log Configuration tab)*

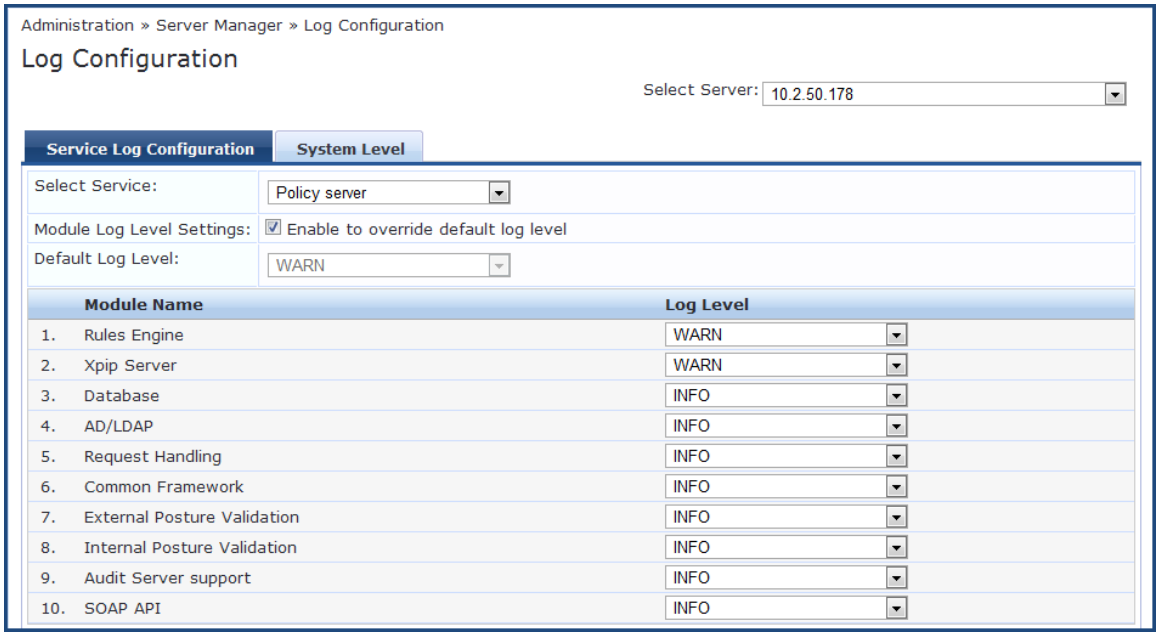


Table 220: *Log Configuration Service Log Configuration tab Parameters*

Parameter	Description
Select Server:	Specify the server for which to configure logs. All nodes in the cluster appear in the drop-down list.
Select Service:	Specify the service for which to configure logs.
Module Log Level Settings:	**Enable** this option to set the log level for each module individually (listed in decreasing level of verbosity. For optimal performance you must run Policy Manager with log level set to ERROR or FATAL): • DEBUG • INFO • WARN • ERROR • FATAL If this option is disabled, then all module level logs are set to the default log level.
Default Log Level:	This drop-down list is available if the **Module Log Level Settings** option is disabled. This sets the default logging level for all modules. Available options include the following: • DEBUG • INFO • WARN • ERROR • FATAL Set this option first, and then override any modules as necessary.
Module Name & Log Level:	If the **Module Log Level Settings** option is enabled, select log levels for each of the available modules (listed in decreasing level of verbosity): • DEBUG • INFO • WARN • ERROR • FATAL
Restore Defaults/Save:	Click **Save** to save changes or **Restore Defaults** to restore default settings.

Figure 337: *Log Configuration System Level tab*

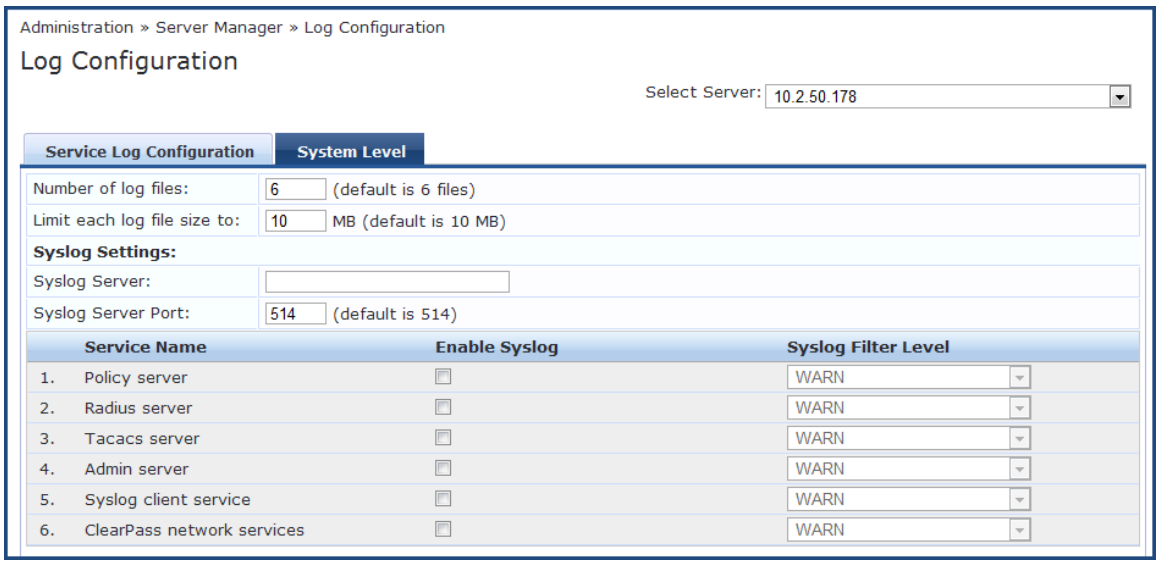


Table 221: *Log Configuration System Level tab Parameters*

Parameter	Description
Select Server	Specify the server for which to configure logs.
Number of log files	Specify the number of log files of a specific module to keep at any given time. When a log file reaches the specified size (see below), Policy Manager rolls the log over to another file until the specified number of log files is reached; once log files exceed this number, Policy Manager overwrites the first numbered file.
Limit each log file size to	Limit each log file to this size, before the log rolls over to the next file.
Syslog Server Syslog Port	Specify the syslog server and port number. Policy Manager will send the configured module logs to this syslog server.
Service Name Enable Syslog Syslog Filter Level	For each service, you can select the **Enable Syslog** check box and then override the Syslog Filter level. The current Syslog Filter level is based on the default log level specified on the **Service Log Configuration** tab.
Restore Defaults/Save	Click **Save** to save changes or **Restore Defaults** to restore default settings.

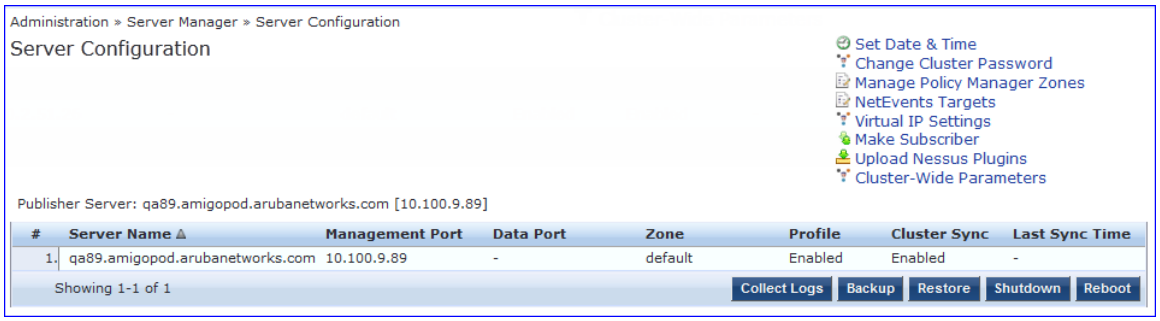
Server Configuration

The Policy Manager Server Configuration page (**Administration > Server Manager > Server Configuration**) provides the following configuration options:

- Editing Server Configuration Settings on page 356
- Set Date & Time on page 382
- Change Cluster Password on page 383

- Manage Policy Manager Zones on page 384
- NetEvents Targets on page 385
- Virtual IP Settings on page 386
- Make Subscriber on page 387
- Upload Nessus Plugins on page 387
- Cluster-Wide Parameters on page 388
- Collect Logs on page 398
- Backup on page 399
- Restore on page 399
- Shutdown/Reboot on page 401
- Drop Subscriber on page 401

Figure 338: *Server Configuration Page*



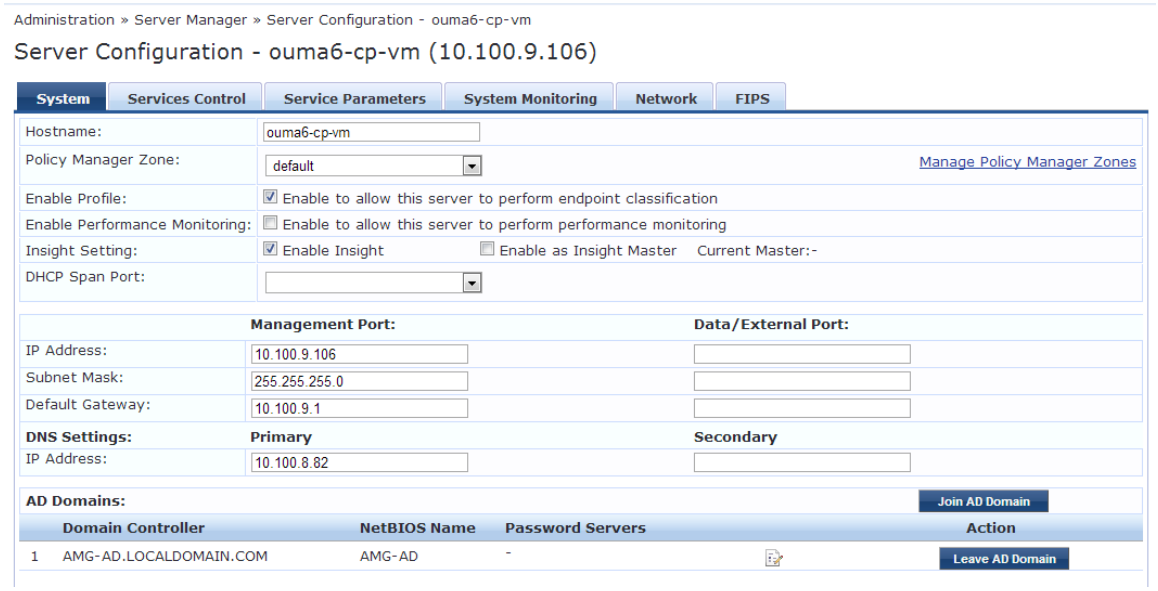
Editing Server Configuration Settings

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on a server name in the table. The Server Configuration form opens by default on the **System** tab.

For more information, see:

- System Tab on page 357
- Services Control Tab on page 361
- Service Parameters Tab on page 362
- System Monitoring Tab on page 374
- Network Tab on page 376
- FIPS Tab

Figure 339: *Editing Server Configuration*



System Tab

The **Server Configuration** page opens by default on the **System** tab.

For more information about the tasks you can perform on this tab, see:

- Manage Policy Manager Zones on page 384
- Join AD Domain on page 359
- Add Password Server on page 360 (for joined AD domains)

The following figure is an example of the **System** tab followed by parameter definition:

Figure 340: *System Tab*

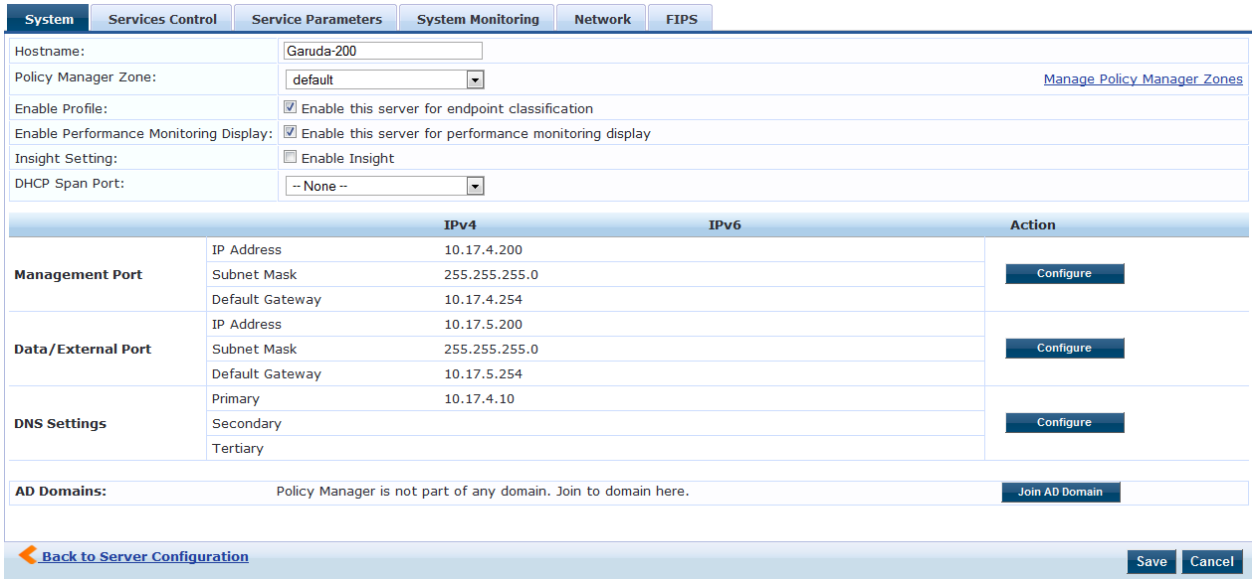


Table 222: *Server Configuration System Tab Parameters*

Parameter	Description
Hostname	Specifies the hostname of Policy Manager appliance. You do not need to enter the fully qualified domain name in this field.
Policy Manager Zone	Select a previously configured timezone from the drop-down list. Click on the **Policy Manager Timezone** link to add and edit timezones.
Enable Profile	Enable the profile to perform endpoint classifications.
Enable Performance Monitoring	Enable the server to perform performance monitoring.
Enable Insight	Enable the Insight reporting tool on this node. **NOTE:** • When the administrator enables this check box for Insight on a node in a cluster, the [Insight Repository] configuration is updated automatically to point to the management IP of that server. • When this check box is enabled for other servers in the cluster, they are added as backups for the same authentication source. • The order of the primary and backup servers in the [Insight Repository] is same in which the user enables Insight on the server.
Enable as Insight Master	In a cluster environment, you can specify that the current server as an Insight Master. **NOTE:** This option is only available if **Enable Insight** is selected.
DHCP Span Port	Specify the port number for DHCP spanning. This field is optional.
Management Port: IP Address	Specify the management interface IP address to access the Policy Manager UI. Open the **Configure Management Port** page by clicking the **Configure** button to specify IPv4 or IPv6 address.
Management Port: Subnet Mask	Specify the management interface subnet mask in the **Configure Management Port** page by clicking the **Configure** button to specify the subnet mask for IPv4 address.
Management Port: Default Gateway	Specify the default gateway for management interface. Open the **Configure Management Port** page by clicking the **Configure** button to specify IPv4 or IPv6 address.
Data/External Port: IP Address	Specify the IP address of the data interface. All authentication and authorization requests appear on the data interface. Open the **Configure Management Port** page by clicking the **Configure** button to specify IPv4 or IPv6 address.

Table 222: *Server Configuration System Tab Parameters (Continued)*

Parameter	Description
Data/External Port: Subnet Mask	Specify the data interface subnet mask in the **Configure Management Port** page by clicking the **Configure** button to specify the subnet mask to specify IPv4 address.
Data/External Port: Default Gateway	Specify the default gateway for data interface. Open the **Configure Management Port** page by clicking the **Configure** button to specify IPv4 or IPv6 address.
DNS: Primary DNS	Specify the primary DNS for name lookup. Open the **Configure Management Port** page by clicking the **Configure** button to specify IPv4 or IPv6 address.
DNS: Secondary DNS	Specify the secondary DNS for name lookup. Open the **Configure Management Port** page by clicking the **Configure** button to specify IPv4 or IPv6 address.
DNS: Tertiary DNS	Specify the tertiary DNS for name lookup. Open the **Configure Management Port** page by clicking the **Configure** button to specify IPv4 or IPv6 address.
AD Domains	Displays a list of joined active directory domains. Select **Join Domain** to join an Active Directory domain. Refer to Join AD Domain on page 359 for more information. After an AD Domain is added, the domain controller can be setup as a password server. Refer to Add Password Server on page 360 for more information.

Join AD Domain

You can join CPPM to an Active Directory (AD) domain to authenticate users and computers that are members of an Active Directory domain. Joining CPPM to an Active Directory domain creates a computer account for the CPPM node in the AD database. Users can then authenticate into the network using 802.1X and EAP methods, such as PEAP-MSCHAPv2, with their own their own AD credentials.

If you need to authenticate users belonging to multiple AD forests or domains in your network, and there is no trust relationship between these entities, then you must join CPPM to each of these untrusting forests or domains.

There is no need to join CPPM to multiple domains belonging to the same AD forest because a one-way trust relationship exists between these domains. In this case, you join CPPM to the root domain.

Join Domain - Click on this button to join this Policy Manager appliance to an Active Directory domain. Password servers can be configured after Policy Manager is successfully joined. Refer to Add Password Server on page 360 for more information.

Leave Domain - If the server is already part of multiple AD domains, click on this button to disassociate this Policy Manager appliance from an Active Directory domain.

For most use cases, if you have multiple nodes in the cluster, you must join each node to the same Active Directory domain.

Figure 341: *Join AD Domain*

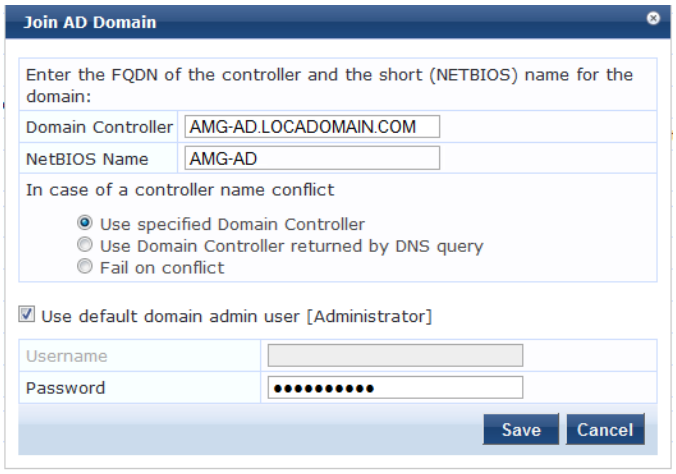


Table 223: *Join AD Domain Parameters*

Parameter	Description
Domain Controller	*Fully qualified* name of the Active Directory domain controller.
NETBIOS name (optional)	The NETBIOS name of the domain. Enter this value only if this is different from your regular Active Directory domain name. If this is different from your domain name (usually a shorter name), enter that name here. Contact your AD administrator about the NETBIOS name. **NOTE:** If you enter an incorrect value for the NETBIOS name, you see a warning message in the UI. If you see this warning message, leave the domain by clicking on the **Leave Domain** button, which replaces the **Join Domain** button once you join the domain. After leaving the domain, join again with the right NETBIOS name.
Domain Controller name conflict	In some deployments (especially if there are multiple domain controllers, or if the domain name has been wrongly entered in the last step), the domain controller FQDN returned by the DNS query can be different from what was entered. In this case, you may: • **Use specified Domain Controller** - Continue to use the domain controller name that you entered. • **Use Domain Controller returned by DNS query** - Use the domain controller name returned by the DNS query. • **Fail on conflict** - Abort the Join Domain operation.
Use default domain admin user	Check this box to use the *Administrator* user name to join the domain
Username	User ID of the domain administrator account. This field is disabled if the **Use default domain admin user** checkbox is selected.
Password	Password of the domain administrator account.

Add Password Server

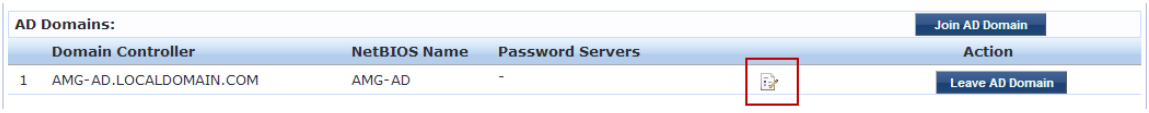
After CPPM is successfully joined to an AD domain, you can configure a restricted list of domain controllers to be used for MSCHAP authentication. If not configured, then all available domain controllers obtained from

DNS will be included.

Perform the following steps to add a password server.

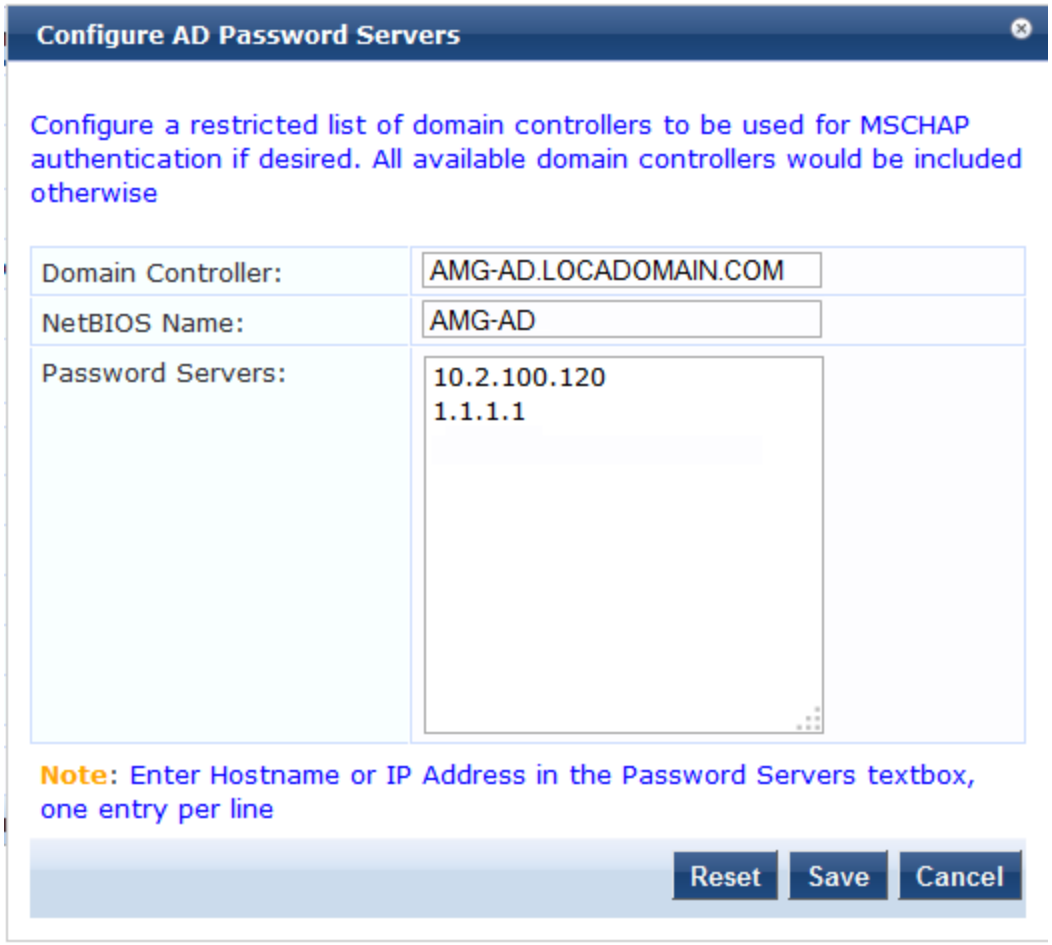
1. In the AD Domains section of the System tab, click the Add Password Server icon. (See Figure 342.)

Figure 342: *Add Password Server icon*



2. The Configure AD Password Servers page appears. Specify the domain name, NetBIOS Name, and the Password Servers. The password servers can be in the format of hostname or IP address. Use a new line for each entry.
3. Click **Save** when you are finished.

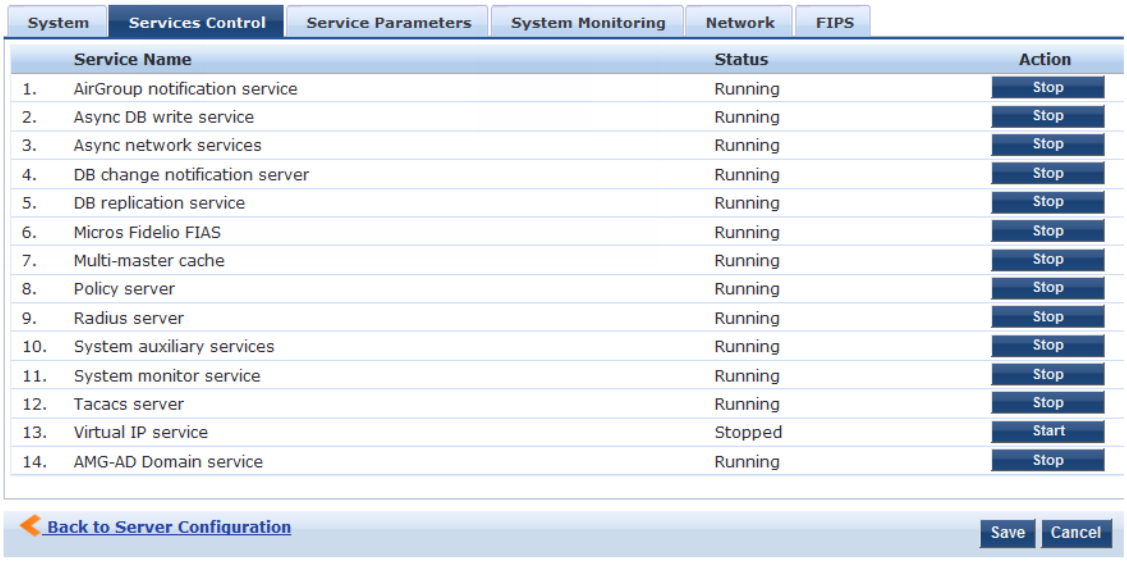
Figure 343: *Configure AD Password Servers*



Services Control Tab

From the **Services Control** tab, you can view a service status and control (stop or start) various Policy Manager services, including any AD Domains to which this server is currently joined.

Figure 344: *Services Control Tab*



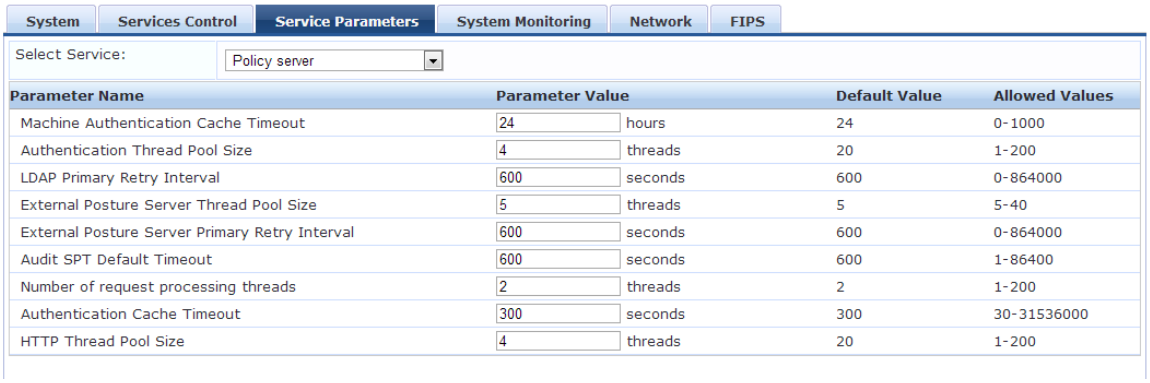
Service Parameters Tab

Navigate to the **Service Parameters** tab to change system parameters of a variety of services. The options on this page vary based on the selected service. Determine the service that you want to edit.

For more information see:

- Async Network Services Options on page 362
- ClearPass Network Services Options on page 363
- ClearPass System Services Options on page 366
- Policy Server Options on page 369
- Radius Server Options on page 370
- Stats Collection Service Options on page 373
- System Monitor Service Options on page 373
- Tacacs Server Options on page 374

Figure 345: *Service Parameters tab - Policy server example*



Async Network Services Options

Configure the Post-Auth and Command Control parameters for the Async network service on this page.

Figure 346: *Async Network Services*

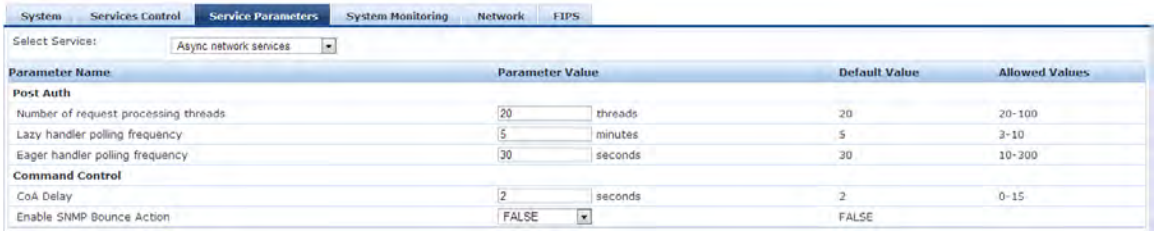


Table 224: *Service Parameters tab - Async Network Services*

Parameter	Description
Post Auth	
Number of request processing threads	Set the number of request processing threads. The default value is 20 threads, and the allowed values are between 20 and 100.
Lazy handler polling frequency	Set the Lazy handler polling frequency. The frequency is configured in minutes. The default value is 5 minutes, and the allowed values are from 3-10 minutes.
Eager handler polling frequency	Set the Eager handler polling frequency. The frequency is measured in seconds. The default value is 30 seconds, and the allowed values are from 10-300 seconds.
Command Control	
CoA Delay	Set the CoA Delay value. The default value is measured in seconds. The default value is 2, and the allowed values are from 0-15 seconds.
Enable SNMP Bounce Action	Set the Enable SNMP Bounce Action value. The default value is FALSE.

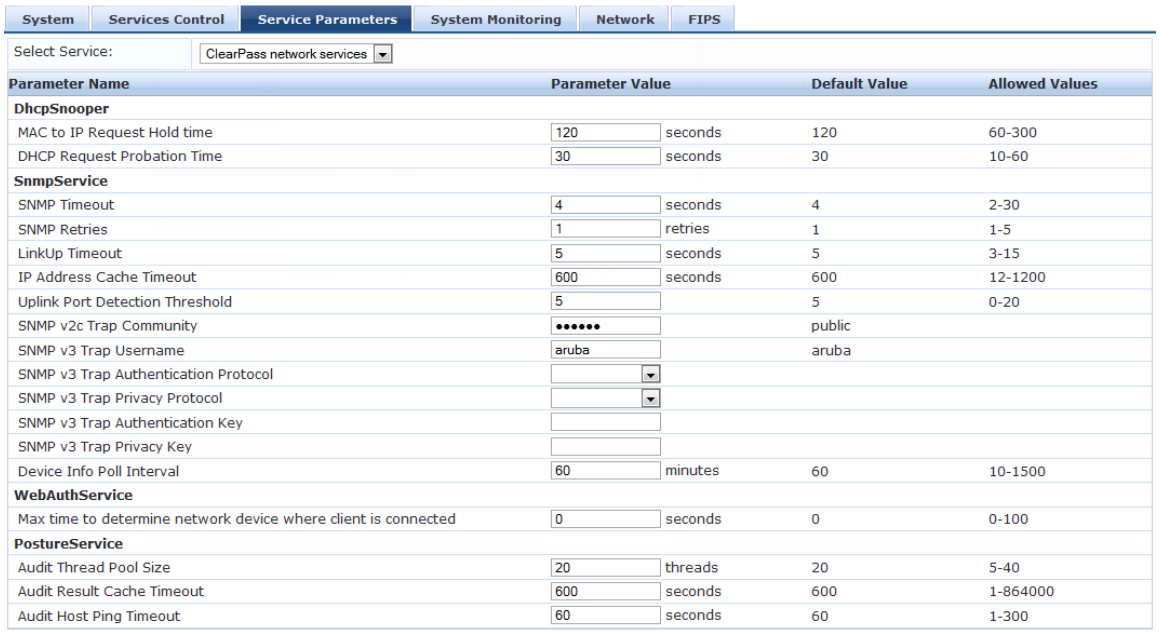
ClearPass Network Services Options

The ClearPass Network Services parameters aggregate service parameters from the following services:

- DhcpSnooper Service
- Snmp Service
- WebAuth Service
- Posture Service

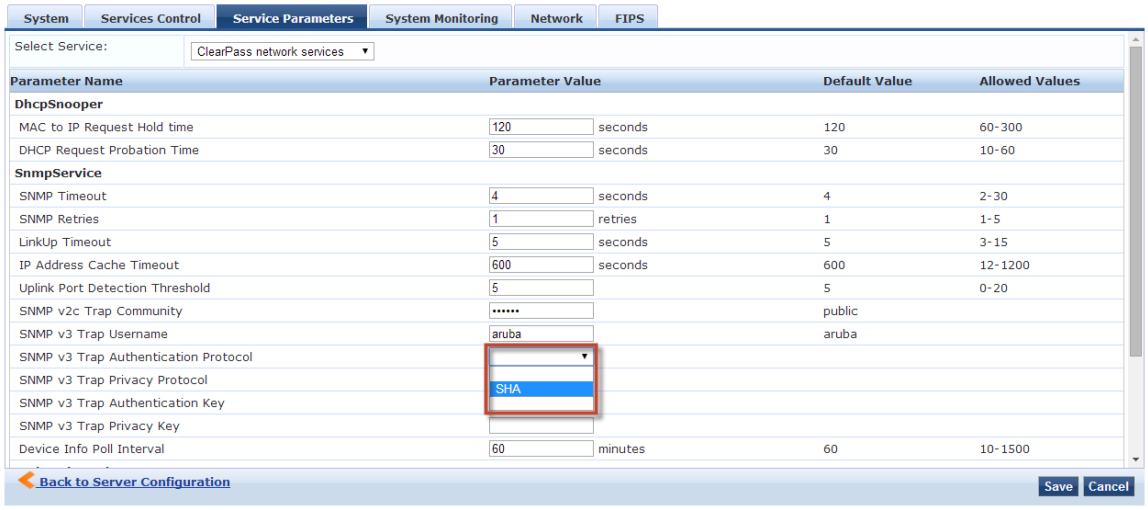
The following figure shows an example of the **ClearPass Network Services - Service Parameters** tab followed by parameter definition:

Figure 347: *ClearPass Network Services - Service Parameters Tab*



Parameter Name	Parameter Value	Default Value	Allowed Values
DhcpSnooper			
MAC to IP Request Hold time	120 seconds	120	60-300
DHCP Request Probation Time	30 seconds	30	10-60
SnmpService			
SNMP Timeout	4 seconds	4	2-30
SNMP Retries	1 retries	1	1-5
LinkUp Timeout	5 seconds	5	3-15
IP Address Cache Timeout	600 seconds	600	12-1200
Uplink Port Detection Threshold	5	5	0-20
SNMP v2c Trap Community	••••••	public	
SNMP v3 Trap Username	aruba	aruba	
SNMP v3 Trap Authentication Protocol			
SNMP v3 Trap Privacy Protocol			
SNMP v3 Trap Authentication Key			
SNMP v3 Trap Privacy Key			
Device Info Poll Interval	60 minutes	60	10-1500
WebAuthService			
Max time to determine network device where client is connected	0 seconds	0	0-100
PostureService			
Audit Thread Pool Size	20 threads	20	5-40
Audit Result Cache Timeout	600 seconds	600	1-864000
Audit Host Ping Timeout	60 seconds	60	1-300

Figure 348: *ClearPass Network Services - Service Parameters Tab FIPS Mode*



Parameter Name	Parameter Value	Default Value	Allowed Values
DhcpSnooper			
MAC to IP Request Hold time	120 seconds	120	60-300
DHCP Request Probation Time	30 seconds	30	10-60
SnmpService			
SNMP Timeout	4 seconds	4	2-30
SNMP Retries	1 retries	1	1-5
LinkUp Timeout	5 seconds	5	3-15
IP Address Cache Timeout	600 seconds	600	12-1200
Uplink Port Detection Threshold	5	5	0-20
SNMP v2c Trap Community	••••••	public	
SNMP v3 Trap Username	aruba	aruba	
SNMP v3 Trap Authentication Protocol	SHA		
SNMP v3 Trap Privacy Protocol			
SNMP v3 Trap Authentication Key			
SNMP v3 Trap Privacy Key			
Device Info Poll Interval	60 minutes	60	10-1500

Table 225: *ClearPass Network Services - Service Parameters tab Parameters*

Service Parameters	Description
DhcpSnooper	
MAC to IP Request Hold time	Specifies the number of seconds to wait before responding to a query to get an IP address corresponding to a MAC address. Any DHCP message received in this time period refreshes the MAC to IP binding. Typically, audit service requests for a MAC to IP mapping as soon the RADIUS request is received, but the client may take some more time receive and IP address through DHCP. This wait period takes into account the latest DHCP IP address that the client got.
DHCP Request Probation Time	Specifies the number of seconds to wait before considering the MAC to IP binding received in a DHCPREQUEST message as final. This wait handles cases where client receives a DHCPNAK for a DHCPREQUEST and receives a new IP address after going through the DHCPDISCOVER process again.
SnmpService	
SNMP Timeout	Specifies the seconds to wait for an SNMP response from the network device.
SNMP Retries	Specifies the number of retries for SNMP requests.
LinkUp Timeout	Specifies the seconds to wait before processing link-up traps. If a MAC notification trap arrives in this time, SNMP service does not try to poll the switch for MAC addresses behind a port for link-up processing.
IP Address Cache Timeout	Specifies the duration in seconds for which MAC to IP lookup response is cached.
Uplink Port Detection Threshold	Shows the limit for the number of MAC addresses found behind a port after which the port is considered an uplink port and not considered for SNMP lookup and enforcement.
SNMP v2c Trap Community	Specifies the community string that must be checked in all incoming SNMP v2 traps.
SNMP v3 Trap Username	Specifies the SNMP v3 Username to be used for all incoming traps.
SNMP v3 Trap Authentication Protocol	Specifies the SNMP v3 Authentication protocol for traps. Must be one of MD5, SHA, or empty (to disable authentication). **NOTE:** The **EAP-MD5** authentication type is not supported if you use the Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.

Table 225: *ClearPass Network Services - Service Parameters tab Parameters (Continued)*

Service Parameters	Description
SNMP v3 Trap Privacy Protocol	Specifies the SNMP v3 Privacy protocol for traps. Must be one of DES_CBC, AES_128, or empty (to disable privacy). **NOTE:** The **DES_CBC** privacy protocol is not supported if you use the Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.
SNMP v3 Trap Authentication Key	Specifies the SNMP v3 authentication key and privacy key for incoming traps.
SNMP v3 Trap Privacy Key	
Device Info Poll Interval	Specifies the time (in minutes) between polling for device information.
WebAuthService	
Max time to determine network device where client is connected	In some usage scenarios where the web authentication request does not originate from the network device. Policy Manager has to determine the network device to which the client is connected through an out-of-band SNMP mechanism. The network device deduction can take some time. This parameter specifies the maximum time to wait for Policy Manager to determine the network device to which the client is connected.
PostureService	
Audit Thread Pool Size	Specifies the number of threads to use for connections to audit servers.
Audit Result Cache Timeout	Specifies the time (in seconds) for which audit result entries are cached by Policy Manager.
Audit Host Ping Timeout	Specifies the number of seconds for which Policy Manager pings an end-host before giving up and deeming the host to be unreachable.

ClearPass System Services Options

You can use the ClearPass system service parameters for PHP configuration as well as if all your http traffic flows through a proxy server. Policy Manager relies on an http connection to the Dell W-ClearPass update portal in order to download the latest version information for posture services.

Figure 349: *ClearPass System Services Parameters (partial view)*

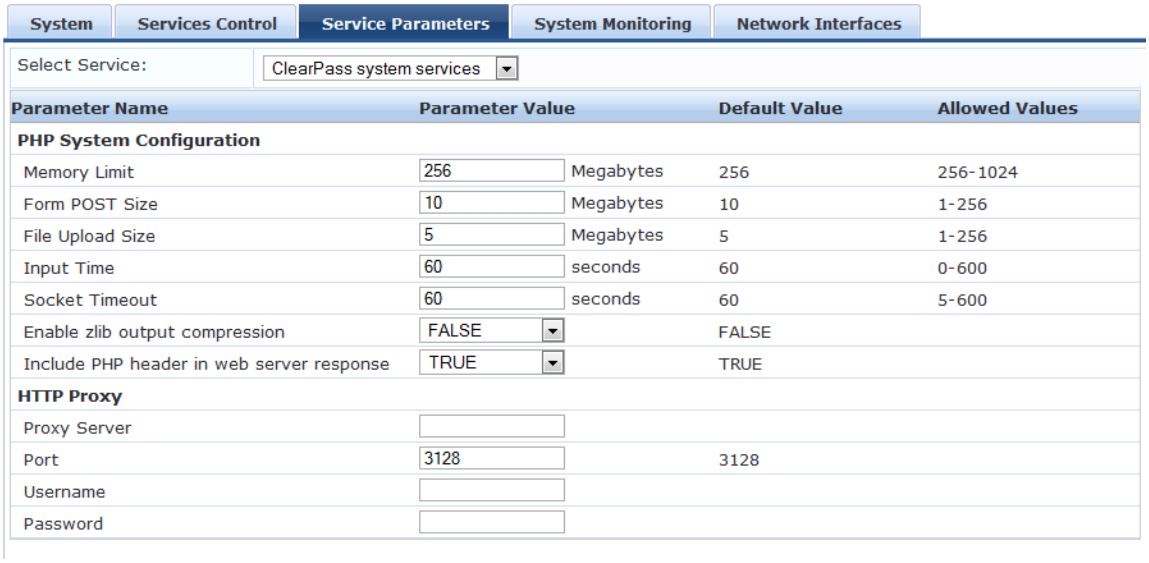


Table 226: *Service Parameters - ClearPass system services*

Service Parameter	Description
PHP System Configuration	
Memory Limit	Maximum memory that can be used by the PHP applications.
Form POST Size	Maximum HTTP POST content size that can be sent to the PHP application.
File Upload Size	Maximum file size that can be uploaded into the PHP application.
Input Time	Time limit after which the server will detect no activity from the user and will take some action.
Socket Timeout	Maximum time for any socket connections.
Enable zlib output compression	Setting to compress the output files.
Include PHP header in web server response	Setting to include PHP header in the HTTP responses.
HTTP Proxy	

Table 226: *Service Parameters - ClearPass system services (Continued)*

Service Parameter	Description
Proxy Server	Hostname or IP address of the proxy server.
Port	Port at which the proxy server listens for HTTP traffic.
Username	Username to authenticate with proxy server.
Password	Password to authenticate with proxy server.
Database Configuration	
Maximum connections	Specify a number between 300 and 2000 for a maximum number of allowed connections.
TCP Keepalive Configurations	
Keep Alive Time	Specify a value in seconds from 10-86400.
Keep Alive Interval	Specify a value in seconds from 1-3600.
Keep Alive Probes	Specify a value from 1-100 for the number of probes.
Web Server Configuration	
Maximum Clients	Specify a value from 10-20000 for the maximum allowed number of clients.
Timeout	Specify a timeout value in seconds from 1-60.
Keep Alive	Specify **TRUE** or **FALSE**. The default value is **TRUE**.
Request Wait	Specify the duration in seconds for a request to wait. The default value is 4 seconds. You can specify the **Request Wait** duration in the range of 1-60 seconds.

Table 226: *Service Parameters - ClearPass system services (Continued)*

Service Parameter	Description
Maximum Requests	Specify the maximum number of requests. The default value is 500. You can specify the range of 0 – 3000.
Enable Host Header check	Specify **TRUE** or **FALSE**. The default value is **TRUE**. When you set this value to **TRUE**, the **Host Header Restriction check** is enabled and only the allowed or whitelisted host headers are allowed. When you set this value to **FALSE**, irrespective of Host Headers in the http packet, Dell Networking W-ClearPass Policy Manager redirects to https://<cppm-server>/tips.
WhiteList Host Names	When the **Enable Host Header check** value is set to **TRUE**, the web access is allowed for Whitelist Host Names, hostnames, IP addresses, and VIP addresses in Dell Networking W-ClearPass Policy Manager. The comma separated whitelist host names are allowed to support multiple hostnames. When the **Enable Host Header check** value is set to **TRUE** and the **WhiteList Host Names** field is blank, the web access is allowed only for hostnames, IP addresses, and VIP addresses in Dell Networking W-ClearPass Policy Manager.

Policy Server Options

Figure 350: *Policy Server Service Parameters*

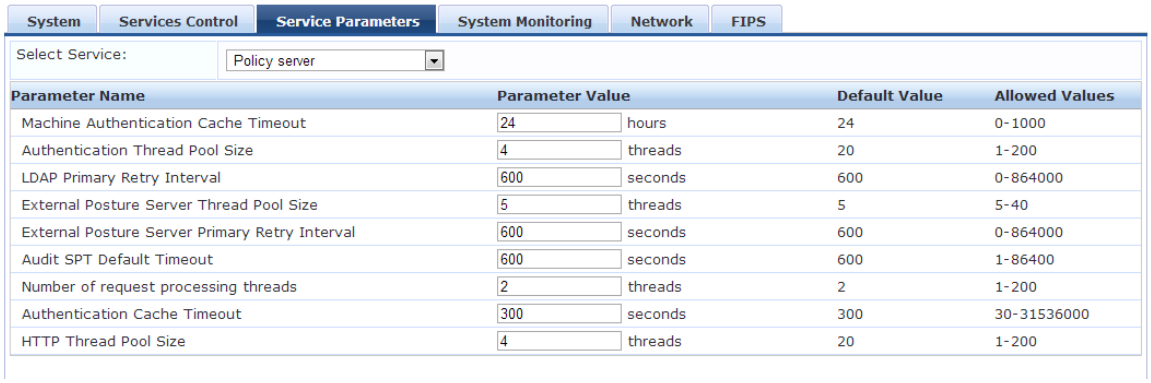


Table 227: *Service Parameters tab - Policy Server service*

Service Parameter	Description
Machine Authentication Cache Timeout	This specifies the time (in hours) for which machine authentication entries are cached by Policy Manager.
Authentication Thread Pool Size	This specifies the number of threads to use for LDAP/AD and SQL connections.
LDAP Primary Retry Interval	After a primary LDAP server is down, Policy Manager connects to one of the backup servers. This parameter specifies how long Policy Manager waits before it tries to connect to the primary server again.

Table 227: *Service Parameters tab - Policy Server service (Continued)*

Service Parameter	Description
External Posture Server Thread Pool Size	This specifies the number of threads to use for posture servers.
External Posture Server Primary Retry Interval	After a primary posture server is down, Policy Manager connects to one of the backup servers. This parameter specifies how long Policy Manager waits before it tries to connect to the primary server again.
Audit SPT Default Timeout	Time for which Audit success or error response is cached in policy server.
Number of request processing threads	Maximum number of threads used to process requests.
Authentication Cache Timeout	Specifies the time in seconds for which authentication information is cached by Policy Manager.
HTTP Thread Pool Size	Specify the number of threads allotted for the HTTP thread pool.

Radius Server Options

Figure 351: *RADIUS Server Service Parameters*

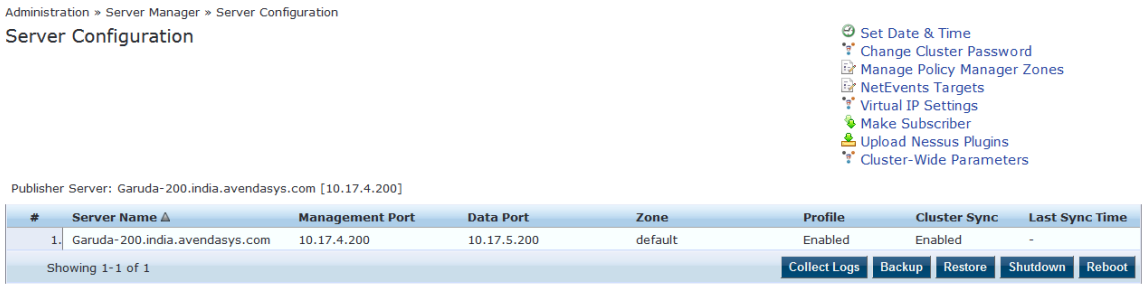


Table 228: *Service Parameters tab - Radius Server Service*

Service Parameter	Description
Proxy	
Maximum Response Delay	Time delay before retrying a proxy request, if the target server has not responded.
Maximum Reactivation Time	Time to elapse before retrying a dead proxy server.
Maximum Retry	Maximum number of times to retry a proxy request if the target server doesn't respond.

Table 228: *Service Parameters tab - Radius Server Service (Continued)*

Service Parameter	Description
Counts	
Security	
Reject Packet Delay	Delay time before sending an actual RADIUS Access-Reject after the server decides to reject the request.
Maximum Attributes	Maximum number of RADIUS attributes allowed in a request.
Process Server-Status Request	Send replies to Status-Server RADIUS packets.
Main	
Authentication Port	Ports on which radius server listens for authentication requests. Default values are 1645, 1812.
Accounting Port	Ports on which radius server listens for accounting requests. Default values are 1646, 1813.
Maximum Request Time	Maximum time allowed for processing a request after which it is considered timed out.
Cleanup Time	Time to cache the response sent to a RADIUS request after sending it. If the RADIUS server gets a duplicate request for which the response is already sent, the cached response is resent if the duplicate request arrives within this time period.
Local DB Authentication Source Connection Count	Maximum number of Local DB connections opened.
AD/LDAP Authentication Source Connection Count	Maximum number of AD/LDAP connections opened.
SQL DB Authentication Source Connection Count	Maximum number of SQL DB.

Table 228: *Service Parameters tab - Radius Server Service (Continued)*

Service Parameter	Description
EAP - TLS Fragment Size	Maximum size of the EAP-TLS fragment size.
Use Inner Identity in Access-Accept Reply	Specify TRUE or FALSE.
TLS Session Cache Limit	Number of TLS sessions to cache before purging the cache (used in TLS based 802.1X EAP Methods).
AD (Active Directory) Errors	
Window Size	Enter a duration during which Active Directory errors are accumulated for possible action. The default is 5 minutes.
Number of Errors	Enter a number. If this number of Active Directory errors occurs within the defined Window Size, the self-healing Recovery Action is taken. The default is 150.
Recovery Action	Select: • None - To initiate no self-recovery action [Default]. • Exit - To restart the RADIUS server (Monitoring daemon will restart it). • Restart Domain Service - To restart the Domain service.
Thread Pool	
Maximum Number of Threads	Maximum number of threads in the RADIUS server thread pool to process requests.
Number of Initial Threads	Initial number of thread in the RADIUS server thread pool to process requests.
EAP-FAST	
Master Key Expire Time	Lifetime of a generated EAP-FAST master key.
Master Key Grace Time	Grace period for an EAP-FAST master key after its lifetime. If a client presents a PAC that is encrypted using the master key in this period after its TTL, it is accepted and a new PAC encrypted with the latest master key is provisioned on the client.

Table 228: *Service Parameters tab - Radius Server Service (Continued)*

Service Parameter	Description
PACs are valid across cluster	Whether PACs generated by this server are valid across the cluster or not.
Accounting	
Log Accounting Interim-Update Packets	Store the Interim-Update packets in session logs.

Stats Collection Service Options

Figure 352: *Stats Collection Service Parameters*

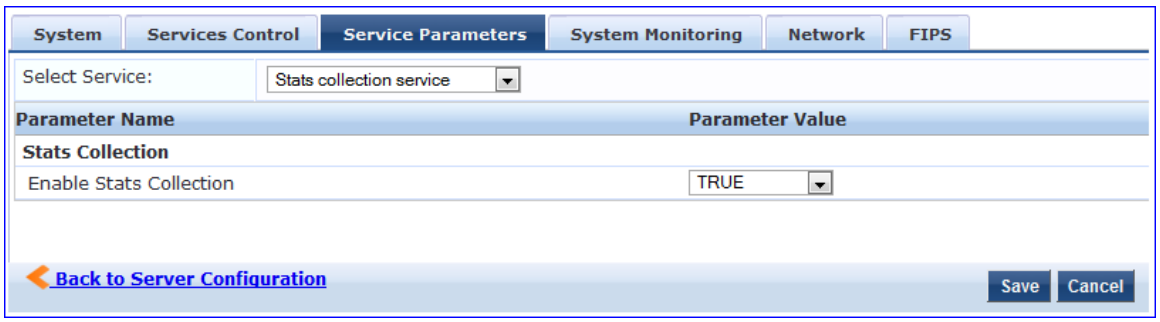


Table 229: *Service Parameters tab - Stats Collection service*

Service Parameter	Description
Enable Stats Collection	This option enables or disables Stats Collection and Stats Aggregation. If this is not enabled, then stats collection and aggregation services will not run on the node. In addition, the following error message will display if the admin attempts to start these services: "Failed to start Stats collection service - Ignoring service start request as Stats Collection option is disabled on the node" **NOTE:** Enabling/disabling this parameter requires a restart of cpass-statsd-server and cpass-carbon-server.

System Monitor Service Options

Figure 353: *System Monitor Service Parameters*

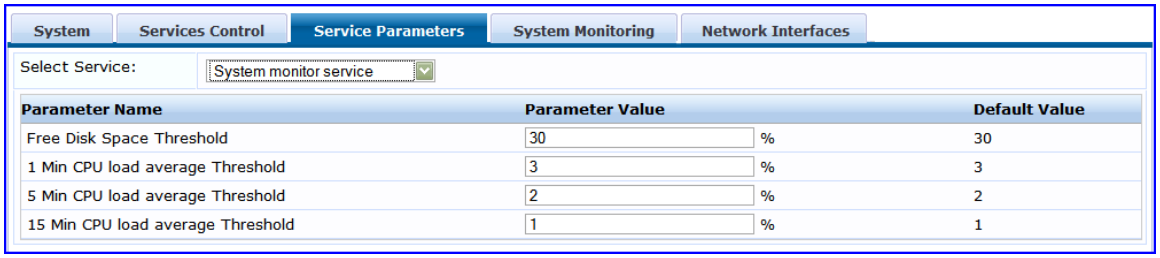


Table 230: *Services Parameters tab - System monitor service*

Service Parameter	Description
Free Disk Space Threshold	This parameter monitors the available disk space. If the available disk free space falls below the specified threshold (default 30%), then system sends SNMP traps to the configured trap servers.
1 Min CPU load average Threshold	These parameters monitor the CPU load average of the system, specifying thresholds for 1-min, 5-min and 15-min averages, respectively. If any of these loads exceed the associated maximum value, then system sends traps to the configured trap servers.
5 Min CPU load average Threshold	
15 Min CPU load average Threshold	

Tacacs Server Options

Figure 354: *TACACS+ Service Parameters*

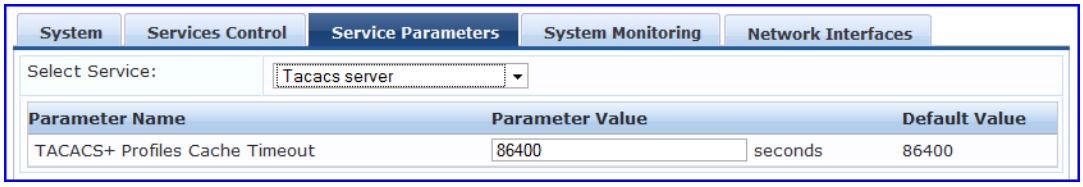


Table 231: *Service Parameters tab - TACACS server*

Service Parameter	Description
TACACS+ Profiles Cache Timeout	This specifies the time (in seconds) for which TACACS+ profile result entries are cached by Policy Manager

System Monitoring Tab

Navigate to **Administration** > **Server Manager** > **Server Configuration** > **System Monitor** tab to configure the SNMP parameters. This ensures that external Management Information Base (MIB) browsers can browse the system level MIB objects exposed by the Policy Manager appliance. The options in this page vary based on the SNMP version that you select. The following figure shows an example of the **System Monitoring** tab followed by parameter definition:

Figure 355: *System Monitoring Tab*

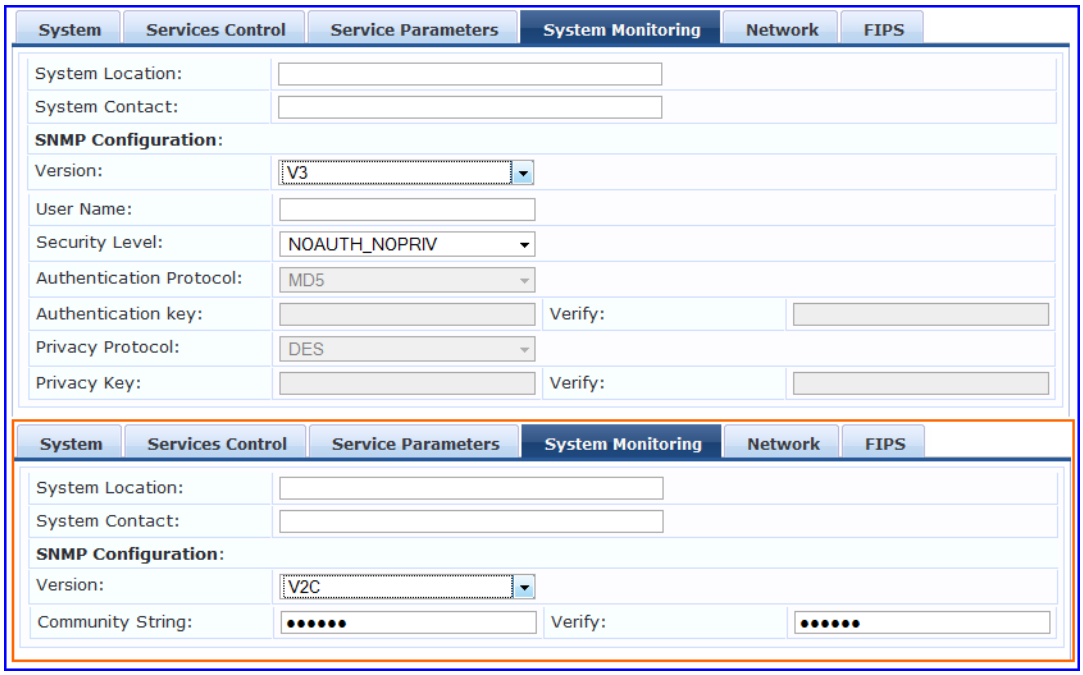


Table 232: *System Monitoring tab Parameters*

Parameter	Description
System Location	Specify the location of the Policy Manager appliance.
System Contact	Specify the contact information of the Policy Manager appliance.
SNMP Configuration	
Version	Specify the SNMP version from the options V1, V2C, or V3. The GUI options on this page vary based on the SNMP version selected.
Community String	Enter and re-enter the community string for sending traps.
SNMP v3: Username	Specify the user name to use for SNMP v3 communication. This field is available only if you selected the **V3** as the SNMP version in the **Version** field.
SNMP v3: Security Level	Select any of the following options: • NOAUTH_NOPRIV (no authentication or privacy) - If you select this security level, only the **SHA** authentication protocol is available. • AUTH_NOPRIV (authenticate, but no privacy) - If you select this security level, the **MD5** and **SHA** authentication protocols are available. • AUTH _PRIV (authenticate and keep the communication private) - If you select this security level, the **MD5** and **SHA** authentication protocols are available. This field is available only if you selected **V3** as the SNMP version in the **Version** field.

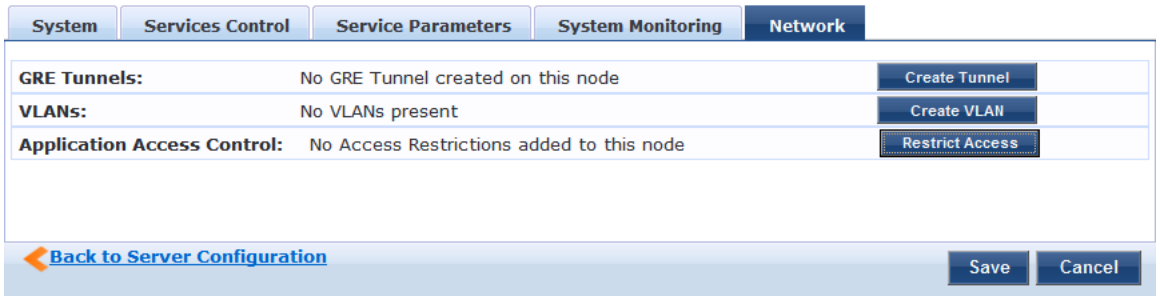
Table 232: *System Monitoring tab Parameters (Continued)*

Parameter	Description
SNMP v3: Authentication Protocol	Select the authentication protocol from **MD5** or **SHA**. These protocols vary depends on the security level that you selected in the **Security Level** field. This field is available only if you selected **V3** as the SNMP version in the **Version** field. **NOTE:** The **MD5** authentication protocol is not supported in the **FIPS** mode.
SNMP v3: Authentication key	Enter and re-enter the authentication key. This field is available only if you selected **V3** as the SNMP version in the **Version** field.
SNMP v3: Privacy Protocol	Select the privacy protocol from **DES** or **AES**. This field is available only if you selected **V3** as the SNMP version in the **Version** field.
SNMP v3: Privacy Key	Enter the privacy key. This field is available only if you selected **V3** as the SNMP version in the **Version** field.

Network Tab

Navigate to the **Network** tab to create generic routing encapsulation (GRE) tunnels and VLANs related to guest users and to control what applications can have access to the node.

Figure 356: *Network Interfaces Tab*



Creating GRE tunnels

The administrator can create a GRE tunnel. This protocol can be used to create a virtual point-to-point link over standard IP network or the internet.

Navigate to the **Network** tab and click **Create Tunnel**.

Figure 357: *Create Tunnel page*

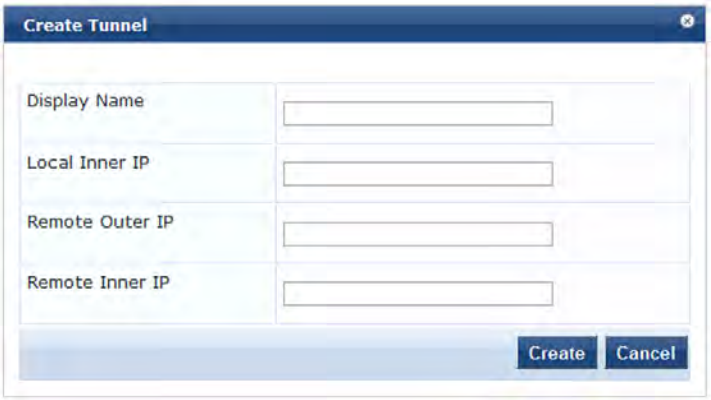


Table 233: *Create Tunnel Page Parameters*

Parameter	Description
Display Name	Specify the name for the tunnel interface. This name is used to identify the tunnel in the list of network interfaces.
Local Inner IP	Local IP address of the tunnel network interface.
Remote Outer IP	IP address of the remote tunnel endpoint.
Remote Inner IP	Remote IP address of the tunnel network interface. Enter a value here to automatically create a route to this address through the tunnel.
Create/Cancel	Commit or dismiss changes.

Creating VLANs

Navigate to the **Network** tab and click **Create VLAN**.

Figure 358: *Creating VLAN Page*

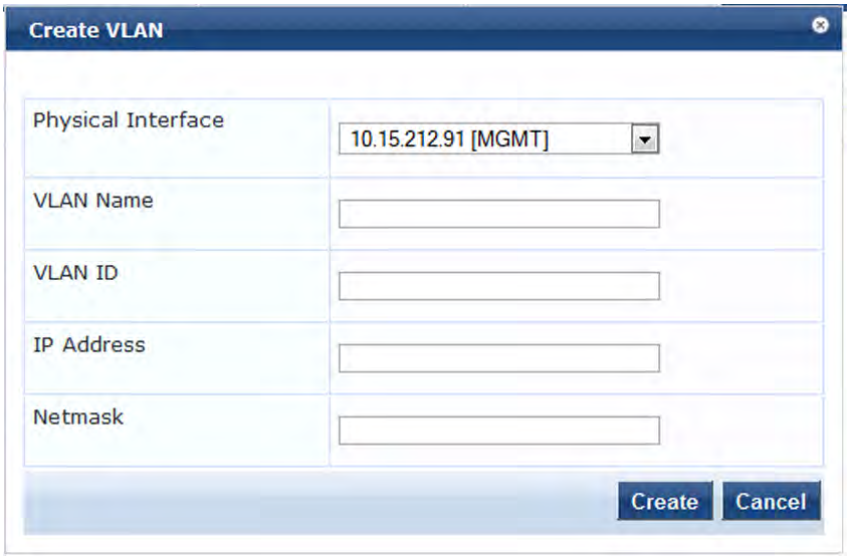


Table 234: *Creating VLAN Parameters*

Parameter	Description
Physical Interface	The physical port on which to create the VLAN interface. This is the interface through which the VLAN traffic will be routed.
VLAN Name	Name for the VLAN interface. This name is used to identify the VLAN in the list of network interfaces.
VLAN ID	802.1Q VLAN identifier. Enter a value between 1- 4094. The VLAN ID cannot be changed after the VLAN interface has been created.
IP Address	IP address of the VLAN.
Netmask	Netmask for the VLAN.
Create/Cancel	Commit or dismiss changes.

Your network infrastructure must support tagged 802.1Q packets on the physical interface selected. VLAN ID 1 is often reserved for use by certain network management components; avoid using this ID unless you know it will not conflict with a VLAN already defined in your network.

Defining Access Restrictions

Use this function to define specific network resources and allow or deny them access to specific applications. You can create multiple definitions. Navigate to the **Network** tab and click **Restrict Access**.

Figure 359: *Restrict Access dialog box*

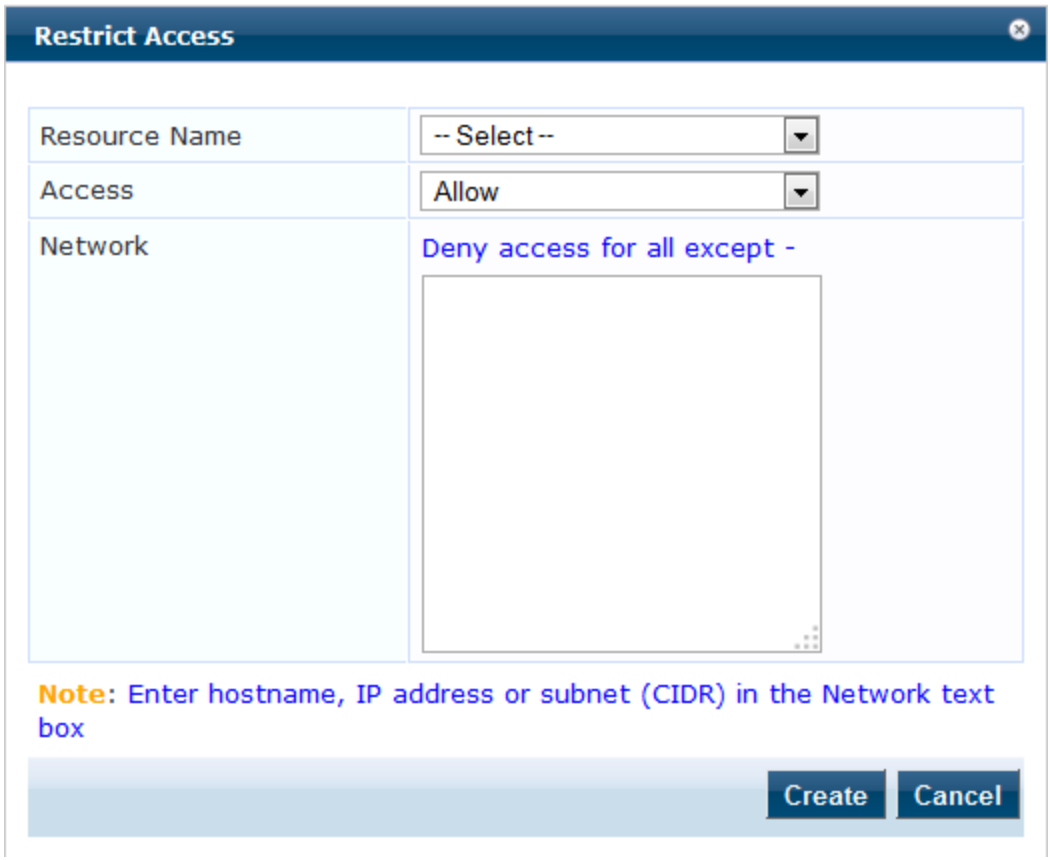


Table 235: *Restrict Access Parameters*

Parameter	Description
Resource Name	Select the application to which you want to allow or deny access.
Access	Select: • **Allow** to define allowed access. • **Deny** to define denied access.
Network	Enter one or more hostnames, IP addresses, or IP subnets per line. The devices defined by what you enter here will be either specifically allowed or specifically denied access to the application you select.

FIPS Tab

This section provides information to use Dell Networking W-ClearPass Policy Manager in the Federal Information Processing Standards (FIPS) mode.

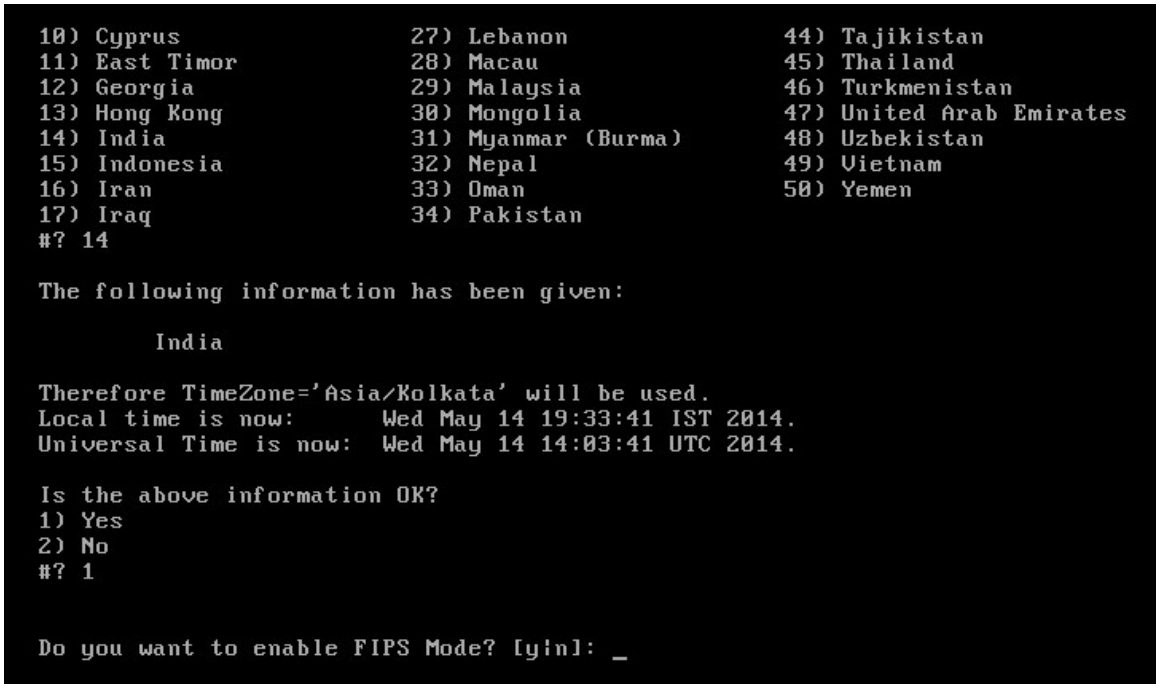
The United States Government developed the FIPS to define procedures, architecture, algorithms, and other techniques used in software systems. In addition to supporting network industry standards, Dell Networking W-ClearPass Policy Manager is compliant with government security validations and accreditations, including the FIPS 140-2 validation.

Dell Networking W-ClearPass Policy Manager is FIPS 140-2 compliant through incorporation of a FIPS validated module which provides all cryptography functions for the application. Policy Manager incorporates the

OpenSSL FIPS Object Module. The OpenSSL FIPS Object Module has obtained FIPS 140-2 certificate number 1747, listed at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747

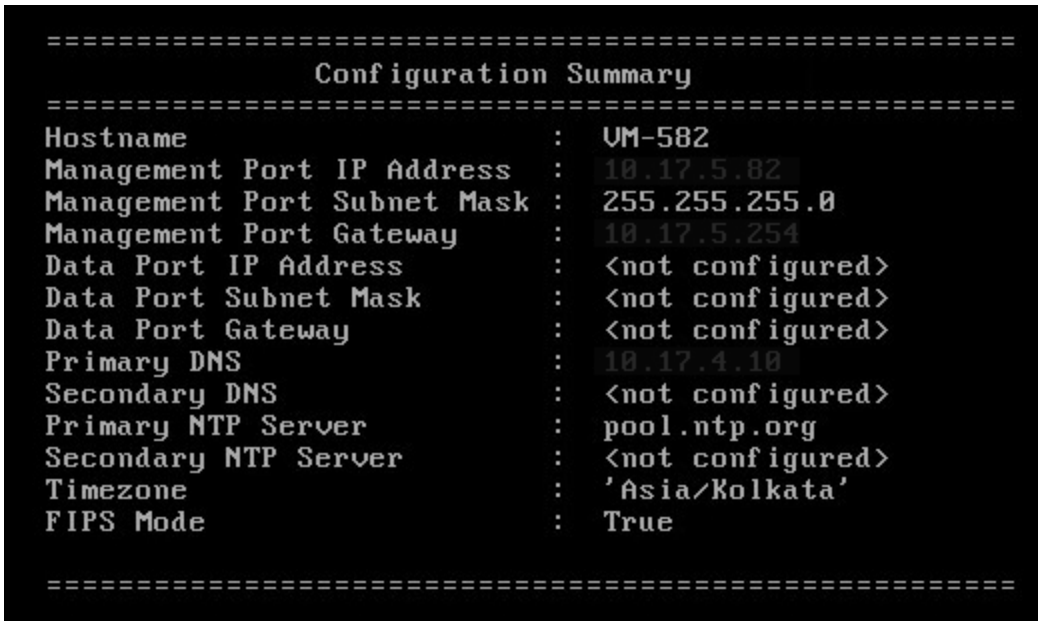
A Dell Networking W-ClearPass Policy Manager server running in FIPS mode is FIPS-compliant. There are no additional steps required to ensure FIPS 140-2 compliant operation of the ClearPass Policy Manager in the FIPS mode. In the FIPS mode, support is not available for legacy authentication methods such as EAP-MD5 and MD5 digest algorithm. You can enable the FIPS mode in Dell Networking W-ClearPass Policy Manager server at post-installation configuration using CLI commands. The following figure shows an example of the prompt to enable the FIPS Mode using the CLI command:

Figure 360: *Enabling FIPS Mode*



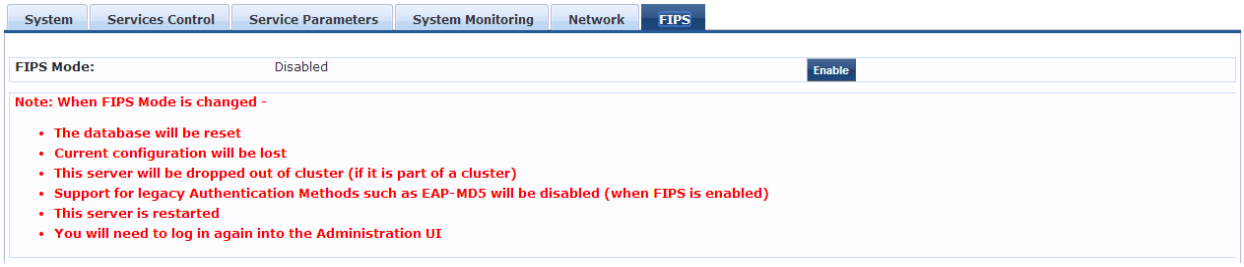
After enabling the FIPS mode using the CLI commands, you can verify whether the FIPS mode is enabled or not in the **Configuration Summary** page. The following figure shows an example of the **Configuration Summary** page:

Figure 361: *FIPS Mode - Configuration Summary*



Alternatively, you can enable or disable the FIPS mode in the **Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab. The following figure shows an example of the **Server Configuration - FIPS** tab with the option to enable or disable the FIPS mode:

Figure 362: *Server Configuration - FIPS Tab*

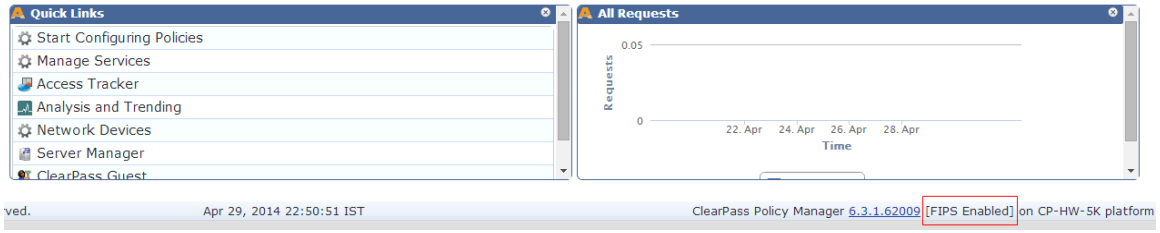


Note the following important points, when you enable the FIPS mode in Dell Networking W-ClearPass Policy Manager as described in the figure above:

- The database is reset when you enable the FIPS mode in Dell Networking W-ClearPass Policy Manager. Ensure that you backed up your database before enabling the FIPS mode.
- Configuration backup file from the Dell Networking W-ClearPass Policy Manager in the non-FIPS mode cannot be restored on Dell Networking W-ClearPass Policy Manager in the FIPS mode. However, configuration backup file from the Dell Networking W-ClearPass Policy Manager in the FIPS mode can be restored on the Dell Networking W-ClearPass Policy Manager in the non-FIPS mode.
- The server will be removed from the cluster if the FIPS mode is enabled.
- All nodes in a cluster must be either in the FIPS or non-FIPS mode. The Dell Networking W-ClearPass Policy Manager nodes in the FIPS mode cannot be connected to the cluster whose nodes are in the non-FIPS mode.
- The legacy authentication method such as EAP-MD5 and MD5 digest algorithm are not supported in the FIPS mode. You cannot import the certificates that are created with the MD5 authentication type to the **Certificates Trust List** (**Administration** > **Certificates** > **Certificate Trust List**) page.
- The server reboots when you enable the FIPS mode. You need to log in again to the Administration UI.

You can view the status of the FIPS mode in the status bar. The following figure shows an example of the **Status** bar with the status of the FIPS mode:

Figure 363: *FIPS Status*



You can also view the status of the FIPS mode using the CLI commands. For more information, see Show Commands on page 494.

Set Date & Time

Navigate to **Administration > Server Manager > Server Configuration**, and click on the **Set Date and Time** link. This opens by default on the **Date &Time** tab.

Figure 364: *Change Date and Time - Date & Time tab*

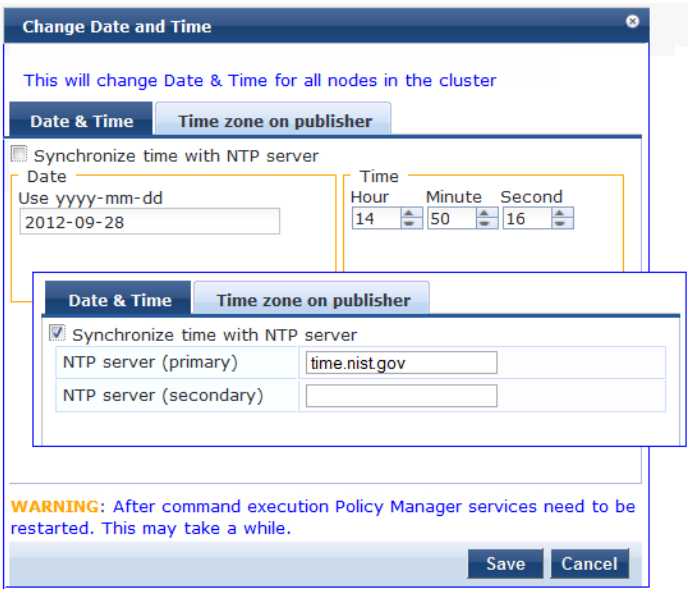


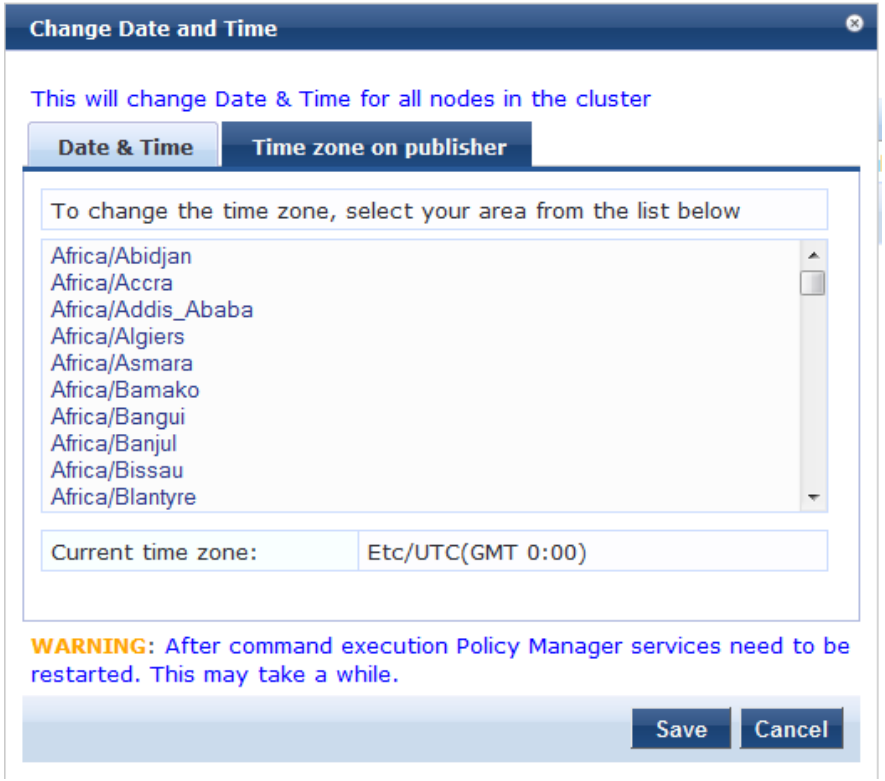
Table 236: *Change Date and Time - Date & Time tab Parameters*

Parameter	Description
Date in yyyy-mm-dd format	To specify date and time, use the indicated syntax. This is available only when Synchronize time with NTP server is unchecked.
Time in hh:mm:ss format	
Synchronize Time With NTP Server	To synchronize with a Network Time Protocol Server, enable this check box and specify the NTP servers. Only two servers may be specified.
NTP Servers	

After configuring the date and time, select the time zone on the **Time zone on publisher** tab. This displays a time zone list alphabetical order. Select a time zone and click **Save**.

This option is only available on the publisher. To set time zone on the subscriber, select the specific server and set time zone from the server-specific page.

Figure 365: *Time zone on publisher tab*



Change Cluster Password

Use this function to change the cluster-wide password.

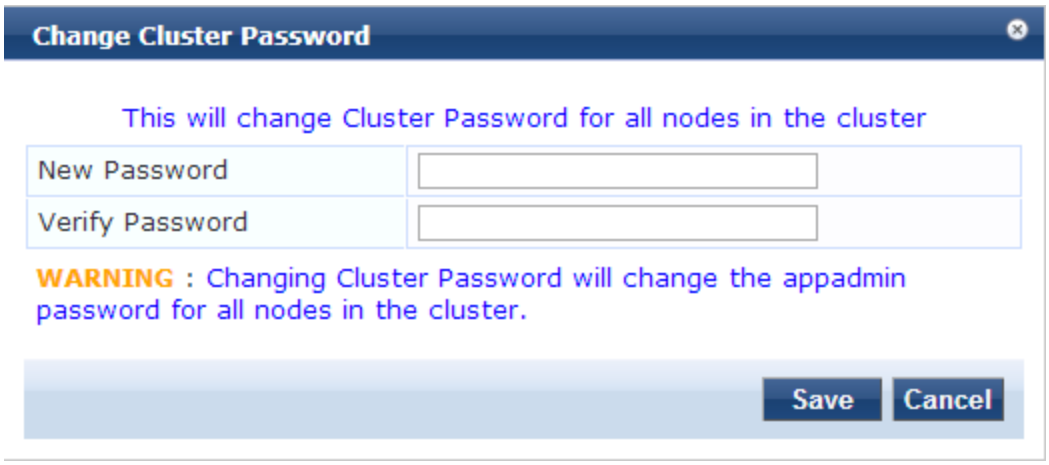
Changing this password also changes the password for the CLI user *appadmin*.

To change the cluster-wide password:

1. Navigate to **Administration > Server Manager > Server Configuration**, and click the **Change Cluster Password** link.

   The Change Cluster Password dialog appears (see Figure 366).

Figure 366: *Change Cluster Password Dialog*



2. Enter the new password, then verify the password.
3. Click **Save**.

Manage Policy Manager Zones

CPPM shares a distributed cache of runtime state across all nodes in a cluster. These runtime states include:

- Roles and Postures of connected entities
- Connection status of all endpoints running OnGuard
- Endpoint details gathered by OnGuard Agent

CPPM uses this runtime state information to make policy decisions across multiple transactions.

In a deployment where a cluster spans WAN boundaries and multiple geographic zones, it is not necessary to share all of this runtime state across all nodes in the cluster. For example, when endpoints present in one geographical area are not likely to authenticate or be present in another area.

When endpoints present in one geographical area are not likely to authenticate or be present in another area, it is more efficient from a network bandwidth usage and processing perspective to restrict the sharing of such runtime state to a given geographical area.

You can configure Zones in Dell Networking W-ClearPass Policy Manager to match with the geographical areas in your deployment. There can be multiple Zones per cluster, and each Zone has a number of Dell Networking W-ClearPass Policy Manager nodes that share runtime state.

Figure 367: *Policy Manager Zones*

Table 237: *Policy Manager Zones*

Parameter	Description
Name	Enter the name of the configured Policy Manager Zone.
Add	Click this to add a zone.
Delete	Select the delete (trashcan) icon to delete a zone.

NetEvents Targets

NetEvents are a collection of details for various ClearPass Policy Manager such as users, endpoints, guests, authentications, accounting details, and so on. This information is periodically posted to a server that is configured as the NetEvents target.

If the ClearPass Insight feature is enabled on a ClearPass Policy Manager, it will receive netevents from all other server nodes within the same CPPM cluster. If you want to post these details to any external server that can aggregate these events or to an external dedicated ClearPass Insight server for multiple CPPM clusters, you have to configure an external NetEvents Target.

Figure 368: *NetEvents Targets*

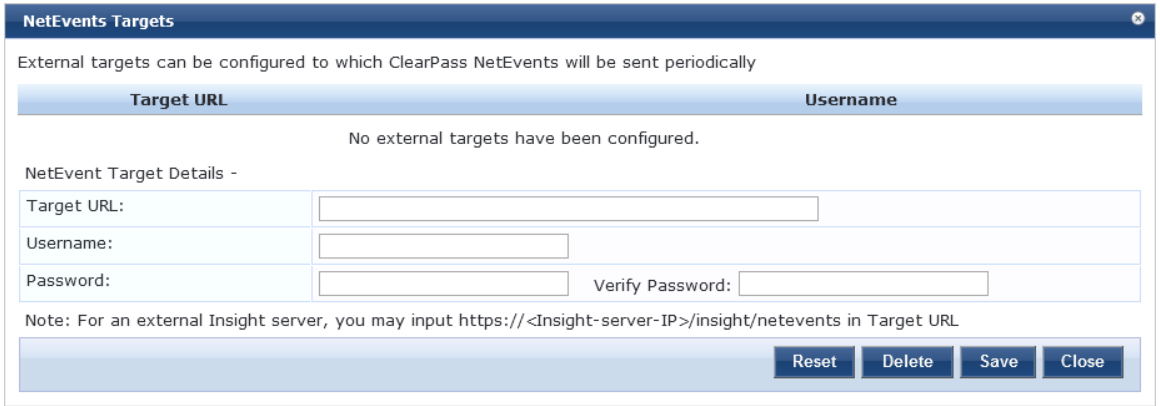


Table 238: *NetEvents targets*

Parameter	Description
Target URL	HTTP URL for the service that support POST and requires Authentication using Username / Password. **NOTE:** For an external Insight server, you can enter https://<Insight-server-IP>/insight/netevents as the Target URL
Username/Password	Credentials configured for authentication for the HTTP service that is provided in the Target URL.
Reset	Reset the dialog.
Delete	Delete the information.

Virtual IP Settings

This configuration allows two nodes in a cluster to share a Virtual IP address. The Virtual IP address is bound to the primary node by default. The secondary node takes over when the primary node is unavailable.

In a virtual machine deployment of Dell Networking W-ClearPass Policy Manager, enable forged transmits on a VMWare distributed virtual switch for the Virtual IP feature to work properly.

Figure 369: *Virtual IP Settings*

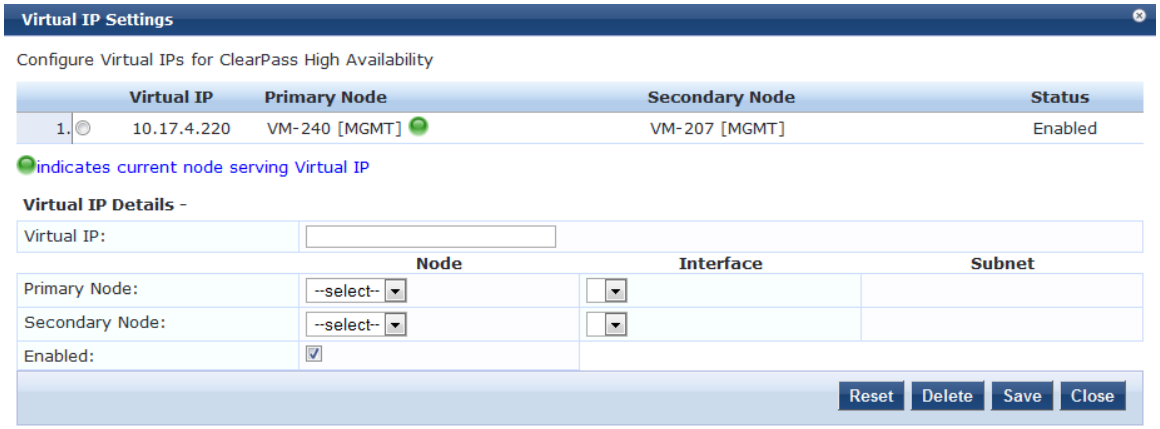


Table 239: *Virtual IP Settings Parameters*

Parameter	Description
Virtual IP	Enter the IP address you want to define as the virtual IP address.
Node	Select the servers to use as the primary and secondary nodes.
Interface	Select the interface on each server where virtual IP address should be bound.
Subnet	This value is automatically entered. You do not need to change it.
Enabled	Select the check box to enable the Virtual IP address.

Make Subscriber

In the Policy Manager cluster environment, the *Publisher node* acts as master. A Policy Manager cluster can contain only one Publisher node. Administration, configuration, and database write operations may occur only on this master node.

The Policy Manager appliance defaults to a Publisher node unless it is made a Subscriber node. Cluster commands can be used to change the state of the node, hence the Publisher can be made a Subscriber. When it is a Subscriber, you will not see this link.

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Make Subscriber** link.

Figure 370: *Add Subscriber Node*

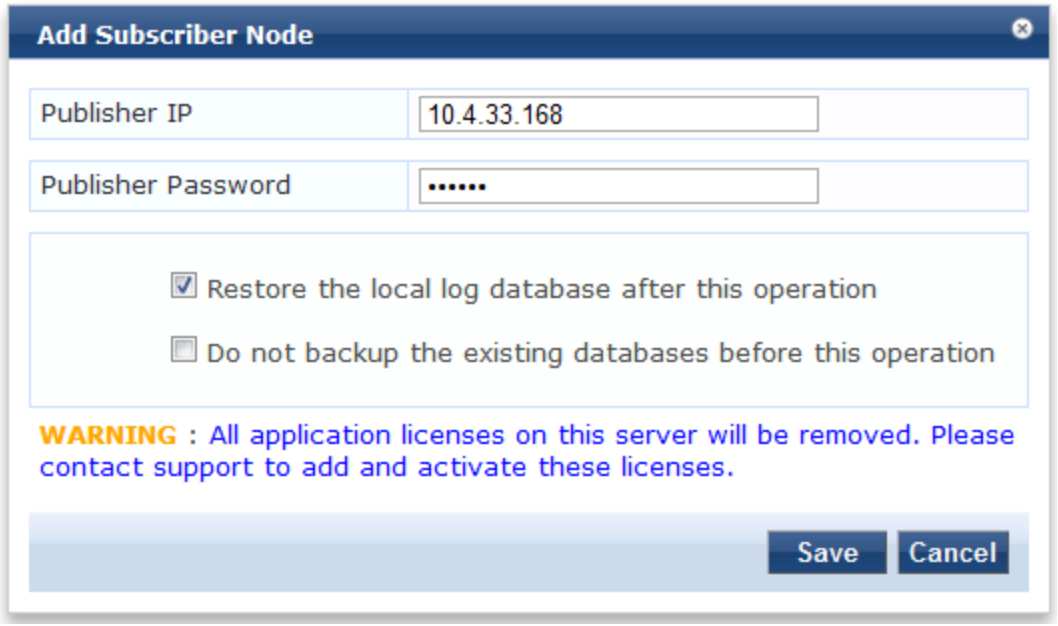


Table 240: *Add Subscriber Node*

Parameter	Description
Publisher IP	Specify publisher address and password. **NOTE:** The password specified here is the password for the CLI user *appadmin*
Publisher Password	
Restore the local log database after this operation	Enable to restore the log database following addition of a subscriber node.
Do not backup the existing databases before this operation	Enable this check box only if you do not require a backup to the existing database.

Upload Nessus Plugins

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Upload Nessus Plugins** link.

Figure 371: *Upload Nessus Plugins*

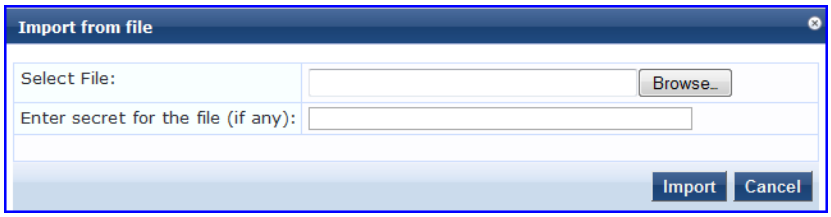


Table 241: *Upload Nessus Plugins*

Parameter	Description
Select File	Click **Browse** and select the plugins file with the extension tar.gz.
Enter secret for the file (if any)	Always leave this blank.
Import/Cancel	Load the plugins, or dismiss. If there are a large number of plugins, the load time can be in the order of minutes.

Cluster-Wide Parameters

Use the **Cluster-Wide Parameters** page to configure the parameters that apply to all the nodes in a cluster. These include Cache timeouts, Cleanup intervals, Auto backup, System Alert Notification, Virtual AP and so on.

To view the Cluster-Wide Parameters page, navigate to the **Administration > Server Manager > Server Configuration** page and click the **Cluster-Wide Parameters** link in the upper right. The Cluster-Wide Parameters page contains the following tabs:

- General
- Cleanup Intervals
- Notifications
- Standby Publisher
- Virtual IP Configuration
- Mode

General

The following figure shows an example of the **Cluster-Wide Parameters - General** tab by parameter definition:

Figure 372: *Cluster-Wide Parameters - General Tab*

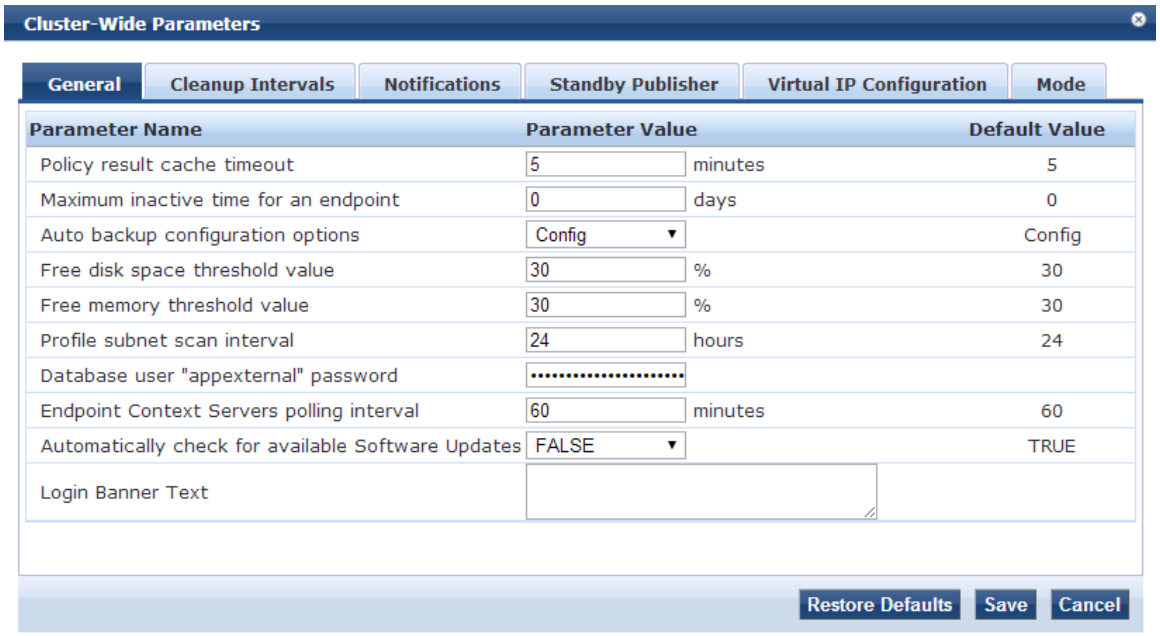


Table 242: *Cluster-Wide Parameters - General tab Parameters*

Parameter	Description
Policy result cache timeout	Specifies the duration allowed in minutes to store the role mapping and posture results derived by the policy engine during a policy evaluation. This result can then be used in subsequent evaluation of policies associated with a service, if the **Use cached Roles and Posture attributes from previous sessions** option is turned on for the service. A value of 0 disables caching. **NOTE:** The value of the **Policy result cache timeout** field must be greater than the highest value set in the **Health Check Interval (in hours)** fields. For example, if you have created the profiles Student-Enforcement-Profile and Staff-Enforcement-Profile with health check interval configured, then the value of the **Policy result cache timeout** field must be greater than the highest value of the **Health Check Quiet Period (in hours)** value configured among the following profiles: • Global Agent Settings • Student-Enforcement-Profile • Staff-Enforcement-Profile
Maximum inactive time for an endpoint	Specifies the duration in number of days to which an endpoint is retained in the endpoints table since its last authentication. If the endpoint is not authenticated for this period, the entry is removed from the endpoint table. 0 specifies no time limit configured.
Auto backup configuration options	Select any of the following auto backup configuration options: • **Off** - Select this to not to perform periodic backups. **NOTE:** Select **Off** before upgrading Dell Networking W-ClearPass Policy Manager to avoid the interference between Auto backup and migration process. • **Config** - Perform a periodic backup of the configuration database only. This is the default auto backup configuration option. • **Config|SessionInfo** - Perform a backup of the configuration database and the session log database.

Table 242: *Cluster-Wide Parameters - General tab Parameters (Continued)*

Parameter	Description
	NOTE: It is recommended to set this option to **Off** or **Config** before starting an upgrade. This ensures the Auto-backup process does not interfere with migration after upgrade. You can change this setting back to the **Config|SessionInfo** option after 24 hours on completion of upgrade if required.
Free disk space threshold value	Specifies the percentage below which disk usage warnings are issued in the Policy Manager Event Viewer. For example, a value of 30% indicates that a warning is issued if only 30% or the disk space below 30% is available.
Free memory threshold value	Specifies the percentage below which RAM usage warnings are issued in the Policy Manager Event Viewer. For example, a value of 30% indicates that a warning is issued if only 30% or RAM below 30% is available.
Profile subnet scan interval	Specify the profile subnet scan interval in hours. The default value is 24 hours.
Database user "appexternal" password	Enter the password for the **appexternal** username for this connection to the database.
Endpoint Context Servers polling interval	Enter the interval in minutes between polling of endpoint context servers. The default interval is 60 minutes.
Login Banner Text	Customize the banner text that appears on the ClearPass login screen and CLI access. You may use the banner to warn users of restrictions to access the website.

Cleanup Intervals

The following figure shows an example of the **Cluster-Wide Parameters - Cleanup Interval** tab followed by parameter definition:

Figure 373: *Cluster-Wide Parameters - Cleanup Interval Tab*

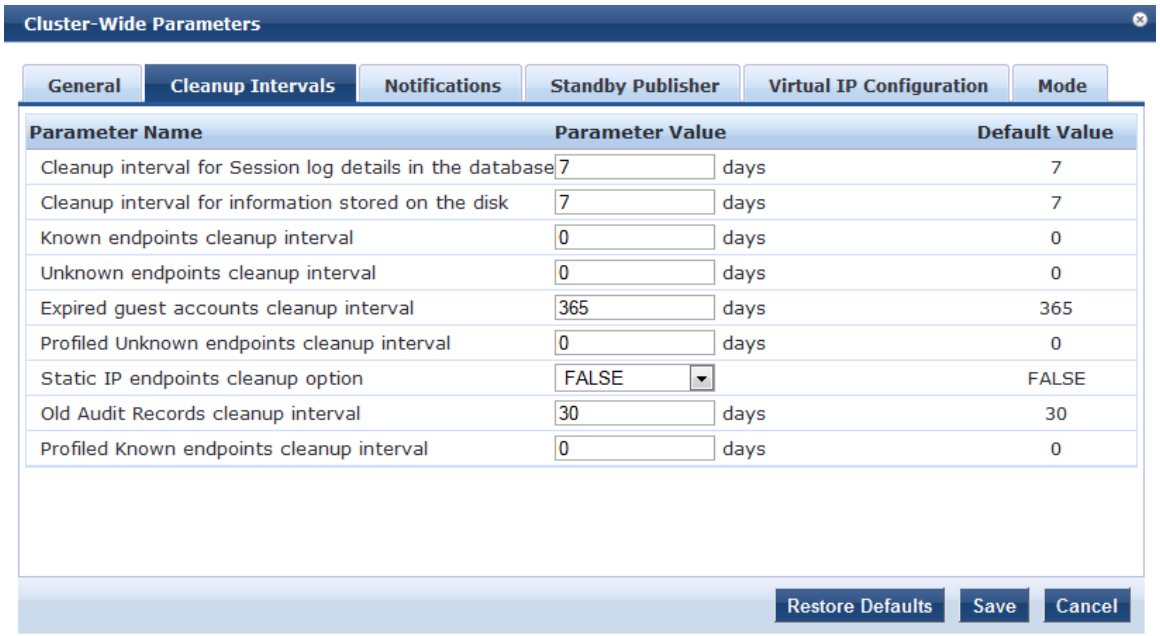


Table 243: *Cluster-Wide Parameters - Cleanup Interval tab Parameters*

Parameter	Description
Cleanup interval for Session log details in the database	Specify the duration in number of days to keep the following data in the Policy Manager DB: • session logs (found on **Access Tracker** page) • event logs (found on **Event Viewer** page) • machine authentication cache The default value is 7 days.
Cleanup interval for information stored on the disk	Specify the duration in number of days to keep log files that are written to the disk. The default value is 7 days.
Known endpoints cleanup interval	Specify the duration in number of days that ClearPass uses to determine when to start deleting known or disabled entries from the Endpoint repository. Known entries are deleted based on the last **Updated At** value for each Endpoint. For example, if this value is 7, then known Endpoints that do not have the **Updated At** value within the last 7 days are deleted. The default value is 0 days. This indicates that no cleanup interval is specified.
Unknown endpoints cleanup interval	Specify the duration in number of days that ClearPass uses to determine when to start deleting unknown entries from the Endpoint repository. Unknown entries are deleted based on the last **Updated At** value for each Endpoint. For example, if this value is 7, then unknown Endpoints that do not have the **Updated At** value within the last 7 days (stale endpoints) are deleted. The default value is 0 days. This indicates that no cleanup interval is specified.
Expired guest	Specify the cleanup interval for expired guest accounts. This indicates the number of days after expiry that the cleanup occurs. 0 specifies no expired guest accounts cleanup interval. The default value is 365 days.

Table 243: *Cluster-Wide Parameters - Cleanup Interval tab Parameters (Continued)*

Parameter	Description
accounts cleanup interval	
Profiled Unknown endpoints cleanup interval	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting profiled unknown entries from the Endpoint repository. Profiled unknown entries are deleted based on their last **Updated At** value for each Endpoint. For example, if this value is 7, then the Profiled Unknown Endpoints that do not have an **Updated At** value within the last 7 days are deleted. The default value is 0.
Static IP endpoints cleanup option	Specify whether to enable the option to cleanup static IP endpoints. You can select TRUE or FALSE. The default options is FALSE.
Old Audit Records cleanup interval	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting old audit records from the **Audit Viewer** page. The default value is 30 days.
Profiled Known endpoints cleanup option	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting profiled known entries from the Endpoint repository. The default value is FALSE.

Notifications

The following figure shows an example of the **Cluster-Wide Parameters - Notifications** tab followed by parameter definition:

Figure 374: *Cluster-Wide Parameters - Notifications Tab*

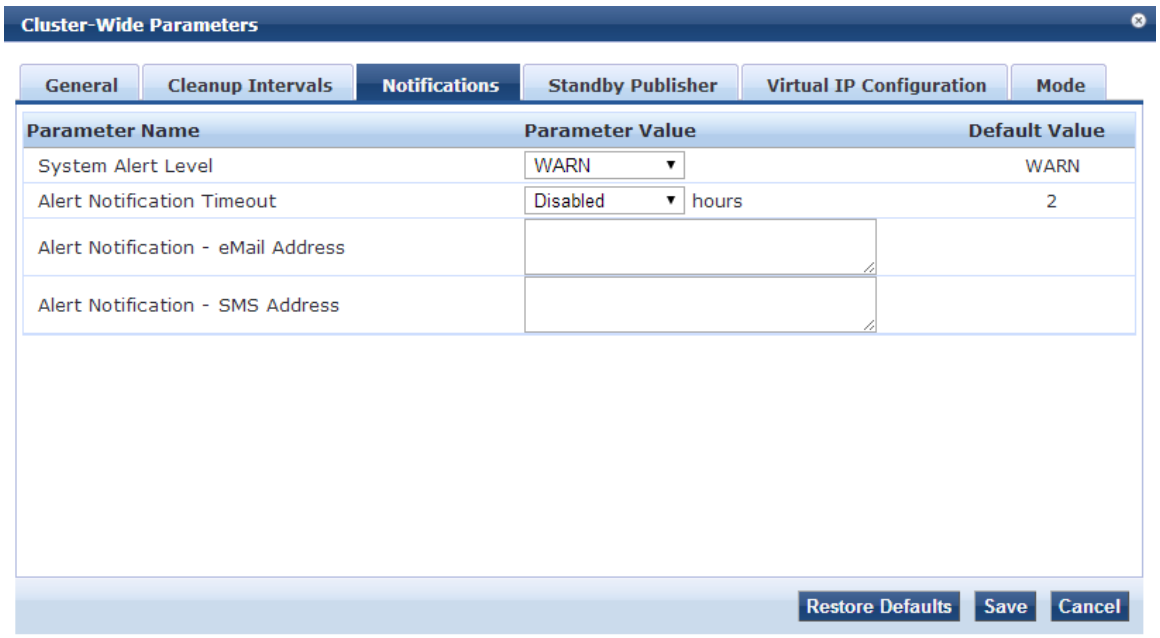


Table 244: *Cluster-Wide Parameters - Notifications tab Parameters*

Parameter	Description
System Alert Level	Specify the alert notifications that are generated for system events logged at this level or higher. Selecting **INFO** generates alerts for INFO, WARN, and ERROR messages. Selecting **WARN** generates alerts for WARN and ERROR messages. Selecting **ERROR** generates alerts for ERROR messages. The default value is WARN.
Alert Notification Timeout	Indicates the timeout in hours that determines how often alert messages are generated and sent out. Selecting the **Disabled** option disables alert generation. The default value is 2 hours.
Alert Notification - eMail Address	Specify comma separated list of email addresses to which alert messages are sent.
Alert Notification - SMS Address	Specify comma separated list of SMS addresses to which alert messages are sent. For example, 40XXX51212, 40XXX53456.

Standby Publisher

The following figure shows an example of the **Cluster-Wide Parameters - Standby Publisher** tab followed by parameter definition:

Figure 375: *Cluster-Wide Parameters - Standby Publisher Tab*

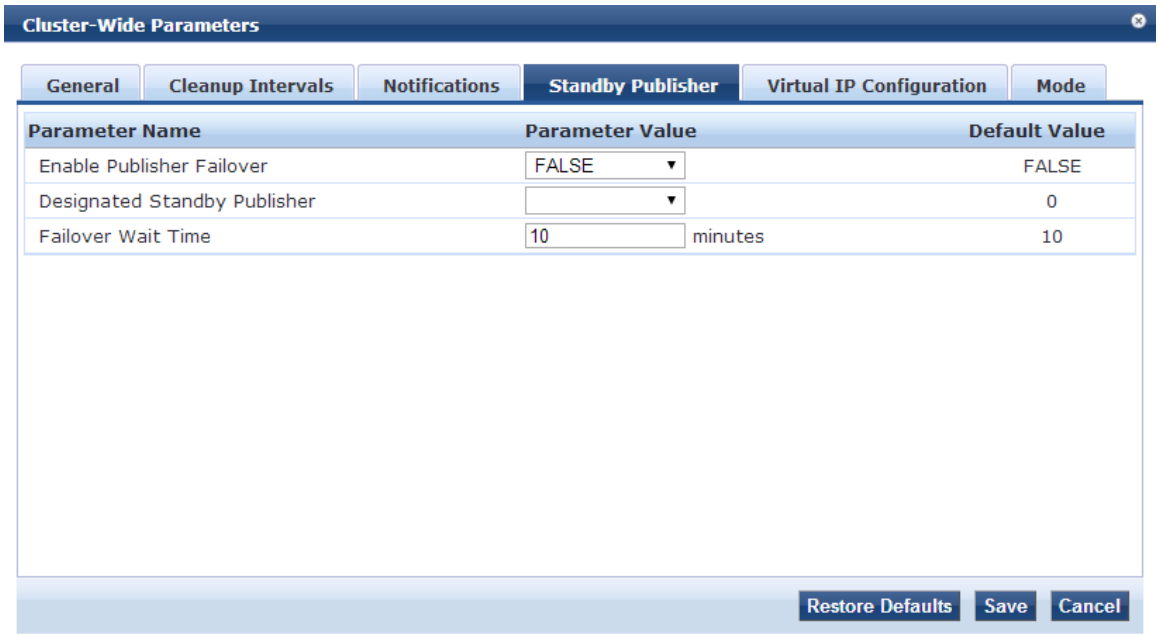


Table 245: *Cluster-Wide Parameters - Standby Publisher tab Parameters*

Parameter	Description
Enable Publisher Failover	Select **TRUE** to authorize a node in a cluster on the system to act as a publisher if the primary publisher fails. The default value is **FALSE**.
Designated Standby Publisher	Select the server in the cluster to act as the standby publisher. The default value is 0. **NOTE:** If the Standby Publisher is on a different subnet from the Publisher, then ensure a reliable connection between the two sub-nets is available to avoid unwanted network segmentation and potential data loss from false failover.
Failover Wait Time	Enter the number of minutes for the secondary node to wait after a primary node failure before it acquires the Virtual IP Address. The default failover wait time is 10 minutes so the secondary node does not take over under the conditions where the primary node is not available temporarily. For example, restart.

Virtual IP Configuration

The following figure displays an example of the **Cluster-Wide Parameters - Virtual IP Configuration** tab followed by parameter definition:

Figure 376: *Cluster-Wide Parameters - Virtual IP Configuration tab*

Table 246: *Cluster-Wide Parameters - Virtual IP Configuration Tab*

Parameter	Description
Failover Wait Time	Enter the number of seconds for the secondary node to wait after primary node failure before it acquires the Virtual IP Address. The default failover wait time is 10 seconds so the secondary node takes over and respond quickly to authentication access and requests.

You can define a virtual IP address by configuring only the primary server and omit the secondary server if required. This can be used to add an additional IP address to the Dell Networking W-ClearPass Policy Manager server without any redundancy.

Mode

The **High Capacity Guest** mode addresses the high volume licensing requirements in the Public Facing Enterprises (PFE) environment, where a large volume of unique endpoints need wireless access. The licensing scheme in the **High Capacity Guest** mode supports high volume of user traffic in the following PFEs where the count of endpoints keep changing everyday:

- Transportation: Airports and Rail Stations
- Hospitality: Hotels, Casinos, and Resorts
- Healthcare: Hospitals, Clinics, and Health Centers
- Retail: Shopping Malls
- Large Public Venues: Stadiums, Convention Centers, and Theaters
- Restaurants and Coffee Shops: Quick-Serve Restaurants

In enterprise deployments, the CPPM licensing accumulates the unique endpoint count for 7 days, which can cause the number of licenses to exceed. To address this license limit in the PFE environment, you can enable the **High Capacity Guest** mode on a cluster. In the **High Capacity Guest** mode, the count of unique endpoints is reset everyday instead of accumulating the count for 7 days. In the **High Capacity Guest** mode, only you can view the supported guest authentication methods such as PAP, CHAP, MSCHAP, EAP_MD5, MAC_AUTH, AUTHORIZE, and EAP_PEAP_in the **Authentication Methods** page.

You cannot enable the RADIUS services with the following authentication methods when the **High Capacity Guest** mode is enabled:

- EAP-FAST
- EAP-GTC
- EAP-MSCHAPv2
- EAP-PEAP
- EAP-TLS
- EAP-TTLS

Licensing

You can add only guest licenses to the **High Capacity Guest** mode and this mode is intended to handle only high volume of guest users in PFE environment. After enabling the **High Capacity Guest** mode, you cannot add enterprise licenses.

If the number of licenses used exceeds the number of licenses purchased, a warning message appears four months after the number is exceeded. The number of licenses used is based on the daily moving average. In the **High Capacity Guest** mode, a maximum of 2x licenses are allowed. For example, if you use the CP-HW-5K platform that supports 5k licenses, a maximum of 10k licenses are allowed in the **High Capacity Guest** mode.

Restrictions

When the **High Capacity Guest** mode is enabled in a cluster, the following restrictions apply:

- Configuration settings cannot be moved from one cluster to another cluster that operates in the **High Capacity Guest** mode.
- Restoring configuration is allowed only with the backup files from the **High Capacity Guest** mode enabled servers.

- The **High Capacity Guest** mode is intended only for high volumes of guest access.
- Use-case related settings other than the **High Capacity Guest** mode are restricted.
- OnGuard and OnBoard access are restricted.
- Default cleanup interval values are reset.
- Only guest application licenses are allowed.

The following figure shows an example of the **Cluster-Wide Parameters - Mode** tab followed by parameter definition:

Figure 377: *Cluster-Wide Parameters - Mode Tab*

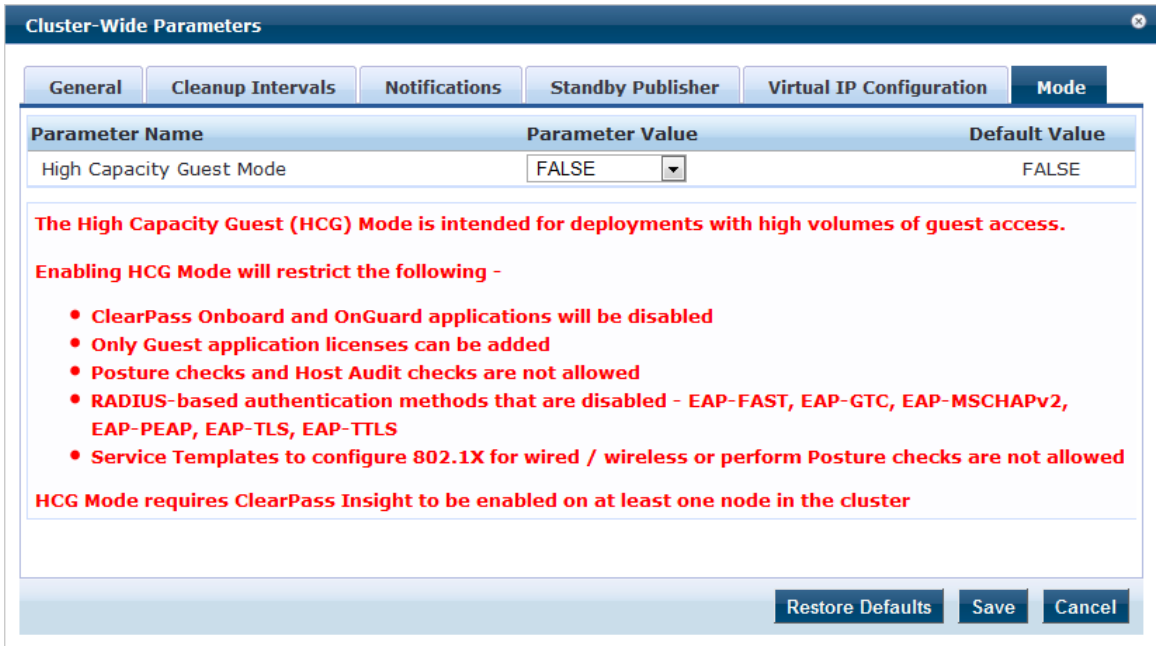


Table 247: *Cluster-Wide Parameters - Mode Tab*

Parameter	Description
High Capacity Guest Mode	Select **TRUE** or FALSE to enable or disable the **High Capacity Guest** mode. By default, the **High Capacity Guest** mode is disabled.

The following table describes the default cleanup interval values when the **High Capacity Guest** mode is enabled:

Table 248: *Cleanup Interval Values in the **High Capacity Guest** Mode*

Parameter	Description
Cleanup interval for Session log details in the database	The default value is 3 days.
Known endpoints cleanup interval	The default value of the known endpoints cleanup interval is 3 days.
Unknown endpoints	The default value of the unknown endpoints cleanup interval is 3 days.

Table 248: *Cleanup Interval Values in the High Capacity Guest Mode (Continued)*

Parameter	Description
cleanup interval	
Expired guest accounts cleanup interval	The default value of the Expired guest accounts cleanup interval is 10 days.
Profiled endpoints cleanup interval	The default value of the Profiled endpoints cleanup interval is 3 days.
Old Audit Records cleanup interval	The default value of the Old Audit Records cleanup interval is 10 days.
Profiled Known endpoints cleanup option	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting profiled known entries from the Endpoint repository. The default value is TRUE.

The following service templates are supported when the High Capacity Guest (HCG) mode is enabled:

- ClearPass Admin Access (Active Directory)
- ClearPass Admin SSO Login (SAML SP Service)
- ClearPass Identity Provider (SAML IdP Service)
- Encrypted Wireless Access via 802.1X Public PEAP method
- Guest Access
- Guest Access - Web Login
- Guest MAC Authentication
- OAuth2 API User Access

The following service types are supported when the HCG mode is enabled:

- MAC Authentication
- RADIUS Authorization
- 1RADIUS Enforcement
- RADIUS Proxy
- Dell Application Authentication
- Dell Application Authorization
- TACACS+ Enforcement
- Web-based Authentication
- Web-based Open Network Access

The following authentication methods are used in service templates in the HCG mode:

- PAP
- CHAP
- MSCHAP
- EAP_MD5
- MAC_AUTH
- AUTHORIZE

- EAP_PEAP_PUBLIC

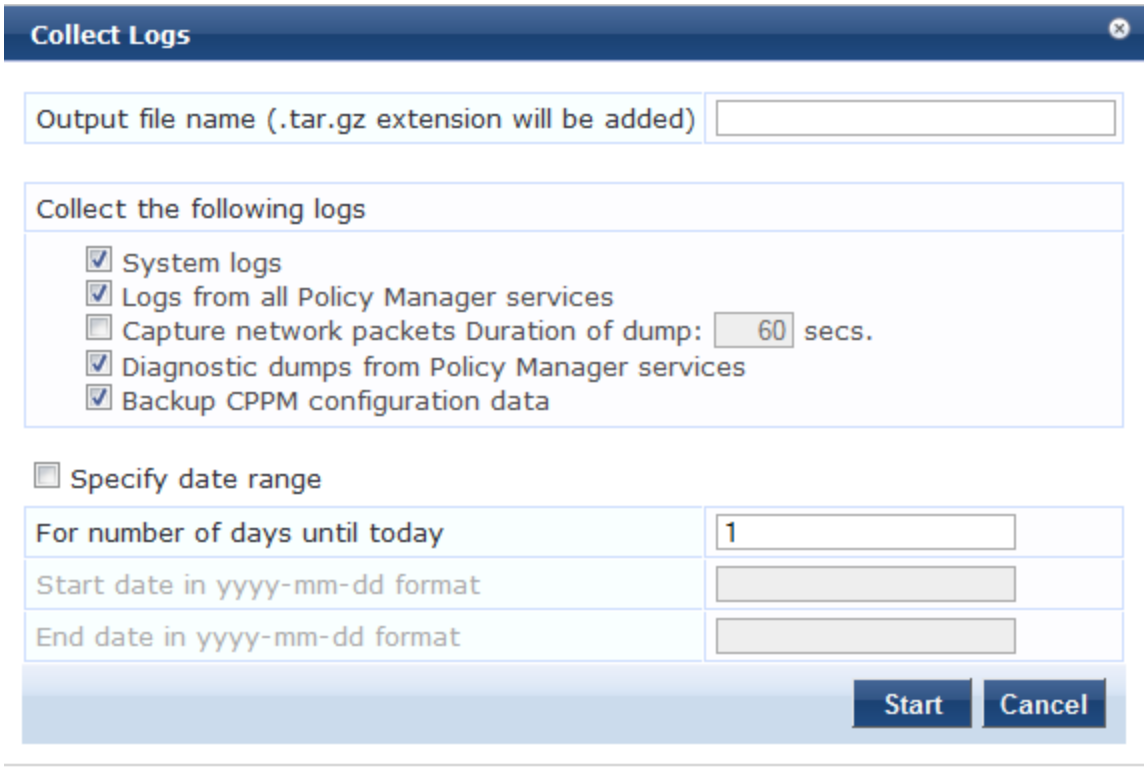
Collect Logs

When you need to review performance or troubleshoot issues in detail, Policy Manager can compile and save transactional and diagnostic data into several log files. These files are saved in Local Shared Folders and can be downloaded to your computer.

To collect logs:

1. Go to **Administration > Server Manager > Server Configuration**,
2. Click **Collect Logs**. The Collect Logs dialog box appears.

Figure 378: *Collect Logs*



3. Enter a filename and add the .tar.gz extension to the filename.
4. Select the types of logging information you want to collect:
   - System Logs
   - Logs from all Policy Manager services
   - Capture network packets for the specified duration. Use this with caution, and use this only when you want to debug a problem. System performance can be severely impacted.
   - Diagnostic dumps from Policy Manager services
   - Backup CPPM Configuration data
5. Enter the time period of the information you want to collect. Either:
   - Enter a number of days. The end of the time period will be defined as the moment you start the collection and the beginning will be 24 hours multiplied by how many days you enter.
   - Click the Specify date range check box, then enter a Start date and End date in yyyy.mm.dd format.
6. Click **Start**. You'll see the progress of the information collection.
7. Click **Close** to finish or click **Download File** to save the log file to your computer.

The following information is useful if you are attempting to open a capture file (.cap or .pcap) using WireShark. First, untar or unzip the file (based on the file extension). When the entire file is extracted, navigate to the PacketCapture folder. Within this folder, you will see a file with a .cap extension. WireShark can be used to open this file and study the network traffic.

Backup

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Back Up** button. This action can also be performed using the "`backup`" CLI command.

Figure 379: *Backup Popup*

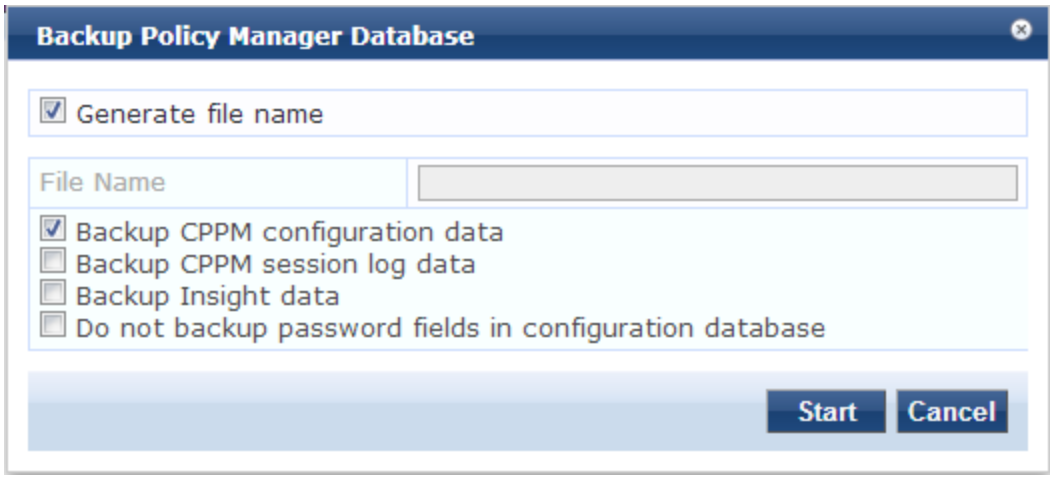


Table 249: *Backup*

Parameter	Description
Generate filename	Enable to have Policy Manager generate a filename; otherwise, specify Filename. Backup files are in the gzipped tar format (tar.gz extension). The backup file is automatically placed in the Shared Local Folder under folder type Backup Files (See Local Shared Folders).
Filename	
Do not backup log database	Select this if you do not want to backup the log database.
Do not backup password fields in configuration database	Select this if you do not want to backup password fields in configuration database.
Backup databases for installed applications	Select this option if you want the backup to include databases for installed applications.

Restore

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Restore** button. This action can also be performed using the "`restore`" CLI command.

Figure 380: *Restore*

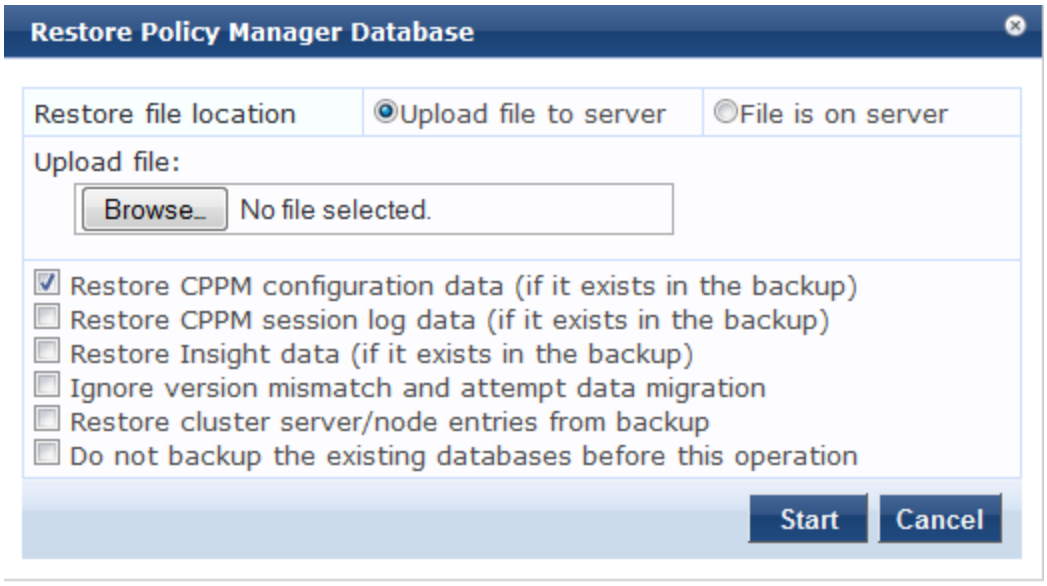


Table 250: *Restore*

Parameter	Description
Restore file location	Select either **Upload file to server** or **File is on server**.
Upload file path	Browse to select name of backup file. **NOTE:** This option is only available only when the **Upload file to server** option is selected.
Shared backup files present on the server	If the files is on a server, select a file from the files in the local shared folders. (See Local Shared Folders.) **NOTE:** This is shown only when the **File on server** option is selected.
Restore CPPM configuration data (if it exists in the backup)	Enable to include an existing configuration data in the restore.
Restore CPPM session log data (if it exists in the backup).	Enable to include the log data in the restore.
Restore Insight data (if it exists in the backup)	Enable to include Insight reporting data in the restore.

Parameter	Description
Ignore version mismatch and attempt data migration	This option must be checked when you are migrating configuration and/or log data from a backup file that was created with a previous compatible version.
Restore cluster server/node entries from backup.	Enable to include the cluster server/node entries in the restore.
Do not backup the existing databases before this operation.	Enable this option if you do not want to backup the existing databases before performing a restore.

Shutdown/Reboot

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Shutdown** or **Reboot** buttons to shutdown or reboot the node.

Drop Subscriber

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Drop Subscriber** button to drop a subscriber from the cluster.

This option is not available in a single node deployment.

Local Shared Folders

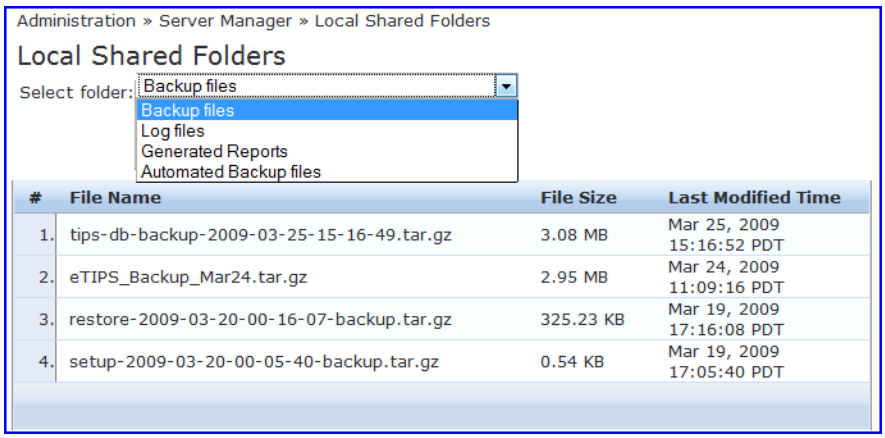
Select the specific folder from the **Select folder** drop-down list. Currently supported folder types are listed below:

- Backup files - Database backup files backed up manually (tar.gz format)
- Log files - Log files backed up via the Collect Logs mechanism (tar.gz format)
- Generated Reports - Historical reports auto-generated on a configured schedule from the Reporting screens (PDF and CSV formats)
- Automated Backup files - Database backup files backed up automatically on a daily basis (tar.gz format)

Select any file in the list to download it to your local machine. The browser download box appears.

For more information, see Collect Logs on page 398

Figure 381: *Local Shared Folders Page*



Licensing

The **Administration > Server Manager > Licensing** page shows all the licenses that have been activated for the entire CPPM cluster. You must have a Dell Networking W-ClearPass Policy Manager base license for every instance of the product. For more information, see:

- Activating an Application License on page 403
- Activating a Server License on page 403
- Adding an Application License on page 404
- Updating an Application License on page 405

On a VM instance of CPPM, the permanent license must be entered.

These licenses are listed in the tables on the **License Summary** tab. There is one entry per server node in the cluster. All application licenses are also listed on the **Applications** tab.

You can add and activate OnGuard, Guest, Onboard, and Enterprise licenses. The **Summary** section shows the number of purchased licenses for Policy Manager, OnGuard, Guest, and Onboard.

Figure 382: *Licensing Page - License Summary tab*

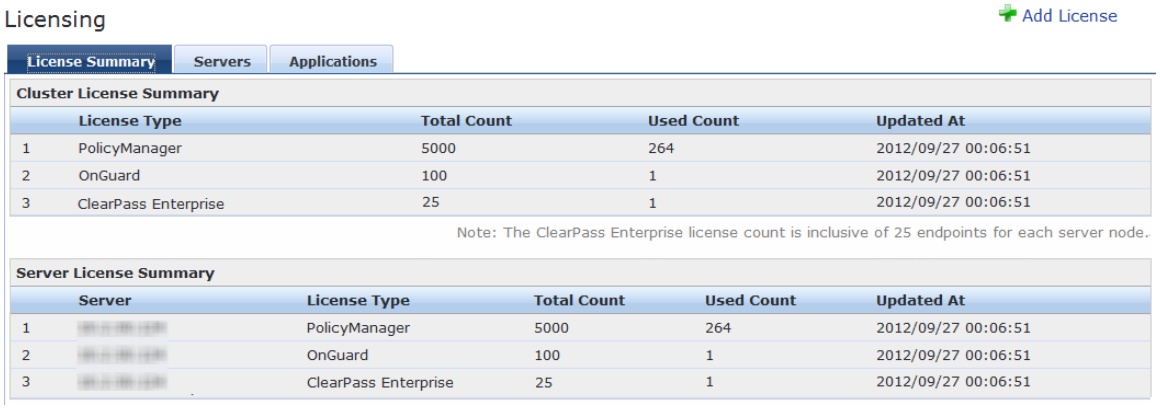
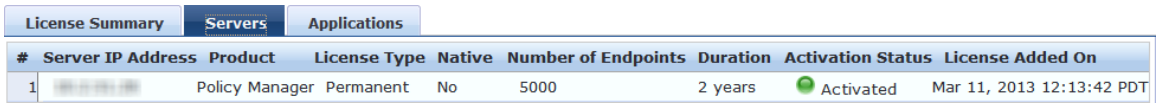


Figure 383: *Licensing Page - Servers tab*



NOTE

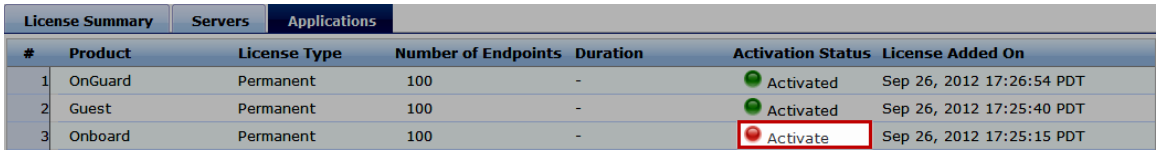
If the number of licenses used exceeds the number purchased, you will see a warning four months after the number is exceeded. The licenses used number is based on the daily moving average.

Activating an Application License

After you add or update an application license, it must be activated. Adding an application license installs an Application tab on the Licensing page.

1. Go to **Administration > Server Manager > Licensing**.
2. Click the **Applications** tab.
3. Click **Activate** in the Activation Status column for the application you want to activate.
4. Click **OK**.

Figure 384: *Application License Page*



Activating a Server License

You need to activate a server license only once, when you first install Policy Manager on a server.

1. Click the **Servers** tab. Servers that are not activated will have a red dot in the Activation Status column.
2. Click **Activate** next to the red dot in the Activation Status column.
3. In the Online Activation section, click **Activate Now**.

If you are not connected to the Internet, follow the instructions in the Offline Activation section. Download an Activation Request Token from the Policy Manager server and email the file to Dell support. You will receive an Activation Key that you can upload.

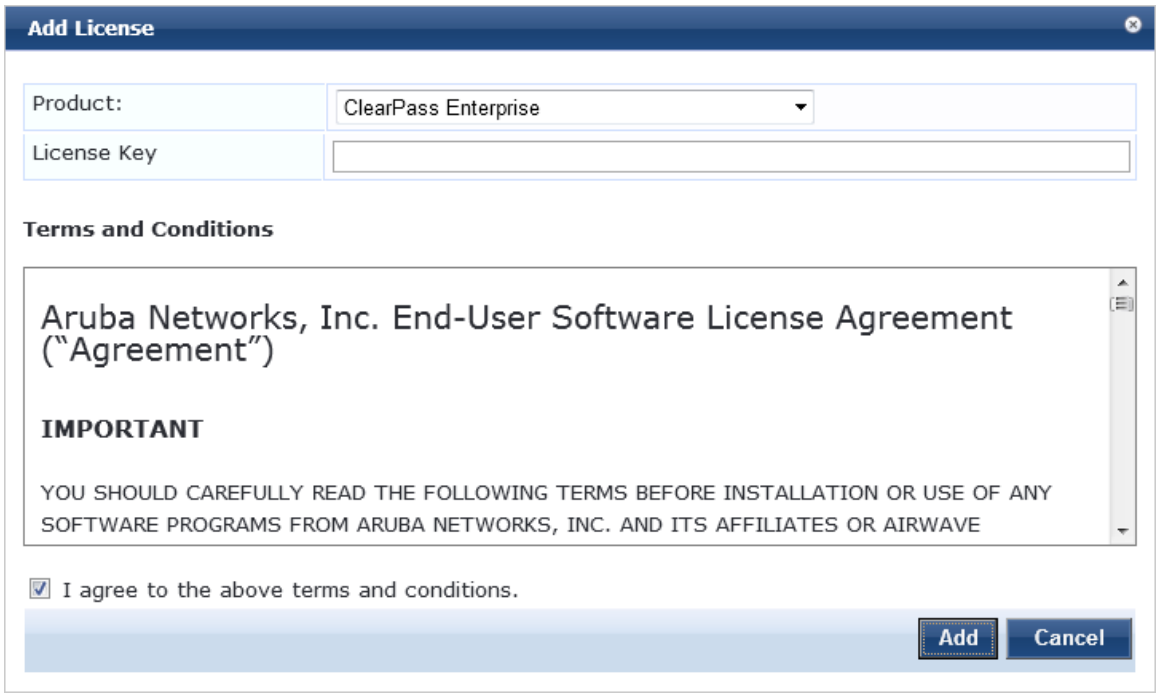
Figure 385: *Online Activation Page*

Adding an Application License

You can add a license by clicking the **Add License** button on the top right portion of this page.

1. Select a product from the drop-down list.
2. Enter the license key for the new license.
3. Read the
4. Terms and Conditions before adding a license.
5. Click the I agree to the above terms and conditions check box.
6. Click the **Add** button.

Figure 386: *Add License Page*



Updating an Application License

Licenses typically require updating after they expire, for example, after the evaluation license expires, or when capacity exceeds its licensed amount. You update an application license by entering a new license key.

1. Go to **Administration > Server Manager > Licensing**.
2. Click the **Applications** tab.
3. Click an application anywhere except in the Activation Status column. The Update License page appears.
4. Enter the **New License Key**.
5. Read the Terms and Conditions, then select the **I agree to the above terms and conditions** check box.
6. Click **Update**.

SNMP Trap Receivers

Policy Manager sends SNMP traps that expose the following server information:

- **System uptime.** Conveys information about how long the system is running.
- **Network interface statistics [up/down].** Provides information if the network interface is up or down.
- **Process monitoring information.** Check for the processes that should be running. Maximum and minimum number of allowed instances. Sends traps if there is a change in value of maximum and minimum numbers.
- **Disk usage.** Check for disk space usage of a partition. The agent can check the amount of available disk space, and make sure it is above a set limit. The value can be in % as well. Sends traps if there is a change in the value.
- **CPU load information.** Check for unreasonable load average values. For example, if 1 minute CPU load average exceeds the configured value [in percentage] then system would send the trap to the configured destination.
- **Memory usage.** Report the memory usage of the system.

For more information, see:

- Adding an SNMP Trap Server on page 407
- Exporting all SNMP Trap Servers on page 407
- Exporting a Single SNMP Trap Server on page 408
- Importing an SNMP Trap Server on page 408

Figure 387: *SNMP Trap Receivers Listing Page*

Adding an SNMP Trap Server

To add a trap server, navigate to **Administration > External Servers > SNMP Trap Receivers** and select the **Add SNMP Trap Server** link.

Figure 388: *Add SNMP Trap Server*

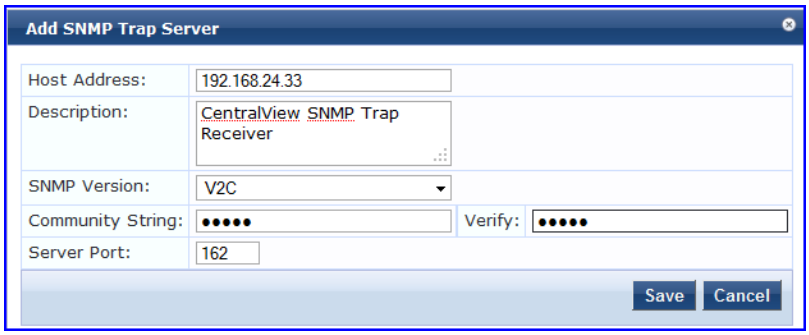


Table 251: *Add SNMP Trap Server fields*

Parameter	Description
Host Address:	Trap destination hostname or ip address. **NOTE:** This server must have an SNMP trap receiver or trap viewer installed.
Description:	Freeform description.
SNMP Version:	V1 or V2C.
Community String /Verify :	Enter and re-enter the community string for sending the traps.
Server Port:	Port number for sending the traps; by default, port 162. **NOTE:** Configure the trap server firewall for traffic on this port.

Exporting all SNMP Trap Servers

To export all SNMP trap servers, navigate to **Administration > External Servers > SNMP Trap Receivers** and select the **Export SNMP Trap Server** link. This link exports all configured SNMP Trap Receivers. Click

Export Trap Server. Enter the XML file name in the **Save As** dialog.

Exporting a Single SNMP Trap Server

To export a single SNMP trap server, navigate to **Administration > External Servers > SNMP Trap Receivers**. Select the SNMP Trap server that you want to export and click the **Export** button in the lower-right corner of the page. Enter the name of the XML file **Save As** dialog.

Importing an SNMP Trap Server

To import a trap server, navigate to **Administration > External Servers > SNMP Trap Receivers** and select the **Import SNMP Trap Server** link.

Figure 389: *Import SNMP Trap Server*

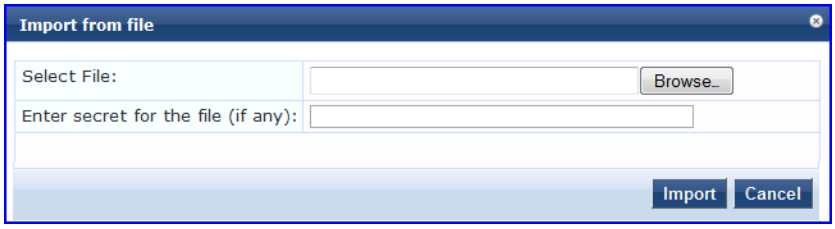


Table 252: *Import SNMP Trap Server*

Parameter	Description
Select File:	Browse to the SNMP Trap Server configuration file to be imported.
Enter secret for the file (if any):	If the file was exported with a secret key for encryption, enter the same key here.

Syslog Targets

Dell Networking W-ClearPass Policy Manager can export session data (see Access Tracker on page 17), audit records (see Audit Viewer on page 51) and event records (see Event Viewer on page 56). This information can be sent to one or more syslog targets (servers). You configure syslog targets from this page.

The Policy Manager Syslog Targets page at **Administration > External Servers > Syslog Targets** provides the following interfaces for configuration:

- Add Syslog Target on page 409
- Import Syslog Target on page 410
- Export Syslog Target on page 410
- Export on page 410

Figure 390: *Syslog Target Listing Page*

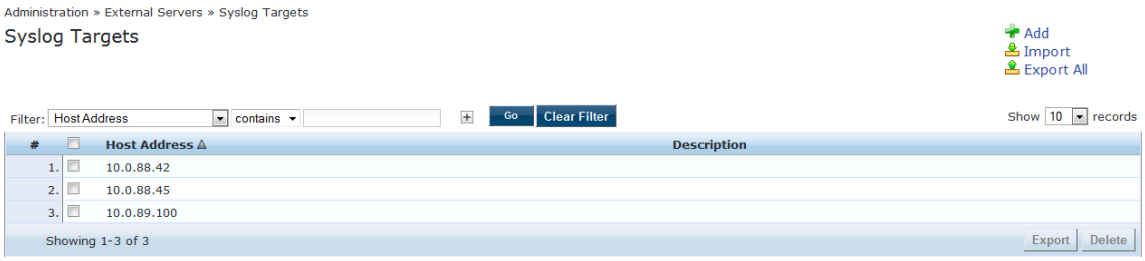


Table 253: *Syslog Target Configuration*

Parameter	Description
Add	Opens the **Add Syslog Target** popup.
Import	Opens the **Import Syslog Target** popup.
Export All	Opens the **Export Syslog Target** popup.
Export	Opens the **Export** popup.
Delete	To delete a Syslog Target, select it (check box at left) and click **Delete**.

Add Syslog Target

To add a Syslog Target, navigate to **Administration > External Servers > Syslog Targets** and select **Add**.

Figure 391: *Add Syslog Target*

Table 254: *Add Syslog Target*

Parameter	Description
Host Address	Syslog server hostname or IP address.
Description	Freeform description.
Protocol	Select from: • UDP: To reduce overhead and latency. • TCP: To provide error checking and packet delivery validation.
Server Port	Port number for sending the syslog messages; by default, port 514.

Import Syslog Target

Navigate to **Administration > External Servers > Syslog Targets** and select **Import**.

Figure 392: *Import Syslog Target*

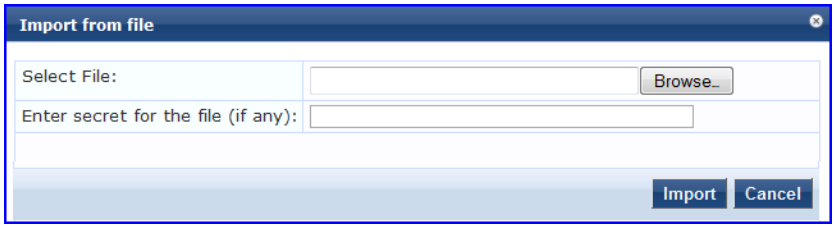


Table 255: *Import from file*

Parameter	Description
Select File	Browse to the Syslog Target configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.
Import/Cancel	Click **Import** to commit, or **Cancel** to dismiss the popup.

Export Syslog Target

Navigate to **Administration > External Servers > Syslog Targets** and select the **Export All** link.

The **Export All** link exports all configured syslog targets. Click **Export Syslog Target**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the Syslog Target configuration.

Export

Navigate to **Administration > External Servers** and select the **Syslog Targets** button.

To export a syslog target, select it (check box at left) and click **Export.** Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Syslog Export Filters

Policy Manager can export session data (see Access Tracker on page 17), audit records (see Audit Viewer on page 51) and event records (see Event Viewer on page 56).

You configure Syslog Export Filters to tell Policy Manager where to send this information, and what kind of information should be sent through Data Filters.

For information, see:

- Adding a Syslog Export Filter (Filter and Columns tab) on page 412
- Adding a Syslog Export Filter (General tab) on page 414
- Adding a Syslog Export Filter (Summary tab) on page 416
- Import Syslog Filter on page 411
- Export Syslog Filter on page 412
- Export on page 412

Figure 393: *Syslog Export Filters Page*

Table 256: *Syslog Export Filters Page Parameters*

Parameter	Description
Add	Opens **Add Syslog Filter** page (**Administration > External Servers > Syslog Export Filters > Add**).
Import	Opens **Import Syslog Filter** popup.
Export All	Opens **Export Syslog Filter** popup.
Enable/Disable	Click the toggle button **Enable/Disable** to enable or disable the syslog filter.
Export	Opens **Export** popup.
Delete	**To delete a Syslog Filter**, select it (check box at left) and click **Delete.**

Import Syslog Filter

Navigate to **Administration > External Servers > Syslog Filters > Import**.

Figure 394: *Import Syslog Filter*

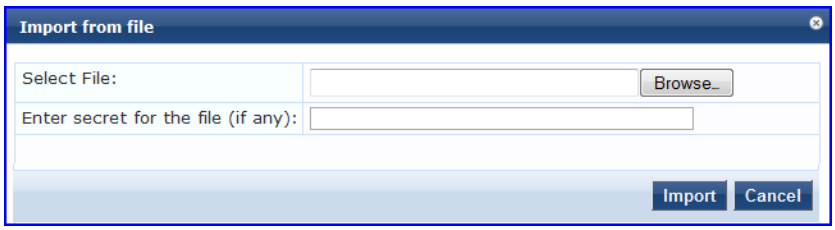


Table 257: *Import from File*

Parameter	Description
Select File	Browse to the Syslog Filter configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.
Import/Cancel	Click **Import** to commit, or **Cancel** to dismiss the popup.

Export Syslog Filter

Navigate to **Administration > External Servers > Syslog Filters** and select the **Export All** link.

The **Export All** link exports all configured syslog filters. Click **Export Syslog Filter**. Your browser will display the Save As dialog. Enter the name of the XML file to contain the Syslog Filer configuration.

Export

Navigate to **Administration > External Servers > Syslog Filters** and select **Export** button.

To export a syslog filter, select it (check box at left) and click **Export**. Your browser will display its normal **Save As** dialog in which to enter the name of the XML file to contain the export.

Adding a Syslog Export Filter (Filter and Columns tab)

This tab provides two methods for configuring data filters and is only visible if you selected **Session Logs** or **Insight Logs** as the export template in the **General** tab.

Session Logs

This section describes the options if you select **Session Logs** as the export template:

Option 1 allows you to choose from pre-defined field groups and to select columns based on the Type.

Option 2 allows you to create a custom SQL query. You can view a sample template for the custom SQL by clicking the link below the text entry field.

It is recommended that users who choose Option 2: the Custom SQL option to contact Support. Support can assist you with entering the correct information in this template.

The following figure shows an example of the **Add Syslog Filters - Filter and Columns** tab with **Session Logs** as the export template followed by parameter definition:

Figure 395: *Add Syslog Filters - Filter and Columns tab (Session Logs)*

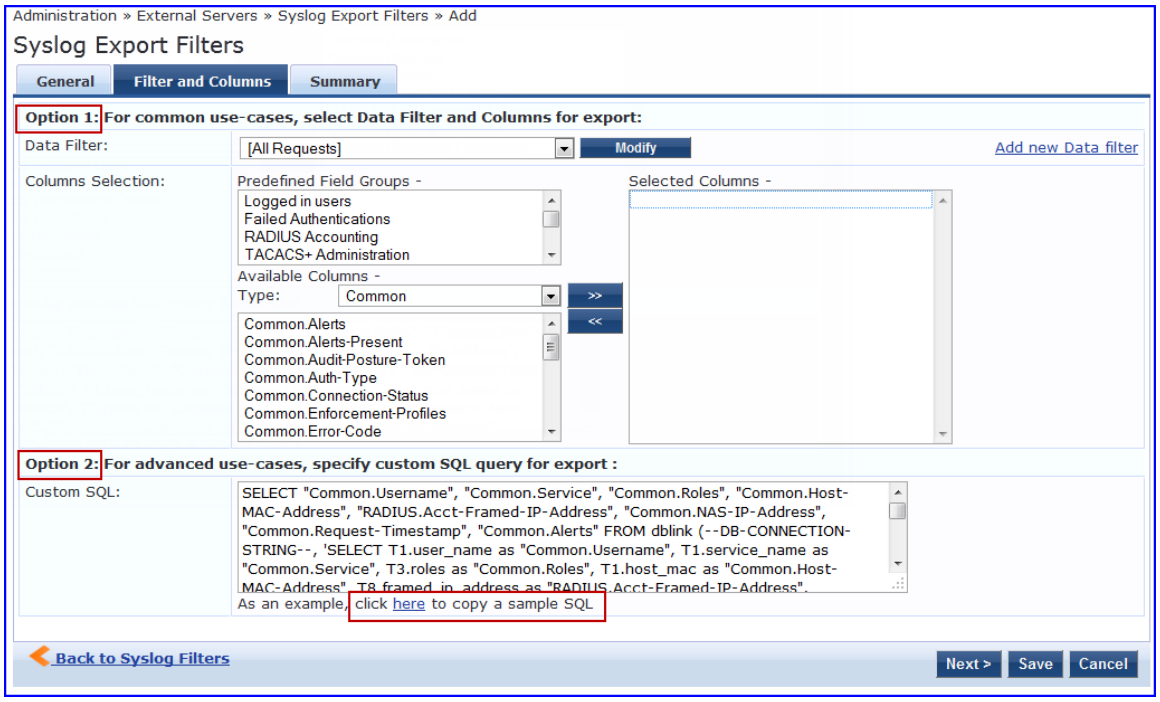


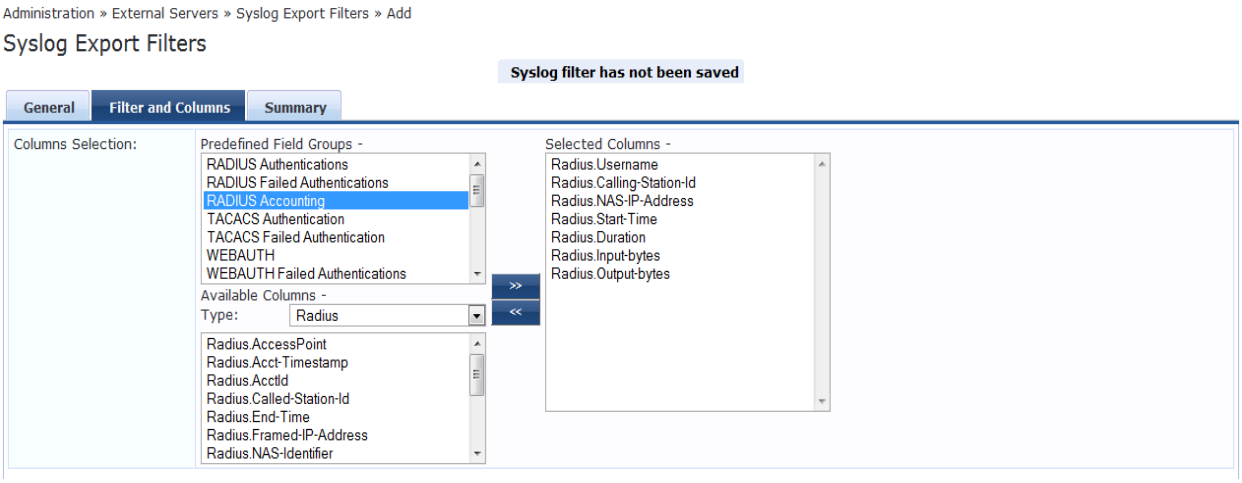
Table 258: *Add Syslog Filters (Filter and Columns tab)*

Parameter	Description
Data Filter	Specify the data filter. The data filter limits the type of records sent to syslog target.
Modify/ Add new Data filter	Modify the selected data filter, or add a new one. Specifying a data filter filters the rows that are sent to the syslog target. You may also select the columns that are sent to the syslog target.
Columns Selection	This helps to limit the type of columns sent to syslog. There are predefined field groups, which are column names grouped together for quick addition to the report. For example, *Logged in users* field group seven predefined columns. When you click *Logged in users* the seven columns automatically appear in the **Selected Columns** list. Additional fields are available to add to the reports. You can select the type of attributes (which are the different table columns available in the session database) from the **Available Columns Type** drop down list. Policy Manager populates these column names by extracting the column names from existing sessions in the session database. After you select a column from the **Available Columns Type**, the columns appear in the box below. From here you can click **>>** to add the selected column to the **Selected Columns** list. Click **<<** to remove a column from the **Selected Columns** list.

Insight Logs

This section describes the options if you select **Insight Logs** as the export template in the **General** tab. The **Insight Logs** option is enabled only if the **Enable Insight** check box is selected from the **Administration** > **Server Manager** > **Server Configuration** > **System** tab. The following figure shows an example of the **Add Syslog Filters - Filter and Columns** tab followed by parameter definition:

Figure 396: *Add Syslog Filters - Filter and Columns tab (Insight Logs)*



NOTE

The data collection interval for Insight logs is - 4 to - 2 minutes from the current time.

Table 259: *Add Syslog Filters - Filter and Columns tab (Insight Logs)*

Parameter	Description
Columns Selection	Determine the group of reports that you want to include in syslog filters in the **Columns Selection** field, This helps to limit the type of columns sent to syslog filters. **NOTE:** You can add only the Insight reports that are already created in Insight. You cannot create a new data filter for Insight logs.
Predefined Field Groups	Select the predefined Insight reports that are grouped for a quick addition.
Available Columns	Displays the reports specific to the group selected in the **Columns Selection** field.
Type	Select the type of records from the drop-down list to filter the records. This provides additional filtering option based on the type of records.
Selected Columns	After you select a column from the **Available Columns**, click **>>** to add the selected column to the **Selected Columns** list. Click **<<** to remove a column from the **Selected Columns** list.

Adding a Syslog Export Filter (General tab)

This topic describes the parameters on the **General** tab of the **Add Syslog Export Filters** page.

NOTE

The **Filter and Columns** tab shown in the figure below is only visible if you select Active sessions as the **Data Filter** type (see Adding a Syslog Export Filter (Filter and Columns tab) on page 412).

Figure 397: *Add Syslog Export Filters (General tab)*

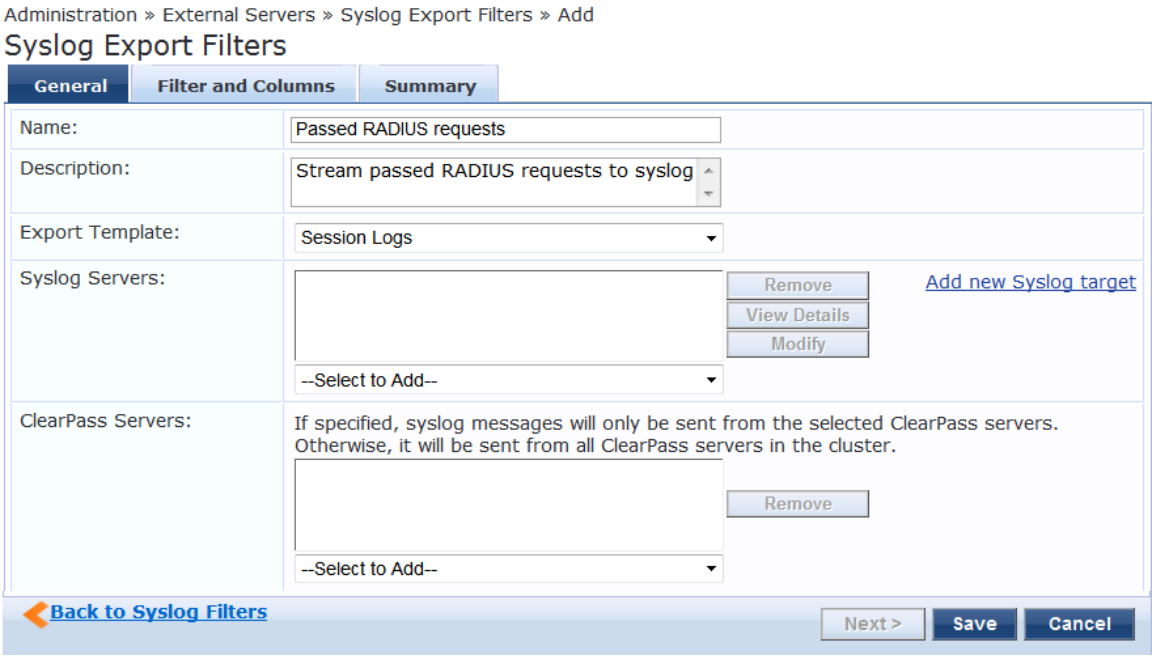


Table 260: *Syslog Export Filters General tab Parameters*

Parameter	Description
Name/Description	Enter name and description in the respective text fields.
Export Template	You can select from the following options: • Audit Records • Insight Logs • Session Logs • System Events
Syslog Servers	Syslog servers define the receivers of syslog messages sent by servers in the ClearPass cluster. • To add a syslog server, select it from the drop-down list. • To view details about a syslog server, select it, then select **View Details**. • To change details about a syslog server, select it, then select **Modify**. For information about syslog server details, see Add Syslog Target • To remove a syslog server (from receiving syslog messages), select it, then select **Remove**. If the syslog server does not appear in the drop-down list, you can click **Add new Syslog target**. See Add Syslog Target for more information.
ClearPass Servers	You can designate syslog messages be sent from exactly one server in the ClearPass cluster or from all of them. • To select the one server, select it from the drop-down list. • To remove the server, select it, then select **Remove**. When no servers are listed, syslog messages are sent from all servers in the cluster.

Adding a Syslog Export Filter (Summary tab)

This topic describes the parameters on the Summary tab of the Add Syslog Export Filters page.

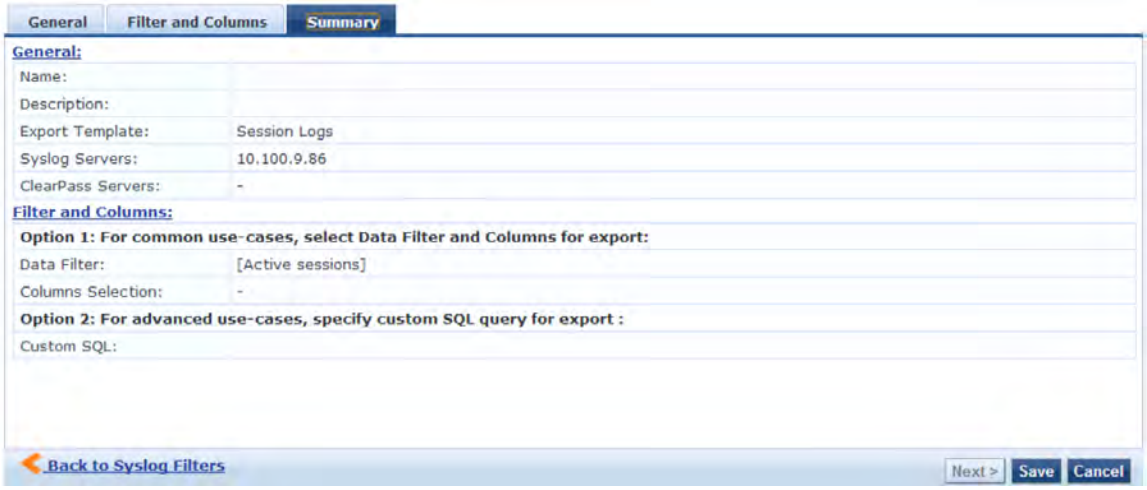


Table 261: *Syslog Export Filters Summary tab Parameters*

Parameter	Description
General	
Name	Name created for the new filter.
Description	Description of the new syslog export filter.
Export Template	The template selected as the export template.
Syslog Servers	IP address of the syslog server selected during configuration.
ClearPass Servers	IP address of the ClearPass Servers selected during configuration.
Filter and Columns	
Data Filter	Displays the data filter selected when configuring Option 1 on the Filter and Columns tab.
Columns Selection	Displays the predefined Field Groups and Available Columns type selected during configuration of Option 1: For common use-cases.
Custom SQL	Displays the SQL query selected during configuration of Option 2: For advanced use-cases.

Messaging Setup

The **Messaging Setup** (**Administration > Server Manager > Messaging Setup**) page provides the interface for configuring the Simple Mail Transfer Protocol (SMTP) server for email and SMS notifications. Click

the **Configure SMS Gateway** link at the top right to configure a new SMS gateway using the ClearPass Guest portal. The following figure shows an example of the **SMTP Server** page followed by parameter definition:

Figure 398: *Messaging Setup SMTP Server Page*

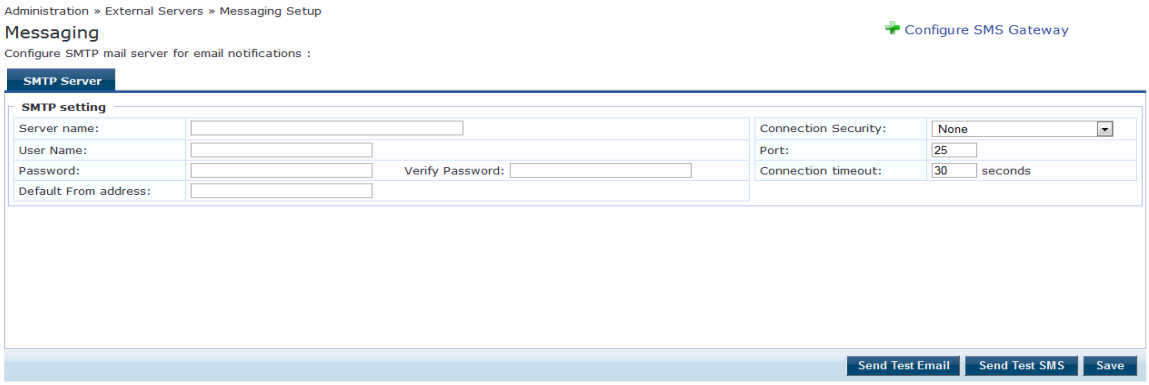
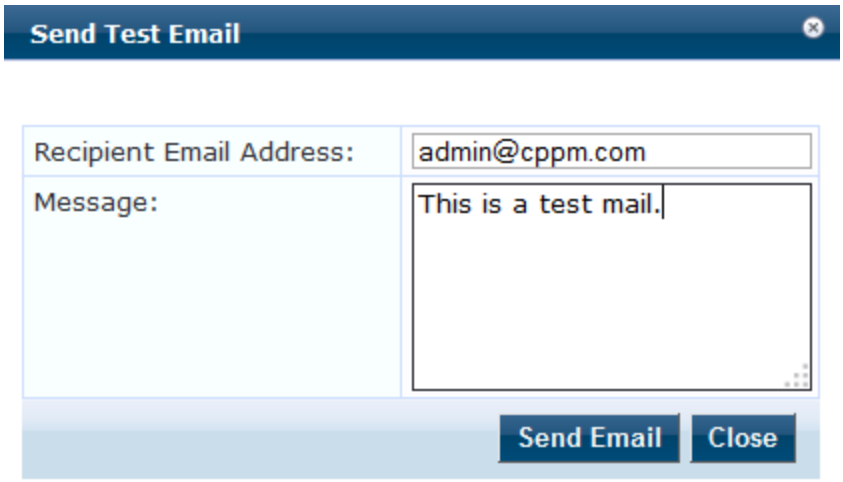


Table 262: *Messaging Setup SMTP Server Page Parameters*

Parameter	Description
Server name	Specify the Fully Qualified Domain Name (FQDN) or the IP address of the server.
Username	Enter the username if your email server requires authentication for sending email messages.
Password	Enter the password for the specified username.
Default From address	Specify the email address that needs to be displayed as sender's address in the message.
Connection Security	Specify the secure **SSL** or **TLS** connection from the drop-down list to establish the communication with the server.
Port	Specify the TCP port number that the SNMP server listens on. The default port is 25.
Connection timeout	Enter the timeout value for connection to the server (in seconds). The default value is 30 seconds.

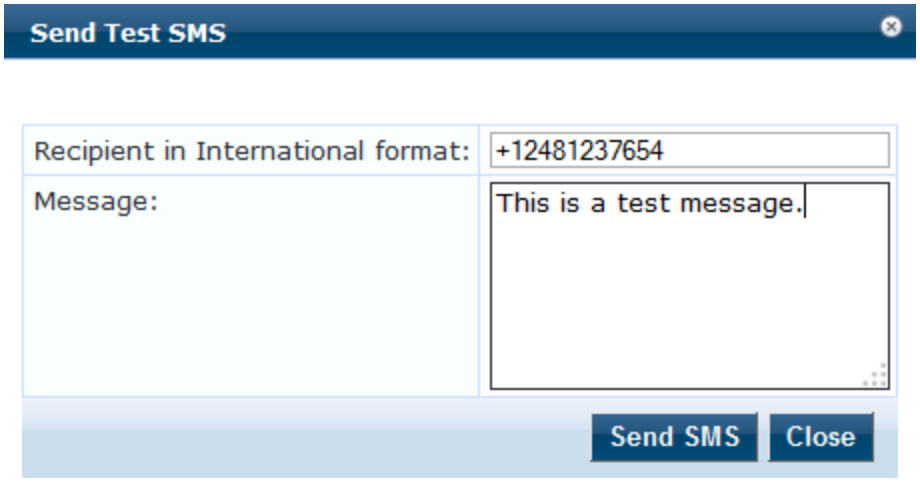
Click the **Send Test Email** button to send the test mail to the preferred email address. The following figure shows an example of the **Send Test Email** page with the options to specify the recipient's address and the message to be sent:

Figure 399: *Send Test Email Page*



Click the **Send Test SMS** button to send the test SMS message to the preferred mobile phone number. The following figure shows an example of the **Send Test SMS** page with the options to specify the recipient's mobile phone number and the message to be sent:

Figure 400: *Send Test SMS page*



The recipient's mobile number must be in international format consists of a + sign, then a country code followed by the mobile phone number (without the first '0' of the number). The format is '+', country code, followed by network prefix without the leading '0'. Number must be entered without spaces and only numerals are allowed. For example, the US number (248) 123-7654 is entered as +12481237654. The number 1 is the country code for the US.

Endpoint Context Servers

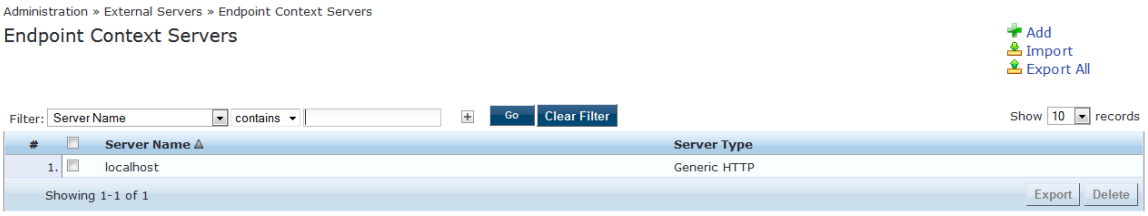
Policy Manager provides the ability to collect endpoint profile information from different types of Dell W-Series IAPs and RAPs via Aruba Activate. Policy Manager supports Aruba Activate, Palo Alto Networks Firewall and Panorama, and MDM (Mobile Device Management) from Airwatch, JAMF, MaaS360, MobileIron, SOTI, and XenMobile.

The mobile device management platforms run on MDM servers. These servers provision mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services.

Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Endpoint context servers are listed and managed at **Administration > External Servers > Endpoint Context Servers**.

Figure 401: *Endpoint Context Servers Page*



Adding an Endpoint Context Server

1. Go to **Administration > External Servers > Endpoint Context Servers**.
2. Click **Add Context Server**.
3. Select a server type. The server type you select determines the configuration parameters you will enter. For example, if you select the "airwatch" Server Type, you must enter an API Key during configuration.

Modify an endpoint context server

1. Go to **Administration > External Servers > Endpoint Context Servers**.
2. Click the server name.
3. Make any desired changes. See Endpoint Context Servers on page 418 for more information.
4. Click **Save**.

Delete an endpoint context server

Deleting an endpoint context server just removes its configuration information from Policy Manager. If you think you might want to add it again, export it before you delete it and save the configuration so you can just import it at a later date.

1. Go to **Administration > External Servers > Endpoint Context Servers**.
2. Click the check box next to the server name.
3. Click **Delete**.
4. Click **Yes**.

Adding an AirWatch Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 402: *Add AirWatch Server tab*

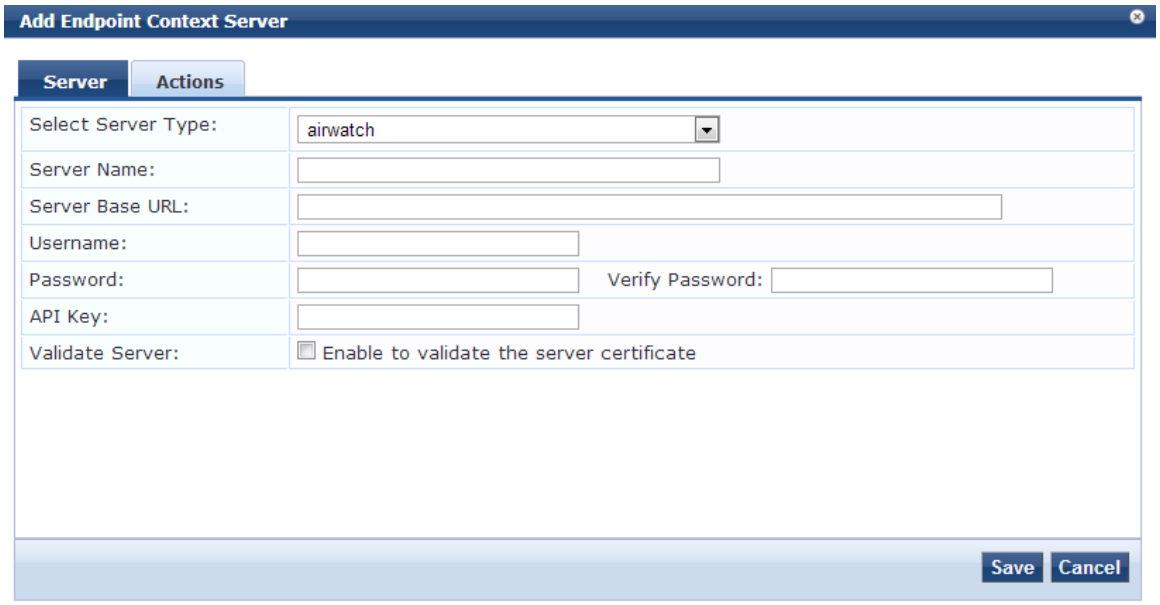


Table 263: *Add Air Watch Server tab Parameters*

Parameter	Description
Select Server Type:	Add AirWatch.
Server Name:	Enter a valid server name. You can enter an IP address or domain name.
Server Base URL:	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username:	Enter the username.
Password:	Enter and verify the password.
Verify Password:	
API Key:	Enter the API key that was provided by the vendor.
Validate Server:	Click to enable validation of the server certificate.

Figure 403: *Add AirWatch Actions tab*

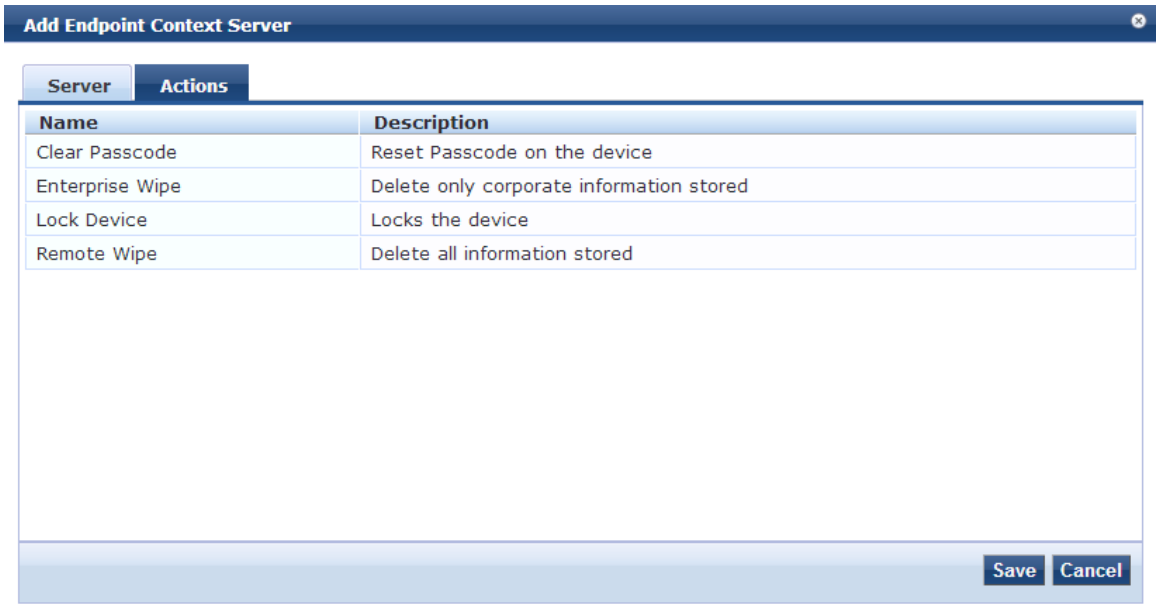


Table 264: *Add AirWatch Actions tab Parameters*

Parameter	Description
Clear Passcode	Reset passcode on the device.
Enterprise Wipe	Deletes only stored corporate information.
Lock Device	Locks the associated device.
Remote Wipe	Deletes all stored information.

Adding an AirWave Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 404: *Add AirWave Endpoint Context Server tab*

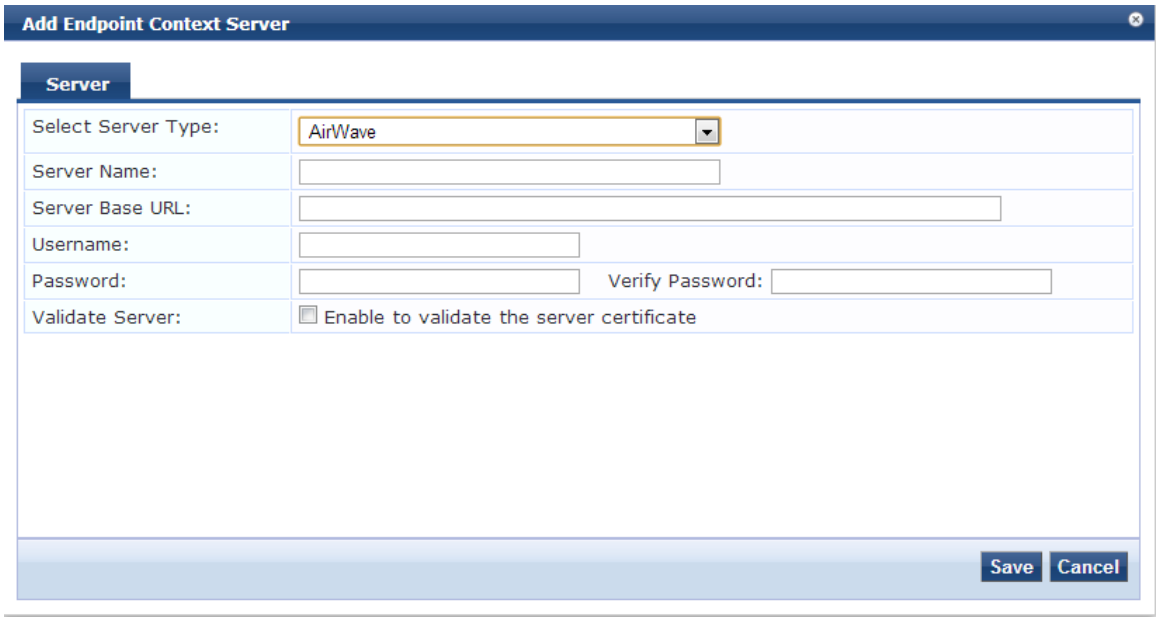


Table 265: *Add AirrWave Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	AirWave
Server Name:	Enter a valid server name. You can enter an IP address or domain name.
Server Base URL:	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username:	Enter the username.
Password:	Enter the password.
Verify Password:	Verify the password.
Validate Server:	Click to enable validation of the server certificate.

Adding an Aruba Activate Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 405: *Add Aruba Activate Endpoint Context Server tab*

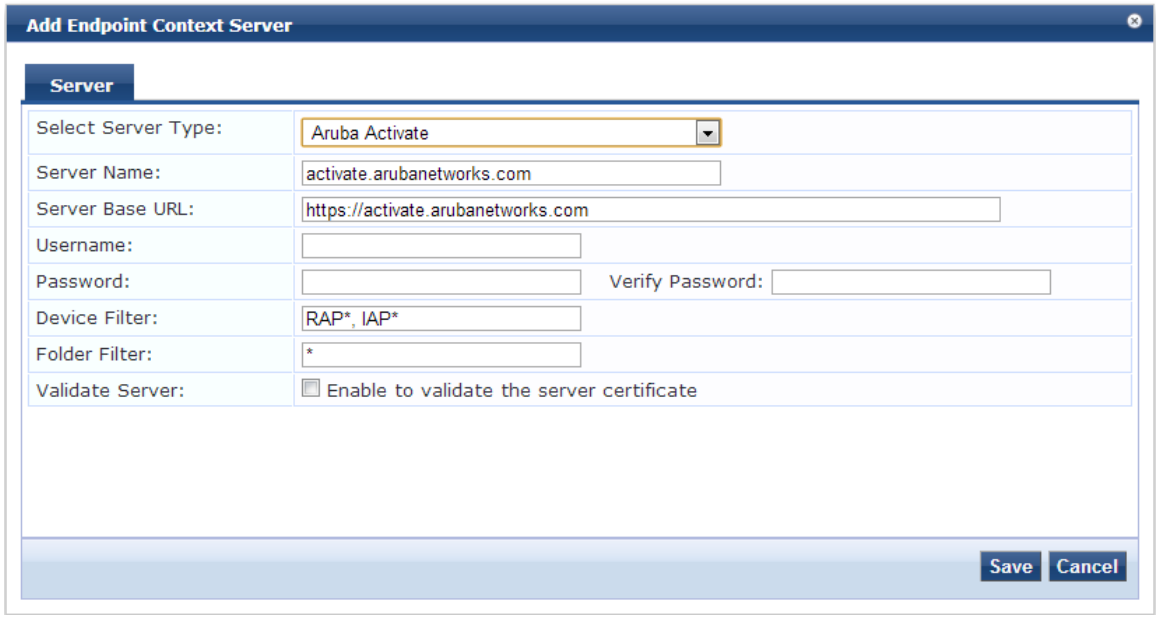


Table 266: *Add Aruba Activate Endpoint Context Server tab Parameter*

Parameter	Description
Select Server Type:	Aruba Activate
Server Name:	Enter a valid server name. You can enter an IP address or domain name.
Server Base URL:	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username:	Enter the username.
Password:	Enter and verify the password.
Verify Password:	Enter the API key that was provided by the vendor.
Device Filter:	This field is populated with a default regex to retrieve only the information of RAP and IAP information.
Folder Filter:	This field is set to "*" by default.
Validate Server:	Click to enable validation of the server certificate.

Adding a ClearPass Cloud Proxy Endpoint Context Server

The Cloud Proxy is a virtual instance configured in the cloud. This multi-tenant and single instance serves multiple customers having many CPPM nodes. Once configured, the CPPM server establishes a Cloud Tunnel to the Cloud Proxy instance given the credentials and Domain. The Domain is required as an identifier to indicate which Cloud Tunnel is applicable for which customer. Individual CPPM nodes in the cluster can be selected to establish the Cloud Tunnel, rather than all nodes in the CPPM cluster.

Figure 406: *Add ClearPass Cloud Proxy Endpoint Context Server tab*

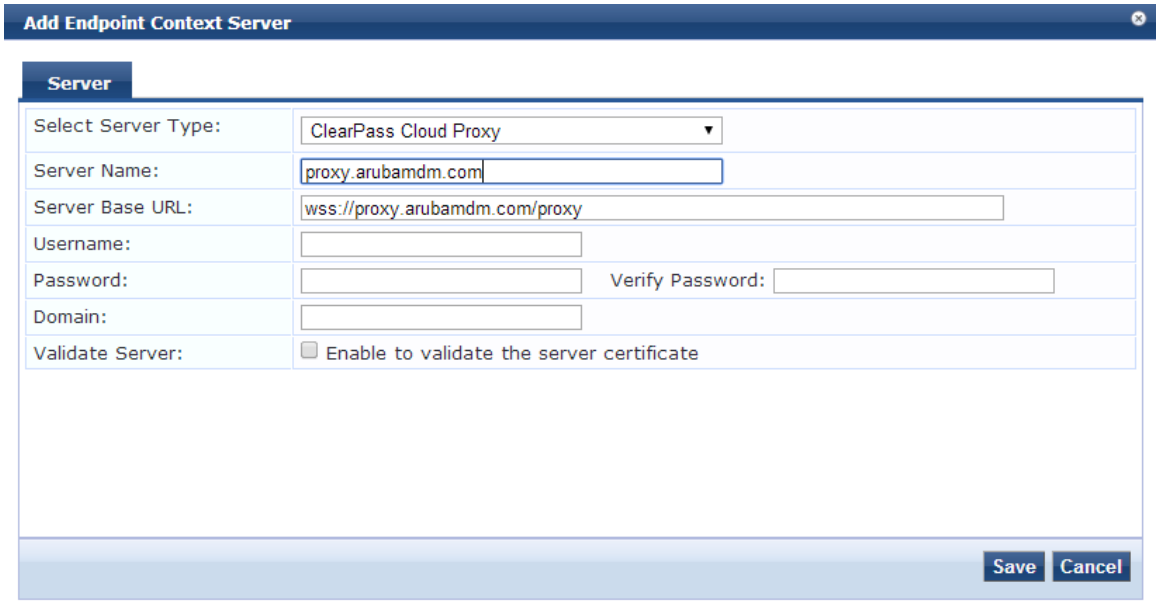


Table 267: *Add ClearPass Cloud Proxy Endpoint Context Server Parameters*

Parameter	Description
Select Server Type	ClearPass Cloud Proxy
Server Name	The hostname of the cloud instance that will proxy all requests directed to the CPPM server in the enterprise.
Server Base URL	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Username/Password based authentication is used when you setup a cloud tunnel from CPPM to the Cloud Proxy instance. Enter the username.
Password	Enter the password.

Verify Password	Verify the password.
Domain	An identifier used to determine the specific Cloud Tunnel to which the request must be sent by the Cloud Proxy.
Validate Server	Click to enable validation of the server certificate.

Adding a Generic HTTP Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 407: *Add Generic HTTP Endpoint Context Server Server tab*

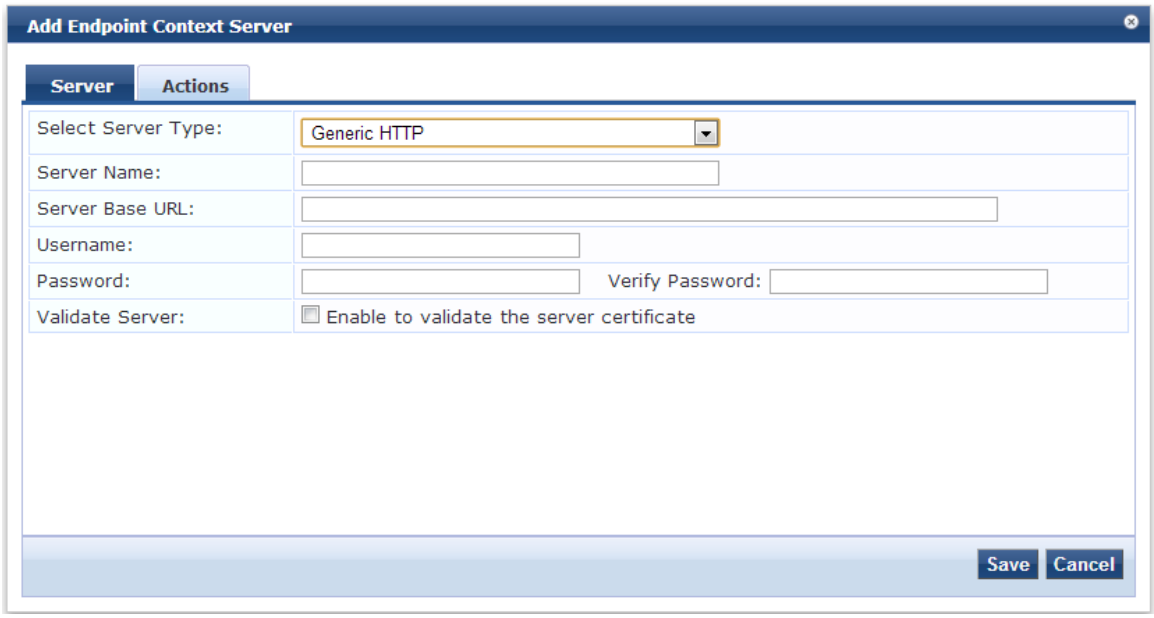


Table 268: *Add Generic HTTP Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	Generic HTTP
Server Name:	Enter a valid server name. You can enter an IP address or domain name.
Server Base URL:	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username:	Enter the username.

Table 268: *Add Generic HTTP Endpoint Context Server tab Parameters (Continued)*

Parameter	Description
Password:	Enter and verify the password.
Verify Password:	
Validate Server:	Click to enable validation of the server certificate.

Figure 408: *Add Generic HTTP Endpoint Context Server Actions tab*

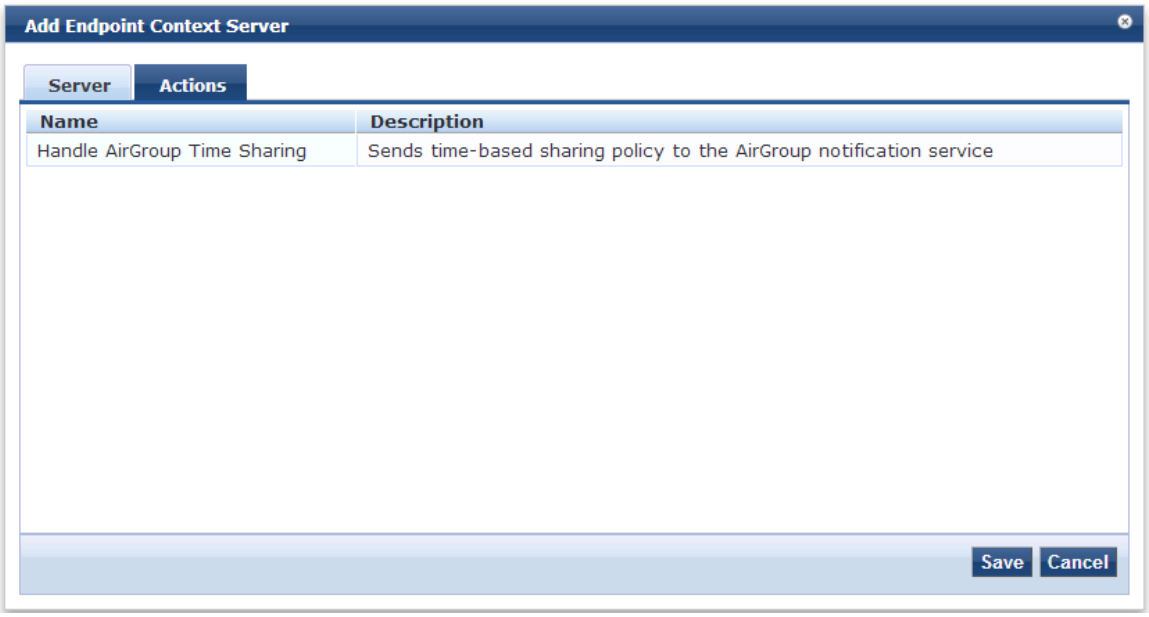


Table 269: *Add Generic HTTP Endpoint Context Server Actions tab Parameters*

Parameter	Description
Handle AirGroup Time Sharing	Sends time-based sharing policy to the AirGroup notification service

Adding a JAMF Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 409: *Add JAMF Endpoint Context Server tab*

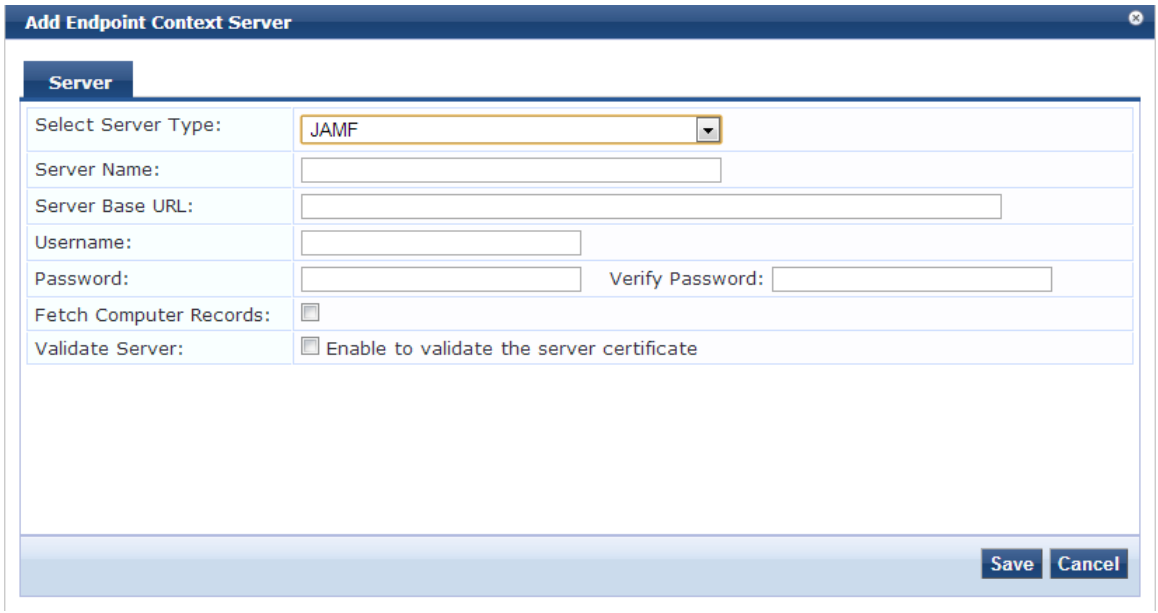


Table 270: *Add JAMF Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type	Select the type of the Policy Manager appliance.
Server Name	Specify the name of the server. For example, V1, V2C, or V3.
Server Base URL	Specify the server base URL.
Username	Specify the username to use for SNMP v3 communication.
Password	Enter and re-enter the password.
Fetch Computer Records	Select the check box to fetch computer records.
Validate Server	Select the check box to validate the server certificate.

Adding a MaaS360 Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 410: *Add MaaS360 Endpoint Context Server tab*

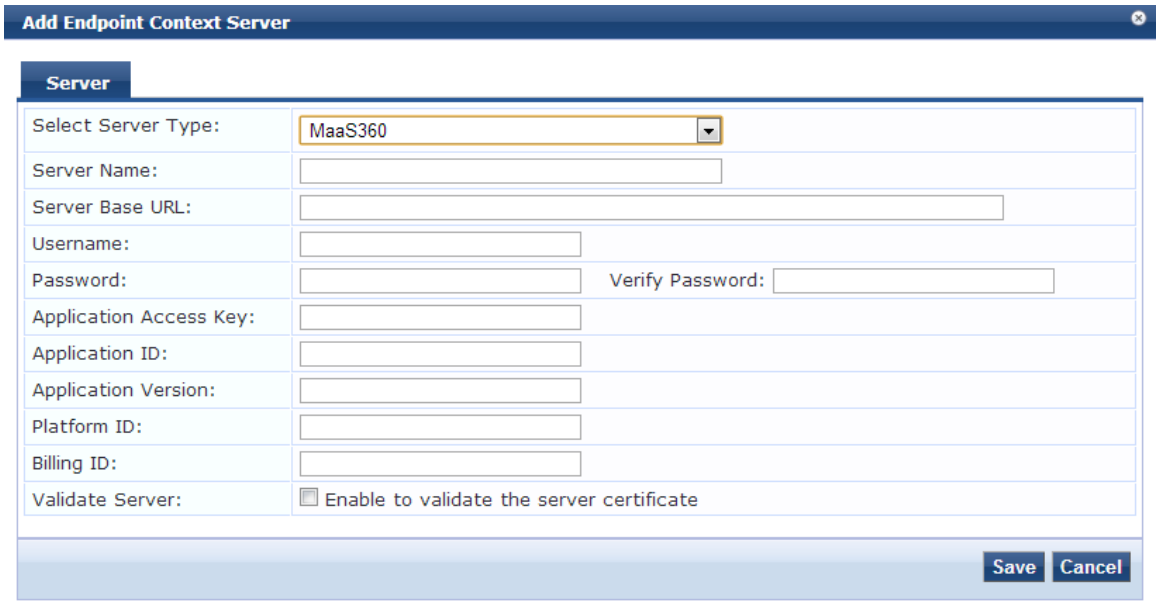


Table 271: *Add MaaS360 Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	MaaS360
Server Name:	Enter a valid server name. You can enter an IP address or domain name.
Server Base URL:	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username:	Enter the username.
Password:	Enter and verify the password.
Application Access Key:	
Application ID:	Enter the application ID.
Application Version:	Enter the application version number.

Table 271: *Add MaaS360 Endpoint Context Server tab Parameters (Continued)*

Parameter	Description
Platform ID:	Enter the application version number.
Billing ID:	Enter the Billing ID.
Validate Server:	Click to enable validation of the server.

Adding a MobileIron Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 411: *Add MobileIron Endpoint Context Server tab*

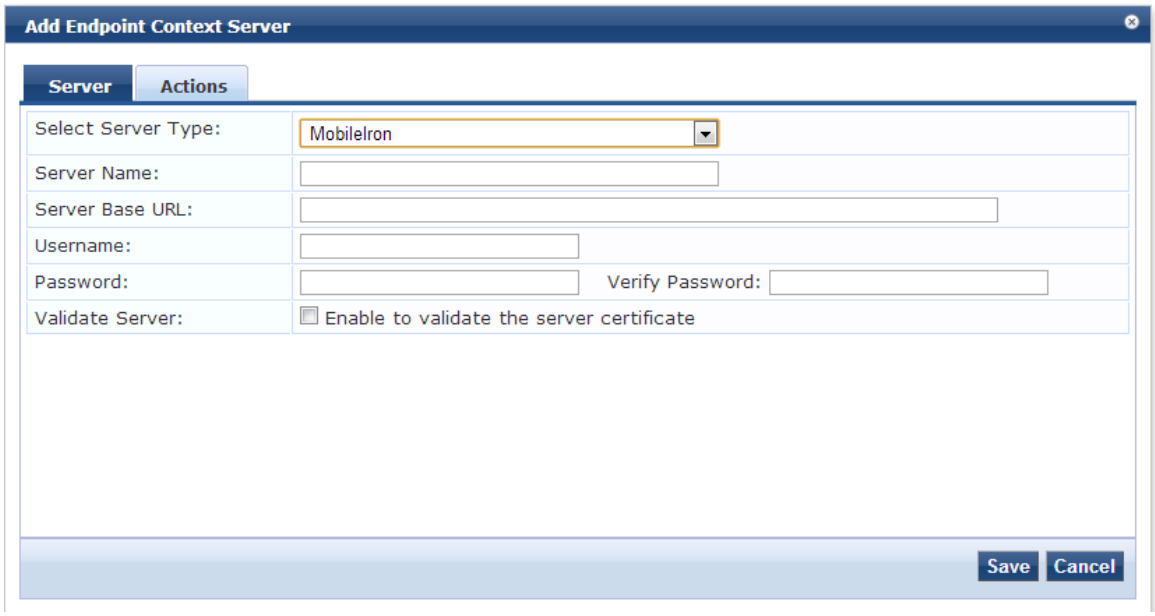


Table 272: *Add MobileIron Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type	Select MobileIron.
Server Name	Enter server name.
Server Base URL	Enter the URL of the base server.
Username	Enter the username.

Table 272: *Add MobileIron Endpoint Context Server tab Parameters (Continued)*

Parameter	Description
Password	Enter the password.
Verify Password	Re-enter the password.
Validate Server	Click to enable validation of the server.

Figure 412: *Add MobileIron Endpoint Context Server Actions tab*

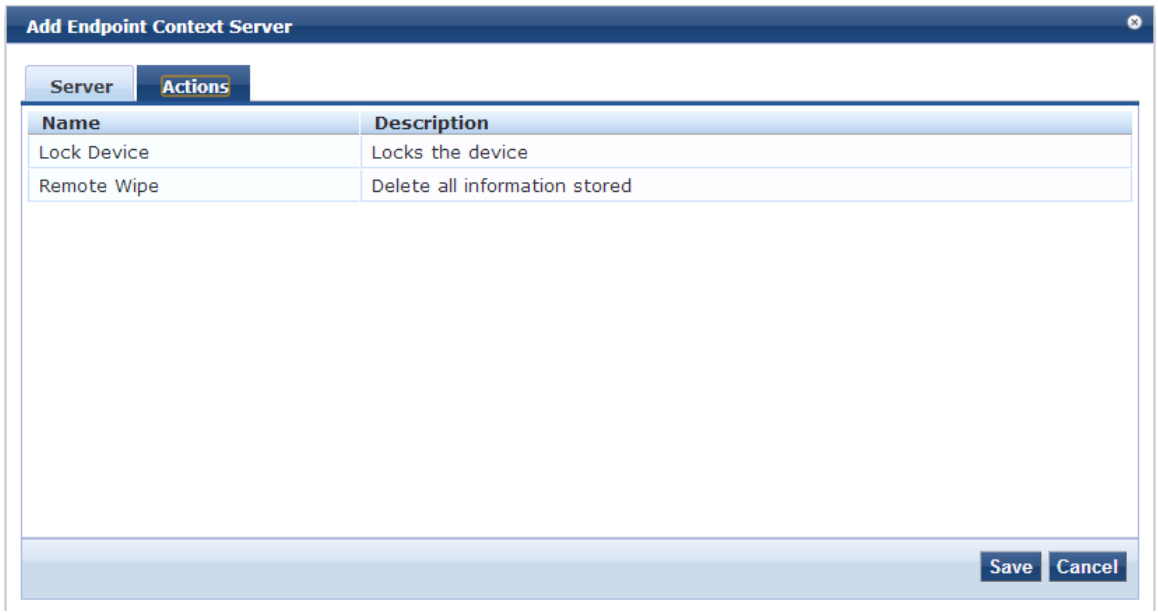


Table 273: *Add MobileIron Endpoint Context Server Actions tab Parameter Description*

Parameter	Description
Lock Device	Locks the associated device.
Remote Wipe	Deletes all stored information.

Adding a Palo Alto Networks Firewall

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 413: *Add Palo Alto Networks Firewall tab*

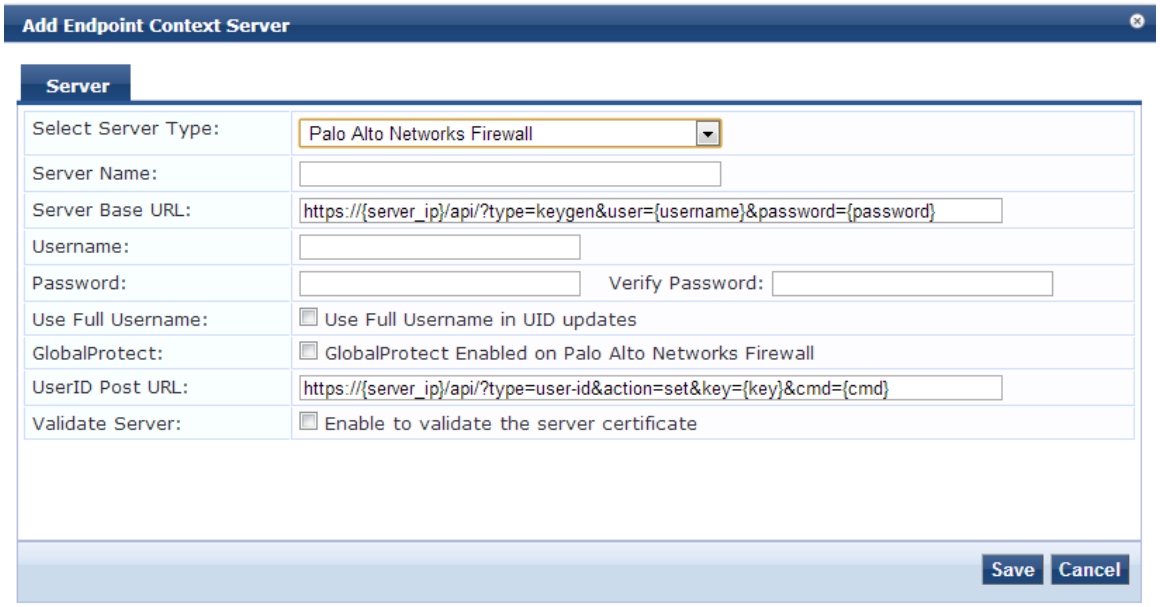


Table 274: *Add Palo Alto Networks Firewall tab Parameters*

Parameter	Description
Select Server Type:	Palo Alto Networks Firewall.
Server Name:	Enter the server name.
Server Base URL:	Enter the server base URL.
Username:	Enter the user name.
Password:	Enter the password.
Verify Password:	Re-enter the password.
Use Full Username:	Click to use full user name in UID updates.
GlobalProtect:	Click to enable GlobalProtect on Palo Alto Networks Firewall.
UserID Post URL:	Enter the user ID Post URL.
Validate Server:	Click to enable validation of the server certificate.

Adding a Palo Alto Networks Panorama Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 414: *Palo Alto Networks Panorama Endpoint Context Server tab*

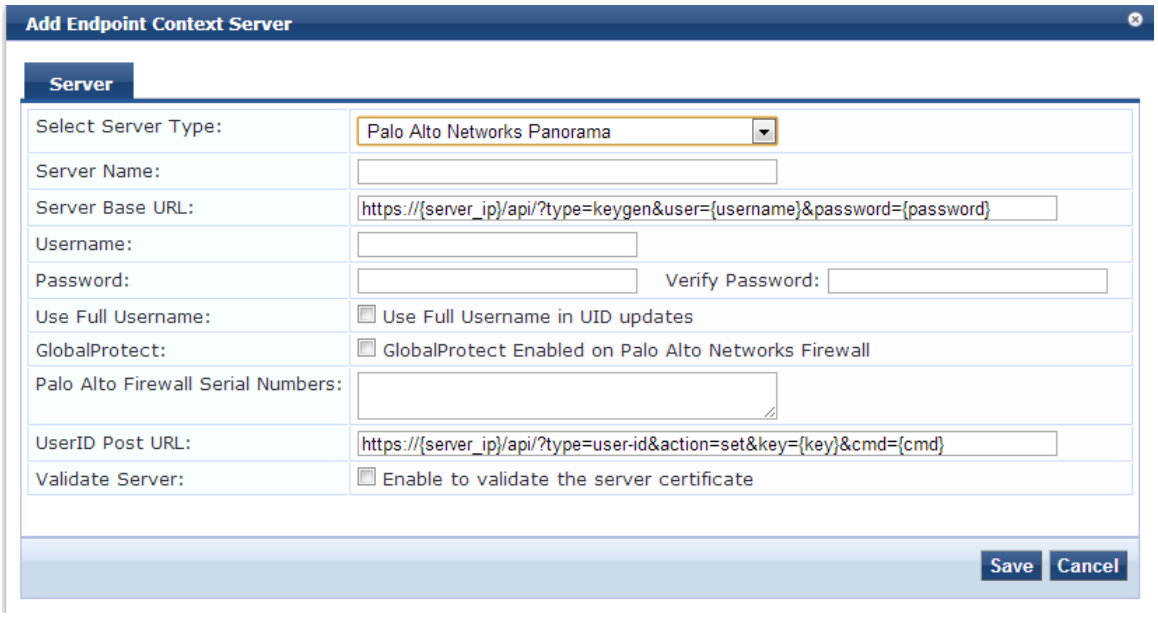


Table 275: *Palo Alto Networks Panorama Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	Palo Alto Networks Panorama.
Server Name:	Enter the server name.
Server Base URL:	Enter the base URL of the server.
Username:	Enter the username.
Password:	Enter the password.
Verify Password:	Re-enter the password.
Use Full Username:	Click to use full username in UID updates.
GlobalProtect:	Click to enable GlobalProtect on Palo Alto Networks Firewall.
Palo Alto Firewall Serial Numbers:	Enter the serial numbers of the Palo Alto firewall.
UserID Post URL:	Enter the user ID of the Post URL.
Validate Server:	Click to enable validation of the server certificate.

Adding a SAP Afaria Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure shows an example of the **Add SAP Afaria Endpoint Context Server - Server** tab followed by parameter definition:

Figure 415: *Add SAP Afaria Endpoint Context Server - Server Tab*

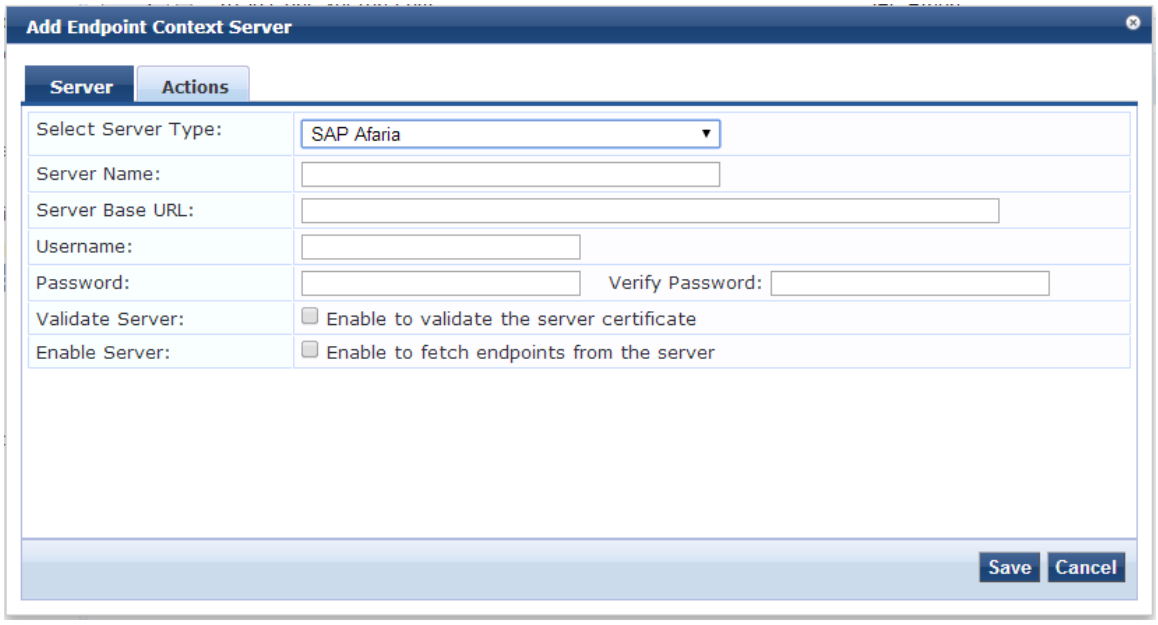


Table 276: *Add SAP Afaria Endpoint Context Server - Server tab Parameters*

Parameter	Description
Select Server Type	Select SAP Afaria.
Server Name	Enter the server name.
Server Base URL	Enter the base URL of the server.
Username	Enter the user name.
Password	Enter the password.
Verify Password	Re-enter the password.
Group ID (optional)	Enter the group ID.
Validate Server	Click to enable validation of the server.

The following figure shows an example of the **Add SAP Afaria Endpoint Context Server - Actions** tab followed by parameter definition:

Figure 416: *Add SAP Afaria Endpoint Context Server - Actions Tab*

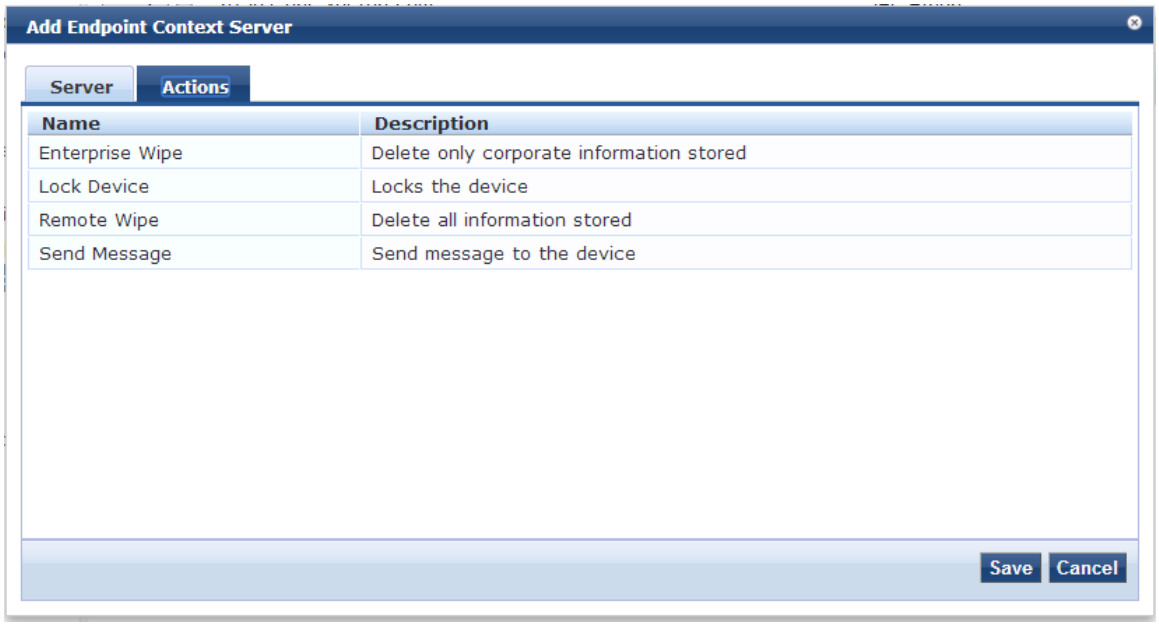


Table 277: *Add SAP Afaria Endpoint Context Server - Actions tab Parameters*

Parameter	Description
Enterprise Wipe	Deletes only stored corporate information.
Lock Device	Locks the associated device.
Remote Wipe	Deletes all stored information.
Send Message	Sends message to the device.

Adding an SOTI Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 417: *Add SOTI Endpoint Context Server tab*

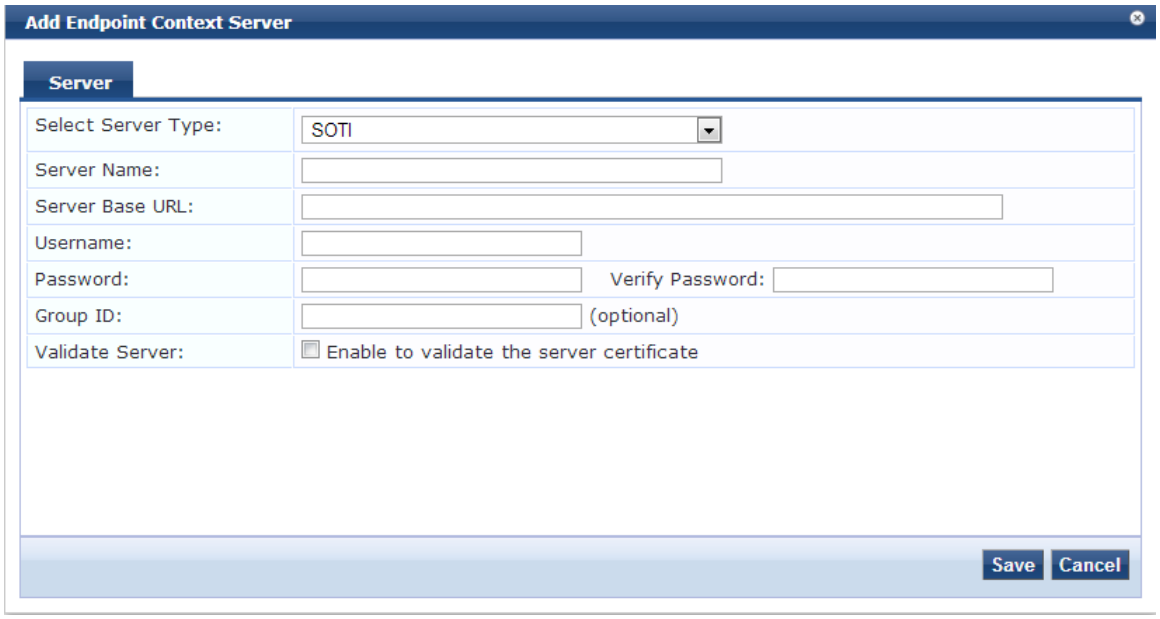


Table 278: *Add SOTI Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	SOTI.
Server Name:	Enter the server name.
Server Base URL:	Enter the base URL of the server.
Username:	Enter the user name.
Password:	Enter the password.
Verify Password:	Re-enter the password.
Group ID: (optional)	Enter the group ID.
Validate Server:	Click to enable validation of the server.

Adding a XenMobile Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 418: *Add XenMobile Endpoint Context Server tab*

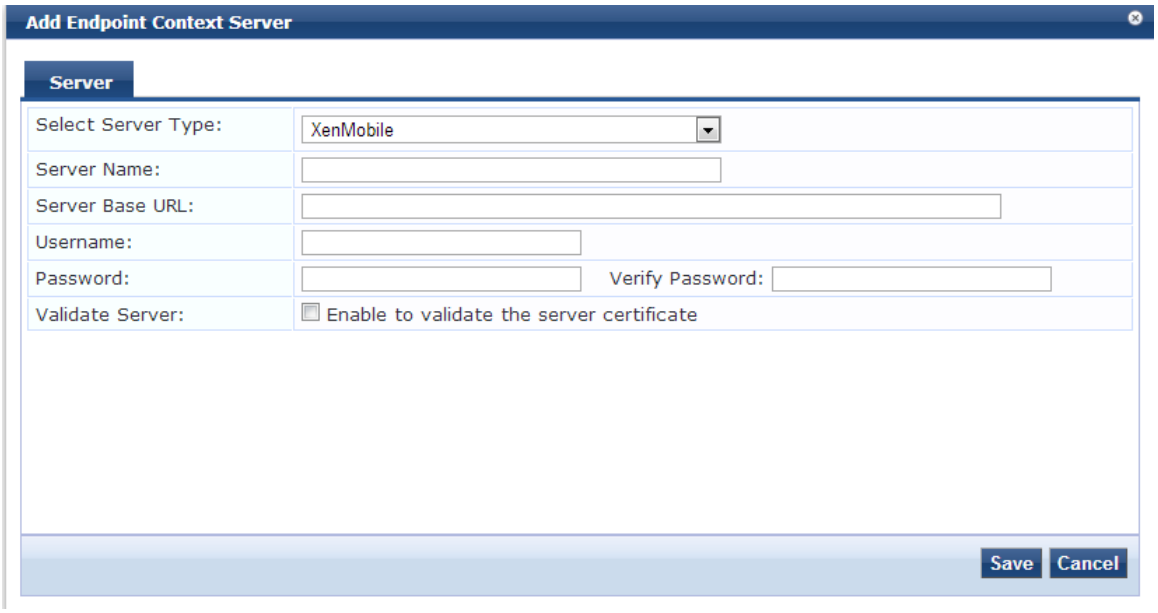


Table 279: *Add XenMobile Endpoint Context Server tab Parameter Description*

Parameter	Description
Select Server Type:	XenMobile.
Server Name:	Enter the server name.
Server Base URL:	Enter the base name of the URL server.
Username:	Enter the user name.
Password:	Enter the password.
Verify Password:	Re-enter the password.
Validate Server:	Click to enable validation of the server certificate.

Server Certificate

The page displayed after you click **Administration > Certificates > Server Certificates** depends on whether the RADIUS Server Certificate Type or the HTTPS Service Certificate Type was assigned to the selected server.

For more information, see:

- Creating a Certificate Signing Request on page 439
- Creating a Self-Signed Certificate on page 442
- Exporting a Server Certificate on page 447
- Importing a Server Certificate on page 447

Server Certificate Page Overview

The page interface controls that are not dependent on the Server Certificate Type are described below.

Table 280: *Server Certificate Interfaces (Common)*

Parameter	Description
Create Self-Signed Certificate	Opens the **Create Self-Signed Certificate** page where you can create and install a Self-Signed Certificate.
Create Certificate Signing Request	Opens the **Create Certificate Signing Request** page where you can create and install a Certificate Signing Request.
Select Server	Select a server in the cluster for server certificate operations.
Select Type	Select a certificate type. The options are RADIUS Server Certificate or HTTPS Server Certificate. The availability of two certificate types (internally signed and publicly signed) can provide deployment flexibility.
Import Server Certificate	Click to open the Import Server Certificate popup. On this popup, you import a certificate that has been exported previously.
Export Server Certificate	After you click this link, the Self-Signed Certificate that is in use is downloaded. The default location for an exported certificate is C:// <user>/Downloads/<HTTPSServerCertificate.zip> or <RADIUSServerCertificate.zip.
View Details	Click to view Certificate Details.

Server Certificate Page (RADIUS Server Certificate Type)

The page displays the parameters configured when a Self-Signed Certificate with a RADIUS Server Certificate Type was created and installed.

Figure 419: *Server Certificate Page (RADIUS Server Certificate Type)*

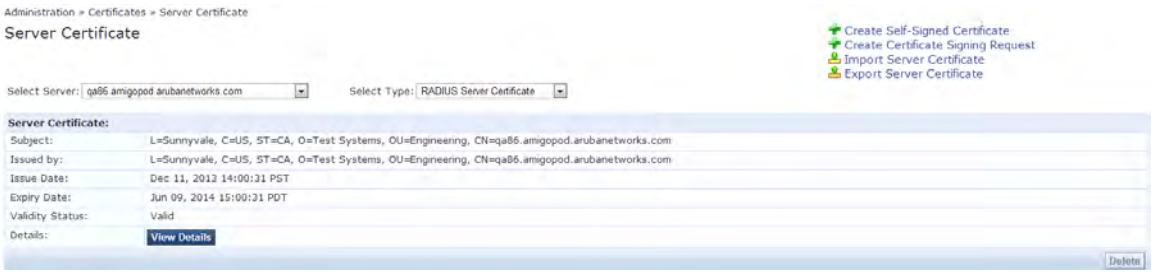


Table 281: *Server Certificate Parameters (RADIUS Server Certificate Type) Parameters*

Parameter	Description
Subject:	Displays Organization and Common Name.
Issued by:	Displays Organization and Common Name.
Issue Date:	The date the Certificate was installed.
Expiry Date:	The date when the Certificate expires.
Validity Status:	The status of the Certificate.
View Details	Click this button to view details about the Certificate, such as Signature Algorithm, Subject Public Key Info, and more.
Delete	This button is disabled.

Server Certificate Page (HTTPS Server Certificate Type)

The page displays the parameters configured after a Self-Signed Certificate with an HTTPS Server Certificate Type was created and installed. The page contains data about the Server Certificate, Intermediate CA Certificate and Root CA Certificate. Click the View Details button for each section to see details about Signature Algorithm, Public Key Info, and more.

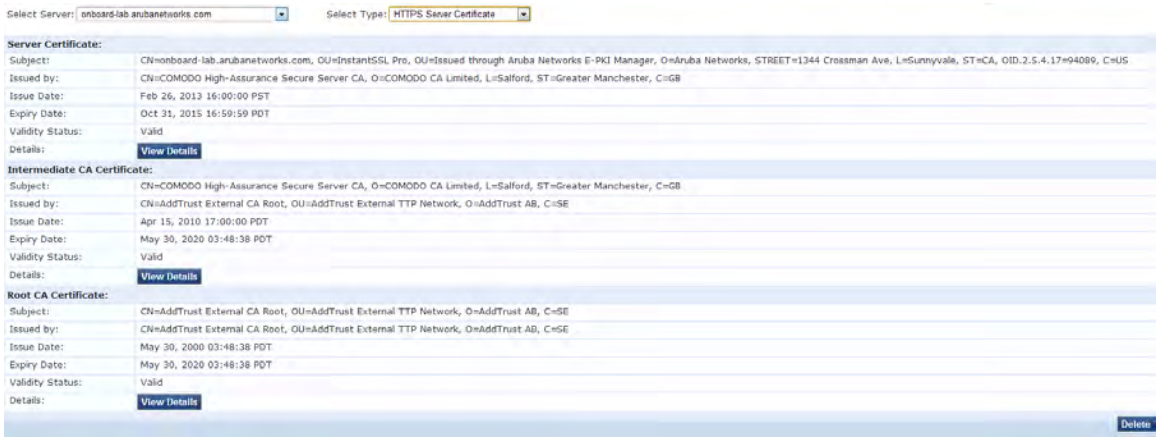


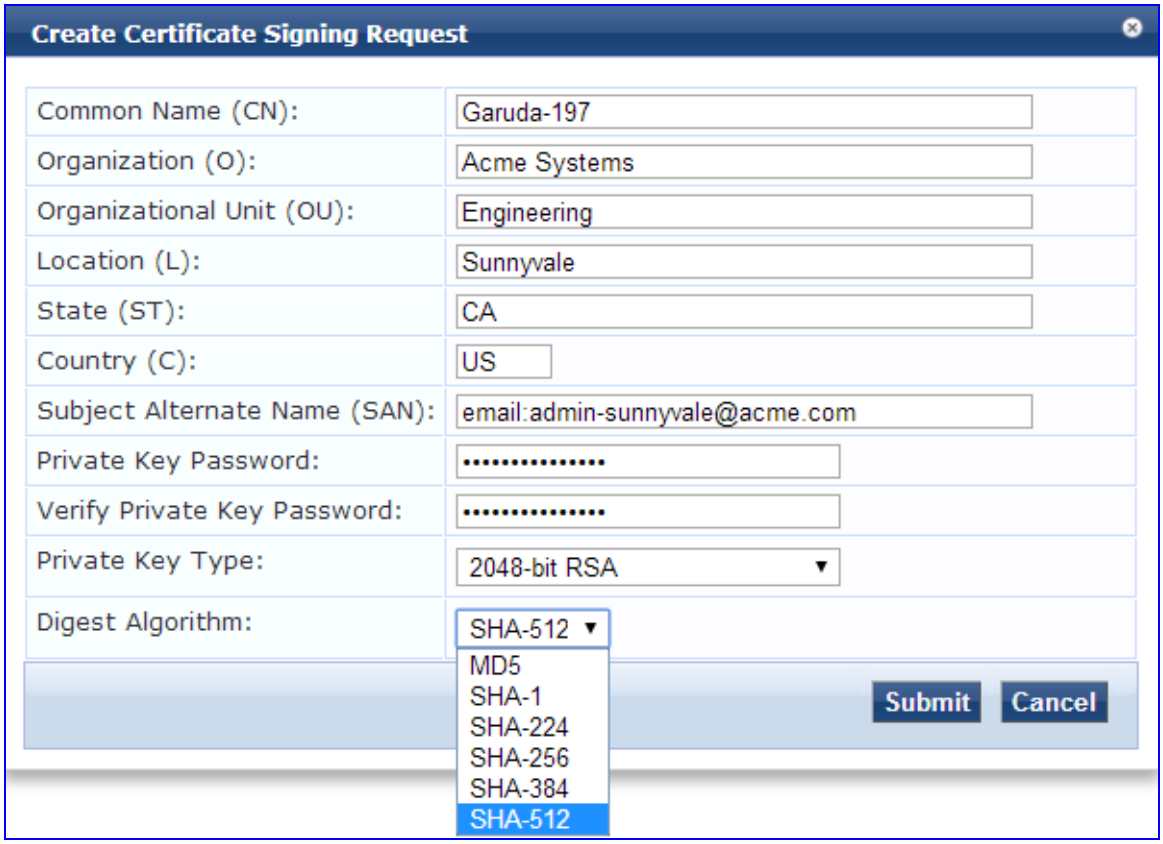
Table 282: *Server Certificate Page (HTTPS Server Certificate Type) Parameters*

Parameter	Description
Subject:	Common.
Issued by:	Displays Organization and Common Name.
Issue Date:	The date the Self-Signed Certificate was installed.
Expiry Date:	The date (in days) for which the Self-Signed Certificate is valid.
Validity Status:	The status of the Self-Signed Certificate.
View Details	Click the View Details button to view information about the Certificate, such as Signature Algorithm, Subject Public Key Info, and more.

Creating a Certificate Signing Request

Navigate to **Administration > Certificates > Server Certificates** and click the **Create Certificate Signing Request** link. This task creates a self-signed certificate to be signed by a CA. The following figure shows an example of the **Create Certificate Signing Request** page followed by parameter definition:

Figure 420: *Create Certificate Signing Request*



The following figure shows an example of the **Create Certificate Signing Request** page in the FIPS mode:

Figure 421: *Create Certificate Signing Request - FIPS Mode*

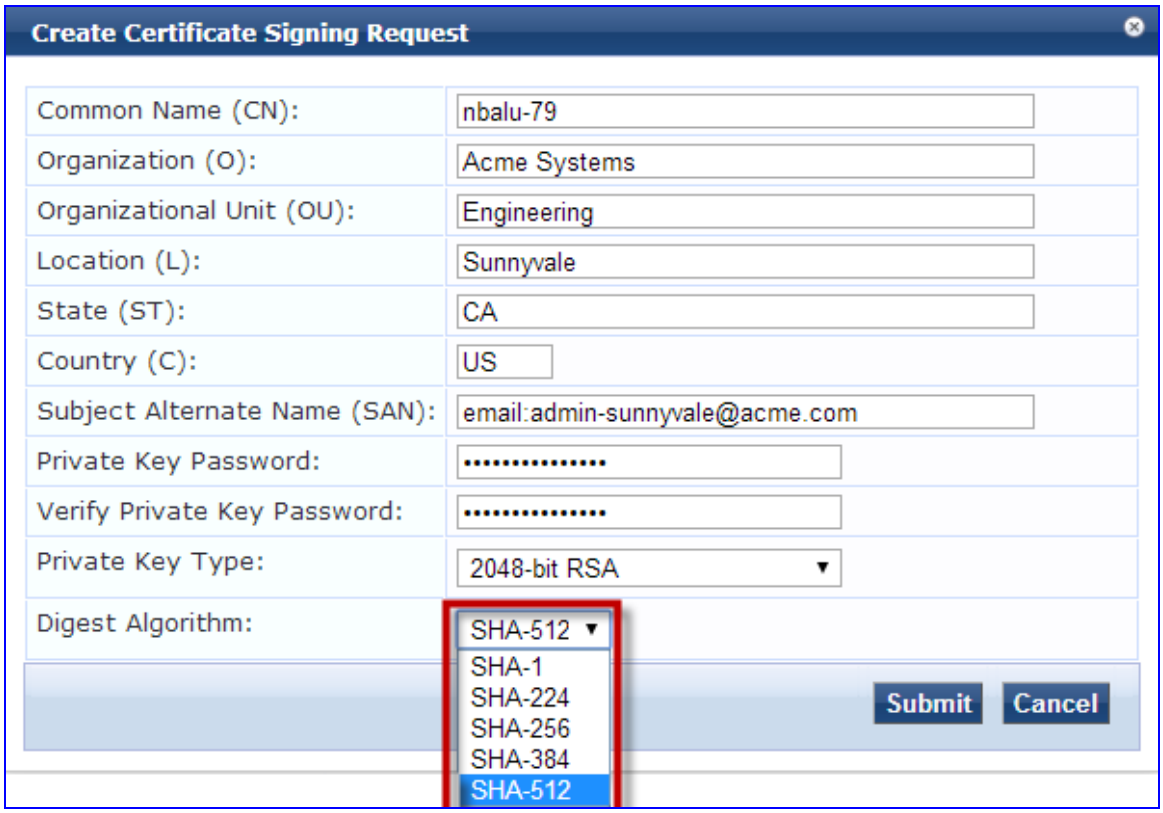


Table 283: *Create Certificate Signing Request Parameters*

Parameter	Description
Common Name (CN)	Displays the name associated with this entity. This can be a host name, IP address, or other name. The default is the fully-qualified domain name (FQDN). This field is mandatory.
Organization (O)	Specify the name of the organization. This field is optional.
Organizational Unit (OU)	Specify the name of the department, division, or section. This field is optional.
Location (L)	Specify the name of the state, country, and/or another location. These fields are optional.
State (ST)	
Country (C)	
Subject Alternate Name (SAN)	Specify the alternative names for the specified Common Name. **NOTE:** Specify the SAN in the following formats: • email: *email_address* • URI: *uri* • IP: *ip_address* • dns: *dns_name*

Table 283: *Create Certificate Signing Request Parameters (Continued)*

Parameter	Description
	• rid: *id* This field is optional.
Private Key Password	Enter and re-enter the Private Key Password.
Verify Private Key Password	
Private Key Type	Select the length for the generated private key types from the following options: • 1024-bit RSA • 2048-bit RSA • 4096-bit RSA • X9.62/SECG curve over a 256 bit prime field • NIST/SECG curve over a 384 bit prime field The default private key type is **2048-bit RSA.**
Digest Algorithm	Select message digest algorithm to use from the following: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 **NOTE:** The MD5 algorithm is not available in the **FIPS** mode.

After you create a **Certificate Signing Request** form and click **Submit**, the generated certificate signing request is displayed. Copy the certificate and paste it into the Web form as part of the enrollment process. You can click **Download CSR and Private Key Files** to save the Certificate Signing Request file and the private key password file. The following figure shows an example of the **Generated Certificate Signing Request** page:

Figure 422: *Generated Certificate Signing Request*

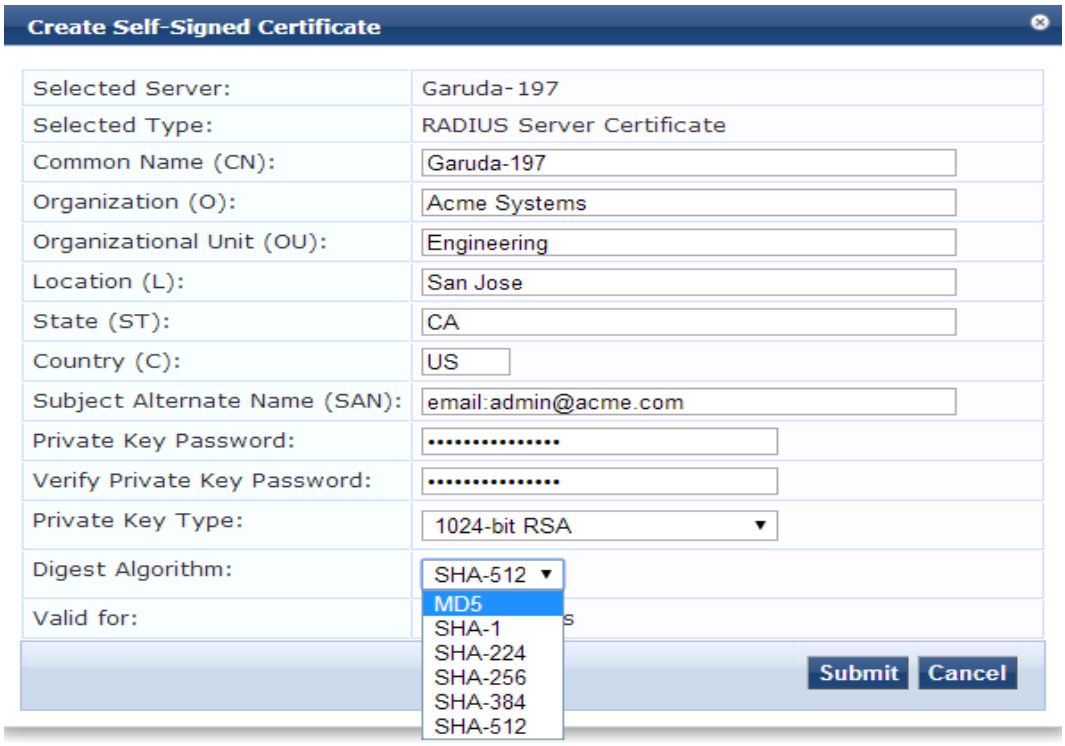
Creating a Self-Signed Certificate

After you select a server and a certificate type, you can create and install a self-signed certificate.

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Select a server, for example, localhost.
3. Select a service by selecting Backend Services or click the **Create Self-Signed Certificate** link. This opens the **Create Self-Signed Certificate** form.

The following figure shows an example of the **Create Self-Signed Certificate** page followed by parameter definition:

Figure 423: *Create Self-Signed Certificate Page*



The following figure shows an example of the **Create Self-Signed Certificate** page in the FIPS mode:

Figure 424: *Create Self-Signed Certificate Page - FIPS Mode*

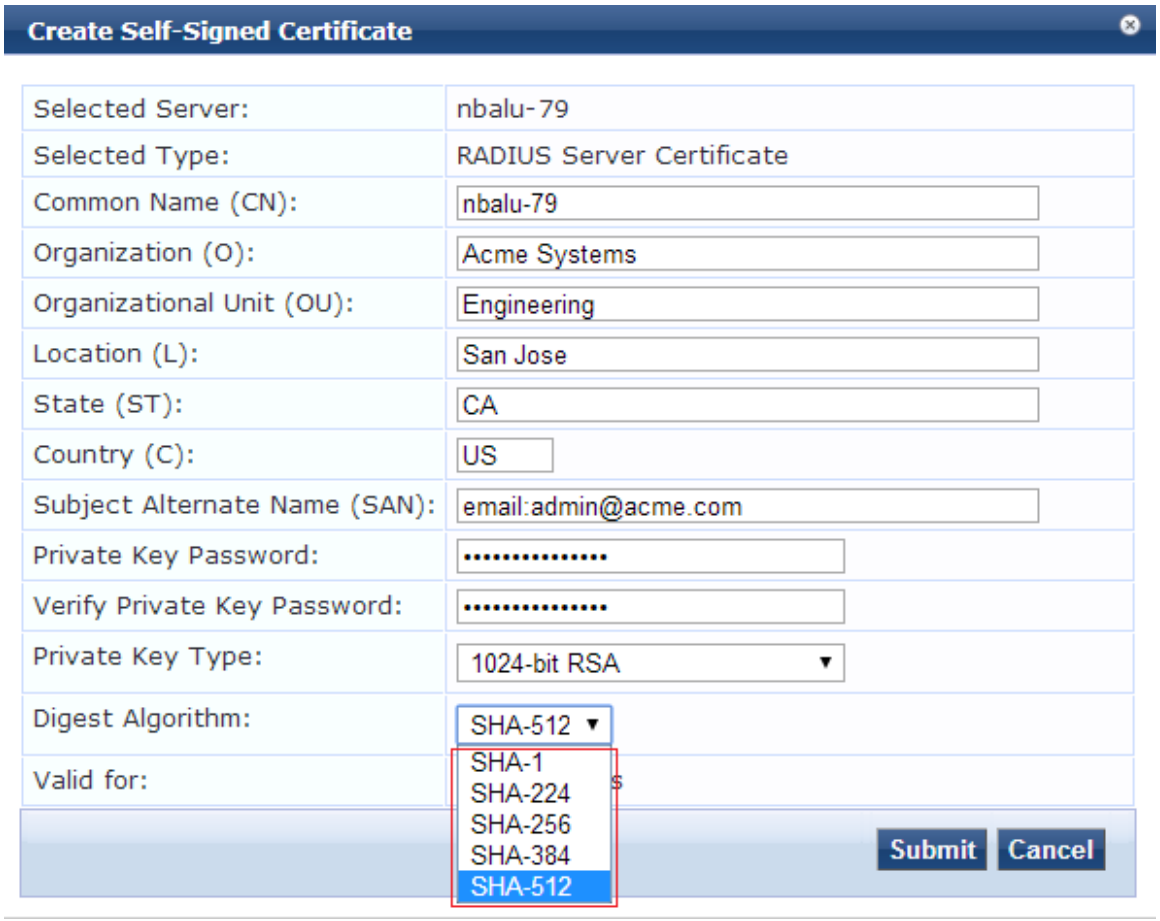


Table 284: *Create Self-Signed Certificate page Parameters*

Parameter	Description
Selected Server	Displays the name of the server selected on the **Server Certificate** page.
Selected Type	Displays the name of the selected certificate type for the server.
Common Name (CN)	Displays the name associated with this entity. This can be a host name, IP address, or other meaningful name. This field is mandatory.
Organization (O)	Specify the name of the organization. This field is optional.
Organizational Unit (OU)	Specify the name of the department, division, section, or other meaningful name. This field is optional.
State (ST)	Specify the name of the state, country, and/or another meaningful location. These fields are optional.
Country (C)	
Location (L)	
Subject Alternate Name (SAN)	Specify the alternative names for the specified Common Name. **NOTE:** Specify the SAN in the following formats: • email: *email_address* • URI: *uri* • IP: *ip_address* • dns: *dns_name* • rid: *id* This field is optional.
Private Key Password	Enter and re-enter the Private Key Password.
Verify Private Key Password	

Table 284: *Create Self-Signed Certificate page Parameters (Continued)*

Parameter	Description
Private Key Type	If you selected the **RADIUS Server Certificate** type for the server, select from the following options: • 1024-bit RSA. • 2048-bit RSA • 4096-bit RSA • X9.62/SECG curve over a 256 bit prime field • NIST/SECG curve over a 384 bit prime field
Digest Algorithm	Select the message digest algorithm to use from the following: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 **NOTE:** The **MD5** algorithm is not available in the **FIPS** mode.
Valid for	Specify the duration in number of days.

Installing the self-signed certificate

After you click **Submit**, you are prompted to install the self-signed certificate. This page displays a summary of the values selected on the **Create Self-Signed Certificate** page. The following figure shows an example of the **Create Self-Signed Certificate** page followed by parameter definition:

Figure 425: *Install Self Signed Certificate*

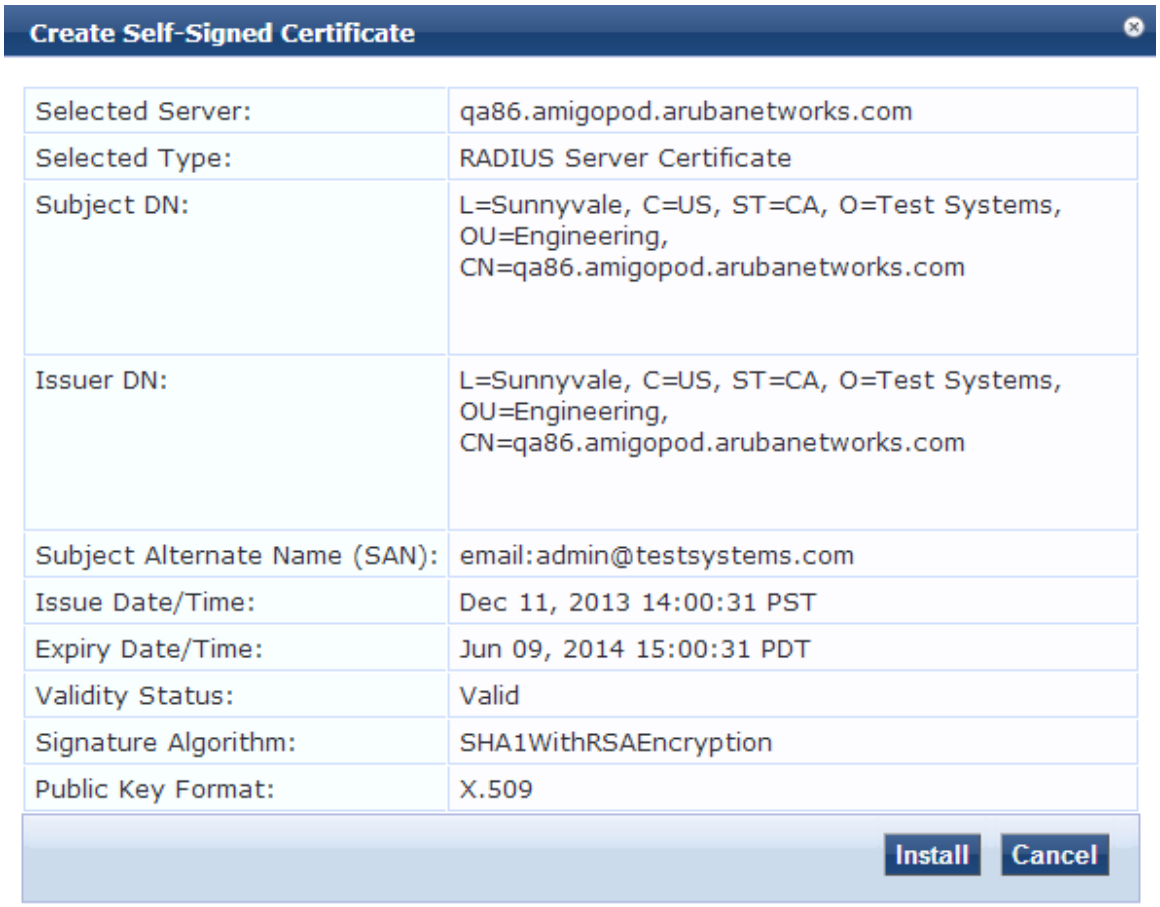


Table 285: *Install Self-Signed Certificate Page Parameters*

Parameter	Description
Selected Server	Displays the name of the server selected on the **Server Certificate** page.
Selected Type	Displays the name of the certificate type selected for the server.
Subject DN	Displays information about the organization, common name, and location of the Subject DN.
Issuer DN	Displays information about the organization, common name, and location of the Subject DN.
Subject Alternate Name (SAN)	Displays the SAN defined during certificate creation.
Issue Date/Time	Displays the certificate issue date and time.
Expire Date/Time	Displays the expiration date and time configured for the certificate.
Validity Status	Displays the status whether the certificate is valid or invalid.
Signature Algorithm	Displays the **Digest Algorithm** and **Private Key Type** selected during certificate configuration.

Exporting a Server Certificate

Navigate to **Administration > Certificates > Server Certificates**, and select the **Export Server Certificate** link. This link provides a form that enables you to save the file **ServerCertifcate.zip**. The zip file has the server certificate (.crt file) and the private key (.pvk file).

Importing a Server Certificate

Navigate to **Administration > Certificates > Server Certificates**, and select the **Import Server Certificate** link.

Figure 426: *Import Server Certificate*

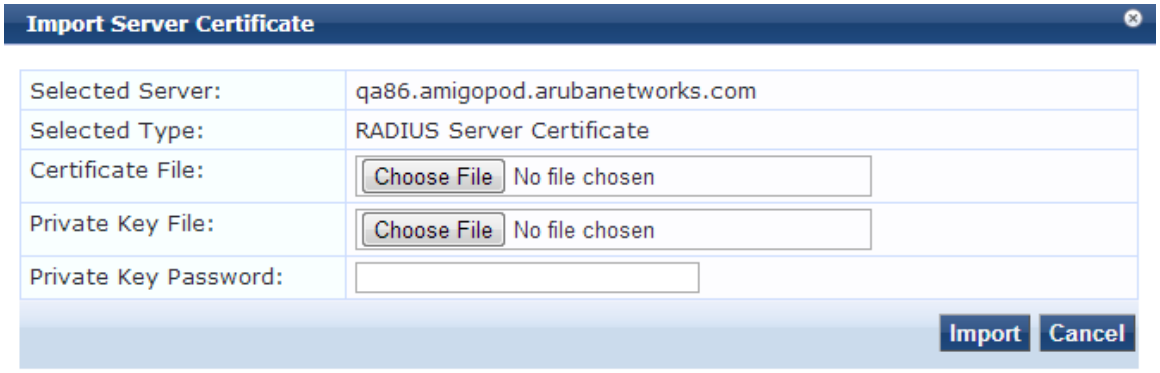


Table 286: *Import Server Certificate Parameters*

Parameter	Description
Selected Server	Enter the name of the server.
Selected Type	Select RADIUS Server Certificate or HTTPS Server Certificate.
Certificate File	Browse to the certificate file to be imported.
Private Key File	Browse to the private key file to be imported.
Private Key Password	Specify the private key password that was entered when the Server Certificate was configured.
Import/Cancel	Click **Import** to commit, or **Cancel** to dismiss the popup.

Certificate Trust List

To display the list of trusted Certificate Authorities (CA), navigate to **Administration > Certificates > Certificate Trust List**. To add a certificate, click **Add**. To delete a certificate, select the check box to the left of the certificate and then click **Delete**. The following figure shows an example of the **Certificate Trust List** page followed by parameter definition:

You cannot import the certificates that are created with the **MD5** digest algorithm to the **Certificate Trust List** in the **FIPS** mode.

Figure 427: *Certificate Trust List page*

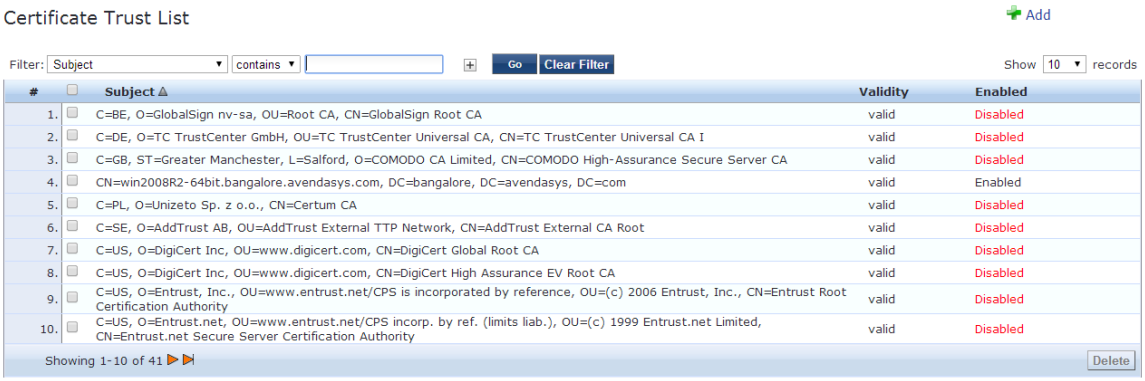


Table 287: *Certificate Trust List page Parameters*

Parameter	Description
Subject	Displays the Distinguished Name (DN) of the subject field in the certificate.
Validity	Indicates whether the CA certificate is valid or expired.
Enabled	Indicates whether the CA certificate is enabled or disabled.

To view the details of a certificate, select the check box to the left of the certificate. From the **View Certificate Details** popup, you can enable the CA certificate. When you enable a CA certificate, Policy Manager considers the entity whose certificate is signed by this CA to be trusted.

Add Certificate

Navigate to **Administration > Certificates > Certificate Trust List** and select the **Add** link. The following figure shows an example of the **Add Certificate** page followed by parameter definition:

Figure 428: *Add Certificate*

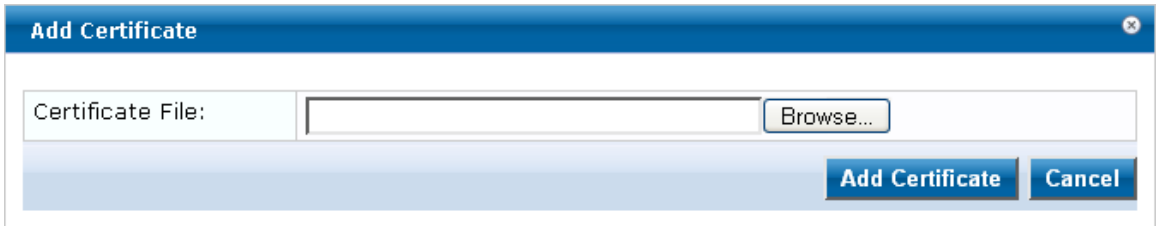


Table 288: *Add Certificate Parameters*

Parameter	Description
Certificate File	Click **Browse** to provide path and select certificate file.
Add Certificate	Click **Add Certificate** to commit.

Revocation Lists

To display available Revocation Lists, navigate to **Administration > Certificates > Revocation Lists.** To add a revocation list, click **Add Revocation List**. To delete a revocation list, select the check box to the left of the list and then click **Delete.**

Figure 429: *Revocation Lists*

Table 289: *Revocation Lists*

Parameter	Description
Add Revocation List	Click to launch the Add Revocation List popup.
Delete	To delete a revocation list, select the check box to the left of the list that you want to delete and then click **Delete.**

Adding a Revocation List

Navigate to **Administration > Certificates > Revocation Lists** and select the **Add Revocation List** link.

Figure 430: *Add Certificate Revocation List Page*

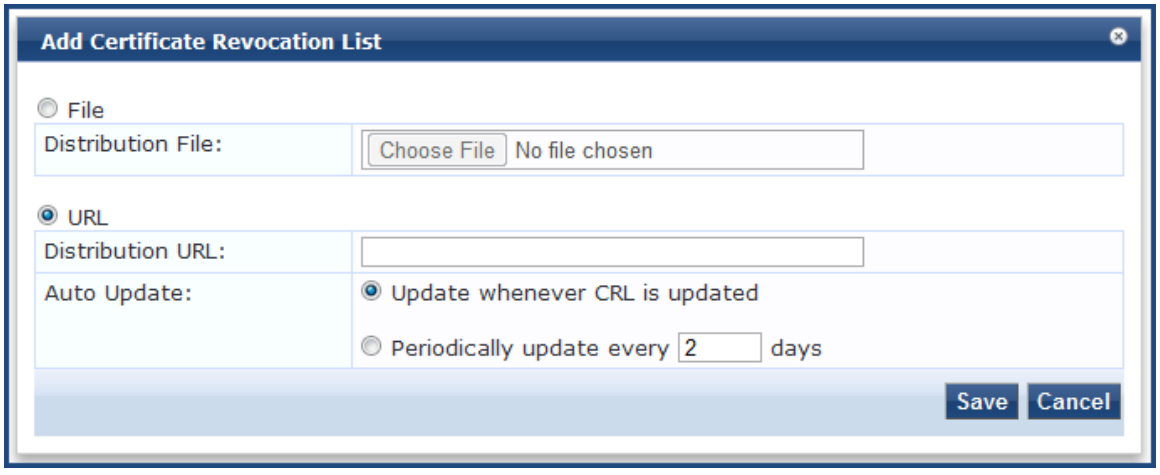


Table 290: *Add Revocation List Page Parameters*

Parameter	Description
File	File enables the Distribution File option.
Distribution File:	Specify the distribution file (e.g., **C:/distribution/crl.verisign.com/Class3InternationalServer.crl**) to fetch the certificate revocation list.
URL	URL enables the Distribution URL option.
Distribution URL:	Specify the distribution URL (e.g., **http://crl.verisign.com/Class3InternationalServer.crl**) to fetch the certificate revocation list.
Auto Update:	Select **Update whenever CRL is updated** to update the CRL at intervals specified in the list. Or select **Periodically update** to check periodically and at the specified frequency (in days).

Dictionaries

Select one of the following topics to find more information about dictionaries.

RADIUS Dictionary

RADIUS dictionaries are available on the **Administration > Dictionaries > RADIUS**. This page includes the list of available vendor dictionaries.

Figure 431: *RADIUS Dictionaries*

Click on a row view the dictionary attributes, to enable or disable the dictionary, and to export the dictionary. For example, click on vendor IETF to see all IETF attributes and their data type.

Figure 432: *RADIUS IETF Dictionary Attributes*

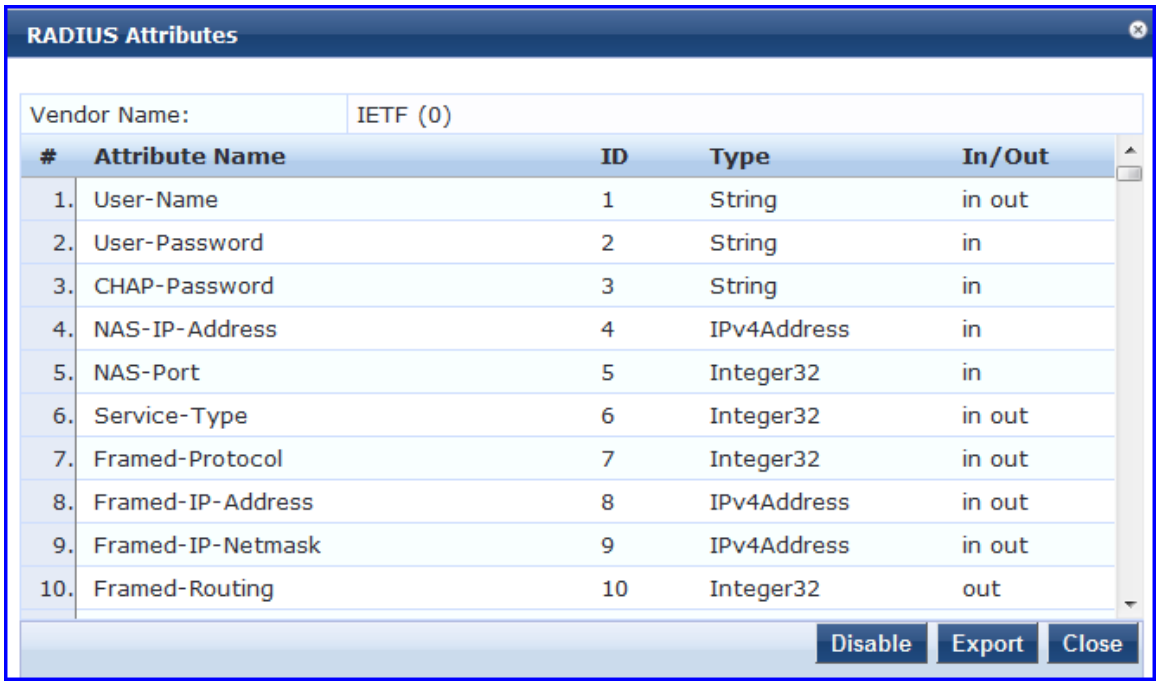


Table 291: *RADIUS Dictionary Attributes*

Parameter	Description
Export	Click to save the dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.
Enable/Disable	Enable or disable this dictionary. Enabling a dictionary makes it appear in the Policy Manager rules editors (Service rules, Role mapping rules, etc.).

Import RADIUS Dictionary

You can add additional dictionaries using the Import too. To add a new vendor dictionary, navigate to **Administration > Dictionaries > RADIUS**, and click on the **Import** link. To edit an existing dictionary, export an existing dictionary, edit the exported XML file, and then import the dictionary. To view the contents of the RADIUS dictionary, sorted by Vendor Name, Vendor ID, or Vendor Prefix, navigate to: **Administration > Dictionaries > RADIUS**.

Figure 433: *Import RADIUS Dictionary*

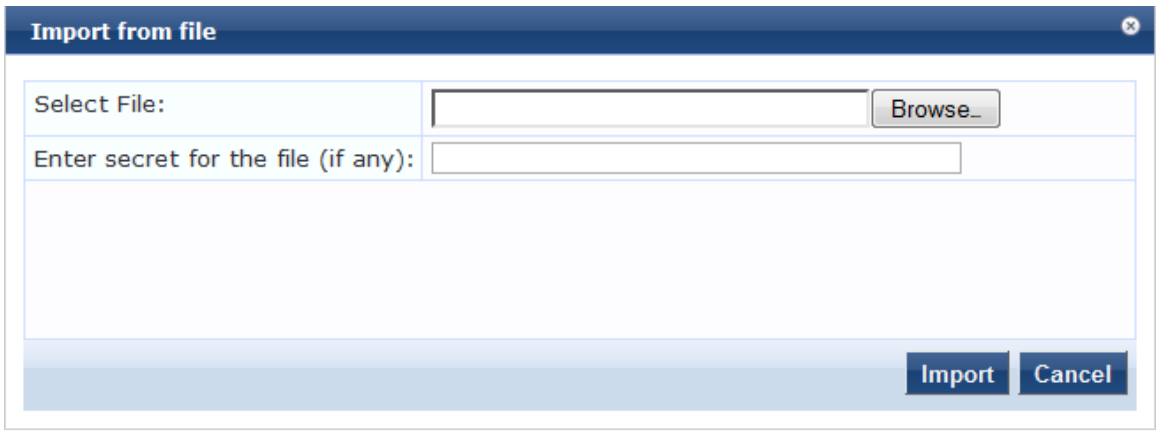


Table 292: *Import RADIUS Dictionary*

Parameter	Description
Select File	Browse to select the file that you want to import.
Enter secret for the file (if any)	If the file that you want to import is password protected, enter the secret here.

Posture Dictionary

To add a vendor posture dictionary, click on **Import**. To edit an existing dictionary, export an existing dictionary, edit the exported XML file, and then import the dictionary.

To view the contents of the Posture dictionary, sorted by Vendor Name, Vendor ID, Application Name, or Application ID, navigate to: **Administration > Dictionaries > Posture**.

Figure 434: *Posture Dictionaries*

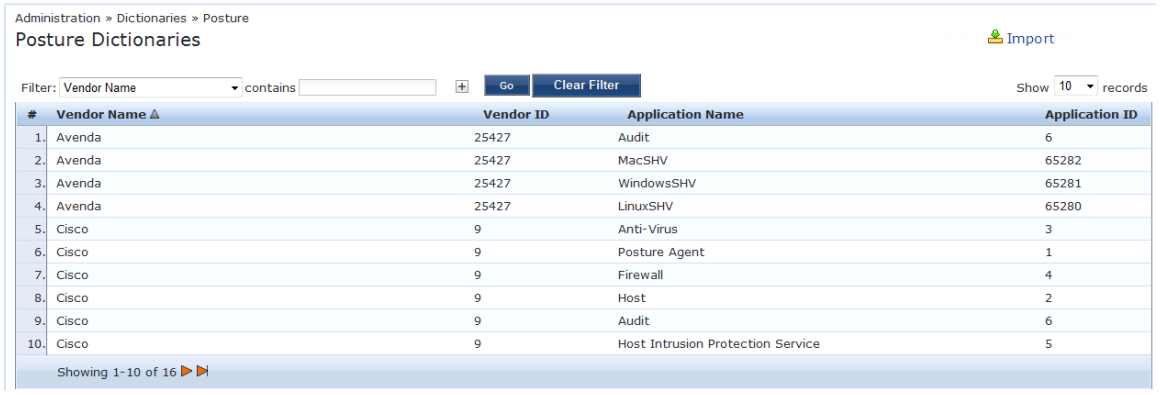


Table 293: *Posture*

Parameter	Description
Import	Click to open the **Import Dictionary** popup.

Click on a vendor row to see all the attributes and their data type. For example, click on vendor Microsoft/System SHV to see all the associated posture attributes and their data type.

Figure 435: *Posture Attributes Page*

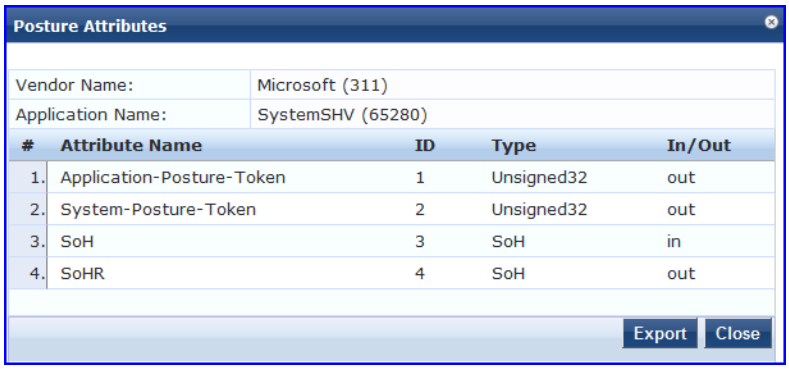


Table 294: *Posture Attributes Parameters*

Parameter	Description
Export	Click to save the posture dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.

TACACS+ Services Dictionary

To view the contents of the TACACS+ service dictionary, sorted by Name or Display Name, navigate to: **Administration > Dictionaries > TACACS+ Services**.

To add a new TACACS+ service dictionary, click on the **Import** link. To add or modify attributes in an existing service dictionary, select the dictionary, export it, make edits to the XML file, and import it back into Policy Manager.

Figure 436: *TACACS+ Services Dictionaries Page*

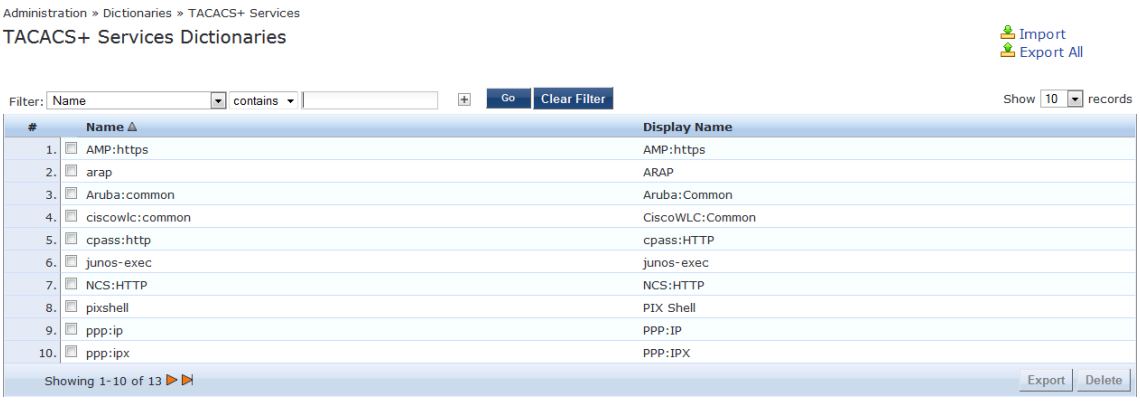


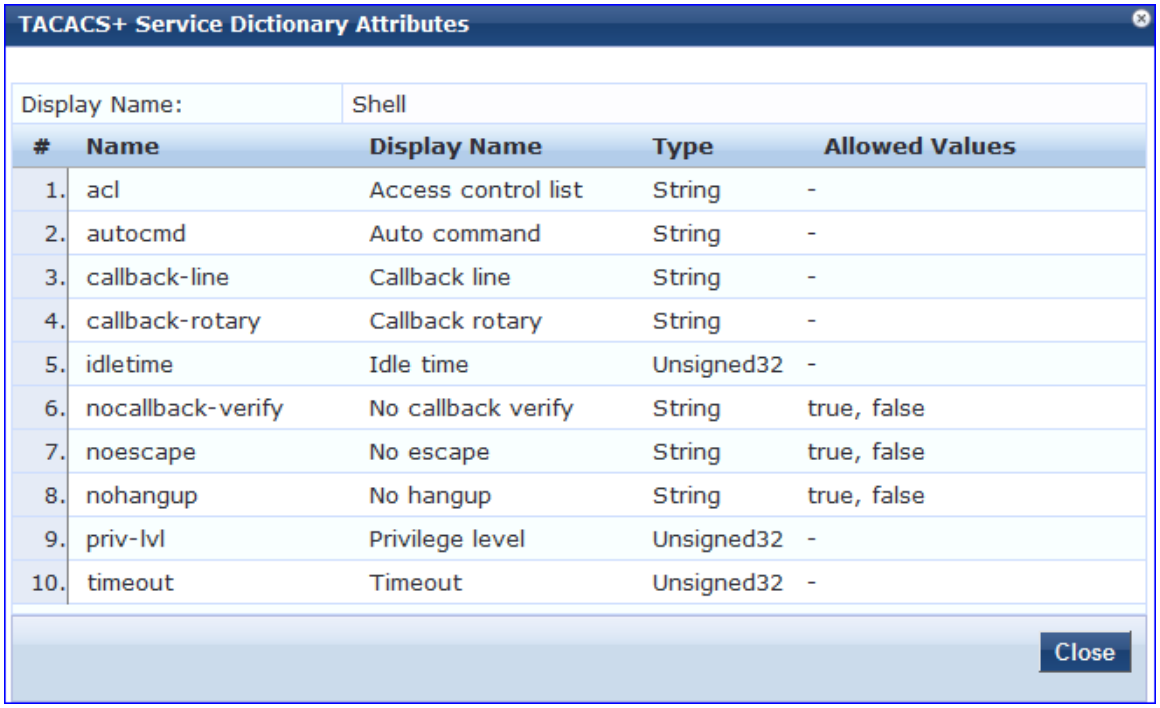
Table 295: *TACACS+ Services Dictionaries Page Parameters*

Parameter	Description
Import	Click to open the **Import Dictionary** popup. Import the dictionary (XML file).
Export All	Export all TACACS+ services into one XML file containing multiple dictionaries

To export a specific service dictionary, select a service and click on **Export**.

To see all the attributes and their data types, click on a service row. For example, click on shell service to see all shell service attributes and their data type.

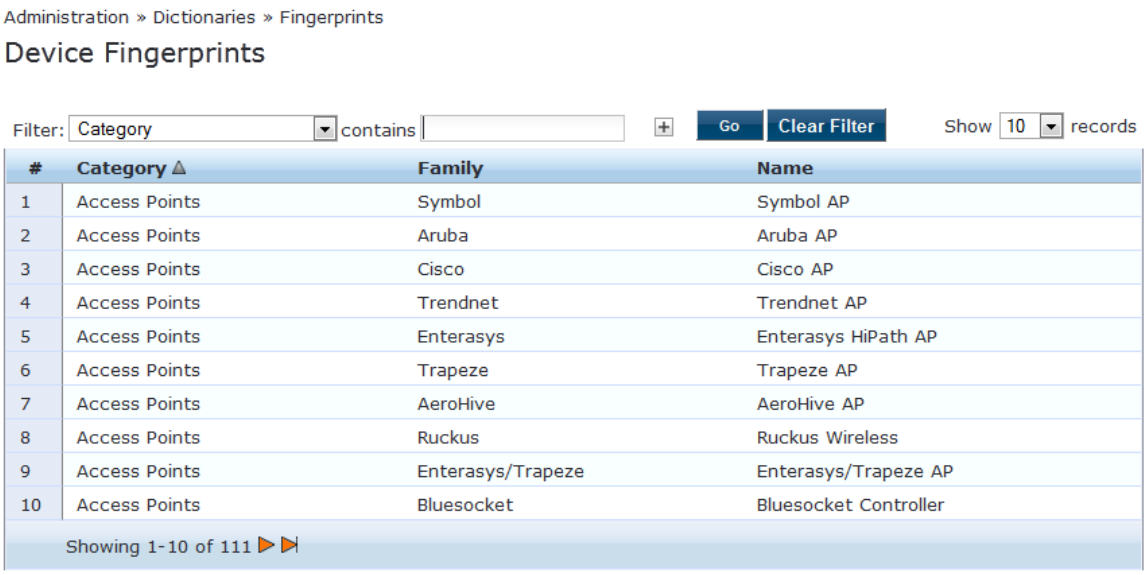
Figure 437: *Shell Service Dictionary Attributes*



Fingerprints Dictionary

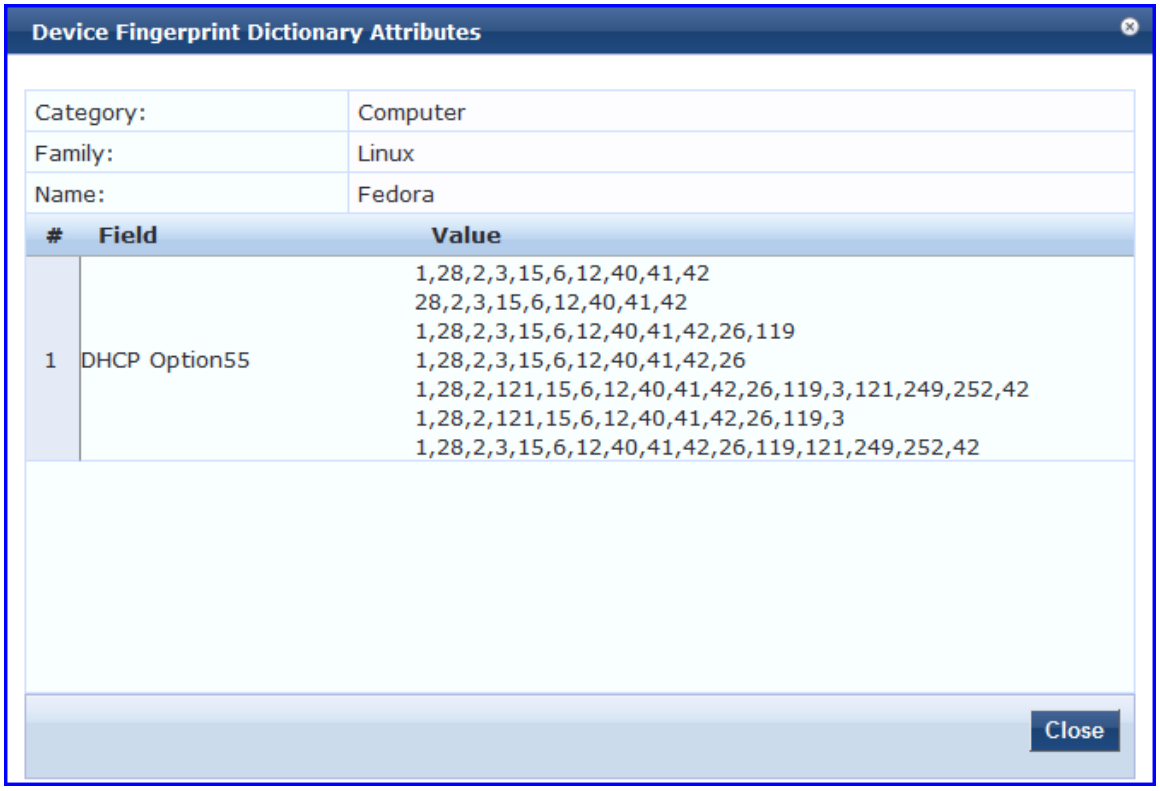
The **Device Fingerprints** table shows a listing of all the device fingerprints recognized by the Profile module. These fingerprints are updated from the Dell W-ClearPass Update Portal (see Software Updates on page 465 for more information.)

Figure 438: *Device Fingerprints Page*



You can click on a line in the Device Fingerprints list to drill down and view additional details about the category.

Figure 439: *Device Fingerprint Dictionary Attributes Page*



Attributes Dictionary

The **Administration > Dictionaries > Attributes** page allows you to specify unique sets of criteria for LocalUsers, GuestUsers, Endpoints, and Devices. This information can then be with role-based device policies for enabling appropriate network access.

The Attributes page provides the following interfaces for configuration:

Figure 440: *Attributes page*

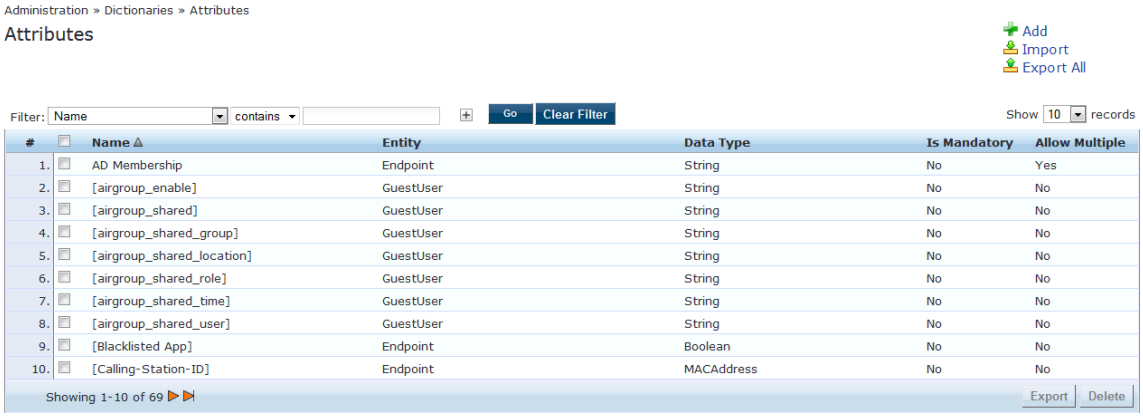


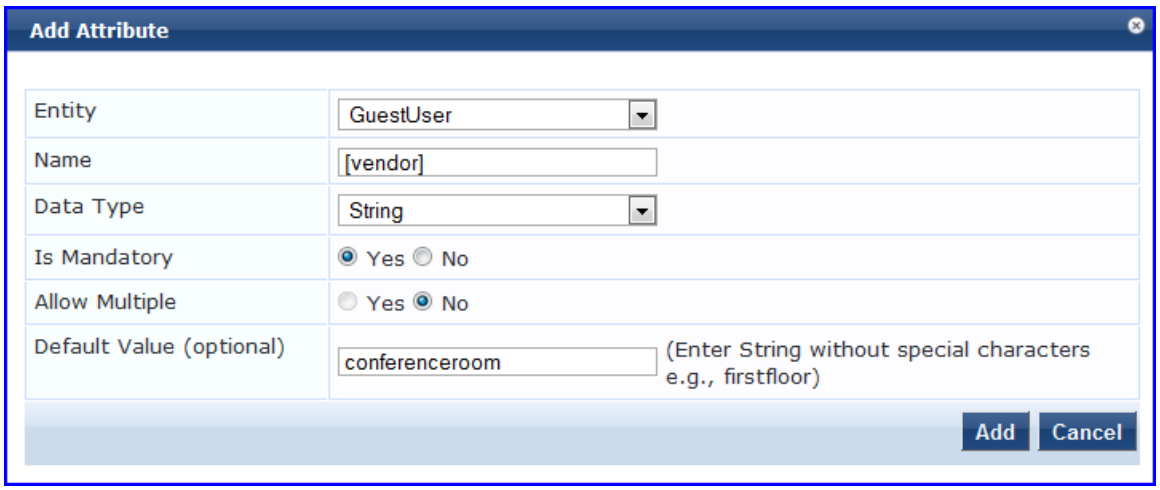
Table 296: *Attributes Page Parameters*

Parameter	Description
Filter	Use the drop-down list to create a search based on the available Name, Entity, Data Type, Is Mandatory, or Allow Multiple settings.
Name	The name of the attribute.
Entity	Shows whether the attribute applies to a LocalUser, GuestUser, Device, or Endpoint.
Data Type	Shows whether the data type is string, integer, boolean, list, text, date, MAC address, or IPv4 address.
Is Mandatory	Shows whether the attribute is required for a specific entity.
Allow Multiple	Shows whether multiple attributes are allowed for an entity.

Adding Attributes

To add an Attribute dictionary, select **Add** in the upper right portion of the page.

Figure 441: *Add Attributes Page*



Enter information in the fields described in the following table. Click **Add** when you are done. To modify attributes in an existing service dictionary, select the attribute, make any necessary changes, and then click **Save**.

Table 297: *Attribute Setting Parameters*

Parameter	Description
Entity	Specify whether the attribute applies to a LocalUser, GuestUser, Device, or Endpoint.
Name	Enter a unique ID for this attribute.
Data Type	Specify whether the data type is string, integer, boolean, list, text, date, MAC address, or IPv4 address.
Is Mandatory	Specify whether the attribute is required for a specific entity.
Allow Multiple	Specify whether multiple attributes are allowed for an entity. **NOTE:** Multiple attributes are not permitted if **Is Mandatory** is specified as **Yes**.

Import Attributes

Select **Import** on the upper right portion of the page.

The imported file is in XML format. To view a sample of this XML format, export a dictionary file and open it in an XML viewer.

Figure 442: *Import from file Page*

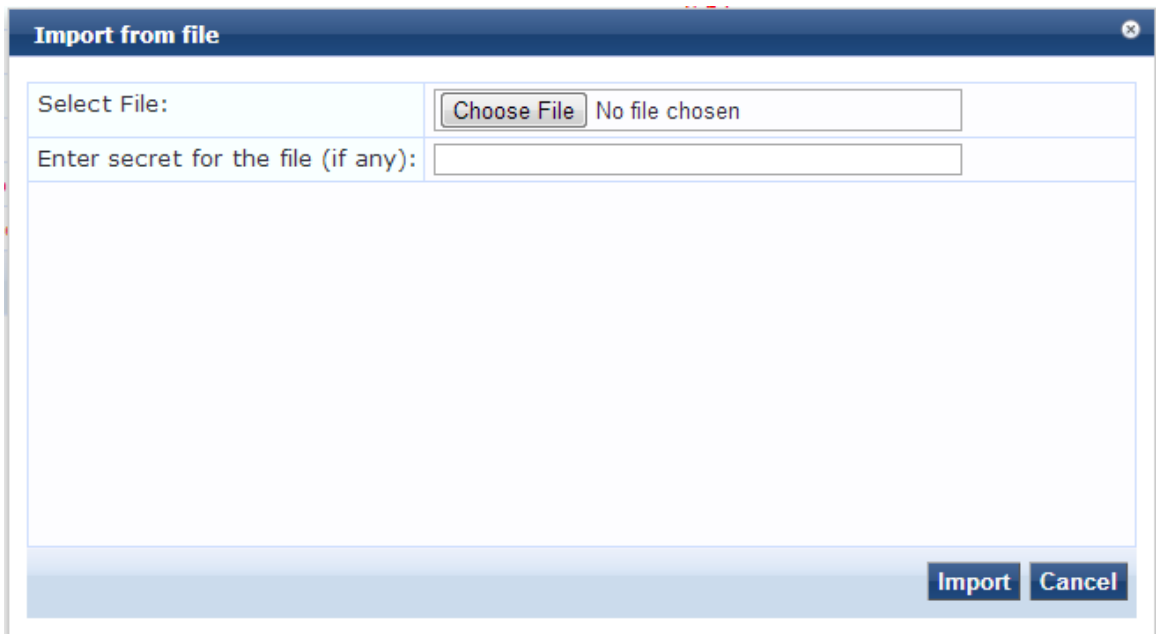


Table 298: *Import From File Setting Parameters*

Parameter	Description
Select File / Enter secret for the file	Browse to the dictionary file to be imported. Enter the secret key (if any) that was used to export the dictionary.
Import/Cancel	Click **Import** to commit, or **Cancel** to dismiss the popup.

Export Attributes

Select **Export All** on the upper right portion of the page to export all attributes.

The **Export Attributes** button saves the file **Attributes.zip.** The zip file consists of the server certificate (.crt file) and the private key (.pvk file).

Export

Select the **Export** button on the lower right side of the page.

To export just one attribute, select it (check box at left) and click **Export.** Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Applications Dictionary

Application dictionaries define the attributes of the Onboard Policy Manager application and the type of each attribute. When Policy Manager is used as the Policy Definition Point (PDP), it uses the information in these dictionaries to validate the attributes and data types sent in a WEB-AUTH request.

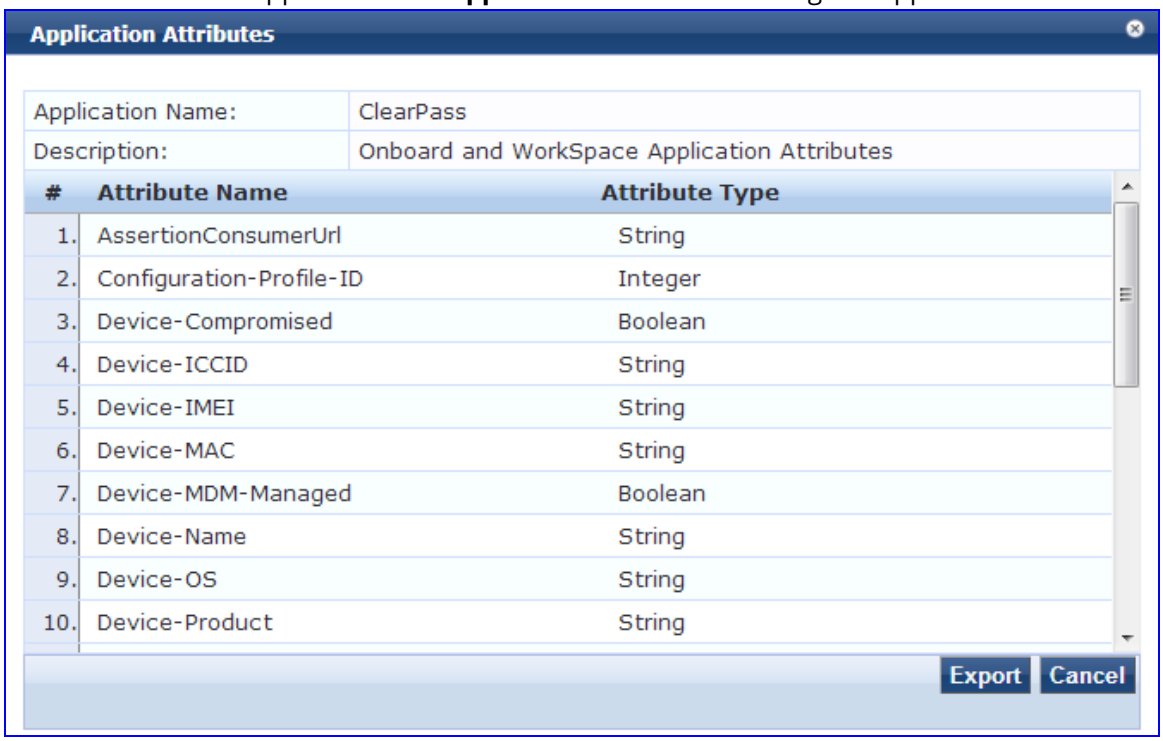
You can:

- View an application dictionary on page 459
- Delete an application dictionary on page 459
- Importing on page 1

- Exporting on page 2

View an application dictionary

1. Go to **Administration > Dictionaries > Applications**.
2. Click the name of an application. The **Application Attributes** dialog box appears.



Delete an application dictionary

In general, you should have no need to delete an application dictionary. They have no effect on Policy Manager performance.

1. Go to **Administration > Dictionaries > Applications**.
2. Click the check box next to an application name.
3. Click **Delete**.

Endpoint Context Server Actions

Use the **Context Server Actions** (**Administration** > **Dictionaries** > **Endpoint Context Server Actions**) page to configure actions that are performed on endpoints, such as locking a device, triggering a remote, or enterprise wipe, and so on. The **Context Server Actions** page displays the report that shows information about all configured Endpoint Context Server Actions.

For more information, see:

- Filtering an Endpoint Context Server Action Report on page 460
- Viewing Details About Endpoint Context Server Actions on page 460
- Adding an Endpoint Context Server Action Item on page 460
- Import Context Server Actions on page 461
- Export Context Server Actions on page 462

The following figure shows an example of the **Endpoint Context Server Actions** page followed by parameter definition:

Figure 443: *Endpoint Context Server Actions Page*

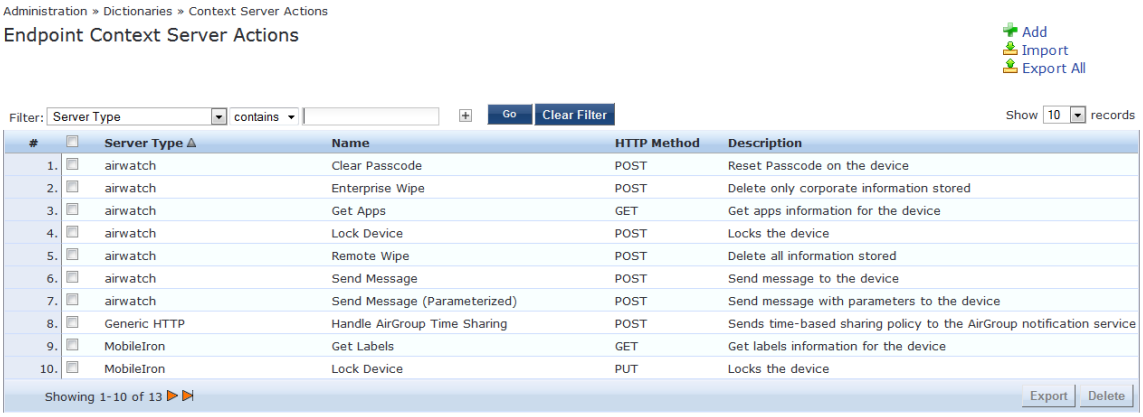


Table 299: *Endpoint Context Server Action Page Parameters*

Parameter	Description
Server Type	Specifies the server type configured when the server action was configured.
Name	Specifies the name of the action such as Enterprise Wipe, Lock Device, and so on.
HTTP Method	Specifies the HTTP method selected when the server action was configured.
Description	Specifies the description of the action. For example, you can provide a description as **Delete all stored information** if the configured action **is Remote Wipe**.

You can perform the following actions from the **Context Server Actions** page.

Filtering an Endpoint Context Server Action Report

Use the **Filter** controls to configure a search for a subset of Endpoint Context Server Action items.

1. Select a Filter from the options: ServerType, Name, or HTTP method.
2. Click the plus icon in the **Option** field to add up to four new search fields.
3. Select a search argument. The search arguments are limited to **contains** or **equals**.
4. Click **Go**.

Viewing Details About Endpoint Context Server Actions

1. Click a row in the report.
2. Click a tab to view details about the selected Endpoint Context Server action. See the table in the next section for parameter definition.

Adding an Endpoint Context Server Action Item

Enter information in the tabs described in the following table. Click **Add** after providing the required information. To modify existing Endpoint Context Server Details, select a row and change detail, make any necessary changes, and then click **Save**.

Figure 444: *Endpoint Context Server Details Action tab*

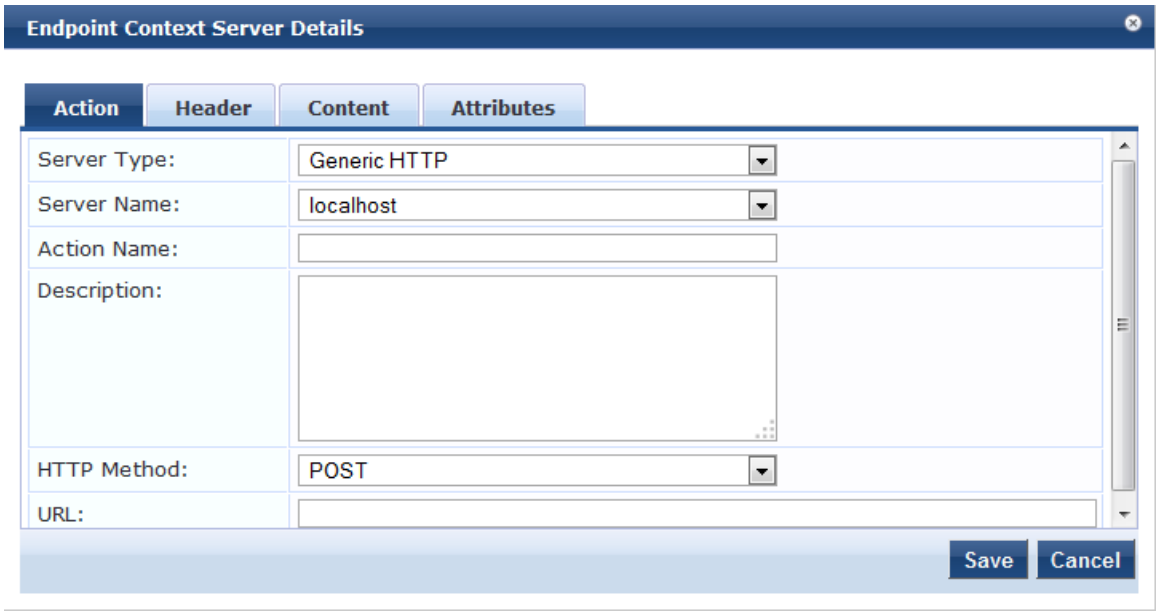


Table 300: *Endpoint Context Server Action tab Parameters*

Parameter	Description
Action	Specifies the following options: **Server Type** - Specifies the Specifies the server type configured when the server action was configured. You can select the server type from the drop-down list. **Server Name** - Lists the context servers specific to the server type selected in the **Server Type** field. **NOTE:** This field is visible only if you selected the service type **Generic HTTP**. **Action Name** - Specifies the name of the action configured. Description - Provides additional information about the action specified. **HTTP method** - Specifies the HTTP method selected when the server action was configured. **URL** - Specifies the URL for the selected HTTP method.
Header	Specifies the key-value pairs to be included in the HTTP Header.
Content	Specifies a content-Type. Choose from the options: CUSTOM, HTML, JSON, PLAIN, XML.
Attributes	Specifies the mapping for attributes used in the content to parametrized values from the request.

Import Context Server Actions

Select **Import** on the upper right corner of the page.

The imported file will be in XML format. To view a sample of this XML format, export a dictionary file and open it in an XML viewer.

Figure 445: *Import Context Server Actions*

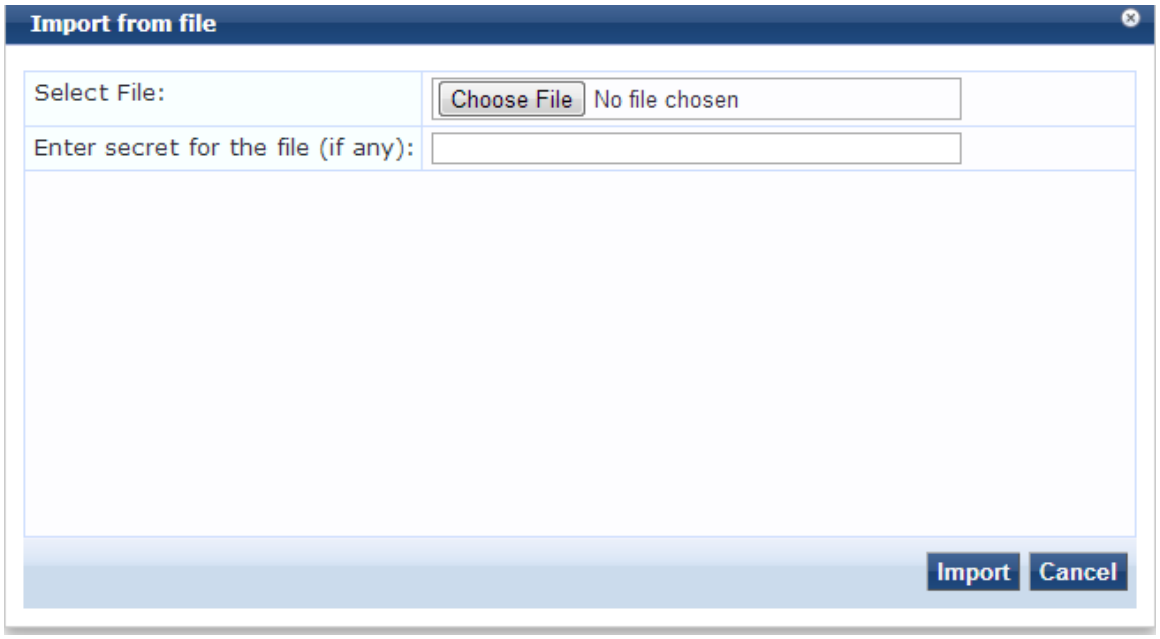


Table 301: *Import Context Server Action*

Parameter	Description
Select File / Enter secret for the file (if any)	Browse to the dictionary file to be imported. Enter the secret key (if any) that was used to export the dictionary.
Import/Cancel	Click **Import** to commit, or **Cancel** to dismiss the popup.

Export Context Server Actions

Select **Export All** on the upper right portion of the page.

The file that you export will be sent to your default download folder in XML format. To view a sample of this XML format, export a dictionary file and open it in an XML viewer.

Table 302: *Export Content Server Action*

Parameter	Description
Export file with password protection	If you click No, the Secret Key and Verify Secret fields are not available. If you click Yes, enter the Secret Key information in the Secret Key field. The secret key that you enter is the same key that was used during Context Server configuration. Enter the Secret Key in the Verify Secret field.
Export/Cancel	Click **Export** to commit, or **Cancel** to dismiss the popup.

OnGuard Settings

Use the **OnGuard Settings** page (**Administration** > **Agents and Software Updates** > **OnGuard Settings**) to configure the agent deployment packages. Once the configuration is saved, agent deployment packages are created for Windows and Mac OS X operating systems and provided at a fixed URL on the Policy Manager appliance. This URL can then be published to the user community. The agent deployment packages can also be downloaded to another location.

The following figure shows an example of the **OnGuard Settings** page followed by parameter definition:

Figure 446: *OnGuard Settings*

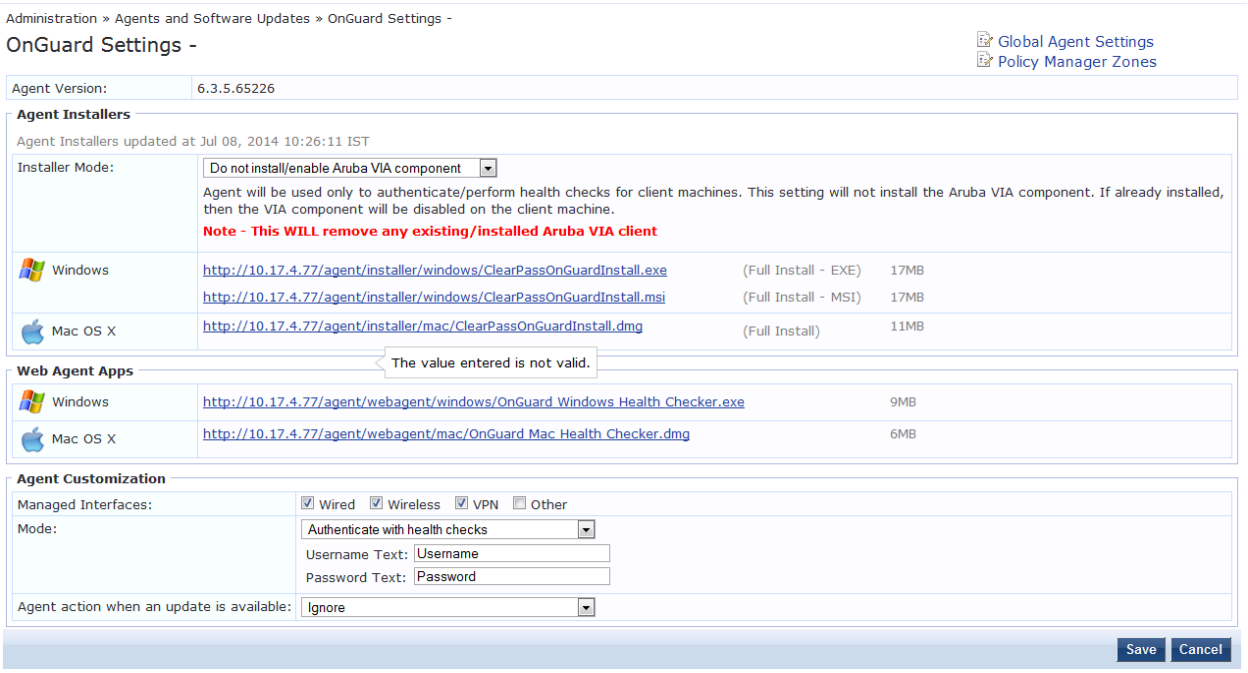


Table 303: *OnGuard Settings*

Container	Description
Global Agent Settings	Configure the global parameters for OnGuard agents. The global parameters include the following: • **Allowed Subnets for Wired access:** Add comma-separated list of IP or subnet addresses. • **Allowed Subnets for Wireless access**: Add comma-separated list of IP or subnet addresses. • **Cache Credentials Interval (in days):** Select the number of days the user credentials should be cached on OnGuard agents. • **Delay to bounce after Logout (in minutes):** Specify the number of minutes that should elapse before OnGuard bounces the interface if OnGuard remains disconnected. • **Enable OnGuard requests load-balancing:** Enable this option to load balance OnGuard authentication requests across Dell Networking W-ClearPass Policy Manager servers in a cluster. • **Enable access over Remote Desktop Session:** Enable this option to allow OnGuard access through a Remote Desktop session. • **Enable to hide Logout button:** Enable this option to hide the **Logout** button on OnGuard agent. • **Install VPNComponent:** Enable this option to install the OnGuard VPN component. • **Enable to use Windows Single-Sign On**: Enable this option to allow use of a user's Windows credentials for authentication. • **Keep-alive Interval (in seconds):** Add a keep alive interval for OnGuard agents. • **OnGuard Health Check Interval (in hours):** Specify the number of hours that OnGuard will skip health checks for healthy clients. **NOTE:** Note the following information when you set the **OnGuard Health Check Interval** parameter: ▪ You can set this parameter if OnGuard mode is set to health only. ▪ This parameter is valid only for wired and wireless interface types. ▪ This parameter is not applicable for the OnGuard Dissolvable Agent, VPN, and other interface types. You can also specify the health check interval in the **Agent enforcement** (**Configuration** > **Agent enforcement** > **New attribute**) profile to create different Agent Enforcement Profiles for different users. • **Support Team Email Address:** Enter an email address that automatically populates the **To** field in the user's email client when they send logs.
Policy Manager Zones	Configure the network (subnet) for a Policy Manager Zone.
Agent Version	Specifies the current agent version.
Agent Installers	
Installer Mode	Specify the action to be taken from the following options when the Dell VIA component is used to provide VPN-based access: • Do not install/enable Dell VIA component • Install and enable Dell VIA Component

Table 303: *OnGuard Settings (Continued)*

Container	Description
Windows	Use the download link to download OnGuard Agent for Windows.This binary file is in .exe and .msi formats.
Mac OS X	Use the download link to download OnGuard Agent for Mac OS X. This binary file is in .DMG format.
Web Agent Apps	
Windows	Click the URL to download Native Dissolvable Agent for Windows.
Mac OS X	Click the URL to download Native Dissolvable Agent for Mac OS X.
Agent Customization	
Managed Interfaces	Select the type(s) of interfaces that OnGuard will manage on the endpoint. Options include: • Wired • Wireless • VPN • Other
Mode	Select one of the following options: • Authenticate - no health checks. • Check health - no authentication. OnGuard does not collect username/password. • Authenticate with health checks - OnGuard collects username/password and also performs health checks on the endpoint.
Username/Password text	The label for the username/password field on the OnGuard agent. This setting is not valid for the **Check health - no authentication** mode.
Agent action when an update is available	Determines what the agent does when an update is available. Select from the following options: • **Ignore** - Dell Networking W-ClearPass Policy Manager ignores the available update. • **Notify User** - Dell Networking W-ClearPass Policy Manager notifies the user that an update is available. • **Download and Install** - Dell Networking W-ClearPass Policy Manager automatically downloads and installs an update is available.

Software Updates

Navigate to **Administration > Agents and Software Updates > Software Updates**.

Use the **Software Updates** page to register for and to receive live updates for:

- Posture updates, including Antivirus, Antispyware, and Windows Updates
- Profile data updates, including Fingerprint

- Software upgrades for the ClearPass family of products
  - Patch binaries, including Onboard, Guest Plugins, and Skins

You can also:

- Reinstall a patch in the event the previous installation attempt fails.
- Uninstall a skin, translation, or plug-in.

The Dell Networking W-ClearPass Policy Manager checks for available updates to the ClearPass webservice server. The administrator can download and install these updates directly from the Software Updates page. The first time the Subscription ID is saved, Dell Networking W-ClearPass Policy Manager performs the following:

- Contacts the webservice to download the latest Posture & Profile Data updates.
- Checks for any available firmware and patch updates.

.

Figure 447: *Software Updates Page*

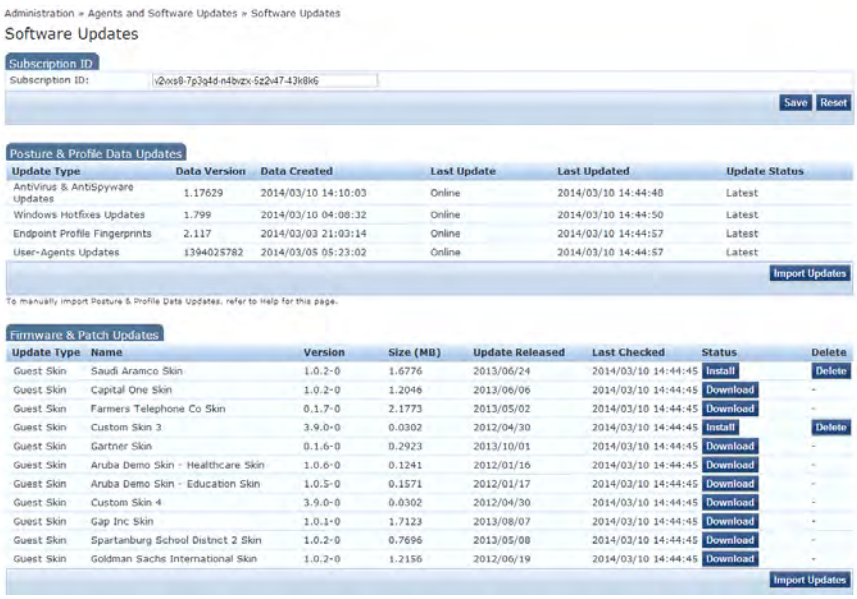


Table 304: *Software Updates Page Parameters*

Parameter	Description
Subscription ID	
Subscription ID	Enter the Subscription ID provided to you. This text box is enabled only on a Publisher node. You can opt out of automatic downloads at any time by saving an empty Subscription ID.
Save	To save the Subscription ID, click the **Save** button. This button is enabled only on a Publisher node.
Reset	Performs an "undo" of any unsaved changes you have made in the Subscription ID field. **NOTE:** Reset does not clear the text box.

Table 304: *Software Updates Page Parameters (Continued)*

Parameter	Description
Posture & Profile Data Updates	
Import Updates	If this Dell Networking W-ClearPass Policy Manager server is not able to reach the webservice server, use **Import Updates** to import (upload) the Posture and Profile Data into this server. You can download the data from the webservice server by accessing the following URL: https://clearpass.dell-pcw.com/cppm/appupdate/cppm_apps_updates.zip When prompted, enter the provided Subscription ID for the username and the password. **NOTE:** In a cluster, the **Import Updates** option is available on the Publisher node only.
Firmware & Patch Updates	
Import Updates	If the server is not able to reach the webservice server, click **Import Updates** to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server. These patch binaries will appear in the table and can be installed by clicking on the **Install** button. When logged in as appadmin, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands: • `system update` (for patches) • `system upgrade` (for upgrades) If a patch requires a prerequisite patch, that patch's **Install** button will not be enabled until the prerequisite patch is installed.
Install	The **Install** button appears after the update has been downloaded. When you click **Install**, the installation of the update starts and the Install Update dialog box displays, showing the log messages being generated.
Re-Install	Click **Re-Install** to reinstall a patch in the event the previous attempt to install fails. Reinstalling a patch is available only for the last installed patch.
Uninstall	Click **Uninstall** to uninstall a skin, translation, or plugin.
Needs Restart	The **Needs Restart** link appears when an update needs a reboot of the server in order to complete the installation. Clicking on this link displays the Install Update dialog box, which shows the log messages generated during the installation.
Installed	The **Installed** link appears when an update has been successfully installed. Clicking on this link displays the Install Update dialog box,which shows the log messages generated during the installation.
Install Error	This link appears when an update install encounters an error. Clicking on this link displays the Install Update dialog box, which shows the log messages generated during the install.

Table 304: *Software Updates Page Parameters (Continued)*

Parameter	Description
Other	
Check Status Now	Click this button to perform an on-demand check for available updates. **Check Status Now** applies to updates (only on a publisher node, as well as Firmware & Patch Updates).
Delete	Use this option to delete a downloaded update.

The Firmware & Patch Updates table shows only the data that is known to webservice or imported using the **Import Updates** button.

Install Update Dialog Box

The Install Update dialog box shows the log messages generated during the installation of an update. This popup appears when you click the **Install** button.

If the popup is closed, you can bring it up again by clicking the **Install in progress...** link while the installation is in progress, or by clicking the **Installed**, **Install Error**, or **Needs Restart** link when the installation is completed.

Figure 448: *Install Update Page*

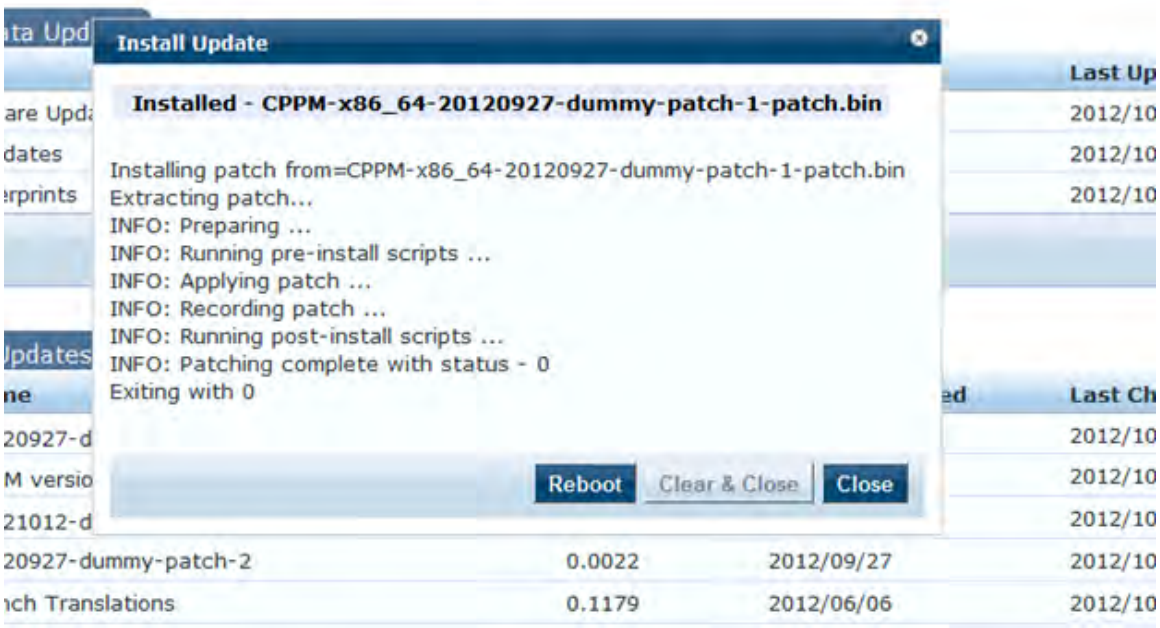


Table 305: *Install Update Page Parameters*

Parameter	Description
Close	Click this button to close the dialog box.
Clear & Close	Click this button to delete the log messages and close the popup. **Clear & Close** also removes the corresponding row from the Firmware & Patch Updates table.
Reboot	The **Reboot** button appears only for updates that require a reboot to complete the installation. To initiate a reboot of the server, click **Reboot**.

To delete the log messages from a failed installation, use the **Clear & Close** button on the Install Update dialog box. After the log messages are cleared, attempt the installation again.

System Events (as seen on the **Monitoring > Event Viewer** page) show records for events, such as communication failures with webservice, successful or failed download of updates, and successful or failed installation of updates.

The Dell Networking W-ClearPass Policy Manager server contacts the webservice server every hour (in the background) to download any newly available Posture & Profile Data updates. The current list of firmware and patch updates is queried from webservice every day at a random minute between 4:00 a.m and 5:00 a.m.

Any new list of firmware and update patches that are available are noted by the Policy Manager server automatically and shown in the UK that they are available for download and installation. The webservice itself is refreshed with the Antivirus and Antispyware data hourly, with Windows Updates daily. Fingerprint data and Firmware & Patches are refreshed as and when new ones are available.

An event is generated (and displayed in the Event Viewer) with the list of new updates that are available. If the event affects an SMTP server, Alert Notification email addresses are configured, and an email (from the Publisher) is sent with the list of downloaded images.

Reinstalling a Patch

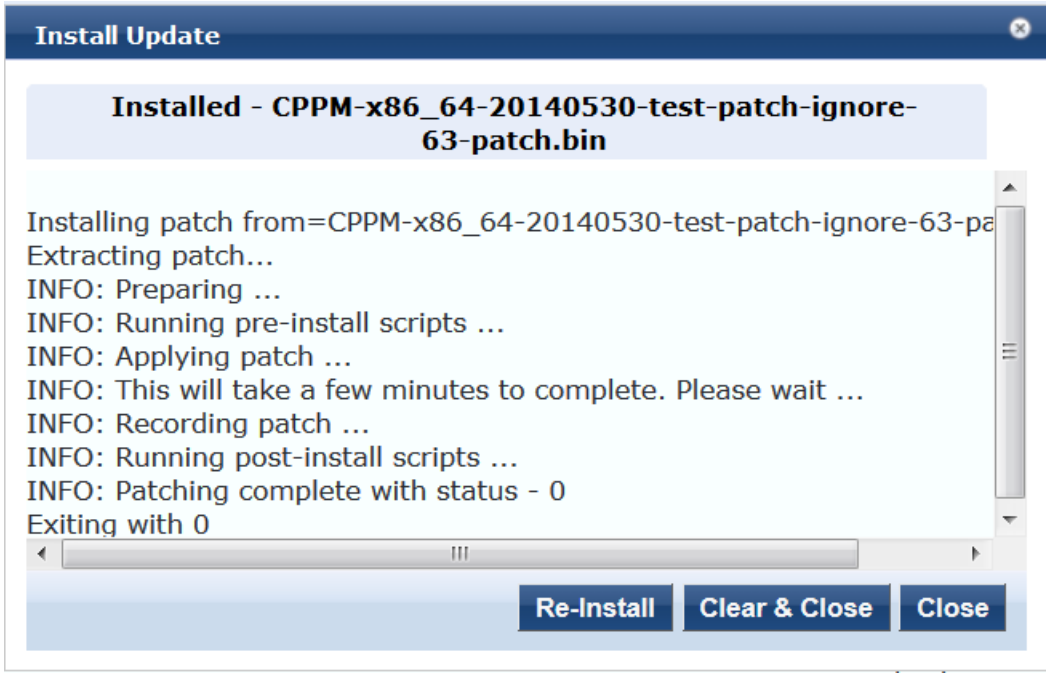
The Reinstall Patch feature allows the ClearPass Policy Manager Administrator to reinstall a patch in the event the previous attempt to install fails. You can only reinstall the last installed patch, which is indicated by a "!" symbol next to it in the Firmware & Patch Updates table on the **Administration > Agents and Software Updates > Software Updates** page.

To reinstall a patch or software update:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.
   The Software Updates screen appears.
2. In the Firmware & Patch Updates section, observe the Status column.
3. To bring up the dialog that shows the logs, click the **Installed**, **Install Error**, or

Needs Restart link.

   The Install Update screen appears.



4. To reinstall the patch or software update, click **Re-Install**.

   The Install Update screen closes and the reinstallation process begins. A pop-up displays, showing the installation progress via log messages.

Uninstalling a Skin, Translation, or Plugin

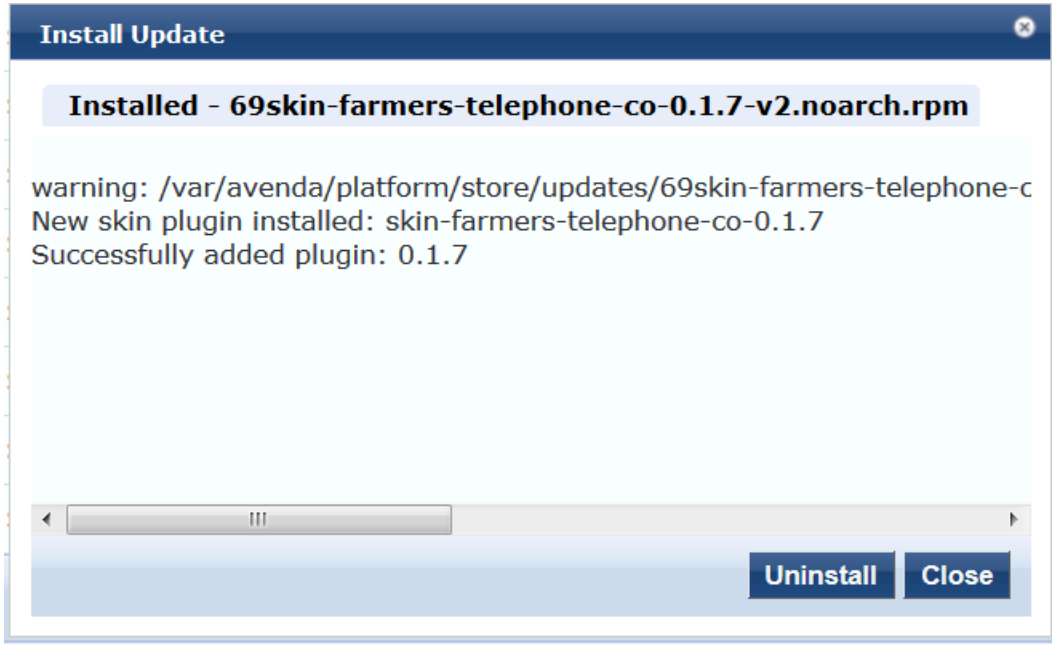
The ClearPass Policy Manager Administrator can uninstall a Skin, Translation, or Plugin.

To uninstall one of these elements:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.

   The Software Updates screen appears.
2. In the Firmware & Patch Updates section, observe the Status column.
3. To bring up the dialog that shows the logs, click the **Installed** link.

   The Install Update screen appears.



4. To uninstall the patch or software update, click **Uninstall**.
   The Install Update screen closes and the software is uninstalled.

Updating the Policy Manager Software

By way of background, the Policy Manager Publisher node acts as master. Administration, configuration, and database write operations are allowed only on this master node. The Policy Manager appliance defaults to a Publisher node unless it is made a Subscriber node. A Policy Manager cluster can contain only one Publisher node. Cluster commands can be used to change the state of the node, hence the Publisher can be made a Subscriber.

NOTE

MySQL is supported in versions 6.0 and newer. Dell does not ship MySQL drivers by default. If you require MySQL, contact Dell support to get the required patch. This patch does not persist across upgrades, so customers using MySQL should contact support before they upgrade.

Upgrade the Image on a Single Policy Manager Appliance

Perform these steps to upgrade the image on a single Policy Manager appliance:

1. From the ClearPass Policy Manager UI, navigate to **Administration > Agents and Software Updates > Software Updates**.
   - If a Subscription ID has been entered, then the server can communicate with the Web service. Available upgrades will be listed in the Firmware & Patches table. Download and install the upgrade, and then reboot the server.
   - If the Subscription ID has not been entered, or if the appliance cannot communicate with the Web service, click **Import Updates** to upload the upgrade image that you received from Support (or through other means). Imported updates will appear in the table and can be installed by clicking the Install button. (The upgrade file is now available and can be specified in the `system upgrade` CLI command.)

Alternatively, transfer the image file to a Policy Manager external machine and make it available via http or SSH.

1. Login to the Policy Manager appliance as *appadmin* user.

2. Use the command `system upgrade`, which will upgrade your second partition, then reboot. Policy Manager boots into the upgraded image.

If you access the appliance via serial console, you should also be able to boot into the previous image by choosing that image in the Grub boot screen.

3. Verify that all configuration and session logs are restored and all services are running. Also verify that node-specific configuration such as the server certificate, log configuration and server parameters are also restored.

Upgrade the Image on all Appliances

Perform these steps to upgrade the image on all appliances in a Policy Manager cluster.

1. Upgrade publisher Policy Manager first, and reboot into the new image.
2. On the first boot after upgrade, all old configuration data is restored. Verify that all configuration and services are intact.

   In the cluster servers screen, all subscriber node entries are present but marked as **Cluster Sync**=**false** (disabled for replication). Any configuration changes performed in this state do not replicate to subscribers until the subscribers are also upgraded (effectively no configuration changes are possible on subscribers in this state).

You can add a subscriber to the cluster from the User Interface: **Configuration** > **Administration** > **Server Configuration** (page) > **Make Subscriber** (link).

3. One node at a time, upgrade the subscriber nodes to the same Policy Manager version as the publisher, using the same steps as for a single Policy Manager server. On the first boot after upgrade, the node is added back to the cluster (the publisher node must be up and available for this to work).
4. Login to the UI and verify that the node is replicating and **Cluster Sync** is set to true.

If the publisher is not available when the subscriber boots up after the upgrade, adding the node back to the cluster fails. In that case, the subscriber comes up with an empty database. Fix the problem by adding the subscriber back into the cluster from the CLI. All node configuration, including certificates, log configuration and server parameters are restored (as long as the node entry exists in the publisher with Cluster Sync=false).

Support

The **Administration** > **Support** pages provide information for contacting support, setting up a remote assistance session, and viewing ClearPass documentation. For more information, see:

- Contact Support on page 472
- Remote Assistance on page 473
- Documentation on page 476

Contact Support

The **Administration > Support > Contact Support** page provides you with information on how to contact Dell Support.

Figure 449: *Contact Support*

Remote Assistance

The Remote Assistance feature enables the Dell Networking W-ClearPass Policy Manager administrator to allow an Aruba Networks support engineer to remotely log in using ssh to the ClearPass Policy Manager server and also view the Administration UI to debug any issues customer is facing or to perform pro-active monitoring of the server.

Remote Assistance Process Flow Description

1. Administrator schedules a Remote Assistance session for a specific duration.
2. The Aruba Networks support contact receives an email with instructions and credentials to login to the remote system.
3. The session is terminated at the end of the specified duration.
4. The Administrator can terminate a session before its stipulated duration from User Interface.
5. The support contact can terminate the session before the specified duration time expires.

Configuring a Remote Assistance session through a CLI can be used if the CPPM UI at the customer site is inaccessible.

Figure 450: *Remote Assistance Session Page*

Table 306: *Remote Assistance Session Page Parameters*

Parameter	Description
Name	Text name of session.
Type	Indicates if the session is a one-time session or a periodic session. Move the cursor over the entry to view the schedule of the session.
Support Contact	The email address of the support contact.
Status	Provides the session state. Available states are: • Saving • Scheduled • Initiated • Running • Terminated • Failed **NOTE:** A session in any of Scheduled, Terminated, and Failed states can be edited and saved. Only a session in Running state can be Terminated by selecting that session and clicking Terminate. A session in any of Scheduled, Terminated and Failed states can be deleted by selecting that session and clicking **Delete**. If a session fails, the Event Viewer will indicate the cause of failure.
Timestamp	The server time when the status was last updated.

Adding a Remote Assistance Session

The Administrator can click the Add Session link to create a session on a ClearPass Policy Manager server in the cluster. Sessions can only be saved and deleted from the Publisher in a cluster. Sessions can be terminated from a Publisher or from Subscribers in a cluster.

To set up a session, click **Add Session**.

Table 307: *Add Session Page*

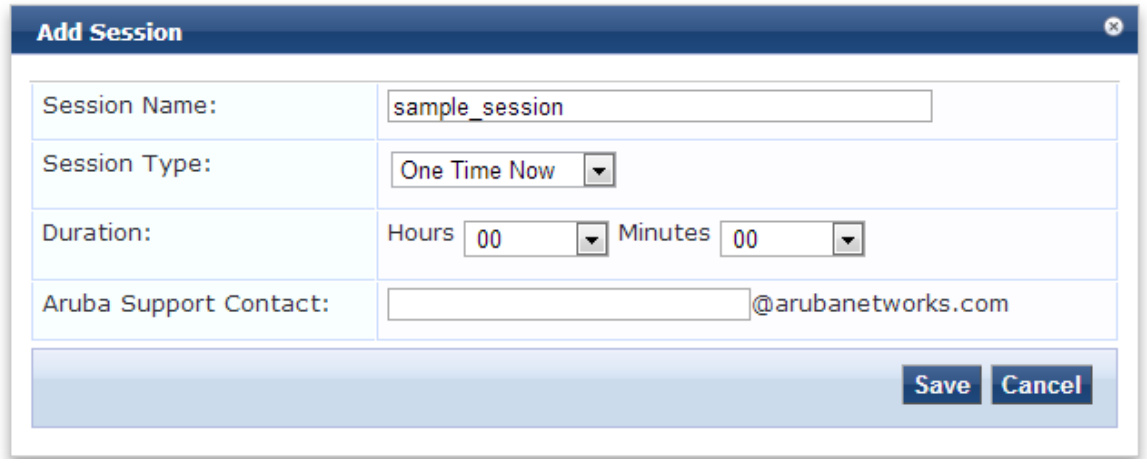
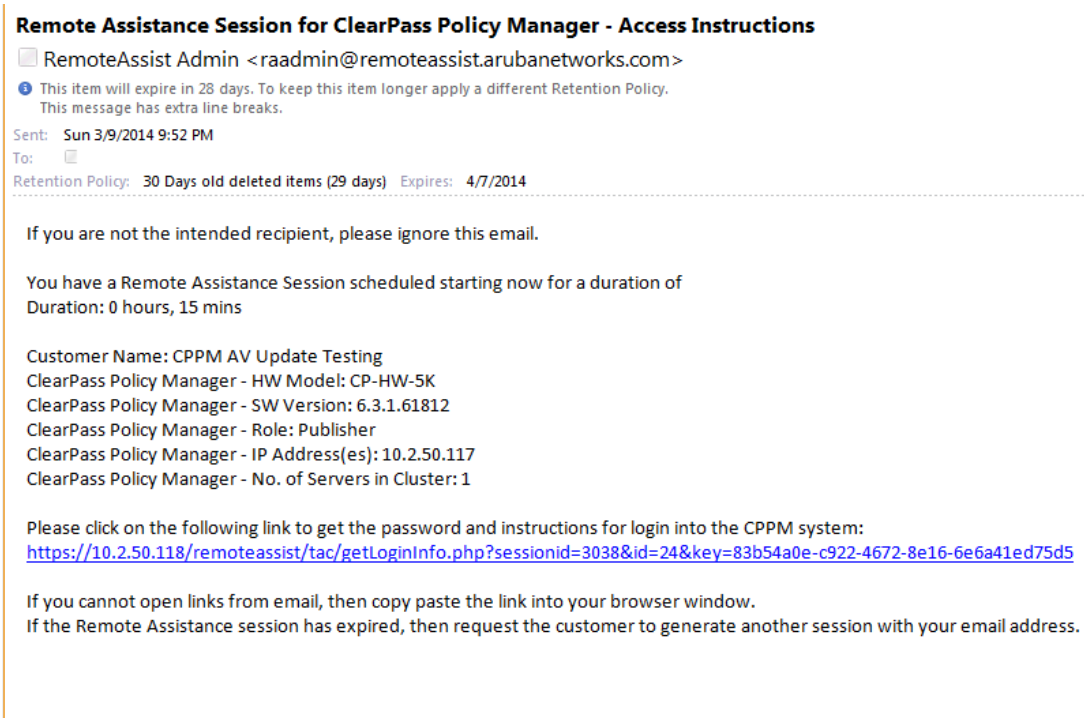


Table 308: *Add Session Page Parameters*

Parameter	Description
Session Name	Text name of session.
Session Type	• One Time Future (will initiate a session in future, on a selected date and time) • Weekly (will initiate a session on a selected Weekday at the selected time) • Monthly (will initiate a session on a selected day of every month at the selected time)
Duration	The duration of a session is specified in Hours and Minutes. The "session begin" time saved is the time relative to server's time, and is specified in a 24-hour clock format.
Status	Indicates the session state. Available states are: • Saving • Scheduled • Initiated • Running • Terminated • Failed
Aruba Support Contact	The Aruba Support Contact is just the email-id of the support contact ('@arubanetworks.com' is appended to the ID.

The next figure is an example of an email that a support technician might receive after a Remote Assistance Session is scheduled.

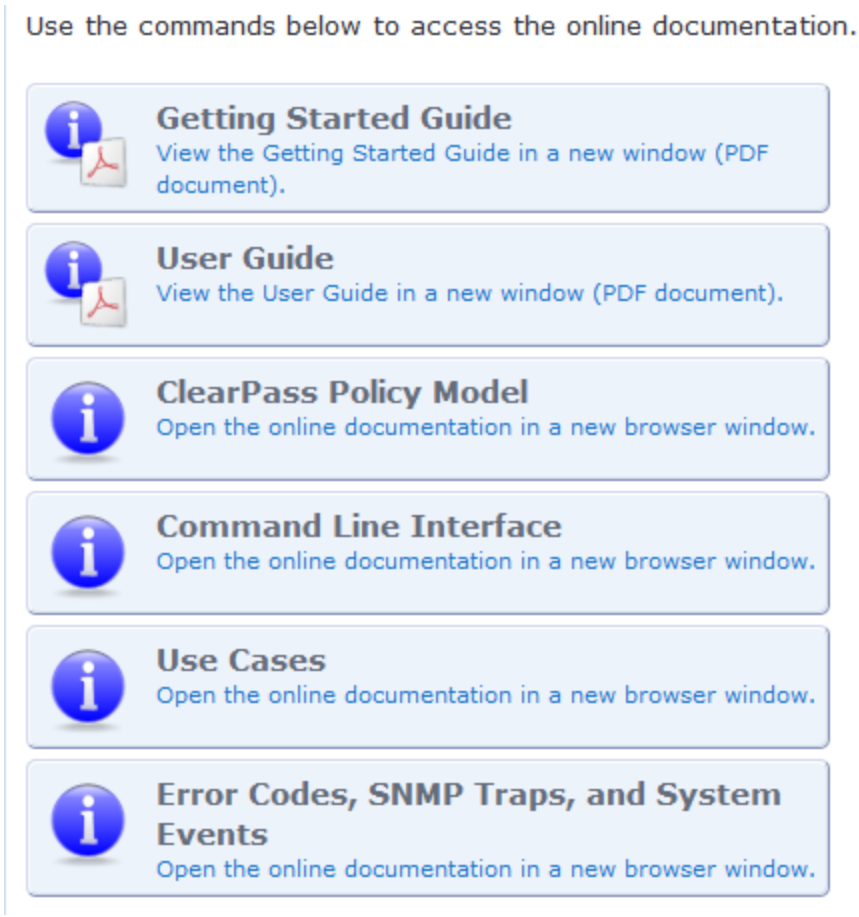
Figure 451: *Example of a Remote Assistance Session Notification Email*



Documentation

The **Administration > Support > Documentation** page includes links to various sections of the ClearPass Policy Manager Online Help system. For example, to view documentation for the CLI, click the Command Line Interface button. This page also provides links to PDF versions of the *Dell Networking W-ClearPass Policy Manager 6.4 User Guide* and the *Dell Networking W-ClearPass Policy Manager 6.4 Getting Started Guide*.

Figure 452: *Documentation page*



Refer to the following sections:

Available Commands

Table 309: *Command Categories*

Command
ad auth See Miscellaneous Commands on page 504
ad netleave See Miscellaneous Commands on page 504
ad netjoin See Miscellaneous Commands on page 504
ad testjoin See Miscellaneous Commands on page 504
alias See Miscellaneous Commands on page 504
backup See Miscellaneous Commands on page 504
cluster drop-subscriber
cluster list
cluster make-publisher
cluster make-subscriber
cluster reset-database
cluster set-cluster-passwd

Table 309: *Command Categories (Continued)*

Command
cluster set-local-passwd
configure date
configure dns
configure hostname
configure ip
configure timezone
dump certchain See Miscellaneous Commands on page 504
dump logs See Miscellaneous Commands on page 504
dump servercert See Miscellaneous Commands on page 504
exit See Miscellaneous Commands on page 504
help See Miscellaneous Commands on page 504
krb auth See Miscellaneous Commands on page 504
krb list See Miscellaneous Commands on page 504
ldapsearch See Miscellaneous Commands on page 504
network ip
network nslookup
network ping
network traceroute
network reset
quit See Miscellaneous Commands on page 504
restore

Table 309: *Command Categories (Continued)*

Command
See Miscellaneous Commands on page 504
service activate
service deactivate
service list
service restart
service start
service status
service stop
show date
show dns
show domain
show all-timezones
show hostname
show ip
*show*license
show timezone
show version
system boot-image
system gen-support-key
system update
system restart
system shutdown
system install-license
system upgrade

Cluster Commands

The Policy Manager command line interface includes the following *cluster* commands:

- drop-subscriber on page 480

drop-subscriber

Use the **drop-subscriber** command to remove a specific subscriber node from the cluster.

Syntax

```
cluster drop-subscriber [-f] [-i <IP Address>] -s
```

The following table describes the required and optional parameters for the **drop-subscriber** command:

Table 310: *Drop-Subscriber Command Parameters*

Flag/Parameter	Description
-f	Forces to drop even the nodes that are down.
-i <IP Address>	Specifies the Management IP address of the node. If this IP address is not specified and the current node is a subscriber, then Policy Manager drops the current node.
-s	Restricts resetting the database on the dropped node. By default, Policy Manager drops the current node (if a subscriber) from the cluster.

Example

The following example removes the IP address 192.xxx.1.1 from the cluster:

```
[appadmin]# cluster drop-subscriber -f -i 192.xxx.1.1 -s
```

list

Use the **list** command to list the cluster nodes.

Syntax

```
cluster list
```

Example

The following example lists all the cluster nodes:

```
[appadmin]# cluster list
cluster list
Publisher  :
Management port IP=192.xxx.5.227

Data port IP=None [local machine]
```

make-publisher

Use the **make-publisher** command to makes a specified node as a publisher.

Syntax

```
cluster make-publisher
```

Example

The following example makes a node as a publisher:

```
[appadmin]#  cluster make-publisher
******************************************************
* WARNING: Executing this command will promote the     *
* current machine (which must be a subscriber in the   *
* cluster) to the cluster publisher. Do not close the  *
* shell or interrupt this command execution.           *
******************************************************
Continue? [y|Y]: y
```

make-subscriber

Use the **make-subscriber** command to make a node as a subscriber node.

Syntax

```
make-subscriber -i <IP Address> [-l]
```

The following table describes the required and optional parameters for the **make-subscriber** command:

Table 311: *Make-Subscriber Command Parameters*

Flag/Parameter	Description
-i <IP Address>	Specifies the publisher IP address. This field is mandatory.
-l	Restores the local log database after this operation. This field is optional.

Example

The following example makes 192.xxx.1.1 as a subscriber node:

```
[appadmin]#  cluster make-subscriber –i 192.xxx.1.1 –p !alore -l
```

reset-database

Use the **reset-database** to reset the local database and erases its configuration.

Syntax

```
cluster reset-database
```

Example

The following example reset the database:

```
[appadmin]#  cluster reset-database
******************************************************
* WARNING: Running this command will erase the Policy Manager    *
* configuration and leave the database with default     *
* configuration. You will lose all the configured data. *
```

```
* Do not close the shell or interrupt this command       *
* execution.                                              *
**********************************************************
Continue? [y|Y]: y
```

set-cluster-passwd

Use the **set-cluster-passwd** to change the cluster password on all publisher nodes. If this command is executed on the publisher, the publisher prompts for the new cluster password.

Syntax

```
cluster set-cluster-passwd
```

Example

The following example changes the cluster password on publisher nodes:

```
[appadmin]#  cluster set-cluster-passwd
cluster set-cluster-passwd
Enter Cluster Passwd: santaclara
Re-enter Cluster Passwd: santaclara
INFO - Password changed on local (publisher) node
Cluster password changed
```

set-local-passwd

Use the **set-local-passwd** command to change the local password. When you execute this command locally, it prompts for the new local password.

Syntax

```
cluster sync-local-password
```

Example

The following example changes the local password:

```
[appadmin]#  cluster set-local-password
cluster sync-local-passwd
Enter Password: !alore
Re-enter Password: !alore
```

Configure Commands

The Policy Manager command line interface includes the following **configuration** commands:

date

Use the **date** command to set System Date, Time, and Time Zone.

Syntax

```
configure date -d <date> [-t <time> ] [-z <timezone>]
```

or

```
configure date -s <ntpserver> [-z <timezone>]
```

The following table describes the required and optional parameters for the **date** command:

Table 312: *Date Command Parameters*

Flag/Parameter	Description
-s <ntpserver>	Synchronizes time with the specified NTP server. This field is optional. **NOTE:** You can specify a destination node with the IPv6 address enabled.
-d <date>	Specifies the syntax: **yyyy-mm-dd**. This field is mandatory.
-t <time>	Specifies the syntax: **hh:mm:ss**. This field is optional.
-z <timezone>	Specifies the syntax. To view the list of supported timezone values, enter `show all-timezones`. This field is optional.

Example 1

The following example configures date, time, or timezone:

```
[appadmin]#  configure date -d 2007-06-22 -t 12:00:31 -z America/Los_Angeles
```

Example 2

The following example synchronizes with a specified NTP server:

```
[appadmin]# -s <ntpserver>
```

dns

Use the **dns** command to configure DNS servers. Specify minimum of one DNS server and you can specify a maximum of three DNS servers.

Syntax

```
configure dns <primary> [secondary] [tertiary]
```

Example 1

The following example configures a DNS server:

```
[appadmin]# configure dns 192.168.xx.1
```

Example 2

The following example configures primary and secondary DNS servers:

```
[appadmin]# configure dns 192.168.xx.1 2001:4860:4860::8888
```

You can configure IPv6 address as described in this example.

Example 3

The following example configures primary, secondary, and tertiary DNS servers:

```
[appadmin]#  configure dns 192.168.xx.1 2001:4860:4860::8888 192.168.xx.2
```

fips-mode

Use the **fips-mode** command to enable or disable the **FIPS** mode.

Syntax

```
configure fip-smode [0|1]
```

The following table describes the required and optional parameters for the **fips-mode** command:

Table 313: *fips-mode Command Parameters*

Flag/Parameter	Description
0	Enter 0 to disable the **FIPS** mode. **NOTE:** Read the warning message carefully before enabling or disabling the **FIPS** mode.
1	Enter 1 to enable the **FIPS** mode.

Example 1

The following example disables the **FIPS** mode:

```
[appadmin]# configure fips-mode 0
*****************************************************************
*                                                               *
* WARNING: Running this command will erase the Policy Manager   *
* configuration and leave the database with default             *
* configuration. You will lose all the configured data.         *
*                                                               *
* This command will also shutdown all applications and reboot   *
* the system.                                                   *
*                                                               *
* Do not close the shell or interrupt this command execution.   *
*                                                               *
*****************************************************************
Continue? [y|n]: y
```

Click **y** to disable the **FIPS** mode.

hostname

Use the **hostname** command to configure the hostname.

Syntax

```
configure hostname <hostname>
```

Example

The following example configures a hostname:

```
[appadmin]#  configure hostname sun.us.dellnetworks.com
```

ip

Use the **ip** command to configure IP address, netmask, and gateway.

Syntax

```
[appadmin]#  configure ip <mgmt|data> <ipaddress> netmask <netmask address> gateway <gateway address>
```

The following table describes the parameters used in the **ip** command:

Table 314: *ip Command Parameters*

Flag/Parameter	Description
ip <mgmt|data> <ip address>	Specifies the network interface type: management or data. **<ip address>** specifies the IPv4 address of the host.
netmask <netmask address>	Specifies the netmask address.
gateway <gateway address>	Specifies the gateway address.

Example

The following example configures the IP, netmask, and gateway addresses:

```
[appadmin]#  configure ip data 192.168.xx.12 netmask 255.255.255.0 gateway 192.168.xx.1
```

ip6

Use the **ip6** command to configure the IPv6 address, netmask, and gateway.

Syntax

```
configure ip6 <mgmt|data> <IPv6Address/PrefixLen> gateway <gateway address>
configure ip6 <mgmt|data> <IPv6Address> netmask <netmask address> gateway <gateway address>
```

The following table describes the parameters used in the **ip6** command:

Table 315: *ip6 Command Parameters*

Flag/Parameter	Description
ip6 <mgmt|data> <ip address>	Specifies the Network interface type: management or data. **NOTE: <ip6 address>** specifies the IPv6 address of the host.
netmask <netmask address>	Specifies the netmask address. For example, ffff:ffff:ffff:ffff:0000:0000:0000:0000.
gateway <gateway address>	Specifies the gateway address. For example, fe90:0000:0000:0000:020c:29ff:fe7e:d3a2.

Example

The following example configures the IPv6 management, netmask, and gateway:

```
[appadmin]# configure ip6 mgmt fe90:0000:0000:0000:020c:29ff:fe7e:d3e1 netmask
ffff:ffff:ffff:ffff:0000:0000:0000:0000 gateway fe90:0000:0000:0000:020c:29ff:fe7e:d3a1
```

mtu

Use the **mtu** command to set the Maximum Transmission Unit (MTU) for the management and data port interfaces.

Syntax

```
configure mtu <mgmt|data> <mtu-value>
```

The following table describes the parameters used in the **mtu** command:

Table 316: *mtu Command Parameters*

Flag/Parameter	Description
mtu <mgmt|data>	Specifies the Network interface types: management or data port.
mtu-value	Specify the MTU value in bytes. The default value is 1500 bytes.

Example 1

The following example configures the mtu management interface:

```
[appadmin] # configure mtu mgmt 1498
******************************************************
*                                                    *
* WARNING: Running this command might cause system     *
* to lose network connectivity and may require relogin.*
*                                                    *
******************************************************
Continue? [y|Y]: y
INFO: Restarting network services
INFO: Successfully applied MTU settings
```

Example 2

The following example configures the mtu data port value:

```
[appadmin]# configure mtu data 1498
******************************************************
*                                                    *
* WARNING: Running this command might cause system     *
* to lose network connectivity and may require relogin.*
*                                                    *
******************************************************
Continue? [y|Y]: y
INFO: Restarting network services
INFO: Successfully applied MTU settings
```

Example 3

The following example displays the settings of the mtu management and data port interfaces:

```
[appadmin]# show ip
========================================
Device Type      :   Management Port
----------------------------------------
IPv4 Address     :   10.2.xx.86
Subnet Mask      :   255.255.255.0
Gateway          :   10.2.xx.1
IPv6 Address     :   2607:f0d0:1002:0011:0000:0000:0000:0002
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
```

```
Gateway          :   2607:f0d0:1002:0011:0000:0000:0000:0001
Hardware Address :   00:0C:29:70:27:40
MTU              :   1499
==========================================
Device Type      :   Data Port
------------------------------------------
IPv4 Address     :   <not configured>
Subnet Mask      :   <not configured>
Gateway          :   <not configured>
IPv6 Address     :   fe80:0000:0000:0000:020c:29ff:fe70:274a
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   fe80:0000:0000:0000:020c:29ff:fe70:2741
Hardware Address :   00:0C:29:70:27:4A
MTU              :   1498
==========================================
DNS Information
------------------------------------------
Primary   DNS  :   10.2.xx.3
Secondary DNS  :   10.1.xx.50
Tertiary  DNS  :   10.1.xx.200
==========================================
```

timezone

Use the **timezone** command to configure time zone interactively.

Syntax

```
configure timezone
```

Example

The following example configures the timezone interactively:

```
[appadmin]#  configure timezone
configure timezone
*******************************************************
* WARNING: When the command is completed Policy Manager services *
* are restarted to reflect the changes.                 *
******************************************************
Continue? [y|Y]:  y
```

Network Commands

The Policy Manager command line interface includes the following **network** commands:

ip

Use the **ip** command to add, delete, or list custom routes to the data or management interface routing table.

Syntax

```
network ip add <mgmt|data|greN> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]> [-g <ViaAddr>]
```

The following table describes the required and optional parameters for the **ip** command:

Table 317: *IP Command Parameters*

Flag/Parameter	Description
<mgmt | data| greN>	Specifies management interface, data interface or the name of the GRE tunnel. In <greN>, N specifies the GRE tunnel number ranging from 1,2,3...N.
-i <id>	Specifies the ID of the network IP rule. If this ID is not specified, the system generates an ID automatically. **NOTE:** This ID determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Specifies the IP address or network. For example, 192.168.xx.0/24 or 0/0 (for all traffic) of traffic originator. You must specify only one SrcAddr or DstAddr. This parameter is optional.
-d <DestAddr>	Specifies the destination IP address or network. For example, 192.168.xx.0/24 or 0/0 (for all traffic). You must specify only one SrcAddr or DstAddr. This parameter is optional.

Syntax

```
network ip del <-i <id>>
```

The following table describes the required and optional parameters for the **ip del <-i <id>>** command:

Table 318: *Network IP Delete Command Parameters*

Flag/Parameter	Description
-i <id>	Specifies the ID of the rule to delete.

Syntax

```
network ip list
```

This command lists all routing rules.

Syntax

```
network ip reset
```

This command reset routing table to factory default setting. All custom routes are removed. The following examples add and list the custom routes:

Example 1

The following example adds a custom route:

```
[appadmin]# network ip add data -s 192.168.xx.0/24
```

Example 2

The following example lists all custom routes:

```
[appadmin]# network ip list
================================================
            IP Rule Information
------------------------------------------------
0:      from all lookup local
10020:  from all to 10.xx.4.0/24 lookup mgmt
10040:  from 10.xx.4.200 lookup mgmt
10060:  from 10.xx.5.200 lookup data
32766:  from all lookup main
32767:  from all lookup default
================================================
```

ip6

Use the **ip6** command to add, delete, or list custom routes to the data or management interface routing table.

Syntax

```
network ip6 add <mgmt|data> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]>
```

The following table describes the required and optional parameters for the **ip6** command:

Table 319: *IP Command Parameters*

Flag/Parameter	Description
<mgmt|data>	Specifies management or data interface
-i <id>	Specifies the ID of the network ip rule. If this ID is not specified, the system generates an ID automatically. **NOTE:** This ID determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Specifies the source interface IPv6 address or netmask from where the network IPv6 rule is specified. For example, fe82::20c:29ff:fe7e:d3e1. The valid IPv6 address or netmask or 0/0 values are allowed. This parameter is optional.
-d <DestAddr>	Specifies the destination interface IPv6 address or netmask where the network IPv6 rule is specified. For example, fe82::20c:29ff:fe7e:d3e9. The valid IPv6 address or netmask or 0/0 values are allowed. This parameter is optional.
-g <ViaAddr>	Specifies the via or gateway IPv6 address through which the network traffic should flow. The valid IPv6 address is allowed. This parameter is optional.

Syntax

```
network ip6 del <-i <id>>
```

This command deletes a custom route.

Syntax

```
network ip6 list
```

This command lists all custom routing rules.

Syntax

```
network ip6 reset
```

This command reset routing table to factory default setting and all custom routes are removed. The following examples add and list the custom routes:

Example 1

The following example adds a custom route:

```
[appadmin]# network ip6 add data -s fe82::20c:29ff:fe7e:d3e1/d3e24
```

You can use IPv6 address when adding a custom route.

Example 2

The following example lists all custom routing rules:

```
[appadmin]# network ip6 list

=============================================
IP Rule Information
---------------------------------------------
0:      from all lookup local
13000:  from all to fe82::20c:99ff:fe7e:d3e1 lookup mgmt
13001:  from all to fe82::20c:99ff:fe7e:d3e4 lookup mgmt
13002:  from all to fe82::20c:99ff:fe7e:d3e7 lookup mgmt
13003:  from all to fe82::20c:99ff:fe7e:d3e8 lookup mgmt
13004:  from all to fe82::20c:99ff:fe7e:d3e9 lookup mgmt
13005:  from all to fe82::20c:99ff:fe7e:d3ea lookup static
32766:  from all lookup main
=============================================
```

nslookup

Use the **nslookup** command to get the IP address of host using DNS.

Syntax

```
nslookup -q <record-type> <host>
```

The following table describes the required and optional parameters for the **nslookup** command:

Table 320: *nslookup Command Parameters*

Flag/Parameter	Description
<record-type>	Specifies the type of DNS record. For example, A, CNAME, and PTR records.
<host>	Specifies the host or domain name to be queried.

Example 1

The following examples obtain the IPv4 and IPv6 addresses of the host or domain using DNS:

```
[appadmin]# nslookup sun.us.dellnetworks.com
[appadmin]# network nslookup 2001:4860:4860::8888
```

Example 2

The following example queries a host or domain for SRV records:

```
[appadmin]# nslookup -q SRV dellnetworks.com
```

Use the **AAAA** flag with the **-q** option to perform network nslookup with IPv6 destinations.

Syntax

```
nslookup -q  AAAA <IPv6_addr>
```

The following example performs network nslookup for the destination with IPv6 address:

Example

```
[appadmin]# network nslookup 2001::93
Server:         2001::94
Address:        2001::94#53
3.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.2.ip6.arpa        name =
ipv6test-n1.cppmipv6.com.
[appadmin]# network nslookup -q AAAA ipv6test-n1.cppmipv6.com
Server:         2001::94
Address:        2001::94#53
ipv6test-n1.cppmipv6.com        has AAAA address 2001::93
```

ping

Use the **ping** command to test the reachability of the network host.

Syntax

```
network ping [-i <SrcIpAddr>] [-t] <host>
```

The following table describes the required and optional parameters for the **ping** command:

Table 321: *Ping Command Parameters*

Flag/Parameter	Description
-i <SrcIpAddr>	Specifies the originating IP address for ping. This field is optional.
-t	Use this parameter to ping indefinitely. This field is optional.
<host>	Specifies the host to be pinged.

Example

The following example pings a network host to test the reachability:

```
[appadmin]# network ping –i 192.168.xx.10 –t sun.us.dellnetworks.com
```

ping6

Use the **ping6** command to test the reachability of the network host.

Syntax

```
network ping6 [-i <SrcIPv6Addr>] [-t] <host>
```

The following table describes the required and optional parameters for the **ping** command:

Table 322: *Ping6 Command Parameters*

Flag/Parameter	Description
-i <SrcIPv6Addr>	Specifies the originating IPv6 address for ping. This field is optional.
-t	Use this parameter to ping indefinitely. This field is optional.
<host>	Specifies the host to be pinged.

Example

The following example pings a network host to test the reachability:

```
[appadmin]#   network ping6 –i fe82::20c:29ff:fe7e:d3e1 –t sun.us.dellnetworks.com
```

reset

Use the **reset** command to reset the network data and management port.

Syntax

```
network reset <data/mgmt>
```

The following table describes the required and optional parameters for the **reset** command:

Table 323: *Reset Command Parameters*

Flag/Parameter	Description
data	Specifies the name of network data port to reset. This parameter is mandatory.
mgmt	Specifies the name of network management port to reset. **NOTE:** You can use this command to reset the IPv4 and IPv6 addresses.

Example

The following example reset the network data port:

```
[appadmin]# network reset data
```

traceroute

Use the **traceroute** command to print the route taken to reach the network host.

Syntax

```
network traceroute <host>
```

The following table describes the required and optional parameters for the **traceroute** command:

Table 324: *Traceroute Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of network host.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]#  network traceroute sun.us.dellnetworks.com
```

traceroute6

Use the **traceroute6** command to print the route taken to reach the network host.

Syntax

```
network traceroute6 <host>
```

The following table describes the required and optional parameters for the **traceroute** command:

Table 325: *Traceroute Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of network host. You can specify the host with IPv6 address.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]# network traceroute6 sun.us.

            dellnetworks
            .com
```

Service Commands

The Policy Manager command line interface includes the following **service** commands:

- start
- stop
- status
- restart
- activate
- deactivate
- list

These commands in this section have identical syntax; therefore, this section presents them as variations on <action>.

<action>

Use the **<action>** command to activate the specified Policy Manager service.

Syntax

```
service <action> <service-name>
```

Where:

Table 326: *Action Command Parameters*

Flag/Parameter	Description
action	Choose an action: *activate, deactivate, list, restart, start, status,* or *stop.*
service-name	Choose a service: *tips-policy-server, tips-admin-server, tips-system-auxiliary-server, tips-radius-server, tips-tacacs-server, tips-dbwrite-server, tips-repl-server,* or *tips-sysmon-server.*

Example 1

```
[appadmin]#  service activate tips-policy-server
```

Example 2

```
[appadmin]#  service list all
service list
Policy server  [ tips-policy-server ]
Admin UI service  [ tips-admin-server ]
System auxiliary services  [ tips-system-auxiliary-server ]
Radius server  [ tips-radius-server ]
Tacacs server  [ tips-tacacs-server ]
Async DB write service  [ tips-dbwrite-server ]
DB replication service  [ tips-repl-server ]
System monitor service  [ tips-sysmon-server ]
```

Example 3

```
[appadmin]#  service status tips-domain-server
```

Show Commands

The Policy Manager command line interface includes the following **`show`** commands:

all-timezones

Use the **`all-timezones`** command to view all available timezones.

Syntax

```
show all-timezones
```

Example

The following example displays all available timezones:

```
[appadmin]#  show all-timezones
Africa/Abidjan
Africa/Accra
.....
WET
Zulu
```

date

Use the **date** command to view the System Date, Time, and Time Zone information.

Syntax

```
show date
```

Example

The following example displays the System Date, Time, and Time Zone information:

```
[appadmin]#  show date
Wed Oct 31 14:33:39 UTC 2012
```

dns

Use the **dns** command to view DNS servers.

Syntax

```
show dns
```

Example

The following example displays DNS servers:

```
[appadmin]#  show dns
show dns
=========================================
          DNS Information
-----------------------------------------
Primary   DNS  :   192.xxx.5.3

Secondary DNS  :   <not configured>
Tertiary  DNS  :   <not configured>
=========================================
```

domain

Use the **domain** command to view the Domain Name, IP Address, and Name Server information.

Syntax

```
show domain
```

Example

The following example displays the domain name:

```
[appadmin]#  show domain
```

fipsmode

Use the **fipsmode** command to find whether the **FIPS** mode is enabled or disabled.

Example

The following example displays that the **FIPS** mode is enabled:

```
[appadmin]# show fipsmode
FIPS Mode: Enabled
```

hostname

Use the **hostname** command to view hostname.

Syntax

```
show hostname
```

Example

The following example displays the hostname:

```
[appadmin]#  show hostname
show hostname
wolf
```

ip

Use the **ip** command to view the IPv4, IPv6, and DNS information of the host.

Syntax

```
show ip
```

Example

The following example displays the IPv4, IPv6, and DNS information of the host:

```
[appadmin]#  show ip
==========================================
Device Type      :   Management Port
------------------------------------------
IPv4 Address     :   10.2.xx.86

Subnet Mask      :   255.255.255.0
Gateway          :   10.2.xx.1

IPv6 Address     :   2607:f0d0:1002:0011:0000:0000:0000:0002
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   2607:f0d0:1002:0011:0000:0000:0000:0001
Hardware Address :   00:0C:29:70:57:40

MTU              :   1499
==========================================
Device Type      :   Data Port
------------------------------------------
IPv4 Address     :   <not configured>
Subnet Mask      :   <not configured>
Gateway          :   <not configured>
IPv6 Address     :   fe80:0000:0000:0000:020c:29ff:fe70:274a
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   fe80:0000:0000:0000:020c:29ff:fe70:2741
Hardware Address :   00:0C:29:70:27:4A
MTU              :   1498
==========================================
DNS Information
------------------------------------------
```

```
Primary   DNS  :   10.2.xx.3

Secondary DNS  :   10.1.xx.50

Tertiary  DNS  :   10.1.xx.200

========================================
```

license

Use the **license** command to view the license key.

Syntax

```
show license
```

Example

The following example displays the license information:

```
[appadmin]#  show license
------------------------------------------------------
Application              : PolicyManager
License key              : VWQO-MW62UO-VMVF-B7GNJT-OHUAZY-IAAM-RTQUPQ-WODIFNJI-CD7N-I5565A

License key type         : Permanent
License added on         : 2014-06-20 10:16:38
Validity                 : <not applicable>
Issued for               : 5000 users
Customer id              : JRC
Licensed features        : <not applicable>
------------------------------------------------------
Application              : PolicyManager
License key              : VWQO-MW62UO-VMVF-B7GNJT-OHUAZY-IAAM-RTQUPQ-WODIFNJI-CD7N-I5565A
License key type         : Permanent
License added on         : 2014-06-20 10:16:38
Validity                 : <not applicable>
Issued for               : 5000 users
Customer id              : JRC
Licensed features        : <not applicable>
======================================================
```

timezone

Use the **timezone** command to view the current system timezone.

Syntax

```
show timezone
```

Example

The following example displays the system timezone:

```
[appadmin]#  show timezone
show timezone

Timezone is set to 'Asia/Kolkata'
```

version

Use the **Version** command to view the Policy Manager software version and the hardware model.

Syntax

```
show version
```

Example

The following example displays the Policy Manager software version and the hardware model:

```
[appadmin]#  show version
=======================================
Policy Manager software version : 2.0(1).6649
Policy Manager model number     : ET-5010
=======================================
```

System Commands

The Policy Manager command line interface (CLI) includes the following **system** commands:

apps-access-reset

Use the **apps-access-reset** command to reset the access control restrictions for Policy Manager.

Syntax

```
system apps-access-reset
```

Example

The following example reset the access control restrictions for Policy Manager:

```
[appadmin]# system apps-access-reset
Policy Manager application access is restored
```

boot-image

Use the **boot-image** to set system boot image control options.

Syntax

```
system boot-image [-l] [-a <version>]
```

The following table describes the required and optional parameters for the **boot-image** command:

Table 327: *Boot-Image Command Parameters*

Flag/Parameter	Description
-l	Lists the boot images installed on the system.
-a <version>	Sets the active boot image version in *A.B.C.D* syntax. This field is optional.

Example

The following example sets the system boot image control options:

```
[appadmin]#  system boot-image -l
```

gen-recovery-key

Use the **gen-recovery-key** command to generate the recovery key for the system.

Example

The following example generates the recovery key for the system:

```
[appadmin]# system gen-recovery-key
Recovery key='04U2FsdGVkX18To8NDWayziQ17LzKA17DW5y+AZvGj41c='
```

gen-support-key

Use the **gen-support-key** command to generate the support key for the system.

Syntax

```
system gen-support-key
```

Example

The following example generates the support key for the system:

```
[appadmin]#  system gen-support-key
system gen-support-key
Support key='01U2FsdGVkX1+/WS9jZKQajERyzXhM8mF6zAKrzxrHvaM='
```

install-license

Use the **install-license** command to replace the current license key with a new one.

Syntax

```
system install-license <license-key>
```

The following table describes the required and optional parameters for the **install-license** command:

Table 328: *Install-License Command Parameters*

Flag/Parameter	Description
<license-key>	Specifies the newly issued license key. This field is mandatory.

Example

The following example replaces the current license key with a new one:

```
[appadmin]#  system install-license
```

morph-vm

Use the **morph-vm** command to convert an evaluation virtual machine (VM) to a production VM. With this command, licenses are still required to be installed after the morph operation is completed.

Syntax

```
system morph-vm <vm-version: CP-VA-500 | CP-VA-5K | CP-VA-25K>
```

The following table describes the required and optional parameters for the **morph-vm** command:

Table 329: *Morph-VM Commands*

Flag/Parameter	Description
<vm-version>	This is the updated ClearPass version. The following three options are available: CP-VA-500 | CP-VA-5K | CP-VA-25K This field is mandatory.

Example

The following example converts an evaluation virtual machine (VM) to a production VM for CP-25K version:

```
[appadmin]# system morph-vm CP-25K
```

refresh-license

Use the **refresh-license** command to refresh the license count information .

Syntax

```
system refresh-license
```

Example

The following example refreshes the license count information:

```
[appadmin]# system refresh-license

INFO: Refreshing license count information

INFO: Successfully refreshed license count information
```

restart

Use the **restart** command to restart the system.

Syntax

```
system restart
```

Example

The following example restarts the system with a confirmation:

```
[appadmin]#  system restart
system restart
******************************************************

* WARNING: This command will shut down all applications *

* and reboot the system                                 *
```

```
******************************************************
Are you sure you want to continue? [y|Y]: y
```

shutdown

Use the **shutdown** command to shut down the system.

Syntax

```
system shutdown
```

Example

The following example shuts down the system with a confirmation:

```
[appadmin]#  system shutdown
******************************************************
* WARNING: This command will shut down all applications *

* and power off the system                            *
******************************************************
Are you sure you want to continue? [y|Y]: y
```

sso-reset

Use the **sso-reset** command to reset the Single Sign-On (SSO) configuration.

Syntax

```
system sso-reset
```

start-rasession

Use the **start-rasession** command to start a RemoteAssist (RA) session.

Syntax

```
system start-rasession [duration_hours | duration_mins | contact_id | cppm_server_ip]
```

The following table describes the required and optional parameters for the **start-rasession** command:

Table 330: *Start RemoteAssist Session Command Parameters*

Flag/Parameter	Description
duration_hours	Specify session duration in hours. You can specify values between 0 to 12.
duration_mins	Specify session duration in minutes. You can specify values between 0 to 59.
contact_id	The username ID part of the Dell TAC or Engineering contact. For example "bjones".
cppm_server_ip	The W-ClearPass Policy Manager server IP address.

status-rasession

Use the **status-rasession** command to view the status of a RemoteAssist session.

Syntax

```
system status-rasession <session_id>
```

Example

The following example displays the status of a RemoteAssist session:

```
[appadmin]# system status-rasession 3001
```

terminate-rasession

Use the **terminate-rasession** command to terminate a running RemoteAssist session.

Syntax

```
system terminate-rasession <session_id>
```

Example

The following example terminates a running RemoteAssist session:

```
[appadmin]# system terminate-rasession 3001
```

update

The **update** command provides options to manage system patch updates.

Syntax

```
system update [-i [-f] <user@hostname:/<filename> | http://hostname/<filename>>]
system update [-f]
system update [-l]
```

The following table describes the required and optional parameters for the **update** command:

Table 331: *Update Commands*

Flag/Parameter	Description
-i user@hostname:/<filename> | http://hostname/<filename>	Installs the specified patch on the system. This field is optional.
-f	Re-installs the patch in the event of a problem with the initial installation attempt. This field is optional.
-l	Lists the patches installed on the system. This field is optional.

This command supports Secure Copy (SCP), HTTP, and local uploads.

Example

The following example provides options to manage system patch updates:

```
[appadmin]#  system update
```

upgrade

The **upgrade** command upgrades the system. This command provides command syntax to upgrade from a Linux server, upgrading from a Web server, and upgrading by performing an offline upgrade.

Syntax

- **Upgrade from a Linux server:**

  ```
  system upgrade user@hostname:/<filepath> [-w] [-l] [-L]
  ```

  See Example 1: Upgrading from a Linux server.
- **Upgrade from a Web server:**
- ```
  system upgrade http://hostname/<filepath> [-w] [-l] [-L]
  ```

  See Example 2: Upgrading from a Web server.
- **Upgrade by performing an offline upgrade:**

  ```
  system upgrade <filepath> [-w] [-l] [-L]
  ```

  See Example 3: Performing an offline upgrade.

Table 332: *Upgrade Commands*

Flag/Parameter	Description
-w	Restores last (one) week of access tracker records after the upgrade.
-l	Restores all access tracker records from this version.
-L	Does not backup or restore access tracker records from this version.
<filepath>	Enter the filepath using the syntax provided in the two examples below. This field is mandatory.

This command supports Secure Copy (SCP), HTTP, and local uploads.

If none of these **Upgrade** command options are provided, access tracker records are backed up, but they are not restored by default.

Example 1: Upgrading from a Linux server

To upgrade the Policy Manager image from a Linux server:

1. Upload the upgrade image to a Linux server.
2. Use the following syntax to upload the upgrade image:

   ```
   system upgrade user@hostname:/<filepath> [-w] [-l] [-L]
   ```

   For example:

   ```
   [appadmin]# system upgrade admin@sun.us.dellnetworks.com:/tmp/PolicyManager-x86-64-upgrade-71.tgz
   ```

Example 2: Upgrading from a Web server

To upgrade the Policy Manager image from a Web server:

1. Upload the upgrade image to a Web server.
2. Use the following syntax to upload the upgrade image:

   ```
   system upgrade http://hostname/<filepath> [-w] [-l] [-L]
   ```
   ```

For example:

```
[appadmin]# system upgrade http://sun.us.dellnetworks.com/downloads/PolicyManager-x86-64-upgrade-71.tgz
```

Example 3: Performing an offline upgrade

To perform an offline upgrade:

1. Log in to the Dell Support Center and select the **Download Software** tab.
2. Navigate to the **ClearPass** > **Policy Manager** > **Current Release** > **Upgrade** folder.
3. In the **Description Remarks** section, click the link for the appropriate upgrade. The upgrade file is uploaded to your local system.
4. Navigate to the ClearPass Policy Manager **Software Updates** page at **Administration** > **Agents and Software Updates** > **Software Updates**.
5. In the **Firmware & Patch Updates** section of the **Software Updates** page, click the **Import Updates** button.

   The **Import from File** dialog appears.
6. Browse to the location of the upgrade file on your system, then click **Import**.

   The selected upgrade file is uploaded to the Dell Networking W-ClearPass Policy Manager.
7. Log in to the Policy Manager command line interface (CLI) with the following user name: *appadmin*.
8. Initiate the upgrade process by entering the following command:

   ```
   system upgrade <filepath> [-w] [-l] [-L]
   ```

   For example:

   ```
   [appadmin]# system upgrade CPPM-upgradeimage.bin
   ```
9. After the upgrade process is complete, restart the machine by issuing the following command in the CLI:

   ```
   system restart
   ```

   The Policy Manager restarts and boots up to the most recent version of Dell Networking W-ClearPass Policy Manager.

Miscellaneous Commands

The Policy Manager command line interface includes the following **`miscellaneous`** commands:

ad auth

Use the **ad auth** command to authenticate the user against Active Directory.

Syntax

```
ad auth --username=<username>
```

The following table describes the required and optional parameters for the **ad auth** command:

Table 333: *Ad Auth Command Parameters*

Flag/Parameter	Description
<username>	Specifies the username of the authenticating user. This is a mandatory field.

Example

The following example authenticates the user against Active Directory:

```
[appadmin]#  ad auth --username=mike
```

ad netjoin

Use the **ad netjoin** command to join host to the domain.

Syntax

```
ad netjoin <domain-controller.domain-name> [domain NETBIOS name]
```

The following table describes the required and optional parameters for the **ad netjoin** command:

Table 334: *Ad Netjoin Command Parameters*

Flag/Parameter	Description
<domain-controller. domain-name>	Specifies the host to be joined to the domain. This field is mandatory.
[domain NETBIOS name]	Specifies the domain name. This field is optional.

Example

The following example joins host to the domain:

```
[appadmin]#  ad netjoin atlas.us.dellnetworks.com
```

ad netleave

Use the **ad netleave** to remove host from the domain.

Syntax

```
ad netleave
```

Example

The following example removes host from the domain:

```
[appadmin]#  ad netleave
```

ad testjoin

Use the **ad testjoin** to test if the **netjoin** command succeeded. This command also test if Policy Manager is a member of the AD domain.

Syntax

```
ad testjoin
```

Example

The following example tests if the **netjoin** command is succeeded:

```
[appadmin]#  ad testjoin
```

alias

Use the **alias** command to create or remove aliases.

Syntax

```
alias <name>=<command>
```

The following table describes the required and optional parameters for the **alias** command:

Table 335: *Alias Commands*

Flag/Parameter	Description
<name>=<command>	Sets <name> as the alias for <command>.
<name>=	Removes the association.

Example 1

```
[appadmin]# alias sh=show
```

Example 2

```
[appadmin]# alias sh=
```

backup

Use the **backup** command to create backup of Policy Manager configuration data. If no arguments are entered, the system auto-generates a filename and backs up the configuration to this file.

Syntax

```
backup [-f <filename>] [-L] [-P]
```

The following table describes the required and optional parameters for the **backup** command:

Table 336: *Backup Command Parameters*

Flag/Parameter	Description
-f <filename>	Specifies the backup target. If not specified, Policy Manager auto-generates a filename. This field is optional.
-L	Do not backup the log database configuration. This field is optional.
-P	Do not backup password fields from the configuration database. This field is optional.

Example

```
[appadmin]#  backup -f PolicyManager-data.tar.gz
Continue? [y|Y]:  y
```

dump certchain

Use the **`dump certchain`** command to dump certificate chain of any SSL secured server.

Syntax

```
dump certchain <hostname:port-number>
```

The following table describes the required and optional parameters for the **`dump certchain`** command:

Table 337: *Dump Certchain Command Parameters*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1

The following example dumps certificate chain of a SSL secured server:

```
[appadmin]#  dump certchain ldap.acme.com:636
dump certchain
```

dump logs

Use the **`dump logs`** command to dump Policy Manager application log files.

Syntax

```
dump logs -f <output-file-name> [-s yyyy-mm-dd] [-e yyyy-mm-dd] [-n <days>] [-t <log-type>] [-
h]
```

The following table describes the required and optional parameters for the **`dump logs`** command:

Table 338: *Dump Logs Command Parameters*

Flag/Parameter	Description
-f <output-file-name>	Specifies target for concatenated logs.
-s yyyy-mm-dd	Specifies the start date range. The default value is today. This field is optional.
-e yyyy-mm-dd	Specifies the end date range. The default value is today. This field is optional.
-n <days>	Specifies the duration in days (from today). This field is optional.
-t <log-type>	Specifies the type of log to collect. This field is optional.
-h	Specifies the print help for available log types.

Example 1

The following example dumps Policy Manager application log files:

```
[appadmin]#  dump logs -f tips-system-logs.tgz -s 2007-10-06 -e 2007-10-17 -t SystemLogs
```

Example 2

The following example prints help for available log types:

```
[appadmin]#  dump logs -h
```

dump servercert

Use the **`dump servercert`** command to dump server certificate of SSL secured server.

Syntax

```
dump servercert <hostname:port-number>
```

The following table describes the required and optional parameters for the **`dump servercert`** command:

Table 339: *Dump Servercert Command Parameters*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example

The following example dumps server certificate of SSL secured server:

```
[appadmin]#  dump servercert ldap.acme.com:636
```

exit

Use the **`exit`** command to exit shell.

Syntax

```
exit
```

Example

The following example exits the shell:

```
[appadmin]#  exit
```

help

Use the **help** command to display the list of supported commands:

Syntax

```
help <command>
```

Example

The following example displays the list of supported commands:

```
[appadmin]#  help
help
 alias                  Create aliases
 backup                 Backup Policy Manager data
 cluster                Policy Manager cluster related commands
 configure              Configure the system parameters
 dump                   Dump Policy Manager information
 exit                   Exit the shell
 help                   Display the list of supported commands
 netjoin                Join host to the domain
 netleave               Remove host from the domain
 network                Network troubleshooting commands
 quit                   Exit the shell
 restore                Restore Policy Manager database
 service                Control Policy Manager services
 show                   Show configuration details
 system                 System commands
```

krb auth

User the **krb auth** command to perform a kerberos authentication against a kerberos server (such as Microsoft AD).

Syntax

```
krb auth <user@domain>
```

The following table describes the required and optional parameters for the **krb auth** command:

Table 340: *Kerberos Authentication Command Parameters*

Flag/Parameter	Description
<user@domain>	Specifies the username and domain.

Example

The following example performs a kerberos authentication against a kerberos server:

```
[appadmin]#  krb auth mike@corp-ad.acme.com
```

krb list

Use the **krb list** command to list the cached kerberos tickets.

Syntax

```
krb list
```

Example

The following example lists the cached kerberos tickets:

```
[appadmin]#  krb list
```

ldapsearch

Use the Linux **ldapsearch** command to find objects in an LDAP directory. Note that only the Policy Manager specific command line arguments are listed. For other command line arguments, refer to ldapsearch man pages on the Internet.

Syntax

```
ldapsearch -B <user@hostname>
```

The following table describes the required and optional parameters for the **ldapsearch** command:

Table 341: *LDAP Search Command Parameters*

Flag/Parameter	Description
<user@hostname>	Specifies the username and the full qualified domain name of the host. The -B command finds the bind DN of the LDAP directory.

Example

The following example finds objects in an LDAP directory:

```
[appadmin]#  ldapsearch -B admin@corp-ad.acme.com
```

quit

Use the **quit** command to exit shell.

Syntax

```
quit
```

Example

The following command quits the shell:

```
[appadmin]# quit
```

restore

Use the **restore** command to restore Policy Manager configuration data from the backup file.

Syntax

```
restore user@hostname:/<backup-filename> [-l] [-i] [-c|-C] [-p] [-s]
```

The following table describes the required and optional parameters for the **restore** command:

Table 342: *Restore Command Parameters*

Flag/Parameter	Description
user@hostname:/<backup-filename>	Specify filepath of restore source.
-c	Restores configuration database (default).
-C	Does not restore configuration database.
-l	If it exists in the backup, restores log database. This field is optional.
-i	Ignores version mismatch errors and proceeds. This field is optional.
-p	Forces restore from a backup file that does not have password fields present. This field is optional.
-s	Restores cluster server/node entries from the backup. Node entries are disabled on restore. This field is optional.

Example

The following example restores Policy Manager configuration data from the backup file:

```
[appadmin]# restore user@hostname:/tmp/tips-backup.tgz -l -i -c -s
```

system start-rasession

The **`system start-rasession`** command allows administrators to configure and start a Remote Assistance session through the Dell Networking W-ClearPass Policy Manager CLI. Configuring a Remote Assistance session through a CLI can be used if the Dell Networking W-ClearPass Policy Manager UI at the customer site is inaccessible.

Syntax

```
system start-rasession <duration_hours> <duration_mins> <contact> <server_ip>
```

The following table describes the required and optional parameters for the **`system start-rasession`** command:

Table 343: *Start Remote Session Command Parameters*

Flag/Parameter	Description
<duration_hours>	Defines the duration in hours of the Remote Assistance Session.
<duration_mins>	Defines the duration in minutes of the Remote Assistance Session.
<contact>	Specifies the name of the TAC engineer.

Table 343: *Start Remote Session Command Parameters (Continued)*

Flag/Parameter	Description
<server_ip>	Specifies the IP address of a Dell Networking W-ClearPass Policy Manager in the cluster.

system terminate-rasession

The **system terminate-rasession** allows administrators to terminate the session on the Dell Networking W-ClearPass Policy Manager where the Remote Assistance session is running.

Syntax

```
system terminate-rasession <sessionid>
```

The following table describes the required and optional parameters for the **system terminate-rasession** command:

Table 344: *Terminate Remote Session Command Parameters*

Flag/Parameter	Description
<sessionid>	Provides the sessionid that can be used to terminate-session.

system status-rasession

The **system status-rasession** command allows administrators to acquire the status on the Dell Networking W-ClearPass Policy Manager in the cluster where the remote session is running.

Syntax

```
system status-rasession <sessionid>
```

The following table describes the required and optional parameters for the **system status-rasession** command:

Table 345: *Terminate Remote Session Command Parameters*

Flag/Parameter	Description
<sessionid>	Specifies the id returned when **system status-rasession** command is executed.

In the Policy Manager administration User Interface (UI) you use the same editing interface to create different types of objects:

- Service rules
- Role mapping policies
- Internal user policies
- Enforcement policies
- Enforcement profiles
- Post-audit rules
- Proxy attribute pruning rules
- Filters for Access Tracker and activity reports
- Attributes editing for policy simulation

When editing all these elements, you are presented with a tabular interface with the same column headers:

- **Type** - Type is the namespace from which these attributes are defined. This is a drop-down list that contains namespaces defined in the system for the current editing context.
- **Name** - Name is the name of the attribute. This is a drop-down list with the names of the attributes present in the namespace.
- **Operator** - Operator is a list of operators appropriate for the data type of the attribute. The drop-down list shows the operators appropriate for data type on the left (that is, the attribute).
- **Value** - The value is the value of the attribute. Again, depending on the data type of the attribute, the value field can be a free-form one-line edit box, a free-form multi-line edit box, a drop-down list containing pre-defined values (enumerated types), or a time or date widget.

In some editing interfaces (for example, enforcement profile and policy simulation attribute editing interfaces) the operator does not change; it is always the EQUALS operator.

Providing a uniform tabular interface to edit all these elements enables you to use the same steps while configuring these elements. Also, providing a context-sensitive editing experience (for names, operators and values) takes the guess-work out of configuring these elements.

The following sections describe namespaces, variables, and operators:

- Namespaces on page 513
- Variables on page 523
- Operators on page 524

Namespaces

Multiple namespaces are displayed in the rules editing interfaces, depending upon what you are editing. For example, multiple namespaces are displayed when you are editing posture policies you work with the posture namespace; when you are editing service rules you work with, among other namespaces, the RADIUS namespace, but not the posture namespace.

For detailed information about the available namespaces, see the following topics:

- Application Namespace on page 514

Application Namespace

The Application namespace has one name attribute. This attribute is an enumerated type currently containing the following string values:

- Guest
- Insight
- PolicyManager
- Onboard
- ClearPass

The Application:ClearPass namespace has the following string values available for the Name field:

- AssertionConsumerUrl
- Configuration-Profile-ID
- Device-Compromised
- Device-ICCID
- Device-IMEI
- Device-MAC
- Device-MDM-Managed
- Device-NAME
- Device-OS
- Device-PRODUCT
- Device-SERIAL
- Device-UDID
- Device-VERSION
- IDDP-COOKIE-TIMEOUT-MINS
- IDPURL
- MDM-Data-Roaming
- MDM-Voice-Roaming

- Onboard-Max-Devices
- Page-Name
- Provisioning-Settings-ID
- SAMLRequest
- SAMLResponse
- Session-Timeout
- User-Email-Address

Audit Namespaces

The Dictionaries in the audit namespace come pre-packaged with the product. The Audit namespace has the notation *Vendor*:Audit, where *Vendor* is the name of the company that has defined attributes in the dictionary.

Examples of dictionaries in the audit namespace are AvendaSystems:Audit or Qualys:Audit.

The Audit namespace appears when editing post-audit rules. See Audit Servers on page 249 for more information.

The Avenda Systems:Audit namespace appears when editing post-audit rules for NESSUS and NMAP audit servers.

Table 346: *Audit Namespace Attributes*

Attribute Name	Values
Audit-Status	• AUDIT_ERROR • AUDIT_INPROGRESS • AUDIT_SUCCESS
Device-Type	Type of device returned by an NMAP port scan.
Output-Msgs	The output message returned by Nessus plugin after a vulnerability scan.
Network-Apps	String representation of the open network ports (http, telnet, etc.).
Mac-Vendor	Vendor associated with MAC address of the host.
OS-Info	OS information string returned by NMAP.
Open-Ports	The port numbers of open applications on the host.

Authentication Namespaces

The authentication namespace can be used in role mapping policies to define roles based on the type of authentication method used or the status of the authentication.

Authentication namespace editing context

Table 347: *Authentication Namespace Attributes*

Attribute Name	Values
InnerMethod	• CHAP • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • EAP-TLS • MSCHAP • PAP **NOTE:** The **EAP-MD5** authentication type is not supported if you use the Dell Networking W-ClearPass Policy Manager in the FIPS mode.
OuterMethod	• CHAP • EAP-FAST • EAP-MD5 • EAP-PEAP • EAP-TLS • EAP-TTLS • MSCHAP • PAP **NOTE:** The **EAP-MD5** authentication type is not supported if you use the Dell Networking W-ClearPass Policy Manager in the FIPS mode.
Phase1PAC	• **None** - No PAC was used to establish the outer tunnel in the EAP-FAST authentication method • **Tunnel** - A tunnel PAC was used to establish the outer tunnel in the EAP-FAST authentication method • **Machine** - A machine PAC was used to establish the outer tunnel in the EAP-FAST authentication method; machine PAC is used for machine authentication (See EAP-FAST in Adding and Modifying Authentication Methods on page 130).
Phase2PAC	• **None** - No PAC was used instead of an inner method handshake in the EAP-FAST authentication method • **UserAuthPAC** - A user authentication PAC was used instead of the user authentication inner method handshake in the EAP-FAST authentication method • **PosturePAC** - A posture PAC was used instead of the posture credential handshake in the EAP-FAST authentication method
Posture	• **Capable** - The client is capable of providing posture credentials • **Collected** - Posture credentials were collected from the client • **Not-Capable** - The client is not capable of providing posture credentials • **Unknown** - It is not known whether the client is capable of providing credentials
Status	• **None** - No authentication took place • **User** - The user was authenticated • **Machine** - The machine was authenticated • **Failed** - Authentication failed

Table 347: *Authentication Namespace Attributes (Continued)*

Attribute Name	Values
	• **AuthSource-Unreachable** - The authentication source was unreachable
MacAuth	• **NotApplicable** - Not a MAC Auth request • **Known Client** - Client MAC address was found in an authentication source • **Unknown Client** - Client MAC address was not found in an authentication source
Username	The username as received from the client (after the strip user name rules are applied).
Full-Username	The username as received from the client (before the strip user name rules are applied).
Source	The name of the authentication source used to authenticate the user.

Authorization Namespaces

Policy Manager supports multiple types of authorization sources. Authorization sources from which values of attributes can be retrieved to create role mapping rules have their own separate namespaces (prefixed with Authorization).

Authorization editing context

Role mapping policies

AD Instance Namespace

For each instance of an Active Directory authentication source, there is an AD instance namespace that appears in the rules editing interface. The AD instance namespace consists of all the attributes that were defined when the authentication source was created. These attribute names are pre-populated. For Policy Manager to fetch the values of attributes from Active Directory, you need to define filters for that authentication source (see Adding and Modifying Authentication Sources on page 154 for more information).

Authorization

The authorization namespace has one attribute: sources. The values are pre-populated with the authorization sources defined in Policy Manager. Use this to check for the authorization source(s) from which attributes were extracted for the authenticating entity.

LDAP Instance Namespace

For each instance of an LDAP authentication source, there is an LDAP instance namespace that appears in the rules editing interface. The LDAP instance namespace consists of all the attributes that were defined when the authentication source was created. These attribute names are pre-populated. For Policy Manager to fetch the values of attributes from an LDAP-compliant directory, you need to define filters for that authentication source (see Adding and Modifying Authentication Sources on page 154).

RSAToken Instance Namespace

For each instance of an RSA Token Server authentication source, there is an RSA Token Server instance namespace that appears in the rules editing interface. The RSA Token Server instance namespace consists of

attributes names defined when you created an instance of this authentication source. The attribute names are pre-populated for administrative convenience.

Sources

This is the list of the authorization sources from which attributes were fetched for role mapping. Authorization namespaces appear in Role mapping policies.

SQL Instance Namespace

For each instance of an SQL authentication source, there is an SQL instance namespace that appears in the rules editing interface. The SQL instance namespace consists of attributes names defined when you created an instance of this authentication source. The attribute names are pre-populated for administrative convenience. For Policy Manager to fetch the values of attributes from a SQL-compliant database, you need to define filters for that authentication source.

Certificate Namespaces

The certificate namespace can be used in role mapping policies to define roles based on attributes in the client certificate presented by the end host. Client certificates are presented in mutually authenticated 802.1X EAP methods (EAP-TLS, PEAP/TLS, EAP-FAST/TLS).

Certificate namespace editing context

Role mapping policies

Table 348: *Certificate Namespace Attributes*

Attribute Name	Values
Version	Certificate version
Serial-Number	Certificate serial number
• Subject-C • Subject-CN • Subject-DC • Subject-DN • Subject-emailAddress • Subject-GN • Subject-L • Subject-O • Subject-OU • Subject-SN • Subject-ST • Subject-UID	Attributes associated with the subject (user or machine, in this case). Not all of these fields are populated in a certificate.
• Issuer-C • Issuer-CN • Issuer-DC • Issuer-DN • Issuer-emailAddress • Issuer-GN • Issuer-L	Attributes associated with the issuer (Certificate Authorities or the enterprise CA). Not all of these fields are populated in a certificate.

Table 348: *Certificate Namespace Attributes (Continued)*

Attribute Name	Values
• Issuer-O • Issuer-OU • Issuer-SN • Issuer-ST • Issuer-UID	
• Subject-AltName-DirName • Subject-AltName-DNS • Subject-AltName-EmailAddress • Subject-AltName-IPAddress • Subject-AltName-msUPN • Subject-AltName-RegisterdID • Subject-AltName-URI	Attributes associated with the subject (user or machine, in this case) alternate name. Not all of these fields are populated in a certificate.

Connection Namespaces

The connection namespace can be used in role mapping policies to define roles based on where the protocol request originated from and where it terminated.

Connection namespace editing contexts

- Role mapping policies
- Service rules

Table 349: *Connection Namespace Pre-defined Attributes*

Attribute	Description
Src-IP-Address	Src-IP-Address and Src-Port are the IP address and port from which the request (RADIUS, TACACS+, etc.) originated.
Src-Port	
Dest-IP-Address	Dst-IP-Address and Dst-Port are the IP address and port at which Policy Manager received the request (RADIUS, TACACS+, etc.).
Dest-Port	
Protocol	Request protocol: RADIUS, TACACS+, WebAuth.
NAD-IP-Address	IP address of the network device from which the request originated.

Table 349: *Connection Namespace Pre-defined Attributes (Continued)*

Attribute	Description
Client-Mac-Address	MAC address of the client.
• Client-Mac-Address-Colon • Client-Mac-Address-Dot • Client-Mac-Address-Hyphen • Client-Mac-Address-Nodelim	Client MAC address in different formats.
Client-IP-Address	IP address of the client (if known).

Date Namespaces

The date namespace has three pre-defined attributes:

- Day-of-Week
- Date-of-Year
- Time-of-Day

For Day-of-Week, the supported operators are BELONG_TO and NOT_BELONGS_TO, and the value field shows a multi-select list box with days from Monday through Sunday.

The Time-of-Day attribute shows a time icon in the value field.

The Date-of-Year attribute shows a date, month and year icon in the value field.

The operators supported for Date-of-Year and Time-of-Day attributes are the similar to the ones supported for the integer data type.

Date namespace editing contexts

- Enforcement policies
- Filter rules for Access Tracker and Activity Reports
- Role mapping policies
- Service rules

Device Namespaces

The Device namespace has four pre-defined attributes:

- Location
- OS-Version
- Device-Type
- Device-Vendor

Custom attributes also appear in the attribute list if they are defined as custom tags for the device.

These attributes can be used only if you have pre-populated the values for these attributes when a network device is configured.

Endpoint Namespaces

Use these attributes to look for attributes of authenticating endpoints, which are present in the Policy Manager endpoints list. The Endpoint namespace has the following attributes:

- Disabled By
- Disabled Reason
- Enabled By
- Enabled Reason
- Info URL

Guest User Namespaces

The GuestUser namespace has the attributes associated with the guest user (resident in the Policy Manager guest user database) who authenticated in this session. This namespace is only applicable if a guest user is authenticated. The GuestUser namespace has six pre-defined attributes:

- Company-Name
- Designation
- Email
- Location
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the guest user.

These attributes can be used only if you have pre-populated the values for these attributes when a guest user is configured in Policy Manager.

Host Namespaces

The Host namespace has the following predefined attributes:

- Name*
- OSType*
- FQDN*
- UserAgent**
- CheckType**
- UniqueID
- AgentType*
- InstalledSHAs*

* Only populated when request is originated by a Microsoft NAP-compatible agent.

** Only present if Policy Manager acts as a Web authentication portal.

Local User Namespaces

The LocalUser namespace has the attributes associated with the local user (resident in the Policy Manager local user database) who authenticated in this session. This namespace is only applicable if a local user is authenticated. The LocalUser namespace has four pre-defined attributes:

- Designation
- Email

- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the local user.

These attributes can be used only if you have pre-populated the values for these attributes when a local user is configured in Policy Manager.

Posture Namespaces

The dictionaries in the posture namespace are pre-packaged with the product. The administration interface provides a way to add dictionaries into the system (see Posture Dictionary on page 452) Posture namespace has the notation *Vendor:*Application, where *Vendor* is the name of the Company that has defined attributes in the dictionary, and Application is the name of the application for which the attributes have been defined. The same vendor typically has different dictionaries for different applications.

Some examples of dictionaries in the posture namespace are:

- ClearPass:LinuxSHV
- Microsoft:SystemSHV
- Microsoft:WindowsSHV
- Trend:AV

Posture Namespace Editing Context

- Filter rules for Access Tracker and Activity Reports
- Internal posture policies actions - Attributes marked with the OUT qualifier
- Internal posture policies conditions - Attributes marked with the IN qualifier
- Policy simulation attributes

RADIUS Namespaces

Dictionaries in the RADIUS namespace come pre-packaged with the product. The administration interface does provide a way to add dictionaries into the system (See RADIUS Dictionary on page 450 for more information). RADIUS namespace has the notation RADIUS:Vendor, where Vendor is the name of the Company that has defined attributes in the dictionary. Sometimes, the same vendor has multiple dictionaries, in which case the "Vendor" portion has the name suffixed by the name of device or some other unique string.

IETF is a special vendor for the dictionary that holds the attributes defined in the RFC 2865 and other associated RFCs. Policy Manager comes pre-packaged with a number of vendor dictionaries. Some examples of dictionaries in the RADIUS namespace are:

- RADIUS:Aruba
- RADIUS:IETF
- RADIUS:Juniper
- RADIUS:Microsoft

RADIUS namespace editing contexts

- Filter rules for Access Tracker and Activity Reports
- Policy simulation attributes
- Post-proxy attribute pruning rules
- RADIUS Enforcement profiles: All RADIUS namespace attributes that can be sent back to a RADIUS client (the ones marked with the OUT or INOUT qualifier)

- Role mapping policies
- Service rules: All RADIUS namespace attributes that can appear in a request (the ones marked with the IN or INOUT qualifier)

Tacacs Namespaces

The Tacacs namespace has the attributes associated with attributes available in a TACACS+ request. Available attributes are:

- AuthSource
- AvendaAVPair
- UserName

Tips Namespaces

The pre-defined attributes for the Tips namespace are *Role* and *Posture*. Values are assigned to these attributes at run-time after Policy Manager evaluates role mapping and posture related policies.

Role

The value for the Role attribute is a set of roles assigned by either the role mapping policy or the post-audit policy. The value of the Role attribute can also be a dynamically fetched "Enable as role" attribute from the authorization source. The posture value is computed after Policy Manager evaluates internal posture policies, and gets posture status from posture servers or audit servers.

Posture

The value for the Posture attribute is one of the following:

- CHECKUP
- HEALTHY
- INFECTED
- QUARANTINE
- TRANSITION
- UNKNOWN

Tips namespace editing context

Enforcement policies

Variables

Variables are populated with the connection-specific values. Variable names (prefixed with % and enclosed in curly braces; for example, %{Username}") can be used in filters, role mapping, enforcement rules, and enforcement profiles. Policy Manager does in-place substitution of the value of the variable during runtime rule evaluation. The following built-in variables are supported in Policy Manager:

Table 350: *Policy Manager Variables*

Variable	Description
%{*attribute-name*}	*attribute-name* is the alias name for an attribute that you have configured to be retrieved from an authentication source. See Adding and Modifying Authentication Sources on page 154.
%{RADIUS:IETF:MAC-Address-Colon}	MAC address of client in aa:bb:cc:dd:ee:ff format
%{RADIUS:IETF:MAC-Address-Hyphen}	MAC address of client in aa-bb-cc-dd-ee-ff format
%{RADIUS:IETF:MAC-Address-Dot}	MAC address of client in aabb.ccdd.eeff format
%{RADIUS:IETF:MAC-Address-NoDelim}	MAC address of client in aabbccddeeff format

You can also use any other dictionary-based attributes (or namespace attributes) as variables in role mapping rules, enforcement rules, enforcement profiles, and LDAP or SQL filters. For example, you can use %{RADIUS:IETF:Calling-Station-ID}or %{RADIUS:Airespace:Airespace-Wlan-Id} in rules or filters.

Operators

The rules editing interface in Policy Manager supports a rich set of operators. The type of operators presented are based on the data type of the attribute for which the operator is being used. Where the data type of the attribute is not known, the attribute is treated as a string type.

The following table lists the operators presented for common attribute data types.

Table 351: *Attribute Operators*

Attribute Type	Operators
String	• BELONGS_TO • NOT_BELONGS_TO • BEGINS_WITH • NOT_BEGINS_WITH • CONTAINS • NOT_CONTAINS • ENDS_WITH • NOT_ENDS_WITH • EQUALS • NOT_EQUALS • EQUALS_IGNORE_CASE • NOT_EQUALS_IGNORE_CASE • EXISTS • NOT_EXISTS • MATCHES_REGEX • NOT_MATCHES_REGEX
Integer	• BELONGS_TO • NOT_BELONGS_TO • EQUALS • NOT_EQUALS • EXISTS • NOT_EXISTS • GREATER_THAN • GREATER_THAN_OR_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS
Time or Date	• EQUALS NOT_EQUALS • GREATER_THAN • GREATER_THAN_OR_EQUALS • LESS_THAN

Table 351: *Attribute Operators (Continued)*

Attribute Type	Operators
	• LESS_THAN_OR_EQUALS • IN_RANGE
Day	• BELONGS_TO • NOT_BELONGS_TO
List (Example: Role)	• EQUALS • NOT_EQUALS • MATCHES_ALL • NOT_MATCHES_ALL • MATCHES_ANY • NOT_MATCHES_ANY • MATCHES_EXACT • NOT_MATCHES_EXACT
Group (Example: Calling-Station-Id, NAS-IP-Address)	• BELONGS_TO_GROUP • NOT_BELONGS_TO_GROUP and all string data types

The following table describes all operator types.

Table 352: *Operator Types*

Operator	Description
BEGINS_WITH	For string data type, true if the run-time value of the attribute begins with the configured value. E.g., `RADIUS:IETF:NAS-Identifier BEGINS_WITH "SJ-"`
BELONGS_TO	For string data type, true if the run-time value of the attribute matches a set of configured string values. E.g., `RADIUS:IETF:Service-Type BELONGS_TO Login-User,Framed-User,Authenticate-Only` For integer data type, true if the run-time value of the attribute matches a set of configured integer values. E.g., `RADIUS:IETF:NAS-Port BELONGS_TO 1,2,3` For day data type, true if run-time value of the attribute matches a set of configured days of the week. E.g., `Date:Day-of-Week BELONGS_TO MONDAY,TUESDAY,WEDNESDAY` When Policy Manager is aware of the values that can be assigned to BELONGS_TO operator, it populates the value field with those values in a multi-select list box; you can select the appropriate values from the presented list. Otherwise, you must enter a comma separated list of values.
BELONGS_TO_GROUP	For group data types, true if the run-time value of the attribute belongs to the configured group (either a static host list or a network device group, depending on the attribute). E.g., `RADIUS:IETF:Calling-Station-Id BELONGS_TO_GROUP Printers`.
CONTAINS	For string data type, true if the run-time value of the attribute is a substring of the configured value. E.g., `RADIUS:IETF:NAS-Identifier CONTAINS "VPN"`
ENDS_WITH	For string data type, true if the run-time value of the attribute ends with the configured value. E.g., `RADIUS:IETF:NAS-Identifier ENDS_WITH "DEVICE"`
EQUALS	True if the run-time value of the attribute matches the configured value. For string data type, this is a case-sensitive comparison. E.g., `RADIUS:IETF:NAS-Identifier EQUALS "SJ-VPN-DEVICE"`
EQUALS_IGNORE_CASE	For string data type, true if the run-time value of the attribute matches the configured value, regardless of whether the string is upper case or lower case. E.g., `RADIUS:IETF:NAS-Identifier EQUALS_IGNORE_CASE "sj-vpn-device"`
EXISTS	For string data type, true if the run-time value of the attribute exists. This is a unary operator. E.g., `RADIUS:IETF:NAS-Identifier EXISTS`

Operator	Description
GREATER_THAN	For integer, time and date data types, true if the run-time value of the attribute is greater than the configured value. E.g., `RADIUS:IETF:NAS-Port GREATER_THAN 10`
GREATER_THAN_OR_EQUALS	For integer, time and date data types, true if the run-time value of the attribute is greater than or equal to the configured value. E.g., `RADIUS:IETF:NAS-Port GREATER_THAN_OR_EQUALS 10`
IN_RANGE	For time and date data types, true if the run-time value of the attribute is less than or equal to the first configured value and less than equal to the second configured value. E.g., `Date:Date-of-Year IN_RANGE 2007-06-06,2007-06-12`
LESS_THAN	For integer, time and date data types, true if the run-time value of the attribute is less than the configured value. E.g., `RADIUS:IETF:NAS-Port LESS_THAN 10`
LESS_THAN_OR_EQUALS	For integer, time and date data types, true if the run-time value of the attribute is less than or equal to the configured value. E.g., `RADIUS:IETF:NAS-Port LESS_THAN_OR_EQUALS 10`
MATCHES_ALL	For list data types, true if all of the run-time values in the list are found in the configured values. E.g., `Tips:Role MATCHES_ALL HR,ENG,FINANCE`. In this example, if the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to true.
MATCHES_ANY	For list data types, true if any of the run-time values in the list match one of the configured values. E.g., `Tips:Role MATCHES_ANY HR,ENG,FINANCE`
MATCHES_EXACT	For list data types, true if all of the run-time values of the attribute match all of the configured values. E.g., `Tips:Role MATCHES_ALL HR,ENG,FINANCE`. In this example, if the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to false, because there are some values in the configured values that are not present in the run-time values.
MATCHES_REGEX	For string data type, true if the run-time value of the attribute matches the regular expression in the configured value. E.g., `RADIUS:IETF:NAS-Identifier MATCHES_REGEX sj-device[1-9]-dev*`

This appendix contains listings of Dell Networking W-ClearPass Policy Manager error codes, SNMP traps, and important system events.

Error Codes

The following table shows the CPPM error codes.

Table 353: *CPPM Error Codes*

Code	Description	Type
0	Success	Success
101	Failed to perform service classification	Internal Error
102	Failed to perform policy evaluation	Internal Error
103	Failed to perform posture notification	Internal Error
104	Failed to query authstatus	Internal Error
105	Internal error in performing authentication	Internal Error
106	Internal error in RADIUS server	Internal Error
201	User not found	Authentication failure
202	Password mismatch	Authentication failure
203	Failed to contact AuthSource	Authentication failure
204	Failed to classify request to service	Authentication failure
205	AuthSource not configured for service	Authentication failure
206	Access denied by policy	Authentication failure
207	Failed to get client macAddress to perform webauth	Authentication failure
208	No response from home server	Authentication failure
209	No password in request	Authentication failure
210	Unknown CA in client certificate	Authentication failure

Table 353: *CPPM Error Codes (Continued)*

Code	Description	Type
211	Client certificate not valid	Authentication failure
212	Client certificate has expired	Authentication failure
213	Certificate comparison failed	Authentication failure
214	No certificate in authentication source	Authentication failure
215	TLS session error	Authentication failure
216	User authentication failed	Authentication failure
217	Search failed due to insufficient permissions	Authentication failure
218	Authentication source timed out	Authentication failure
219	Bad search filter	Authentication failure
220	Search failed	Authentication failure
221	Authentication source error	Authentication failure
222	Password change error	Authentication failure
223	Username not available in request	Authentication failure
224	CallingStationID not available in request	Authentication failure
225	User account disabled	Authentication failure
226	User account expired or not active yet	Authentication failure
227	User account needs approval	Authentication failure
228	User account has exceeded bandwidth limit	Authentication failure
229	User account has exceeded session duration limit	Authentication failure
230	User account has exceeded session count limit	Authentication failure
5001	Internal Error	Command and Control
5002	Invalid MAC Address	Command and Control
5003	Invalid request received	Command and Control
5004	Insufficient parameters received	Command and Control
5005	Query - No MAC address record found	Command and Control

Table 353: *CPPM Error Codes (Continued)*

Code	Description	Type
5006	Query - No supported actions	Command and Control
5007	Query - Cannot fetch MAC address details	Command and Control
5008	Request - MAC address not online	Command and Control
5009	Request - No MAC address record found	Command and Control
6001	Unsupported TACACS parameter in request	TACACS Protocol
6002	Invalid sequence number	TACACS Protocol
6003	Sequence number overflow	TACACS Protocol
6101	Not enough inputs to perform authentication	TACACS Authentication
6102	Authentication privilege level mismatch	TACACS Authentication
6103	No enforcement profiles matched to perform authentication	TACACS Authentication
6201	Authorization failed as session is not authenticated	TACACS Authorization
6202	Authorization privilege level mismatch	TACACS Authorization
6203	Command not allowed	TACACS Authorization
6204	No enforcement profiles matched to perform command authorization	TACACS Authorization
6301	New password entered does not match	TACACS Change Password
6302	Empty password	TACACS Change Password
6303	Change password allowed only for local users	TACACS Change Password
6304	Internal error in performing change password	TACACS Change Password
9001	Wrong shared secret	RADIUS Protocol
9002	Request timed out	RADIUS Protocol
9003	Phase2 PAC failure	RADIUS Protocol
9004	Client rejected after PAC provisioning	RADIUS Protocol
9005	Client does not support posture request	RADIUS Protocol

Table 353: *CPPM Error Codes (Continued)*

Code	Description	Type
9006	Received error TLV from client	RADIUS Protocol
9007	Received failure TLV from client	RADIUS Protocol
9008	Phase2 PAC not found	RADIUS Protocol
9009	Unknown Phase2 PAC	RADIUS Protocol
9010	Invalid Phase2 PAC	RADIUS Protocol
9011	PAC verification failed	RADIUS Protocol
9012	PAC binding failed	RADIUS Protocol
9013	Session resumption failed	RADIUS Protocol
9014	Cached session data error	RADIUS Protocol
9015	Client does not support configured EAP methods	RADIUS Protocol
9016	Client did not send Cryptobinding TLV	RADIUS Protocol
9017	Failed to contact OCSP Server	RADIUS Protocol
9018	RADIUS protocol error	RADIUS Protocol
9019	Client sent conflicting identities	RADIUS Protocol

SNMP Trap Details

Dell Networking W-ClearPass Policy Manager leverages native SNMP support from the UC Davis 'net-SNMP' MIB package to send trap notifications for the following events.

In these trap OIDs, the value of X varies from 1 through N, depending on the number of process states that are being checked. Details about specific OIDs associated with the processes are listed in this section.

For more information, see:

- SNMP Daemon Trap Events on page 533
- CPPM Processes Stop and Start Events on page 533
- Network Interface up and Down Events on page 533
- Disk Utilization Threshold Exceed Events on page 533
- CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds on page 533
- SNMP Daemon Traps on page 533
- Process Status Traps on page 533
- Network Interface Status Traps on page 541
- Disk Space Threshold Traps on page 541
- CPU Load Average Traps on page 542

SNMP Daemon Trap Events

OIDs:

.1.3.6.1.6.3.1.1.5.1 ==> Cold Start

.1.3.6.1.6.3.1.1.5.2 ==> Warm Start

CPPM Processes Stop and Start Events

OIDs:

.1.3.6.1.4.1.2021.8.1.2.X ==> Process Name

.1.3.6.1.4.1.2021.2.1.101.X ==> Process Status Message

Network Interface up and Down Events

OIDs:

.1.3.6.1.6.3.1.1.5.3 ==> Link Down

.1.3.6.1.6.3.1.1.5.4 ==> Link Up

Disk Utilization Threshold Exceed Events

OIDs:

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag for disk partition

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition

CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds

OIDs

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag for disk partition

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition

SNMP Daemon Traps

This section contains OIDs for various trap events that are sent from CPPM.

.1.3.6.1.6.3.1.1.5.1 ==> Coldstart trap indicating the reinitialization of 'netsnmp' daemon and its configuration file may have been altered.

.1.3.6.1.6.3.1.1.5.2 ==> Warmstart trap indicating the reinitialization of 'netsnmp' daemon and its configuration file is not altered.

Figure 453: *SNMP daemon traps example*

Process Status Traps

1 (a) RADIUS server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.5

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.5: cpass-radius-server

.1.3.6.1.4.1.2021.8.1.101.5: Radius server [cpass-radius-server] is stopped

1 (b) RADIUS server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.5

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.5: cpass-radius-server

.1.3.6.1.4.1.2021.8.1.101.5: Radius server [cpass-radius-server] is running

2 (a) Admin Server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.1

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.1: cpass-admin-server

.1.3.6.1.4.1.2021.8.1.101.1: Admin server [cpass-admin-server] is stopped

2 (b) Admin Server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.1

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.1: cpass-admin-server

.1.3.6.1.4.1.2021.8.1.101.1: Admin server [cpass-admin-server] is running

3 (a) System Auxiliary server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.2

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.2: cpass-system-auxiliary-server

.1.3.6.1.4.1.2021.8.1.101.2: System auxiliary service [cpass-system-auxiliary-server] is stopped

3 (b) System Auxiliary server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.2

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.2: cpass-system-auxiliary-server

.1.3.6.1.4.1.2021.8.1.101.2: System auxiliary service [cpass-system-auxiliary-server] is running

4 (a) Policy server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.3

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.3: cpass-policy-server

.1.3.6.1.4.1.2021.8.1.101.3: Policy server [cpass-policy-server] is stopped

4 (b) Policy server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.3

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.3: cpass-policy-server

.1.3.6.1.4.1.2021.8.1.101.3: Policy server [cpass-policy-server] is running

5 (a) Async DB write service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.6

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.6: cpass-dbwrite-server

.1.3.6.1.4.1.2021.8.1.101.6: Async DB write service [cpass-dbwrite-server] is stopped

5 (b) Async DB write service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.6

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.6: cpass-dbwrite-server

.1.3.6.1.4.1.2021.8.1.101.6: Async DB write service [cpass-dbwrite-server] is running

6 (a) DB replication service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.7

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.7: cpass-repl-server

.1.3.6.1.4.1.2021.8.1.101.7: DB replication service [cpass-repl-server] is stopped

6 (b) DB replication service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.7

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.7: cpass-repl-server

.1.3.6.1.4.1.2021.8.1.101.7: DB replication service [cpass-repl-server] is running

7 (a) DB Change Notification server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.8

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.8: cpass-dbcn-server

.1.3.6.1.4.1.2021.8.1.101.8: DB change notification server [cpass-dbcn-server] is stopped

7 (b) DB Change Notification server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.8

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.8: cpass-dbcn-server

.1.3.6.1.4.1.2021.8.1.101.8: DB change notification server [cpass-dbcn-server] is running

8 (a) Async netd service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.9

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.9: cpass-async-netd

.1.3.6.1.4.1.2021.8.1.101.9: Async netd service [cpass-async-netd] is stopped

8 (b) Async netd service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.9

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.9: cpass-async-netd

.1.3.6.1.4.1.2021.8.1.101.9: Async netd service [cpass-async-netd] is running

9 (a) Multi-master Cache service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.10

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.10: cpass-multi-master-cache-server

.1.3.6.1.4.1.2021.8.1.101.10: Multi-master cache [cpass-multi-master-cache-server] is stopped

9 (b) Multi-master Cache service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.10

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.10: cpass-multi-master-cache-server

.1.3.6.1.4.1.2021.8.1.101.10: Multi-master cache [cpass-multi-master-cache-server] is running

10 (a) AirGroup Notification service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.11

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.11: airgroup-notify

.1.3.6.1.4.1.2021.8.1.101.11: AirGroup notification service [airgroup-notify] is stopped

10 (b) AirGroup Notification service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.11

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.11: airgroup-notify

.1.3.6.1.4.1.2021.8.1.101.11: AirGroup notification service [airgroup-notify] is running

11 (a) Micros Fidelio FIAS service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.12

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.12: fias_server

.1.3.6.1.4.1.2021.8.1.101.12: Micros Fidelio FIAS [fias_server] is stopped

11 (b) Micros Fidelio FIAS service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.12

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.12: fias_server

.1.3.6.1.4.1.2021.8.1.101.12: Micros Fidelio FIAS [fias_server] is running

12 (a) TACACS server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.4

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.4: cpass-tacacs-server

.1.3.6.1.4.1.2021.8.1.101.4: TACACS server [cpass-tacacs-server] is stopped

12 (b) TACACS server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.4

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.4: cpass-tacacs-server

.1.3.6.1.4.1.2021.8.1.101.4: TACACS server [cpass-tacacs-server] is running

13 (a) Virtual IP service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.13

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.13: cpass-vip-service

.1.3.6.1.4.1.2021.8.1.101.13: ClearPass Virtual IP service [cpass-vip-service] is stopped

13 (b) Virtual IP service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.13

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.13: cpass-vip-service

.1.3.6.1.4.1.2021.8.1.101.13: ClearPass Virtual IP service [cpass-vip-service] is running

14 (a) Stats Collection service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.15

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.15: cpass-statsd-server

.1.3.6.1.4.1.2021.8.1.101.15: Stats collection service [cpass-statsd-server] is stopped

14 (b) Stats Collection service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.15

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.15: cpass-statsd-server

.1.3.6.1.4.1.2021.8.1.101.15: Stats collection service [cpass-statsd-server] is running

15 (a) Stats Aggregation service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.14

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.14: cpass-carbon-server

.1.3.6.1.4.1.2021.8.1.101.14: Stats aggregation service [cpass-carbon-server] is stopped

15 (b) stats Aggregation service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.14

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.14: cpass-carbon-server

.1.3.6.1.4.1.2021.8.1.101.14: Stats aggregation service [cpass-carbon-server] is running.

Network Interface Status Traps

.1.3.6.1.6.3.1.1.5.3 ==> Indicates the linkdown trap with the 'ifAdminStatus' and 'ifOperStatus' values set to 2.

.1.3.6.1.6.3.1.1.5.4 ==> Indicates the linkup trap with the 'ifAdminStatus' and 'ifOperStatus' values set to 1.

In each case, the 'ifIndex' value is set to 2 for management interface and 3 for the data port interface.

Figure 454: *Network interface status traps example*

25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3 1.3.6.1.2.1.2.2.1.1.3 = 3 1.3.6.1.2.1.2.2.1.7.3 = 2 1.3.6.1.2.1.2.2.1.8.3 = 2
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4 1.3.6.1.2.1.2.2.1.1.2 = 2 1.3.6.1.2.1.2.2.1.7.2 = 1 1.3.6.1.2.1.2.2.1.8.2 = 1

Disk Space Threshold Traps

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag indicating the disk or partition is under the minimum required space configured for it. Value of 1 indicates the system has reached the threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition which has met the above condition.

Figure 455: *Disk space threshold traps example*

25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.2 1.3.6.1.2.1.88.2.1.1.0 = dskTable 1.3.6.1.2.1.88.2.1.2.0 = 1.3.6.1.2.1.88.2.1.3.0 = 1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.9.1.100.1 1.3.6.1.2.1.88.2.1.5.0 = 1 1.3.6.1.4.1.2021.9.1.2.1 = / 1.3.6.1.4.1.2021.9.1.101.1 = /: less than 99% free (= 13%)
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.2.1.1.3.0 = 43 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3 1.3.6.1.2.1.88.2.1.1.0 = memory 1.3.6.1.2.1.88.2.1.2.0 = 1.3.6.1.2.1.88.2.1.3.0 = 1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.4.100.0 1.3.6.1.2.1.88.2.1.5.0 = 0 1.3.6.1.4.1.2021.4.2.0 = swap 1.3.6.1.4.1.2021.4.101.0 =

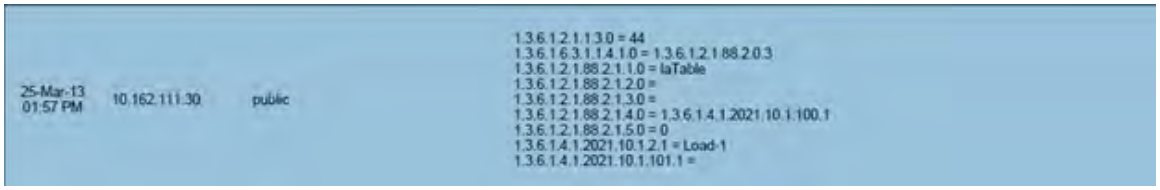
CPU Load Average Traps

OIDs

.1.3.6.1.4.1.2021.10.1.100.1 ==> Error flag on the CPU load-1 average. Value of 1 indicates the load-1 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.1 ==> Name of CPU load-1 average

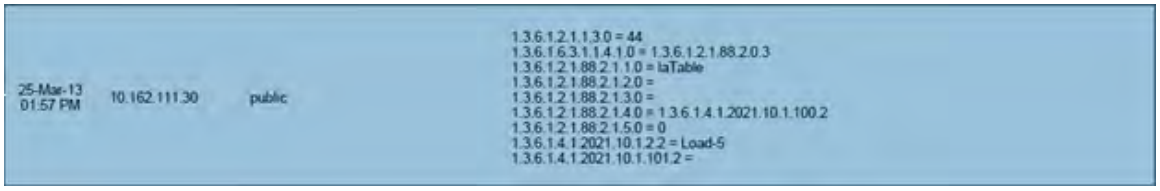
Figure 456: *CPU load-1 average example*



.1.3.6.1.4.1.2021.10.1.100.2 ==> Error flag on the CPU load-5 average. Value of 1 indicates the load-5 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.2 ==> Name of CPU load-5 average

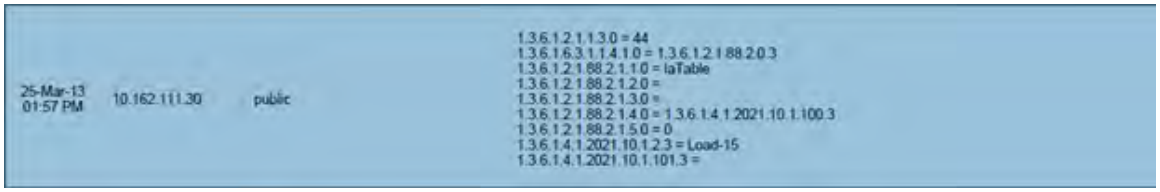
Figure 457: *CPU load-5 average example*



.1.3.6.1.4.1.2021.10.1.100.3 ==> Error flag on the CPU load-15 average. Value of 1 indicates the load-15 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.3 ==> Name of CPU load-15 average.

Figure 458: *CPU load-15 average example*



Important System Events

This topic describes the important System Events logged by ClearPass. These messages are available for consumption on the administrative interface, and in the form of a syslog stream. The events below are in the following format

<Source>, <Level>, <Category>, <Message>

Elements listed below within angular brackets (<content>) are variable, and are substituted by ClearPass as applicable (such as an IP address).

Refer to the Service Names on page 546 section for the list of available service names.

Admin UI Events

Critical Events

“Admin UI”, “ERROR” “Email Failed”, “Sending email failed”

“Admin UI”, “ERROR” “SMS Failed”, “Sending SMS failed”

“Admin UI”, “WARN”, “Login Failed”, “User:<X>”

"Admin UI", "WARN", "Login Failed", description

Info Events

"Admin UI", "INFO", "Logged out"

"Admin UI", "INFO", "Session destroyed"

"Admin UI", "INFO", "Logged in", description

"Admin UI", "INFO", "Clear Authentication Cache", “Cache is cleared for authentication source <X>"

"Admin UI", "INFO", "Clear Blacklist User Cache", “Blacklist Users cache is cleared for authentication source <X>"

"Admin UI", "INFO", "Server Certificate", "Subject:<X>“, "Updated"

"Admin UI", "INFO", "Updated Nessus Plugins"

"Install Update", "INFO", "Installing Update", "File: <X>", "Success"

"Admin UI", “INFO” “Email Successful”, “Sending email succeeded”

"Admin UI", “INFO” “SMS Successful”, “Sending SMS succeeded”

Admin Server Events

Info Events

“Admin server”, “INFO”, “Performed action start on Admin server”

Async Service Events

Info Events

“Async DB write service”, “INFO”, “Performed action start on Async DB write service”

“Multi-master cache”, “INFO”, “Performed action start on Multi-master cache”

“Async netd service”, “INFO”, “Performed action start on Async netd service”

ClearPass/Domain Controller Events

Critical Events

“netleave”, “ERROR”, “Failed to remove <HOSTNAME> from the domain <DOMAIN_NAME>”

“netjoin”, “WARN”, “configuration”, “<HOSTNAME> failed to join the domain <DOMAIN NAME> with domain controller as <DOMAIN CONTROLLER>”

Info Events

“Netjoin”, “INFO”, "<HOSTNAME> joined the domain <REALM>"

“Netjoin”, “INFO”, “<HOSTNAME> removed from the domain <DOMAIN_NAME>“

ClearPass System Configuration Events

Critical Events

“DNS”, “ERROR”, “Failed configure DNS servers = <X>”

“datetime”, “ERROR”, “Failed to change system datetime.”

“hostname”, “ERROR”, “Setting hostname to <X> failed”

“ipaddress”, “ERROR”, “Testing cluster node connectivity failed”

“System TimeCheck “, “ WARN ,” , “Restarting CPPM services as the system detected time drift , Current system time= 2013-07-27 17:00:01, System time 5 mins back = 2013-01-25 16:55:01”

Info Events

“Cluster”, “INFO”, “Setup”, “Database initialized”

“hostname”, “INFO”, “configuration”, “Hostname set to <X>”

“ipaddress”, “INFO”, “configuration”, Management port information updated to - IpAddress = <X>, Netmask = <X>, Gateway = <X>”

“IpAddress”, “INFO”, "Data port information updated to - IpAddress = <X>, Netmask = <Y>, Gateway = <Z>"

“DNS”, “INFO”, “configuration”, “Successfully configured DNS servers - <X>”

“Time Config”, “INFO”, “Remote Time Server”, “Old List: <X>\nNew List: <Y>”

“timezone”, “INFO”, “configuration”, “”

“datetime”, “INFO”, “configuration”, “Successfully changed system datetime.\nOld time was <X>”

ClearPass Update Events

Critical Events

“Install Update”, “ERROR”, “Installing Update”, “File: <X>”, “Failed with exit status - <Y>”

“ClearPass Firmware Update Checker”, “ERROR”, “Firmware Update Checker”, “No subscription ID was supplied. To find new plugins, you must provide your subscription ID in the application configuration”

Info Events

“ClearPass Updater”, “INFO”, “Hotfixes Updates”, “Updated Hotfixes from File”

“ClearPass Updater”, “INFO”, “Fingerprints Updates”, “Updated fingerprints from File”

“ClearPass Updater”, “INFO”, “Updated AV/AS from ClearPass Portal (Online)”

“ClearPass Updater”, “INFO”,” Updated Hotfixes from ClearPass Portal (Online)”

Cluster Events

Critical Events

“Cluster”, “ERROR”, “SetupSubscriber”, “Failed to add subscriber node with management IP=<IP>“

Info Events

"AddNode", “INFO”, "Added subscriber node with management IP=<IP>"

"DropNode", “INFO”, "Dropping node with management IP=<IP>, hostname=<Hostname>"

Command Line Events

Info Events

"Command Line", "INFO", "User:appadmin"

DB Replication Services Events

Info Events

"DB replication service", "INFO", "Performed action start on DB replication service"

"DB replication service", "INFO", "Performed action stop on DB replication service"

"DB change notification server", "INFO", "Performed action start on DB change notification server"

"DB replication service", "INFO", "Performed action start on DB replication service"

Licensing Events

Critical Events

"Admin UI", "WARN", "Activation Failed", "Action Status: This Activation Request Token is already in use by another instance\nProduct Name: Policy Manager\nLicense Type: <X>\nUser Count: <Y>"

Info Events

"Admin UI", "INFO", "Add License", "Product Name: Policy Manager\nLicense Type: <X>\nUser Count: <Y>"

Policy Server Events

Info Events

"Policy Server", "INFO", "Performed action start on Policy server"

"Policy Server", "INFO", "Performed action stop on Policy server"

RADIUS/TACACS+ Server Events

Critical Events

"TACACSServer", "ERROR", "Request", "Nad Ip=<X> not configured"

"RADIUS", "WARN", "Authentication", "Ignoring request from unknown client <IP>:<PORT>"

"RADIUS", "ERROR", "Authentication", "Received packet from <IP> with invalid Message-Authenticator! (Shared secret is incorrect.)"

"RADIUS", "ERROR", "Received Accounting-Response packet from client <IP Address> port 1813 with invalid signature (err=2)! (Shared secret is incorrect.)"

"RADIUS", "ERROR", "Received Access-Accept packet from client <IP Address> port 1812 with invalid signature (err=2)! (Shared secret is incorrect.)"

Info Events

"RADIUS", "INFO", "Performed action start on Radius server"

"RADIUS", "INFO", "Performed action restart on Radius server

"TACACS server", "INFO", "Performed action start on TACACS server"

"TACACS server", "INFO", "Performed action stop on TACACS server"

SNMP Events

Critical Events

“SNMPService”, “ERROR”, “ReadDeviceInfo”, “SNMP GET failed for device <X> with error=No response received\nReading sysObjectId failed for device=<X>\nReading switch initialization info failed for <X>”

"SNMPService","ERROR", "Error fetching table snmpTargetAddr. Request timed out. Error reading SNMP target table for NAD=10.1.1.1 Maybe SNMP target address table is not supported by device? Allow NAD update. SNMP GET failed for device 10.1.1.1 with error=No response received Reading sysObjectId failed for device=10.1.1.1 Reading switch initialization info failed for 10.1.1.1”

Info Events

“SNMPService”, “INFO”, “Device information not read for <Ip Address> since no traps are configured to this node”

Support Shell Events

Info Events

“Support Shell” , “INFO”, “User:arubasupport”

System Auxiliary Service Events

Info Events

“System auxiliary service”, “INFO”, “Performed action start on System auxiliary service”

System Monitor Events

Critical Events

“Sysmon”, “ERROR”, “System”, “System is running with low memory. Available memory = <X>%”

“Sysmon”, “ERROR”, “System”, “System is running with low disk space. Available disk space = <X>%”

“System TimeCheck”, “WARN”, “Restart Services”, “Restarting CPPM services as the system detected time drift. Current system time= <X>, System time 5 mins back = <Y>”

Info Events

“<Service Name>”, “INFO”, “restart”, “Performed action restart on <Service Name>”

“SYSTEM”, “INFO”, “<X> restarted”, “System monitor restarted <X>, as it seemed to have stopped abruptly”

"SYSTEM", "ERROR", "Updating CRLs failed", "Could not retrieve CRL from <URL>."

“System monitor service”, “INFO”, “Performed action start on System monitor service”

"Shutdown” “INFO” system "System is shutting down" Success

Service Names

- AirGroup notification service
- Async DB write service
- Async network services
- DB change notification server
- DB replication service
- Micros Fidelio FIAS

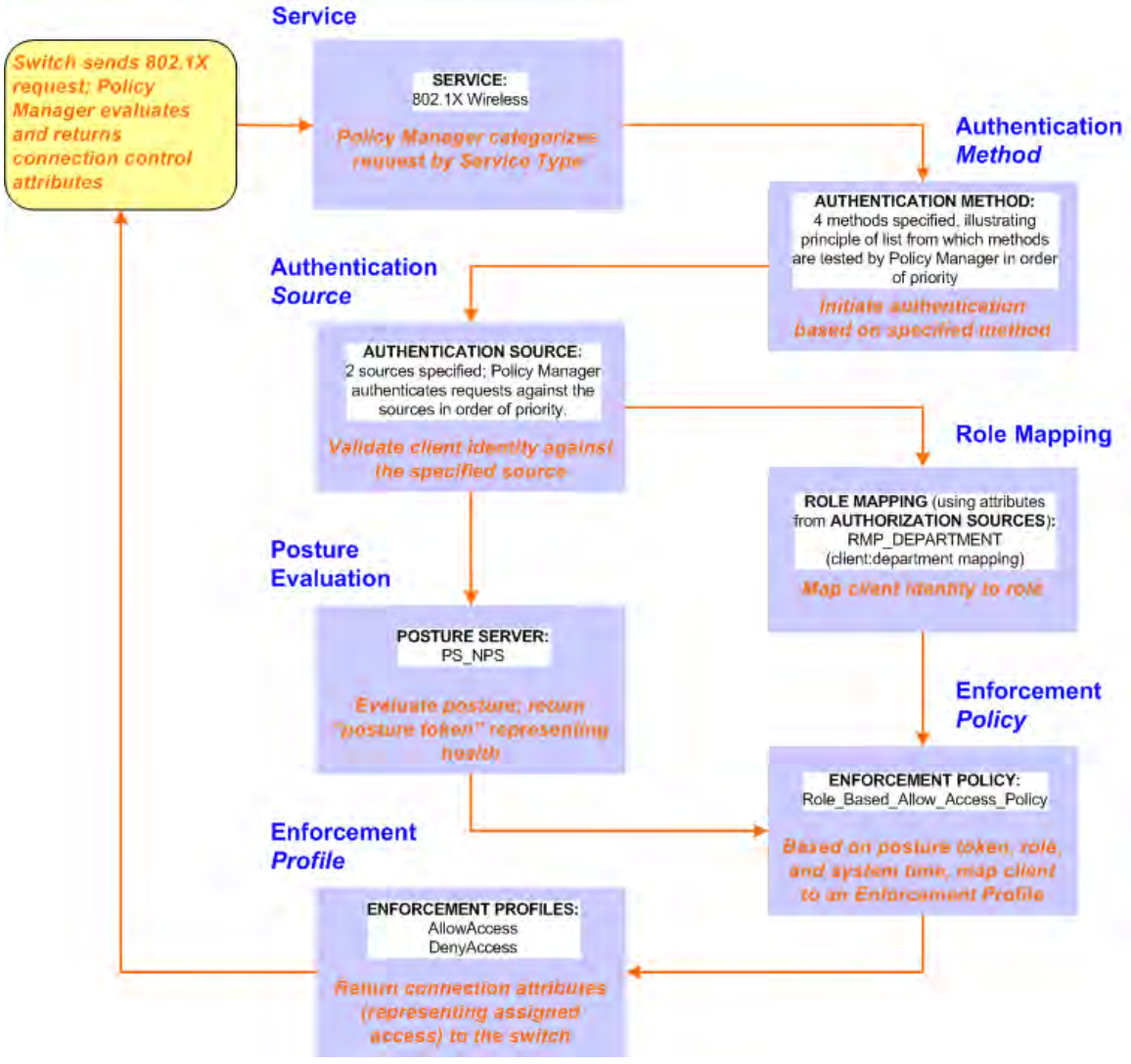
- Multi-master cache
- Policy server
- RADIUS server
- System auxiliary services
- System monitor service
- TACACS server
- Virtual IP service
- [YOURSERVERNAME] Domain service

This appendix contains several specific Dell Networking W-ClearPass Policy Manager use cases. Each one explains what it is typically used for, and then describes how to configure Policy Manager for that use case.

802.1X Wireless Use Case

The basic Policy Manager Use Case configures a Policy Manager Service to identify and evaluate an 802.1X request from a user logging into a Wireless Access Device. The following image illustrates the flow of control for this Service.

Figure 459: *Flow of Control, Basic 802.1X Configuration Use Case*



Configuring the Service

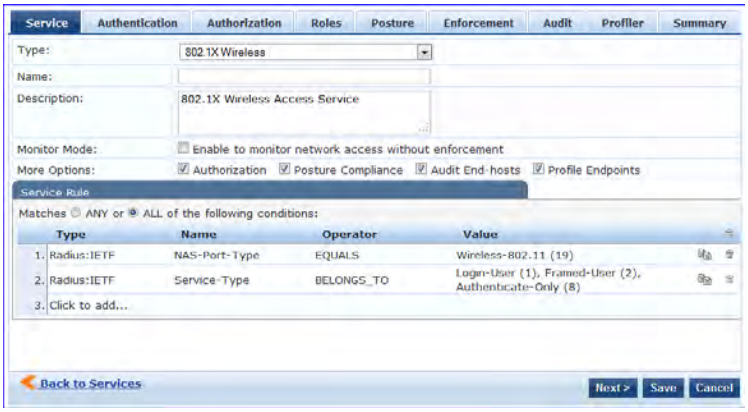
Follow the steps below to configure this basic 802.1X service:

1. Create the Service.

   The following table provides the model for information presented in Use Cases, which assume the reader's ability to extrapolate from a sequence of navigational instructions (left column) and settings (in summary form in the right column) at each step. Below the table, we call attention to any fields or functions that may not have an immediately obvious meaning.

   Policy Manager ships with fourteen preconfigured Services. In this Use Case, you select a Service that supports 802.1X wireless requests.

Table 354: *802.1X - Create Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link)	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **802.1X Wireless** > • **Name/Description** (freeform) > • Upon completion, click **Next** (to Authentication)	

   The following fields deserve special mention:

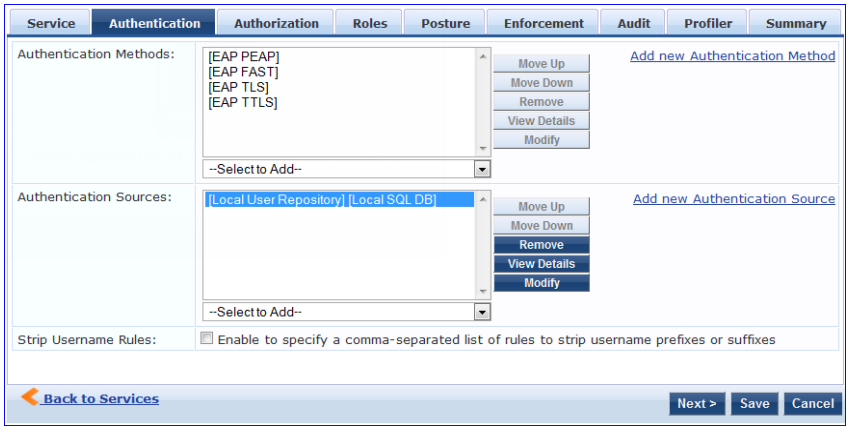
   - **Monitor Mode:** Optionally, check here to allow handshakes to occur (for monitoring purposes), but without enforcement.
   - **Service Categorization Rule:** For purposes of this Use Case, accept the preconfigured Service Categorization Rules for this Type.

2. Configure Authentication.

   Follow the instructions to select **[EAP FAST]**, one of the pre-configured Policy Manager Authentication Methods, and **Active Directory Authentication Source (AD)**, an external Authentication Source within your existing enterprise.

Policy Manager fetches attributes used for role mapping from the Authorization Sources (that are associated with the authentication source). In this example, the authentication and authorization source are one and the same.

Table 355: *Configure Authentication Navigation and Settings*

Navigation	Settings
Select an Authentication Method and an Active Directory server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (Select a method from the drop-down list) • **Add** > • **Sources** (**Select** drop-down list): [Local User Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB] [Guest Device Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] [Onboard Devices Repository] [Local SQL DB] > [Admin User Repository] [Local SQL DB] > AmigoPod AD [Active Directory> • **Add** > • Upon completion, **Next** (to configure Authorization)	

The following field deserves special mention:

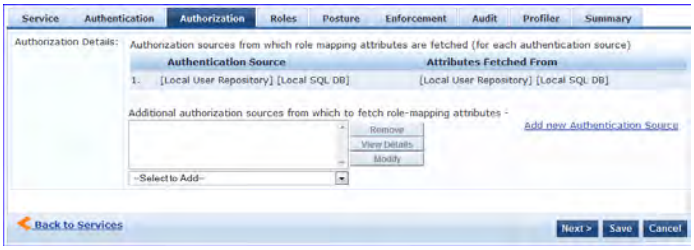
- **Strip Username Rules:** Optionally, check here to pre-process the user name (to remove prefixes and suffixes) before sending it to the authentication source.

To view detailed setting information for any preconfigured policy component, select the item and click **View Details**.

3. Configure Authorization.

   Policy Manager fetches attributes for role mapping policy evaluation from the Authorization Sources. In this use case, the Authentication Source and Authorization Source are one and the same.

Table 356: *02.1X - Configure Authorization Navigation and Settings*

Navigation	Settings
• Configure Service level authorization source. In this use case there is nothing to configure. Click the **Next** button. • Upon completion, click **Next** (to Role Mapping).	

4. Apply a Role Mapping Policy.

   Policy Manager tests client identity against role-mapping rules, appending any match (multiple roles acceptable) to the request for use by the Enforcement Policy. In the event of role-mapping failure, Policy Manager assigns a default role.

   In this Use Case, create the role mapping policy RMP_DEPARTMENT that distinguishes clients by department and the corresponding roles ROLE_ENGINEERING and ROLE_FINANCE, to which it maps:

Table 357: *Role Mapping Navigation and Settings*

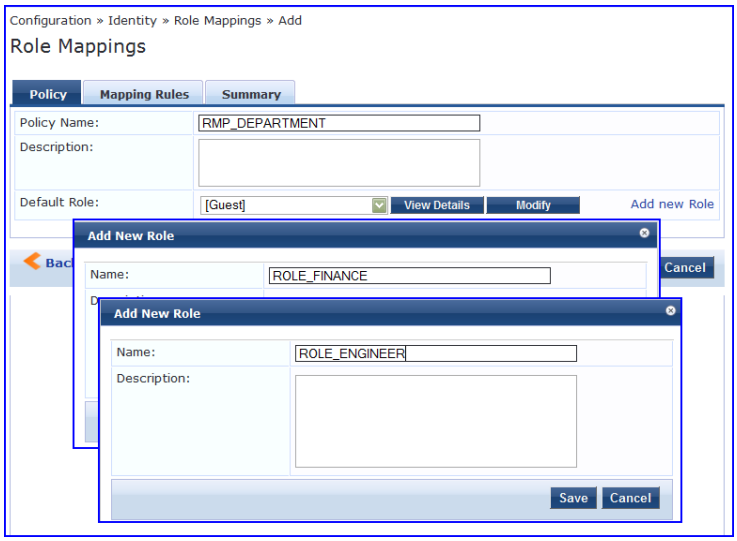
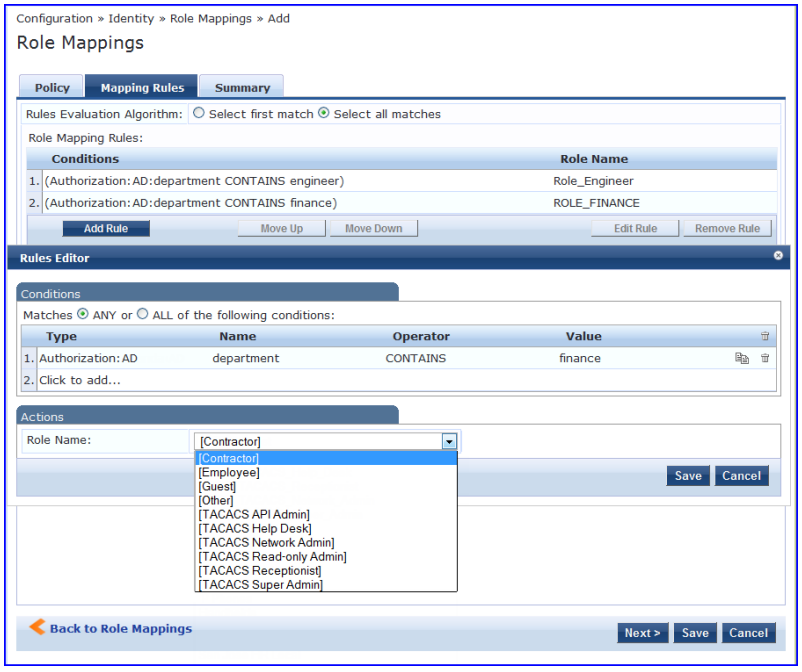
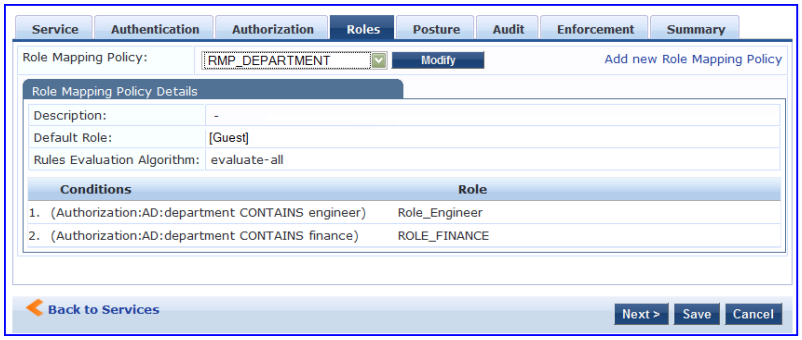
Navigation	Settings
Create the new Role Mapping Policy: • Roles (tab) > • Add New Role Mapping Policy (link)	
Add new Roles (names only): • **Policy** (tab) > • **Policy Name** (freeform): ROLE_ ENGINEER > • **Save** (button) > • Repeat for ROLE_FINANCE > • When you are finished working in the **Policy** tab, click the **Next** button (in the Rules Editor)	
Create rules to map client identity to a Role: • **Mapping Rules** (tab) > • **Rules Evaluation Algorithm** (radio button): **Select all matches** > • **Add Rule** (button opens popup) > • **Add Rule** (button) > • **Rules Editor** (popup) > • **Conditions/ Actions:** match Conditions to Actions (drop-down list) > • Upon completion of each rule, click the **Save** button (in the Rules Editor) > • When you are finished working in the **Mapping Rules** tab, click the **Save** button (in the Mapping Rules tab)	

Table 357: *Role Mapping Navigation and Settings (Continued)*

Navigation	Settings
Add the new Role Mapping Policy to the Service: • Back in **Roles** (tab) > • **Role Mapping Policy** (selector): *RMP_DEPARTMENT* > • Upon completion, click **Next** (to Posture)	

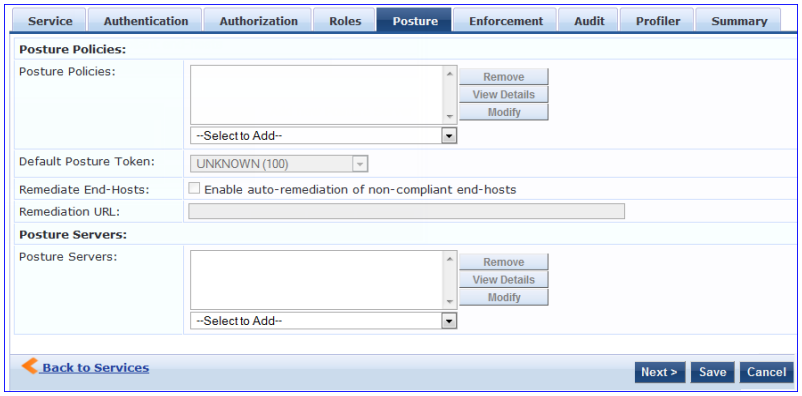
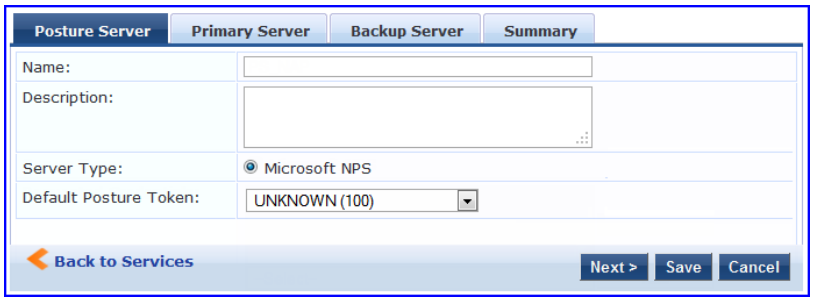
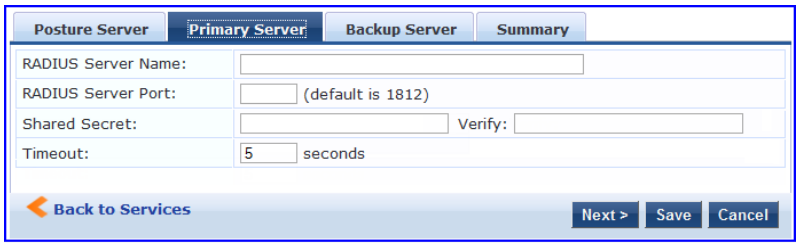
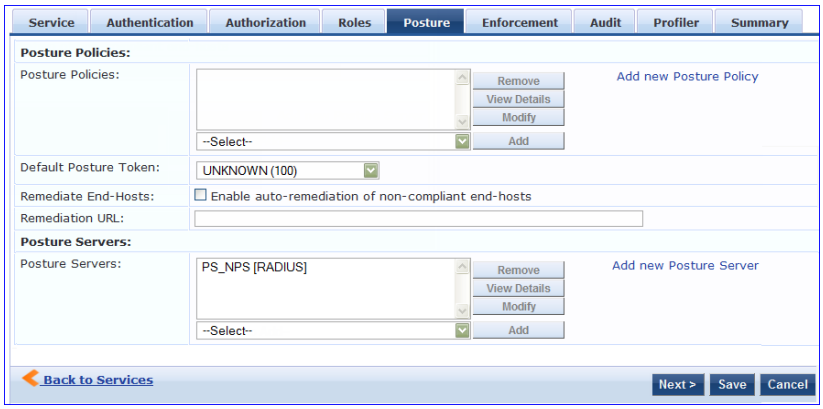
5. Configure a Posture Server.

For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options; here, the Posture Server.

Policy Manager can be configured for a third-party posture server, to evaluate client health based on vendor-specific credentials, typically credentials that cannot be evaluated internally by Policy Manager (that is, not in the form of internal posture policies). Currently, Policy Manager supports the following posture server interface: **Microsoft NPS (RADIUS)**.

Refer to the following table to add the external posture server of type **Micrsoft NPS** to the 802.1X service:

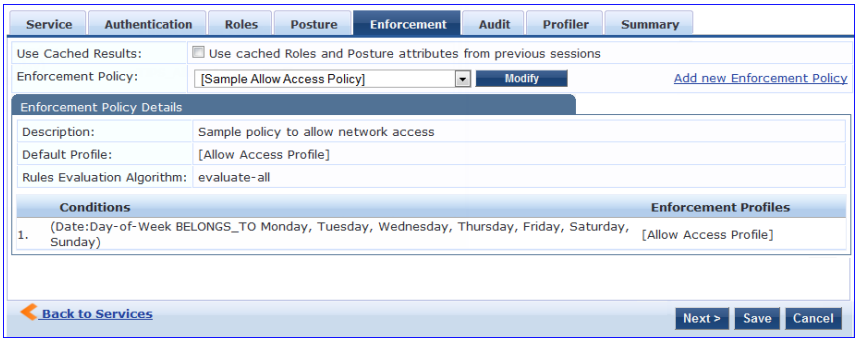
Table 358: *Posture Navigation and Settings*

Navigation	Setting
Add a new Posture Server: • **Posture** (tab) > • **Add new Posture Server** (button) >	
Configure Posture settings: • **Posture Server** (tab) > • **Name** (freeform): **PS_NPS** • **Server Type** (radio button): **Microsoft NPS** • **Default Posture Token** (selector): **UNKOWN** • **Next** (to Primary Server)	
Configure connection settings: • **Primary/ Backup Server** (tabs): Enter connection information for the RADIUS posture server. • **Next** (button): from Primary Server to Backup Server. • To complete your work in these tabs, click the **Save** button.	
Add the new Posture Server to the Service: • Back in the **Posture** (tab) > • **Posture Servers** (selector): **PS_NPS**, then click the **Add** button. • Click the **Next** button.	

6. Assign an Enforcement Policy.

   Enforcement Policies contain dictionary-based rules for evaluation of Role, Posture Tokens, and System Time to Evaluation Profiles. Policy Manager applies all matching Enforcement Profiles to the Request. In the case of no match, Policy Manager assigns a default Enforcement Profile.

Table 359: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Configure the Enforcement Policy: • **Enforcement** (tab) > • **Enforcement Policy** (selector): **Role_Based_ Allow_Access_ Policy**	

For instructions about how to build such an Enforcement Policy, refer to Configuring Enforcement Policies on page 298.

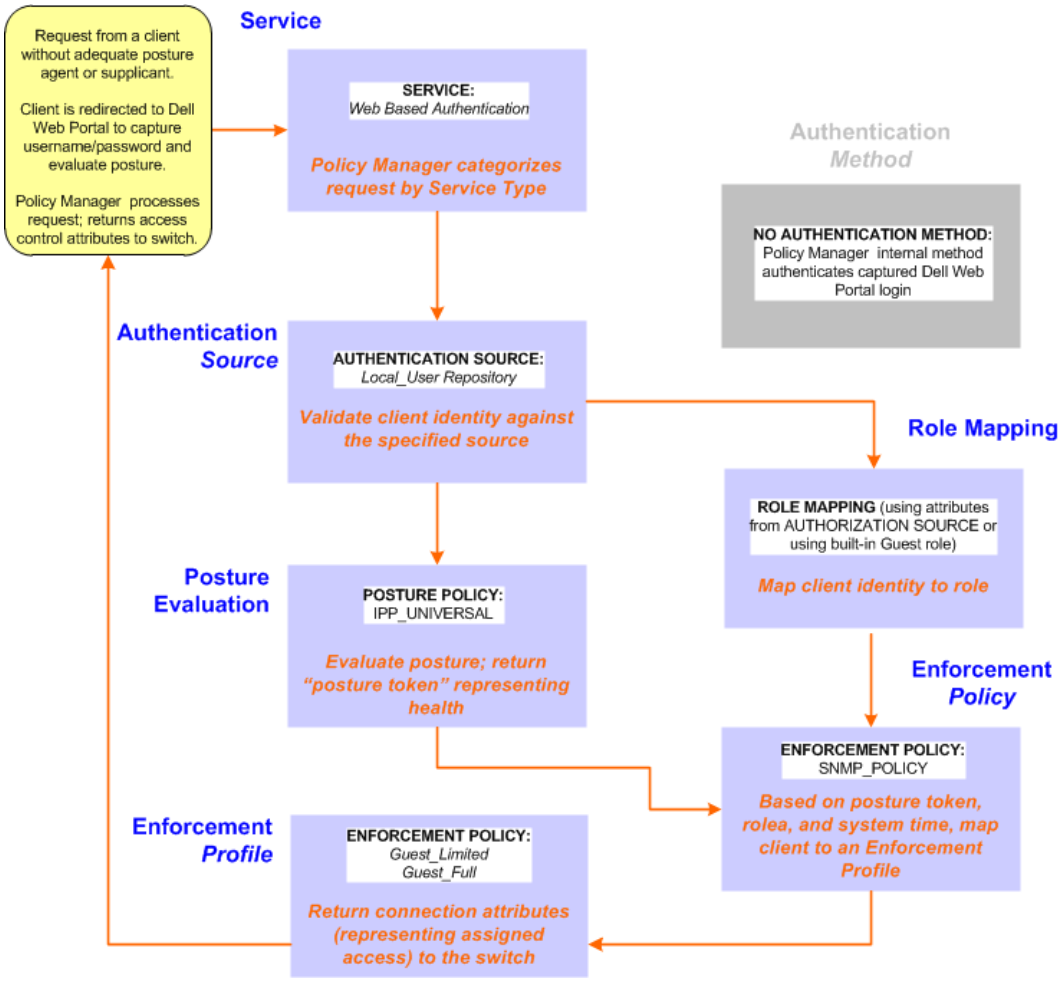
7. Save the Service.

   Click **Save**. The Service now appears at the bottom of the **Services** list.

Web Based Authentication Use Case

This Service supports known Guests with inadequate 802.1X supplicants or posture agents. The following figure illustrates the overall flow of control for this Policy Manager Service.

Figure 460: *Flow-of-Control of Web-Based Authentication for Guests*



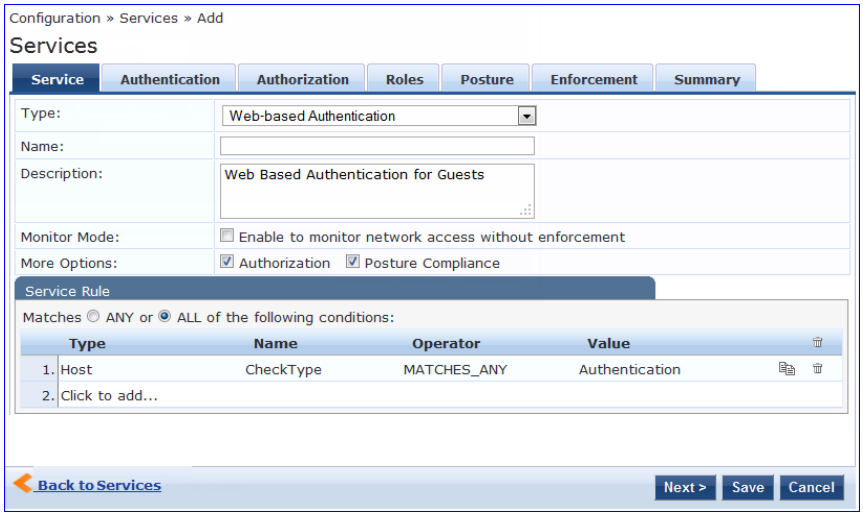
Configuring the Service

Perform the following steps to configure Policy Manager for WebAuth-based Guest access.

1. Prepare the switch to pre-process WebAuth requests for the Policy Manager *Dell WebAuth* service.

   Refer to your Network Access Device documentation to configure the switch such that it redirects HTTP requests to the *Dell Guest Portal*, which captures username and password and optionally launches an agent that returns posture data.
2. Create a WebAuth-based Service.

Table 360: *Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): Dell Web-Based Authentication > • **Name/Description** (freeform) > • Upon completion, click **Next**.	

3. Set up the Authentication.
   a. Method: The Policy Manager WebAuth service authenticates WebAuth clients internally.
   b. Source: Administrators typically configure Guest Users in the local Policy Manager database.
4. Configure a Posture Policy.

For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options. This use case demonstrates the Posture Policy.

As of the current version, Policy Manager ships with five pre-configured posture plugins that evaluate the health of the client and return a corresponding posture token.

To add the internal posture policy *IPP_UNIVERSAL_XP*, which (as you will configure it in this Use Case, checks any Windows® XP clients to verify the most current Service Pack).

Table 361: *Local Policy Manager Database Navigation and Settings*

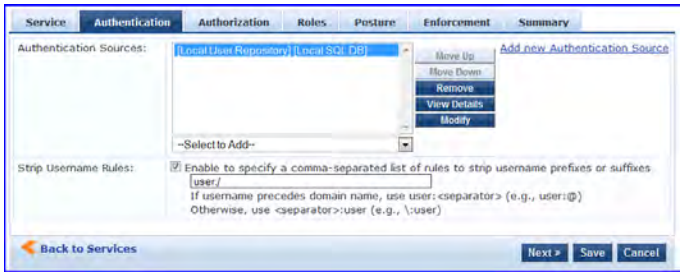
Navigation	Settings
Select the local Policy Manager database: • **Authentication** (tab) > • **Sources** (**Select** drop-down list): **[Local User Repository]** > • **Add** > • **Strip Username Rules** (check box) > • Enter an example of preceding or following separators (if any), with the phrase “user” representing the username to be returned. For authentication, Policy Manager strips the specified separators and any paths or domains beyond them. • Upon completion, click **Next** (until you reach Enforcement Policy).	

Table 362: *Posture Policy Navigation and Settings*

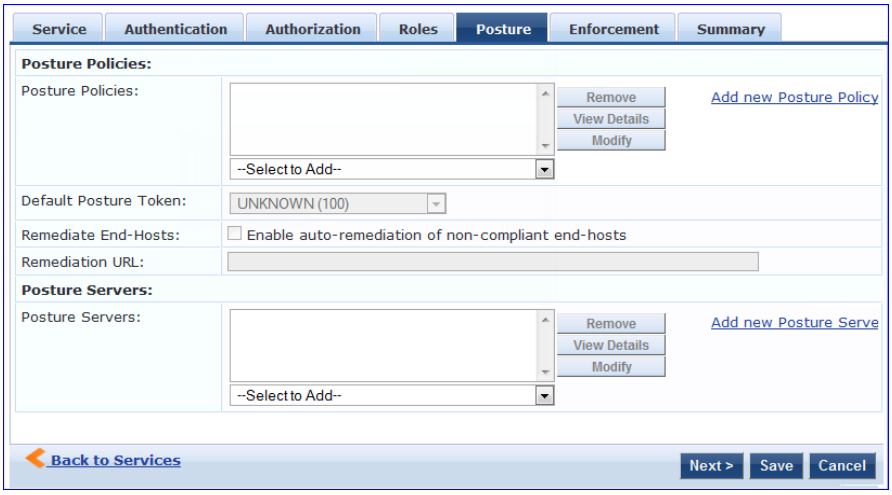
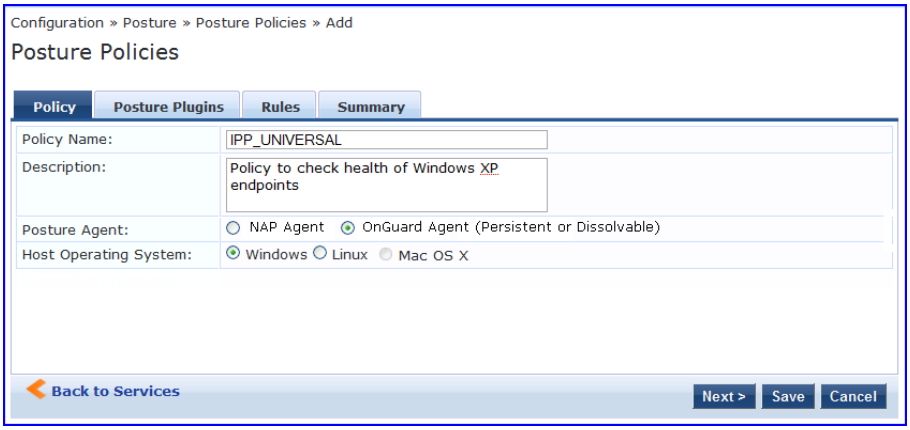
Navigation	Setting
Create a Posture Policy: • **Posture** (tab) > • Enable **Validation Check** (check box) > • **Add new Internal Policy** (link) >	
Name the Posture Policy and specify a general class of operating system: • **Policy** (tab) > • **Policy Name** (freeform): *IPP_UNIVERSAL* > • **Host Operating System** (radio buttons): **Windows** > • When finished working in the **Policy** tab, click **Next** to open the Posture Plugins tab	

Table 362: *Posture Policy Navigation and Settings (Continued)*

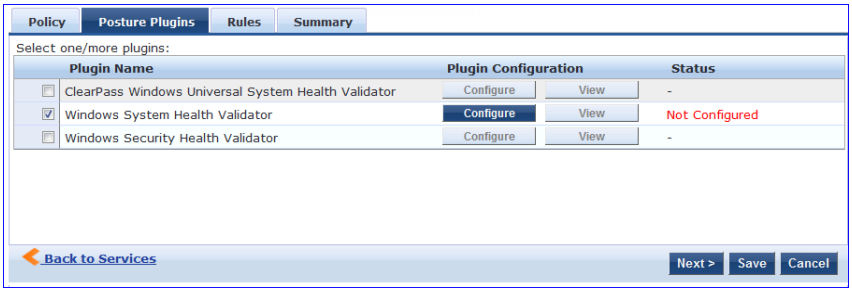
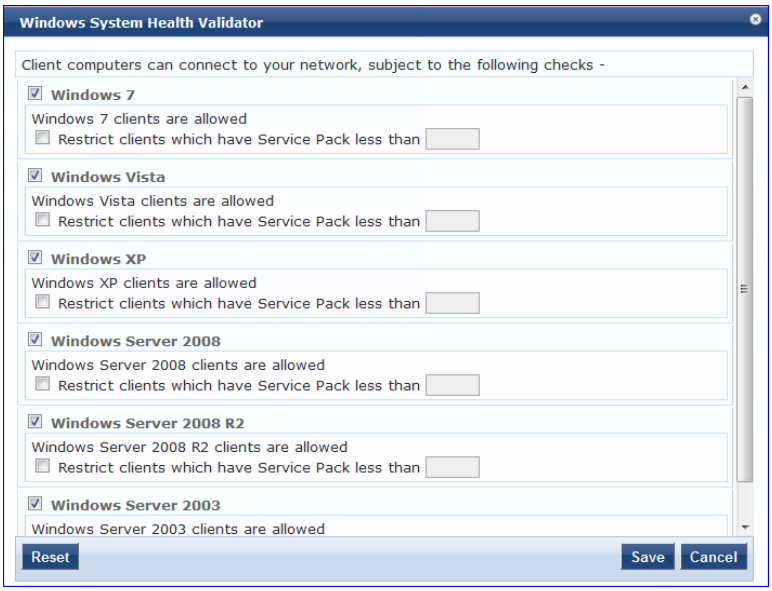
Navigation	Setting
Select a Validator: • **Posture Plugins** (tab) > • Enable **Windows Health System Validator** >• **Configure** (button) >	
Configure the Validator: • **Windows System Health Validator** (popup) >• **Enable all Windows operating systems** (check box) >• Enable Service Pack levels for Windows 7, Windows Vista®, Windows XP Windows Server® 2008, Windows Server 2008 R2, and Windows Server 2003 (check boxes) >• **Save** (button) >	

Table 362: *Posture Policy Navigation and Settings (Continued)*

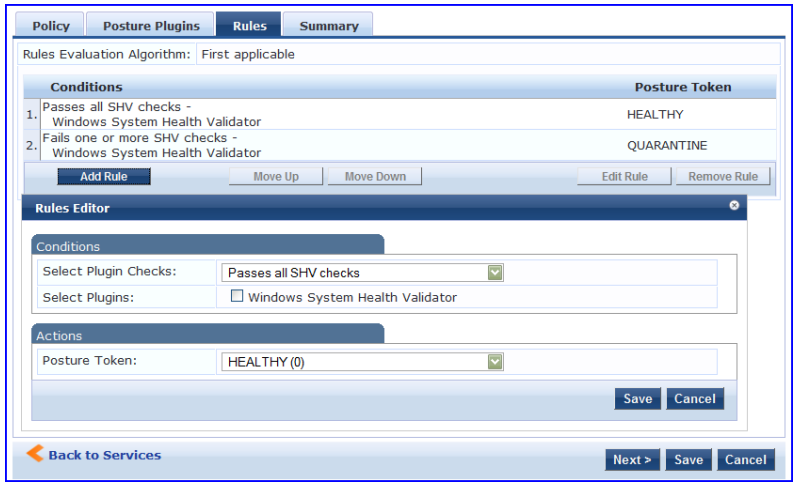
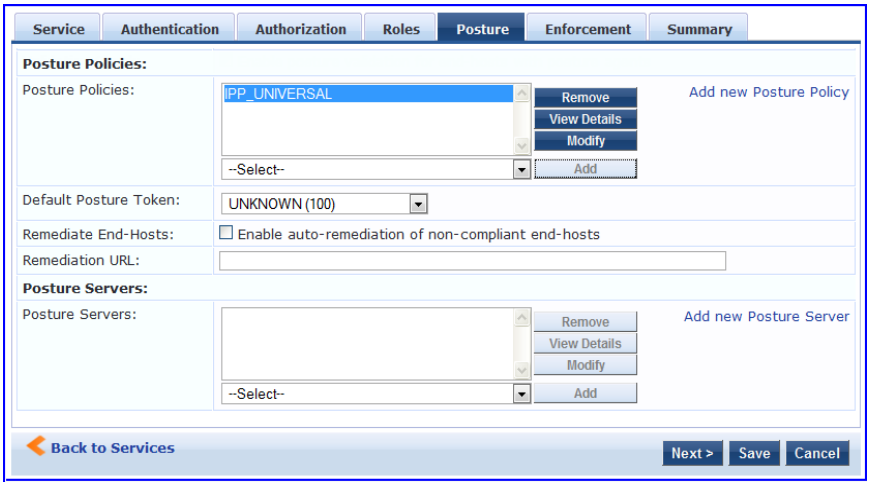
Navigation	Setting
• When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)	
Set rules to correlate validation results with posture tokens: • **Rules** (tab) > • **Add Rule** (button opens popup) > • **Rules Editor** (popup) > • **Conditions/ Actions:** match Conditions (Select Plugin/ Select Plugin checks) to Actions (Posture Token)> • In the **Rules Editor,** upon completion of each rule, click the **Save** button > • When finished working in the **Rules** tab, click the **Next** button.	

Table 362: *Posture Policy Navigation and Settings (Continued)*

Navigation	Setting
Add the new Posture Policy to the Service: Back in **Posture** (tab) > **Internal Policies** (selector): **IPP_UNIVERSAL_XP**, then click the **Add** button	

The following fields deserve special mention:

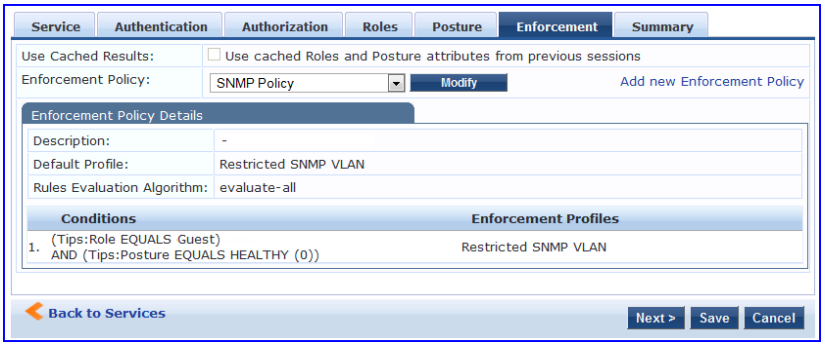
- **Default Posture Token.** Value of the posture token to use if health status is not available.
- **Remediate End-Hosts.** When a client does not pass posture evaluation, redirect to the indicated server for remediation.
- **Remediation URL.** URL of remediation server.

5. Create an Enforcement Policy.

   Because this Use Case assumes the *Guest* role, and the *Dell Web Portal* agent has returned a posture token, it does not require configuration of Role Mapping or Posture Evaluation.

The SNMP_POLICY selected in this step provides full guest access to a Role of [Guest] with a Posture of Healthy, and limited guest access.

Table 363: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Add a new Enforcement Policy: • **Enforcement** (tab) > • Enforcement Policy (selector): **SNMP_POLICY** • Upon completion, click **Save**.	

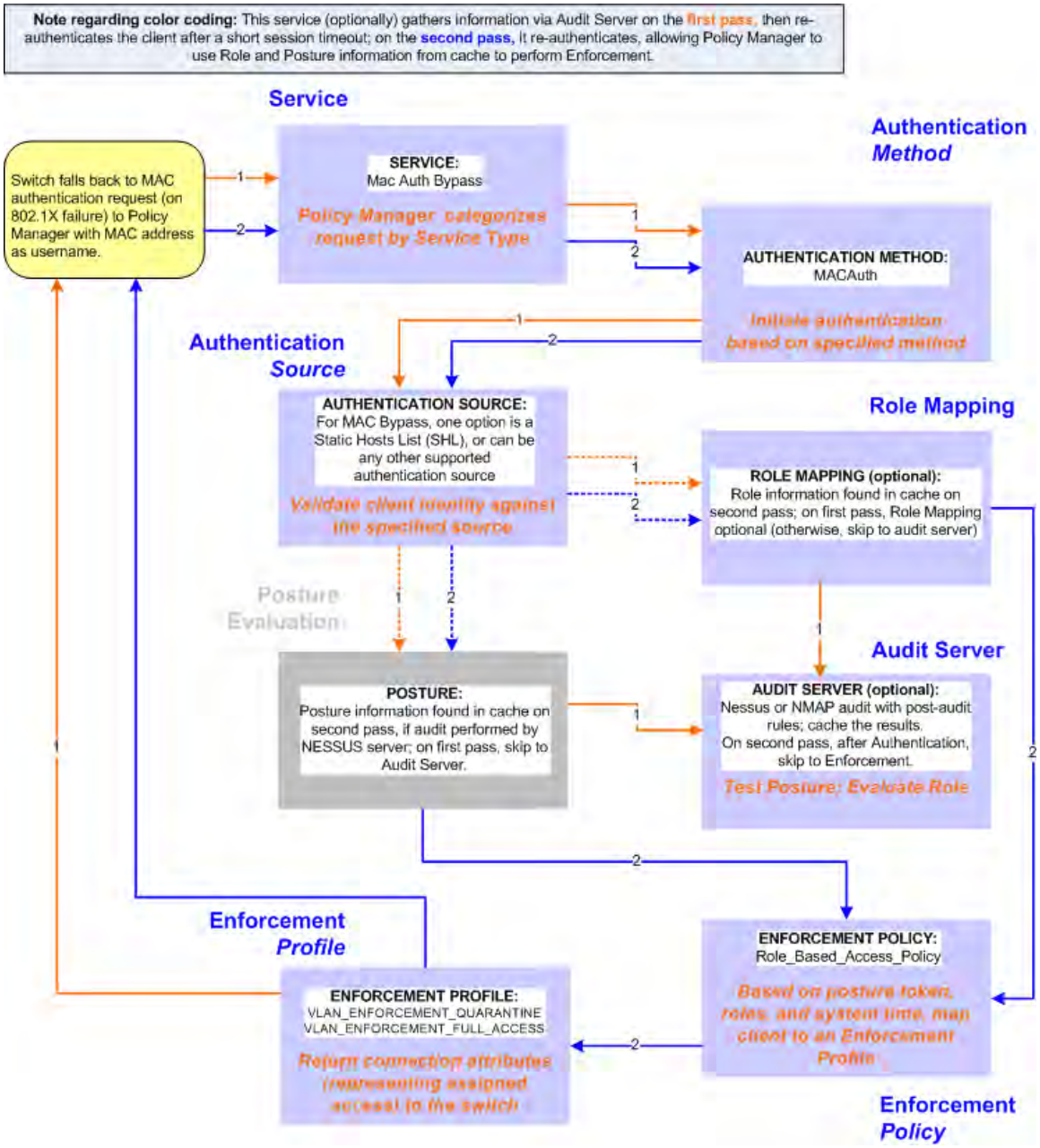
6. Save the Service.

   Click **Save**. The Service now appears at the bottom of the **Services** list.

MAC Authentication Use Case

This Service supports *Network Devices,* such as printers or handhelds. The following image illustrates the overall flow of control for this Policy Manager Service. In this service, an audit is initiated on receiving the first MAC Authentication request. A subsequent MAC Authentication request (forcefully triggered after the audit, or triggered after a short session timeout) uses the cached results from the audit to determine posture and role(s) for the device.

Figure 461: *Flow-of-Control of MAC Authentication for Network Devices*

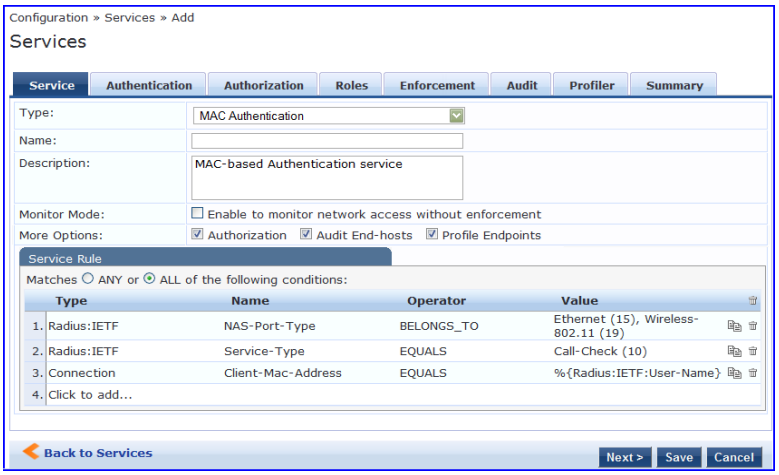


Configuring the Service

Follow these steps to configure Policy Manager for MAC-based Network Device access.

1. Create a MAC Authentication Service.

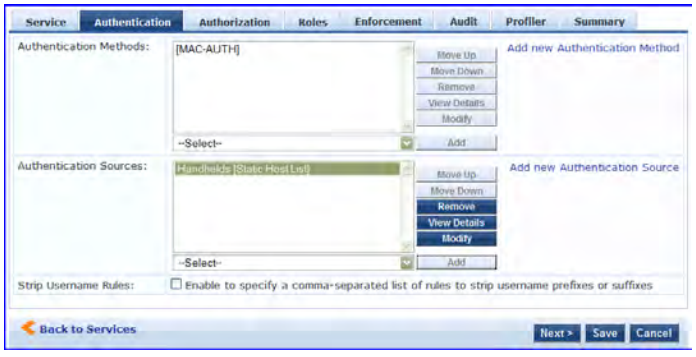
Table 364: *MAC Authentication Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **MAC Authentication** > • **Name/Description** (freeform) > • Upon completion, click **Next** to configure Authentication	

2. Set up Authentication.

   You can select any type of authentication/authorization source for a MAC Authentication service. Only a Static Host list of type MAC Address List or MAC Address Regular Expression shows up in the list of authentication sources (of type Static Host List). Refer to Adding and Modifying Static Host Lists on page 200 for more information. You can also select any other supported type of authentication source.

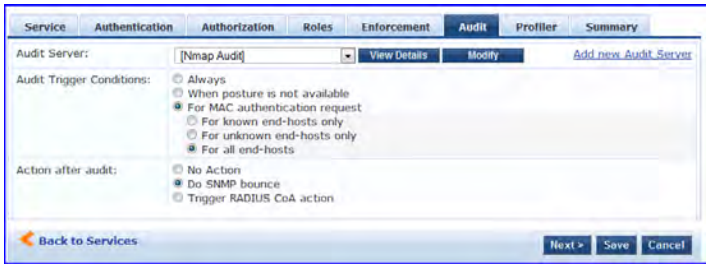
Table 365: *Authentication Method Navigation and Settings*

Navigation	Settings
Select an Authentication Method and two authentication sources - one of type Static Host List and the other of type Generic LDAP server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (This method is automatically selected for this type of service): **[MAC AUTH]** > • **Add** > • **Sources** (**Select** drop-down list): **Handhelds [Static Host List]** and Policy Manager Clients White List [Generic LDAP] > • **Add** > • Upon completion, **Next** (to Audit)	

3. Configure an Audit Server.

This step is optional if no Role Mapping Policy is provided, or if you want to establish health or roles using an audit. An audit server determines health by performing a detailed system and health vulnerability analysis (NESSUS). You can also configure the audit server (NMAP or NESSUS) with post-audit rules that enable Policy Manager to determine client identity.

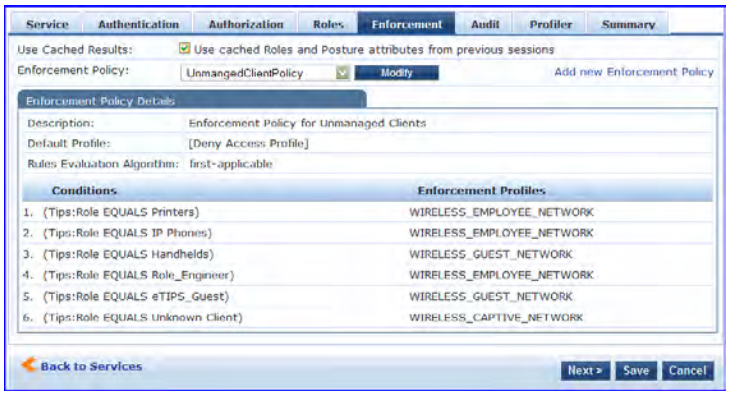
Table 366: *Audit Server Navigation and Settings*

Navigation	Settings
Configure the Audit Server: • **Audit** (tab) > • **Audit End Hosts** (enable) > • **Audit Server** (selector): **NMAP** • **Trigger Conditions** (radio button): **For MAC authentication requests** • **Reauthenticate client** (check box): **Enable**	

Upon completion of the audit, Policy Manager caches Role (NMAP and NESSUS) and Posture (NESSUS), then resets the connection (or the switch reauthenticates after a short session timeout), triggering a new request, which follows the same path until it reaches Role Mapping/Posture/Audit; this appends cached information for this client to the request for passing to Enforcement. Select an Enforcement Policy.

4. Select the Enforcement Policy *Sample_Allow_Access_Policy*:

Table 367: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: • **Enforcement** (tab) > • **Use Cached Results** (check box): Select **Use cached Roles and Posture attributes from previous sessions** > • **Enforcement Policy** (selector): UnmanagedClientPolicy • When you are finished with your work in this tab, click **Save**.	

Unlike the 802.1X Service, which uses the same Enforcement Policy (but uses an explicit Role Mapping Policy to assess Role), in this use case Policy Manager applies post-audit rules against attributes captured by the Audit Server to infer Role(s).

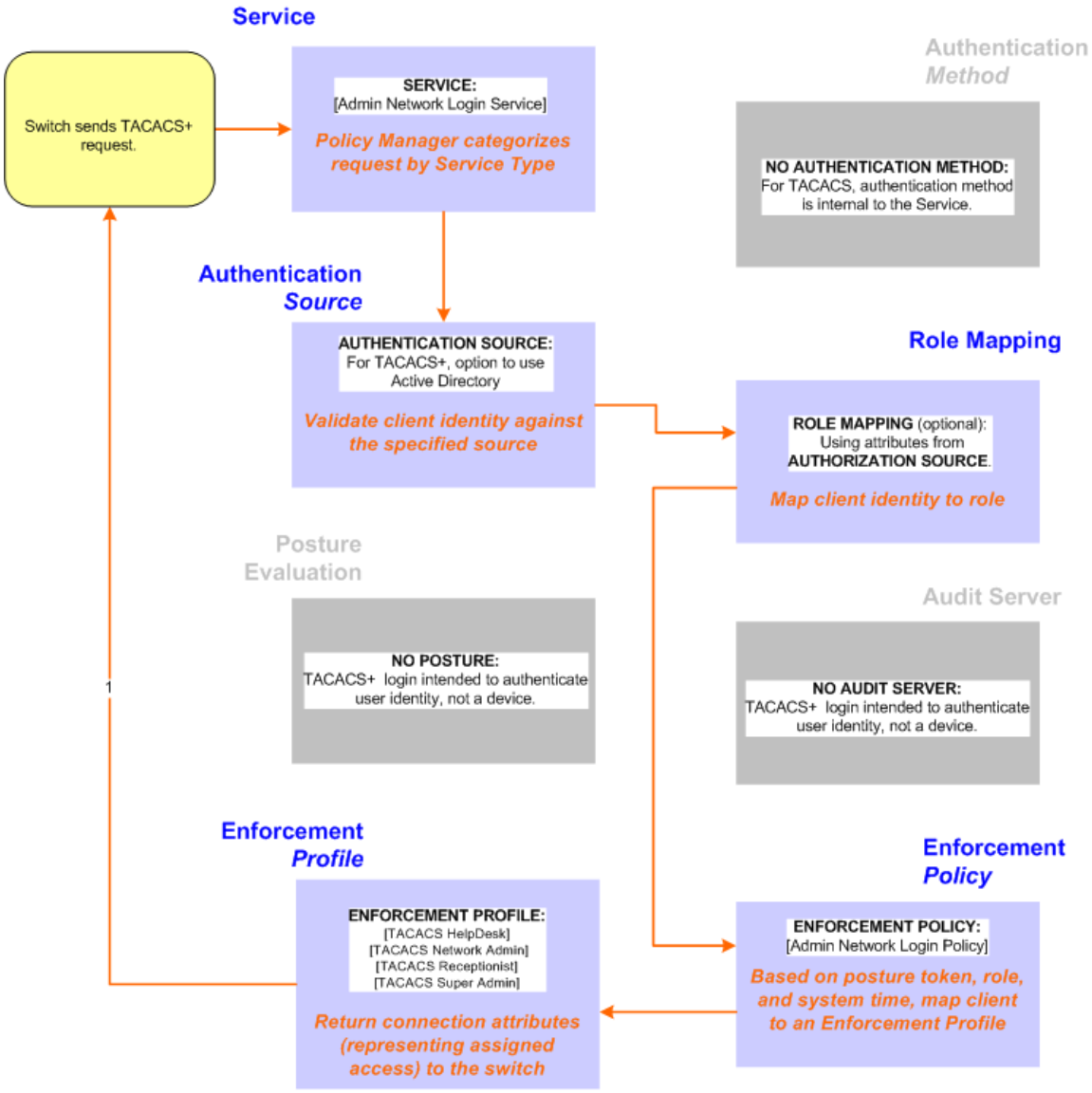
5. Save the Service.

   Click **Save.** The Service now appears at the bottom of the **Services** list.

TACACS+ Use Case

This Service supports Administrator connections to Network Access Devices via TACACS+. The following image illustrates the overall flow of control for this Policy Manager Service.

Figure 462: *Administrator connections to Network Access Devices via TACACS+*

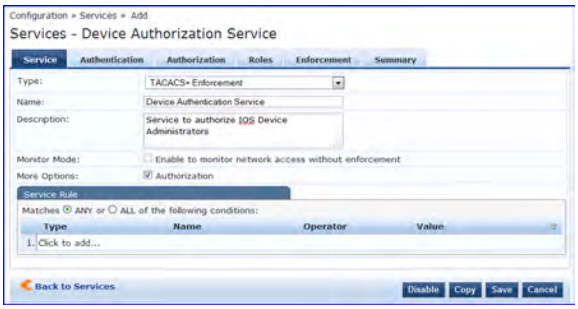


Configuring the Service

Perform the following steps to configure Policy Manager for TACACS+-based access:

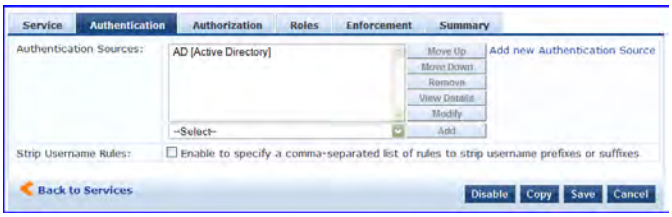
1. Create a TACACS+ Service.

Table 368: *TACACS+ Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **[Policy Manager Admin Network Login Service]** > • **Name/Description** (freeform) > • Upon completion, click **Next** (to Authentication)	

2. Set up the Authentication.
   a. Method: The Policy Manager TACACS+ service authenticates TACACS+ requests internally.
   b. Source: For purposes of this use case, Network Access Devices authentication data will be stored in the Active Directory.

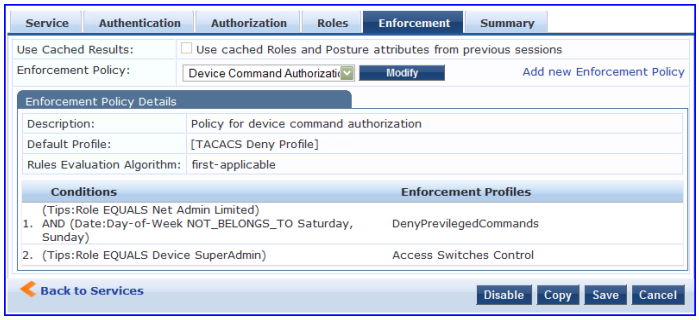
Table 369: *Active Directory Navigation and Settings*

Navigation	Settings
Select an Active Directory server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Add** > • **Sources** (**Select** drop-down list): AD (Active Directory) > • **Add** > • Upon completion, click **Next** (to Enforcement Policy)	

3. Select an Enforcement Policy.

   Select the Enforcement Policy **[Admin Network Login Policy]** that distinguishes the two allowed roles (**Net Admin Limited** and **Device SuperAdmin**.

Table 370: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: • **Enforcement** (tab) > • **Enforcement Policy** (selector): **Device Command Authorization Policy** • When you are finished with your work in this tab, click **Save**.	

4. Save the Service.

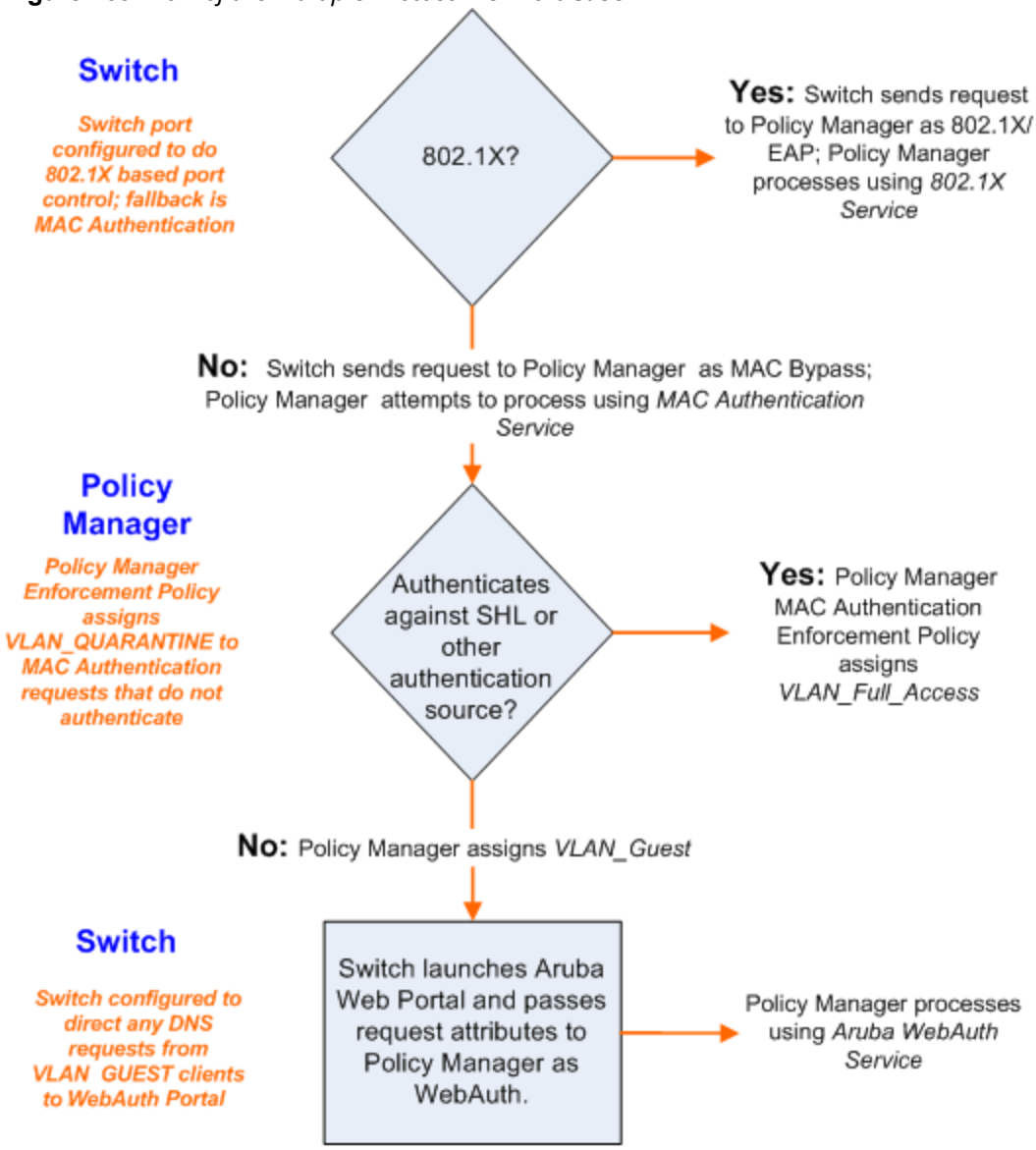
   Click **Save.** The Service now appears at the bottom of the **Services** list.

Single Port Use Case

This Service supports all three types of connections on a single port.

The following figure illustrates both the overall flow of control for this hybrid service, in which complementary switch and Policy Manager configurations allow all three types of connections on a single port:

Figure 463: *Flow of the Multiple Protocol Per Port Case*



You can configure the OnGuard Dissolvable Agent flow in different modes to perform health scan on endpoints. This section provides information on configuring OnGuard Dissolvable Agent in the following modes and the end-to-end flow:

- **Native agents only** - Native Dissolvable Agent communicates with ClearPass Guest to send information about endpoints such as status, health status, remediation messages and so on. This communication is independent of the operating systems and browsers.
- **Native agents with Java fallback** - The configuration for the **Native agents with Java fallback** mode is similar to the **Native agents only** mode. The posture assessment is performed based on the user's preference.
- **Java Only** - The communication is dependent on the browsers and the Java Runtime Environment (JRE) versions installed. For the supported Java versions and browsers, see Supported Browsers and Java Versions.

Native Agents Only Mode

Native Dissolvable Agent communicates with ClearPass Guest portal to send information about endpoints such as status, health status, remediation messages, and so on. This communication is independent of the operating systems and browsers. Native Dissolvable Agent supports the following browsers and operating systems:

Table 371: *Supported Operating Systems and Browsers*

OS	Browsers
Windows	• Internet Explorer • FireFox • Google Chrome
Mac OS X	• Safari • FireFox • Google Chrome

Dell Networking W-ClearPass Policy Manager hosts the Native Dissolvable Agent binary files with OnGuard Persistent Agent installers. You can use the links to download the binaries in the **OnGuard Settings** (**Administration** > **Agents and Software Updates** > **OnGuard Settings**) page for Windows (.exe) and Mac OS X (.DMG).

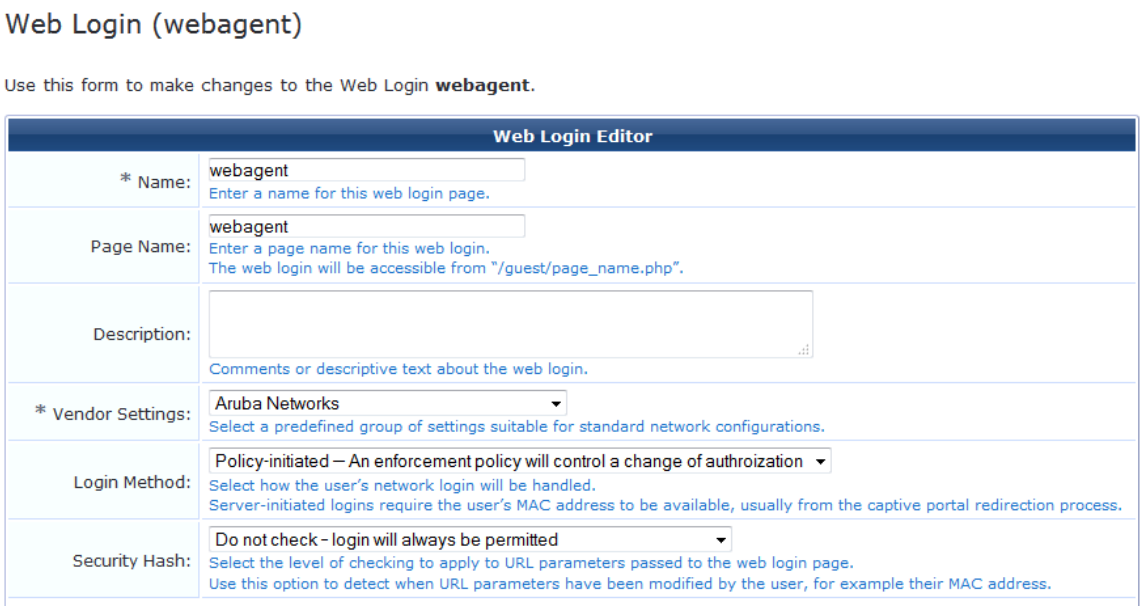
Configuring Workflow in Native Agents Only Mode

In the Dell Networking W-ClearPass Policy Manager 6.4, the web login page is enhanced to avoid an additional web authentication service and simplifies the configuration on dissolvable agent flow with policy-initiated login method.

Use the following steps to configure the OnGuard Dissolvable Agent in **Native agents only** mode:

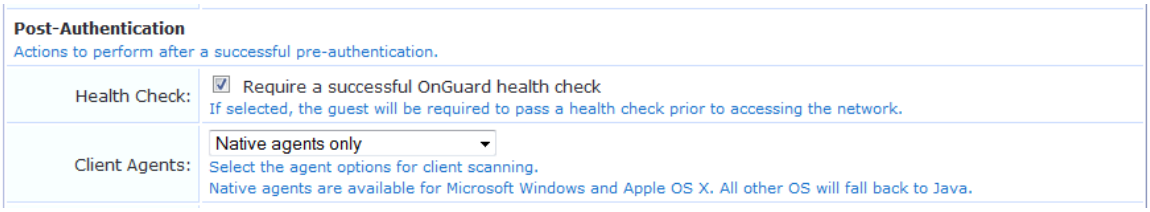
1. Select the **Policy-initiated - An enforcement policy will control a change of authorization** option from the drop-down list in the **Login Method** field. The following figure shows an example configuration of the policy-initiated login method in the **Web Login Editor** page:

Figure 464: *Policy-initiated Login Method*



2. Select the **Require a successful OnGuard health check** option in the **Health Check** field. If you select this field, the guest needs to pass a health check before accessing the network. Select the **Native agents only** mode in the **Client Agents** field:

Figure 465: *Native Agents Only Mode*

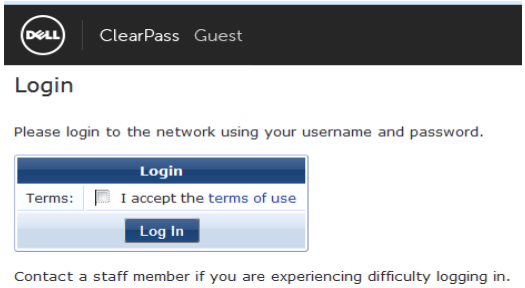


End-to-end flow in Native Agents Only Mode

The following steps describe the end-to-end flow of the OnGuard Dissolvable Agent running on the **Native agents only** mode:

1. You are redirected to the ClearPass Guest portal where you can download the native agent installer. Run the Native Agent Installer after accepting the terms and conditions for collecting end point posture assessment scan checks and performing remediation actions. The following figure shows an example of the Native Dissolvable Agent **Login** page:

Figure 466: *Native Dissolvable Agent - Login Page*

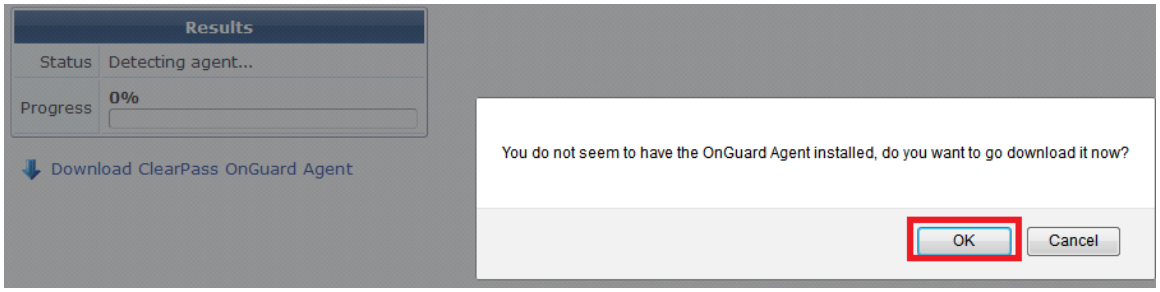


NOTE

The **Terms** specified in the **Login** page is optional. You can configure this optionally by selecting the **Require a Terms and Conditions confirmation** check box in the **Terms** field in ClearPass Guest Login Form.

2. The figure similar to the following OnGuard Agent download prompt appears when you login for the first time to the Native Dissolvable Agent:

Figure 467: *Native Dissolvable Agent Installer Prompt*

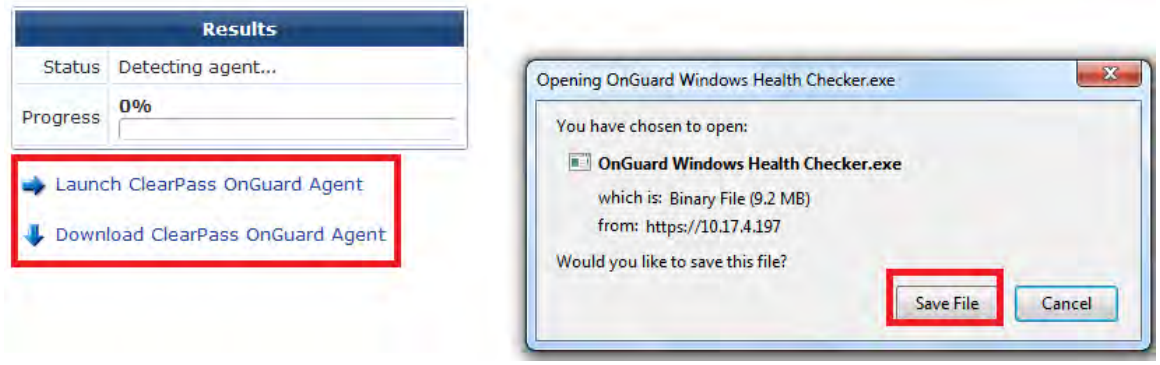


NOTE

The download options are available only when you login for the first time. Alternatively, you can download the OnGuard agent by clicking the **Download ClearPass OnGuard Agent** link.

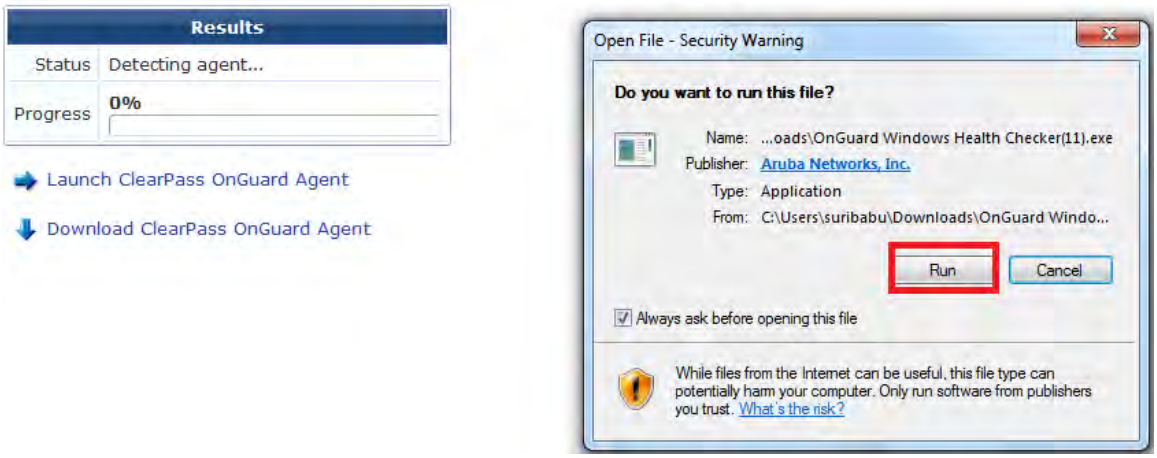
3. Click **OK** to download the OnGuard Agent. The figure shows an example of the **OnGuard Windows Health Checker** binary download window:

Figure 468: *Native Dissolvable Agent Binary Downloader*



4. Click **Save File** to download the OnGuard agent. Click **Run** to install the OnGuard agent.

Figure 469: *Native Dissolvable Agent Installation*



NOTE

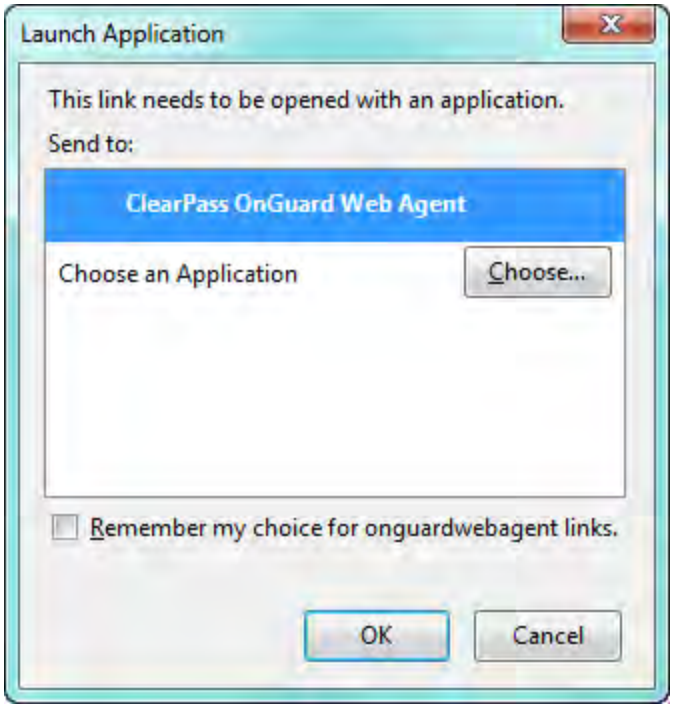
If you are running Windows OS, Internet Explorer provides options to **Run** or **Save**. FireFox and Chrome browsers provide option to save the .exe files.

NOTE

If you are running Mac OS X, FireFox provides options to open the binary with **DiskImageMounter** or **Save** the .DMG files. Safari and Google Chrome browsers provide the option to **Save** only.

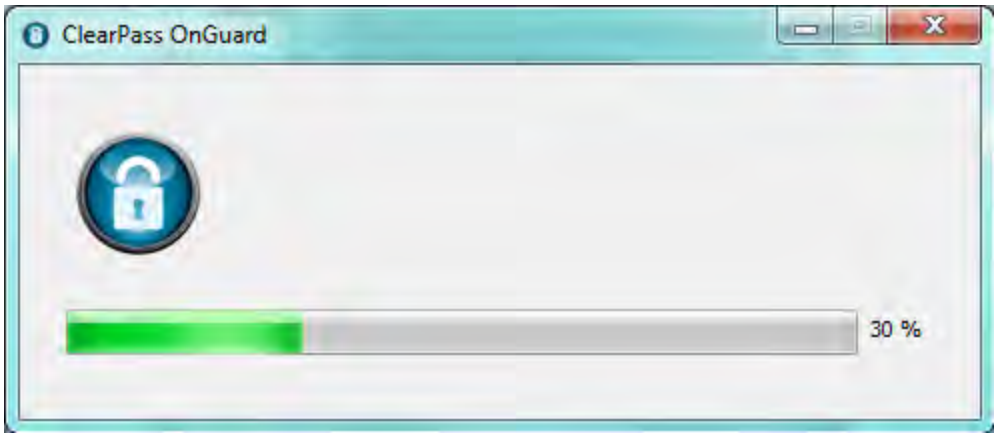
5. Select the **ClearPass OnGuard Web Agent** application in the **Launch Application** page. Select **Remember my choice for onguardwebagent links** to register and perform auto-launch of native OnGuard agent on successive log-ins. Click **OK**.

Figure 470: *Native Dissolvable Agent Application Launcher*



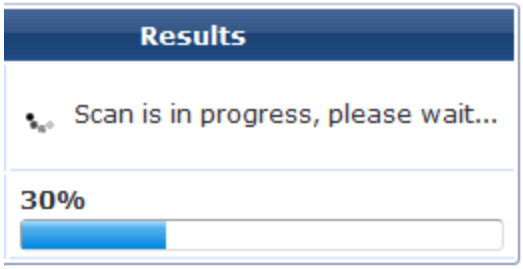
6. The following progress screen appears and shows the progress:

Figure 471: *Native Dissolvable Agent Installation Progress*



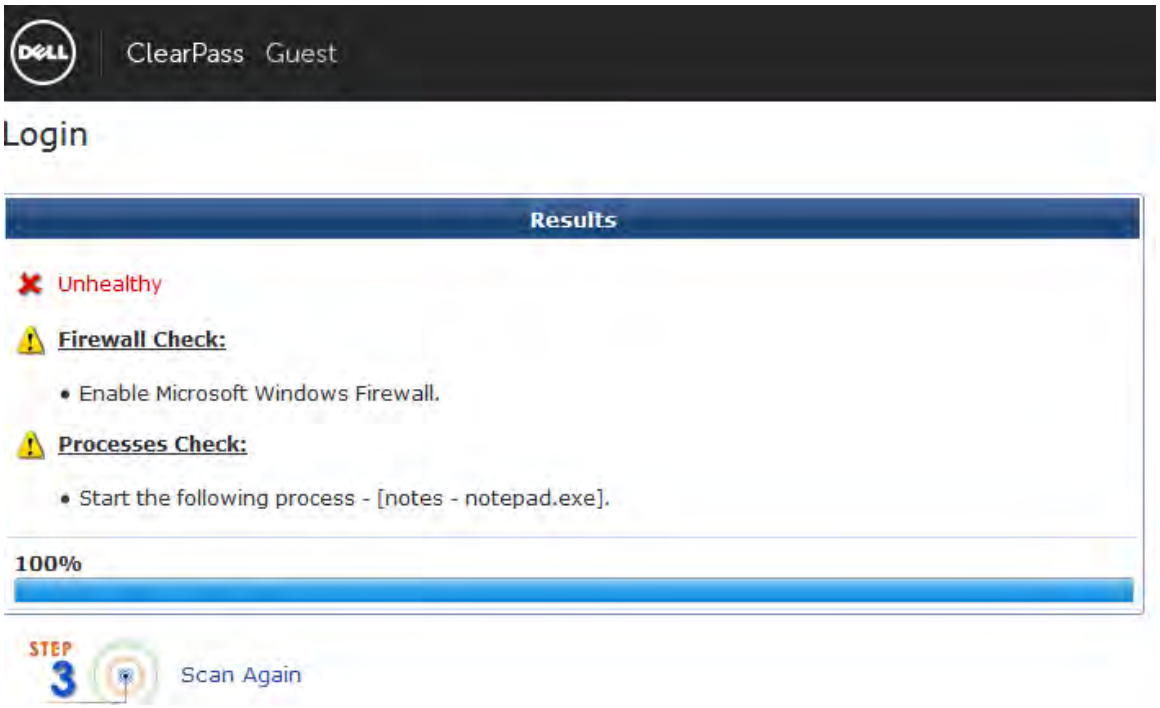
7. After the successful installation, the health check scanning is initiated. The following figure shows an example of the progress indicator:

Figure 472: *Health Check Progress*



8. After the health check scanning is completed, the figure similar to the following example appears with the health check results if the client is unhealthy:

Figure 473: *Health Check Results*



9. Take the appropriate actions to fix the issues listed in remediation and agent enforcement messages and click **Scan Again**. Repeat this step till the client becomes healthy. Once the client is healthy, you can access the destination URL.
10. You can track the events with the end-to-end flow in the **Access Tracker** page. The following figure shows an example of the **Access Tracker** page with the native dissolvable agent flow:

Figure 474: *Access Tracker Page*

The Auto-launch feature works in the **Native agents only** and **Java Only** modes without user intervention to click pop ups and options that are described in the complete end-to-end flow above except configuring **Terms** in the ClearPass Guest **Login** page.

Auto-Login

The Native dissolvable agent supports **Auto-Login** method which eliminates the **Require a Terms and Conditions confirmation** check box in the **Guest Web Login** page by avoiding the web page and submitting automatically.

Troubleshooting

In Windows, Native Dissolvable Agent flow logs are available at **%appdata%Aruba Networks/ ClearPassOnguard Temp/Logs**. In MAC OS X, the Native dissolvable agent flow logs are available at **~/Library/Logs/ClearPassOnGuardTemp/logs**.

Native Agents with Java Fallback Mode

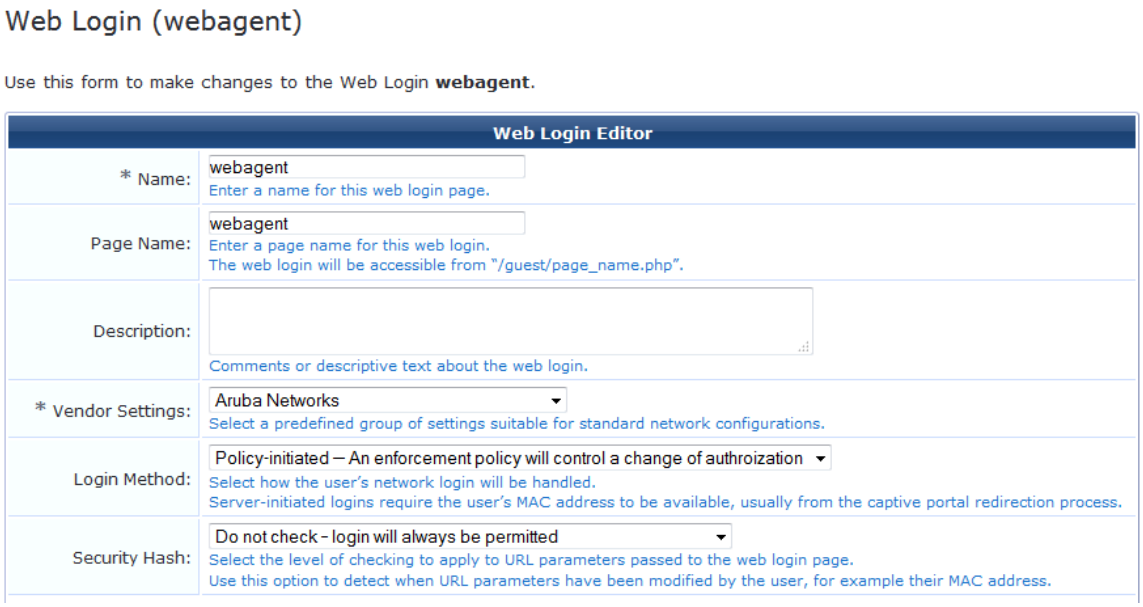
The configuration steps for **Native agents with or Java fallback** work flow is similar to the **Native agents only** mode. The posture assessment is performed based on your selection.

Configuring Native Agents with Java Fallback Mode

Use the following steps to configure the OnGuard Dissolvable Agent in **Native agents with Java fallback** mode:

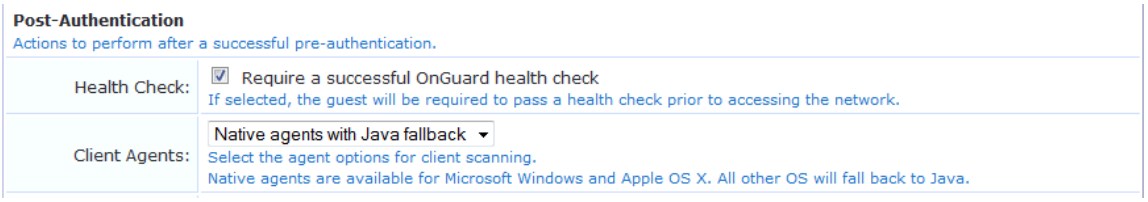
1. Select the **Policy-initiated - An enforcement policy will control a change of authorization** option from the drop-down list in the **Login Method** field. The following figure shows an example configuration of the Policy-initiated **Login** method:

Figure 475: *Policy-initiated Login Method*



2. Select the **Require a successful OnGuard health check** option in the **Health Check** field. If you select this field, the guest needs to pass a health check before accessing the network. Select the **Native agents with Java fallback** mode in the **Client Agents** field:

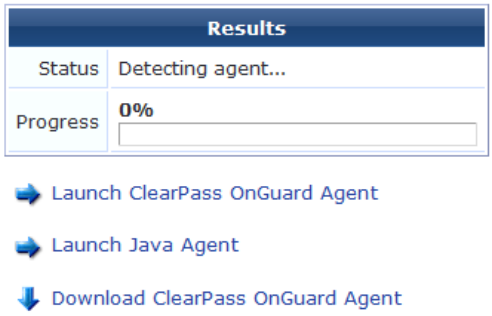
Figure 476: *Native Agents with Java Fallback Mode*



End-to-end flow in Native Agents with Java Fallback Mode

The posture assessment is performed based on your selection. If you select Java, the Java applet is downloaded and posture assessment is performed. The native agent link is provided in **Java launcher** to avoid the JRE files loaded into the system. The following figure shows an example of the **Native agents with Java fallback** options:

Figure 477: *Native Dissolvable Agents with Java Fallback*



Configuring Web Agent Flow - Java Only Mode

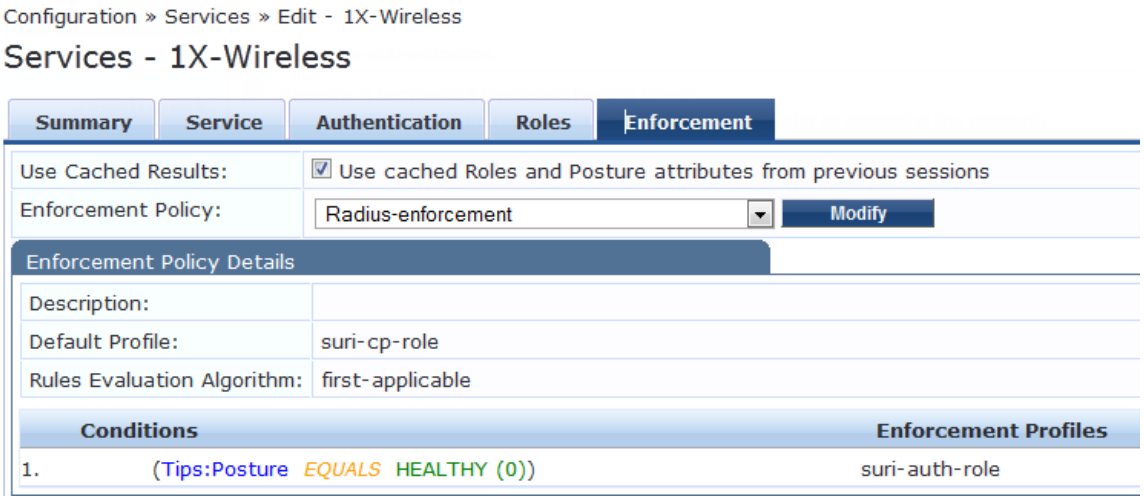
You can configure a new web agent flow in two different locations (Dell Networking W-ClearPass Policy Manager and ClearPass Guest) to perform health scan on endpoints.

Configuring Web Agent Flow in Dell Networking W-ClearPass Policy Manager

Use the following steps to configure a new web agent flow in Dell Networking W-ClearPass Policy Manager:

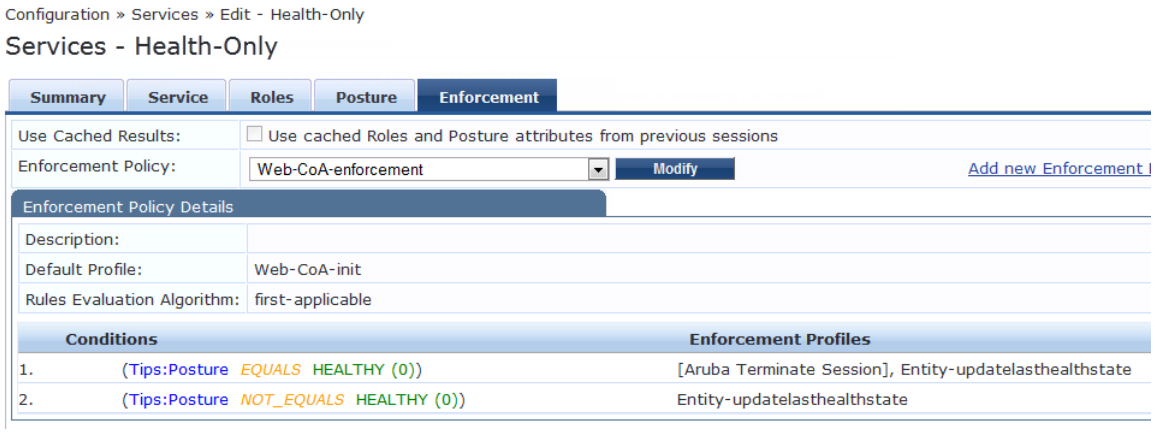
1. Create a 802.1X service to perform RADIUS authentication and enforce restricted or full access based on end point posture assessments. The following figure shows an example of the **Web Agent Flow - 802.1X Service** page:

Figure 478: *Web Agent Flow - 802.1X Service*



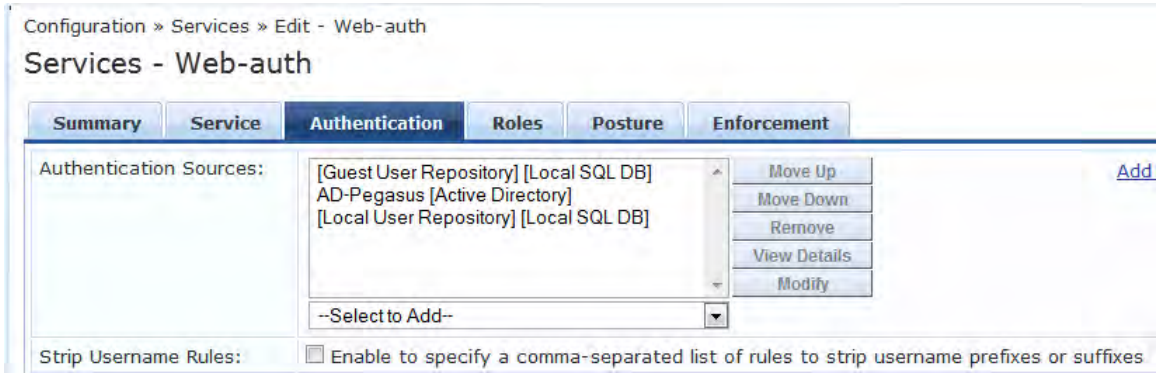
2. Create a service named **Web-based Health Check Only** on the Dell Networking W-ClearPass Policy Manager server. The following figure shows an example of the **Web Agent Flow - Health Only** page:

Figure 479: *Web Agent Flow - Health Only*



3. Create a simple Web Auth service to authenticate users against ClearPass Guest user database to accept or perform App authentication request after completing a sandwich flow. The following figure shows an example of the **Web Agent Flow - Services Web Auth** page:

Figure 480: *Web Agent Flow - Services Web Auth*

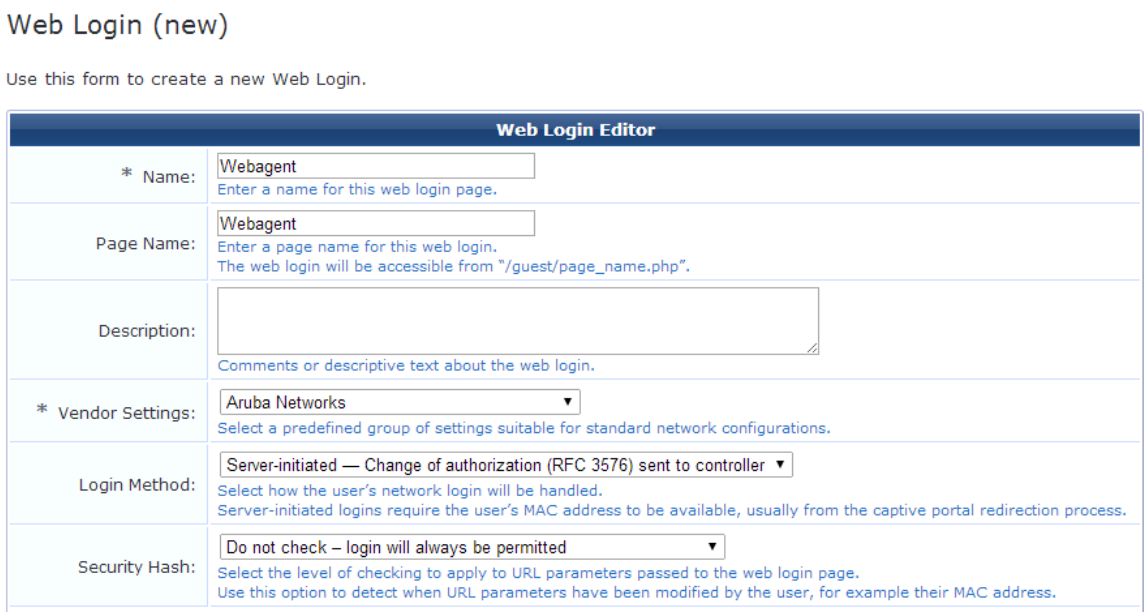


Configuring Web Agent Flow in ClearPass Guest

Use the following steps to create a web agent flow in ClearPass Guest:

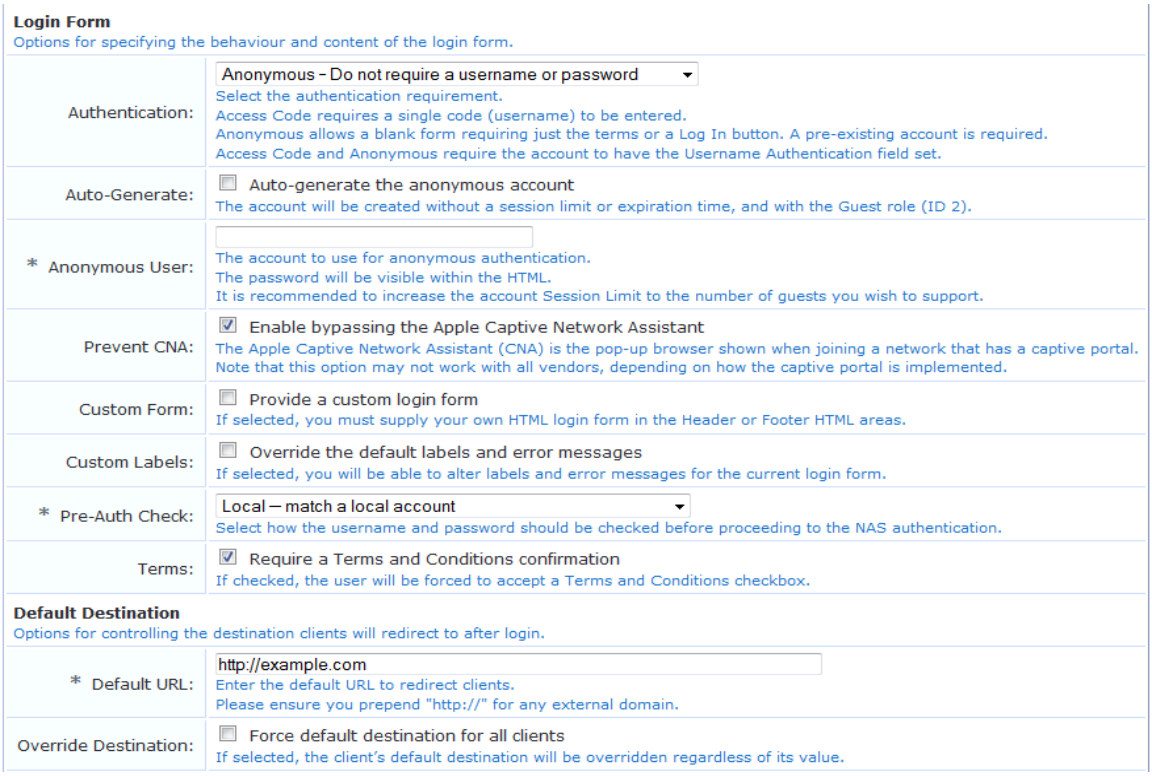
1. Click **Create a new web login page** on the right corner of the ClearPass Guest UI. The following figure shows an example of the **Web Login Editor** page:

Figure 481: *Web Login Editor*



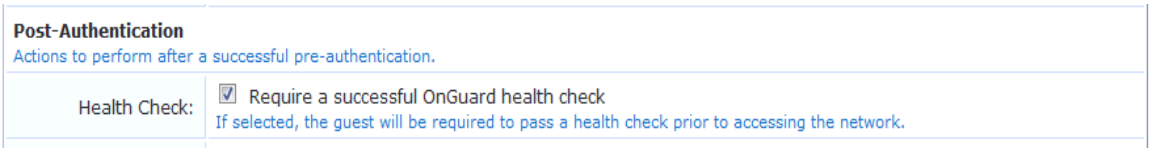
2. Select the **Anonymous - Do not require a username or password** option from the drop-down.
3. Check the **Enable bypassing the Apple Captive Network Assistant** option in the **Prevent CNA** field.
4. Select the **Local - match a local account** option in the **Pre-Auth Check** field.
5. Check the **Require Terms and Conditions confirmation** option in the **Terms** field.
6. Specify the destination URL to which the client must be redirected after health checks in the **Default destination** field.

Figure 482: *Web Login - Login Form*

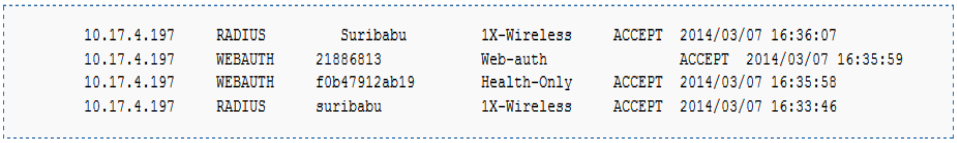


7. Select the **Local - match a local account** option in the **Post Authentication** field. The following figure shows an example of the **Web Login - Post-Authentication** page:

Figure 483: *Web Login - Post-Authentication*



The following figure shows an example of the final web agent flow:



For more information, refer to ClearPass Guest Online Help.

Native Dissolvable Agent - Supported Browsers

This section provides information on supported browsers for the Native Dissolvable Agent. The versions given in the following table are tested and are up to date at the time of this release:

Table 372: *Supported Browsers and Java Versions*

Operating System	Browser	Test Results	Known Issues	Tested Versions
Windows 7 64-bit	Chrome	Passed	#24518	Dell Networking W-ClearPass Policy Manager 6.4.0.65408 and Chrome 35.X
	Firefox	Passed	#24566, #24534	Dell Networking W-ClearPass Policy Manager 6.4.0.65408 and Firefox 30.X
	IE	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65408 and IE 11.X
	IE 64- bit	Failed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and IE 10.X
Windows 7 32-bit	Chrome	Passed	#24518	Dell Networking W-ClearPass Policy Manager 6.4.0.65408 and Chrome 34.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65408 and Firefox 30.X
	IE	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65408 and IE 11.X
Windows 8 64-bit	Chrome	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Chrome 34.X
	Firefox	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Firefox 29.X
	IE 32-bit	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and IE 10.X
Windows 8 32-bit	Chrome	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Chrome 35.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Firefox 30.X
	IE	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and IE 10.X
Windows 8.1 64-bit	Chrome	Passed	NA	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Chrome 35.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Firefox 30.X
	IE 32-bit	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and IE 11.X
Windows	Chrome	Passed		Dell Networking W-ClearPass Policy

Table 372: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
2008 64-bit				Manager 6.4.0.65823 and Chrome 34.X
	Firefox	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Firefox 30.X
	IE 32-bit	Passed	#24766	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and IE 8.X
Windows XP SP3	Chrome	Not supported		Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and Chrome 34.X
	Firefox	Not supported		Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and Firefox 30.X
	IE 32-bit	Not supported	#24768	Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and IE 8.X
Windows 2003 32-bit	Chrome	Not supported	#24768	Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and Chrome 35.X
	Firefox	Not supported	#24898	Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and Firefox 30.X
	IE	Not supported	#24898	Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and IE 8.X
Windows Vista	Chrome	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and Chrome 34.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and Firefox 26.X
	IE 32-bit	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and IE 8.X
MAC 10.9	Safari	Passed	NA	Dell Networking W-ClearPass Policy Manager 6.4.0.65408 and Safari 7.X
	Firefox	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65552 and Firefox 30.X
	Chrome	Passed	#24518	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Chrome 35.X
MAC 10.8	Safari	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Safari 6.X
	Firefox	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Firefox 31.X

Table 372: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
	Chrome	Passed	#24933	Dell Networking W-ClearPass Policy Manager 6.4.0.65823 and Chrome 35.X
MAC 10.7.5	Safari	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Safari 6.X
	Firefox	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 31.X
	Chrome	Passed		Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 36.X

For latest information on supported browsers and java versions, refer to *Dell Networking W-ClearPass Policy Manager 6.4.4 Release Notes*.

Supported Browsers and Java Versions

This section provides information on supported browsers and Java versions for the OnGuard Dissolvable Agent. The versions given in the following table are tested and are up to date at the time of this release:

Table 373: *Supported Browsers and Java Versions*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 7 64-bit	Chrome	7u65 32-bit	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and Chrome 35.X
	Firefox	7u65 32-bit	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and Firefox 11.X
	IE	7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and IE 10.X
	IE 64- bit	7u65 32-bit	Failed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and IE 10.X

Table 373: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 7 32-bit	Chrome	7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 36.X
	Firefox	7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 30.X
	IE	7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and IE 11.X
Windows 8 64-bit	Chrome	JRE: 7u65 32-bit	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and Chrome 36.X
	Firefox	JRE: 7u65 32-bit	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and Firefox 30.X
	IE 32-bit	JRE: 7u65	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and IE 10.X
Windows 8 32-bit	Chrome	JRE: 7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and Chrome 35.X
	Firefox	JRE: 7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and Firefox 30.X
	IE	JRE: 7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and IE 10.X
Windows 8.1 64-bit	Chrome	JRE: 7u65 32-bit	Passed	#7165	Dell Networking

Table 373: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
					W-ClearPass Policy Manager 6.4.0.65658 and Chrome 36.X
	Firefox	JRE: 7u65 32-bit	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and Firefox 30.X
	IE 32-bit	7U65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65762 and IE 11.X
Windows 2008 64-bit	Chrome	JRE: 7u65 32-bit	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 34.X
	Firefox	JRE: 7u65 32-bit	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 30.X
	IE 32-bit	JRE: 7u65	Passed	#7165	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and IE 9.X
Windows 2003 32-bit	Chrome	JRE: 7u65	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 35.X
	Firefox	JRE: 7u65	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 30.X
	IE	JRE: 7u65	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and IE 8.X

Table 373: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows XP 32-bit	Chrome	JRE: 7u65	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 35.X
	Firefox	JRE: 7u65	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 30.X
	IE	JRE: 7u65	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and IE 8.X
MAC 10.9	Safari	JRE: 7u65	Passed	#20191	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Safari 7.X
	Firefox	JRE: 7u65	Passed	None	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 30.X
	Chrome	JRE: 7u65	Failed	#18031	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 35.X
MAC 10.8	Firefox	JRE: 7u65	Passed	#20191	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 30.X
	Chrome	JRE: 7u65	Failed	#18031	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 35.X

Table 373: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
MAC 10.7.5	Safari	JRE: 7u65	Passed	#20191	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Safari 6.X
	Firefox	JRE: 7u65	Passed	#23340	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Firefox 30.X
	Chrome	JRE: 7u65	Failed	#18031	Dell Networking W-ClearPass Policy Manager 6.4.0.65658 and Chrome 34.X

For latest information on supported browsers and java versions, refer to *Dell Networking W-ClearPass Policy Manager 6.4.4 Release Notes*.