Dell Networking W-ClearPass Policy Manager 6.3

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.

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 any wired, wireless, and VPN. Software modules for the Dell Networking W-ClearPass Policy Manager platform, such as Guest, Onboard, Profile, OnGuard, QuickConnect, and Insight simplify and automate device configuration, provisioning, profiling, health checks, and guest access.

With built-in RADIUS, SNMP and TACACS+ protocols, 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 as devices connect to the network.

For information about common tasks, see "Common Tasks in Policy Manager" on page 21.

Common Tasks in Policy Manager

As you work in Policy Manager, you'll encounter many things that work similarly in different places. For example, importing or exporting from a list of items. This section explains how to do these common tasks.

- "Importing" on page 21
- "Exporting" on page 22

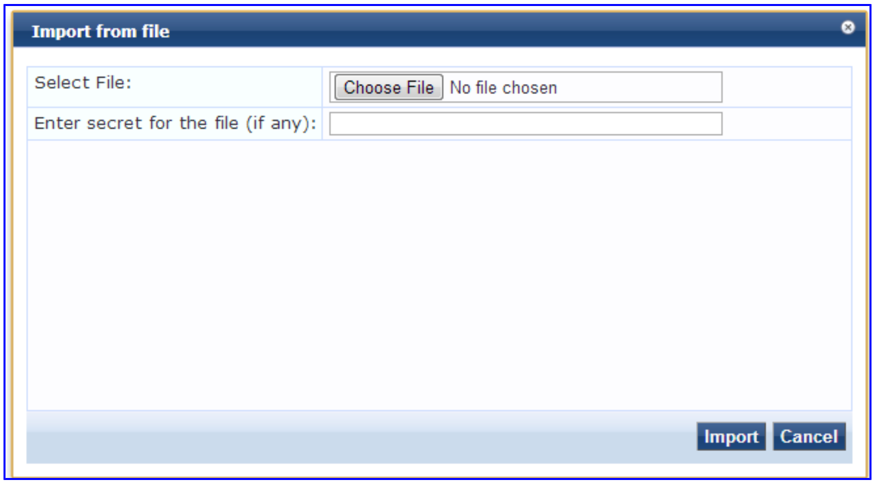
Importing

On most pages with lists in Dell Networking W-ClearPass Policy Manager, you can import the information about one or more items. That information is stored as an XML file, and this file can be password protected. The tags and attributes in the XML file are explained in the API Guide.

In the popup you see an icon that is similar to the following two examples:

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

Figure 1: *Import from file screen example*



Import from file

Select File: Choose File No file chosen

Enter secret for the file (if any):

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

The file you select must be an XML file in the correct format. If you've exported files from different places in Policy Manager, make sure you're selecting the correct one to be imported. The API Guide contains more information about the format and contents of XML files.

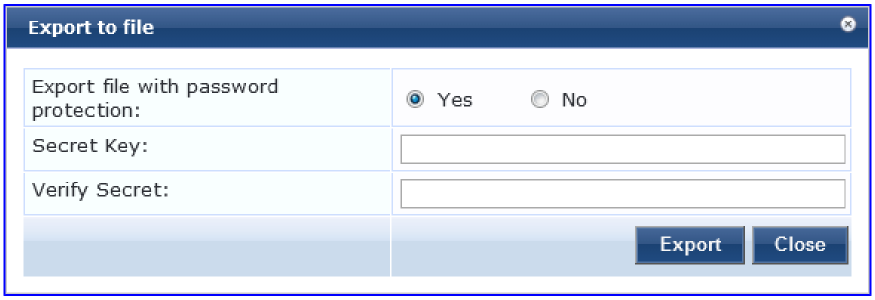
4. If the file is password protected, enter the password (secret).
5. Click **Import**.

Exporting

On most pages with lists in Dell Networking W-ClearPass Policy Manager, you can export the information about one or more items. That 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 API Guide.

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

Figure 2: *Export to File*



Export to file

Export file with password protection:	● Yes ○ No
Secret Key:	
Verify Secret:	

2. If you want the file password protected, select **Yes** and enter a password twice (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 asked to save it and specify the location.

NOTE

To export multiple items, select the checkboxes in the table beside the items that you want to export.

Chapter 2
Powering Up and Configuring Policy Manager Hardware

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).

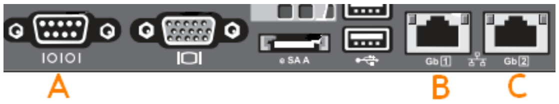
For more information, see:

- "Server Port Overview" on page 23
- "Server Port Configuration" on page 23
- "Powering Off the System" on page 25
- "Resetting the Passwords to Factory Default" on page 26
- "Generating a Support Key for Technical Support" on page 26

Server Port Overview

The Policy Manager server requires initial port configuration. Its backplane contains three ports.

Figure 3: *Policy Manager Backplane*



The ports 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, via hardwired terminal.
B - eth0	Management (gigabit Ethernet)	Provides access for cluster administration and appliance maintenance via Web access, CLI, or internal cluster communications. Configuration required.
C - eth1	Data (gigabit Ethernet)	Provides point of contact for RADIUS, TACACS+, Web Authentication and other data-plane requests. Configuration optional. If not configured, requests redirected to the management port.

Server Port Configuration

Before starting the installation, gather the following information that you will 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**

   Using the null modem cable provided, connect a serial port on the appliance to a terminal, then connect power and switch on. The appliance immediately becomes 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**

   Later, you will create a unique appliance/cluster administration password. For now, use the following preconfigured credentials:

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

   This starts 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 of at least six characters:

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

   Going forward, you will use this 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
   ```

   After the timezone information is entered, you are asked to confirm the selection.

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 your 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 414 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 via 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 Administrator passwords 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 via the front serial port (using any terminal program). See "Resetting the Passwords to Factory Default" on page 26 for details.
2. Reboot the system. See the `restart` command.
3. After the system restarts, 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 the recovery key, select option 1.
5. To generate a support key and a recovery key and support, select option 3.
6. 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.
7. Enter the following 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
   ```

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 Command Line Interface (CLI) and enter the command: **`system gen-support-key`**. See "gen-support-key" on page 435 for details.
2. Connect to the Policy Manager appliance via the front serial port (using any terminal program). See "Server Port Configuration" on page 23 for details.
3. Reboot the system. See the `restart` command.
4. When the system restarts it waits at the following prompt 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. Select 3 if you want to generate a password recovery key, as well.
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.

Chapter 3
Policy Manager Dashboard

Drag and drop elements from the left pane to customize the **Dashboard** layout.

Table 3: *Dashboard Layout Parameters*

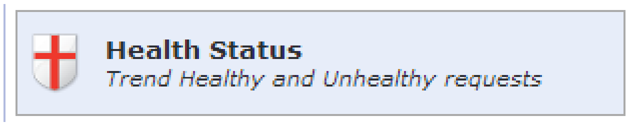
 All Requests *Trend all Policy Manager requests*	The graph displays all requests processed by Policy Manager over the past week. Processed requests include RADIUS, TACACS+ and WebAuth requests. The default data filter “All Requests” is used to plot this graph. Clicking on each bar in the graph drills down into the Access Tracker and shows the requests for that day.
 **Health Status** *Trend Healthy and Unhealthy requests*	This shows a graph of the “Healthy” vs. “Unhealthy” requests over the past week. Healthy requests are those requests where the health state was deemed to be healthy (based on the posture data sent from the client). Unhealthy requests are those requests whose 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 and shows the healthy or unhealthy requests for that day.
 Authentication Status *Trend Successful and Failed authentications*	This shows a graph of the “Failed” vs. “Successful” requests over the past week. This 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 and shows the failed or successful requests for that day.
 Latest Authentications *Latest Authentications*	This shows a table of the last few authentications. Clicking on a row drills down into the Access Tracker and shows requests sorted by timestamp with the latest request showing first.

Table 3: *Dashboard Layout Parameters (Continued)*

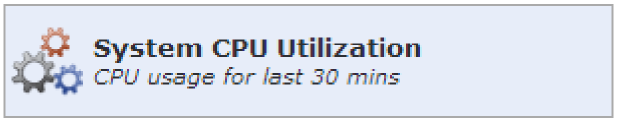
 Device Category *Device Categories*	This chart shows the graph of all profiled devices categorized into built in categories - Smartdevices, Access Points, Computer, VOIP phone, Datacenter Appliance, Printer, Physical Security, Game Console, Routers, Unknown, and Conflict. Unknown devices are devices that the profiler was not able to profile. Conflict indicates a conflict 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, a conflict is flagged, and the device is marked as Conflict.
 Device Family *Device Family*	The Device Family widget allows you to drill down further into each of the built-in device categories. For example, selecting **SmartDevice** shows the different kinds of smart devices identified by Profile.
 **System CPU Utilization** *CPU usage for last 30 mins*	Add the System CPU Utilization widget to the 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 your mouse over the red section of the graph.
 Request Processing Time *Trend total request processing time*	Add the Request Processing Time widget to the Dashboard to view the trend of total request processing time.
 System Summary *Snapshot of system usage*	Add the System Summary widget to the Dashboard to view the Percentage Used statistics for Main Memory, Swap Memory, Disk, and Swap Disk
 Successful Authentications *Track the latest successful authentications*	This shows a table of the last few successful authentications. Clicking on a row drills down into the Access Tracker and shows successful requests sorted by timestamp with the latest request showing first.

Table 3: *Dashboard Layout Parameters (Continued)*

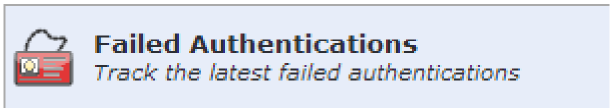
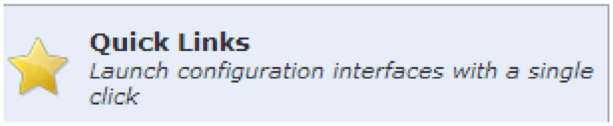
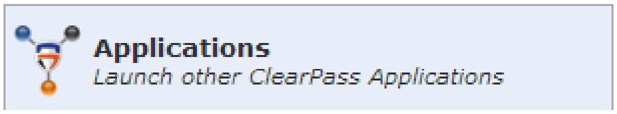
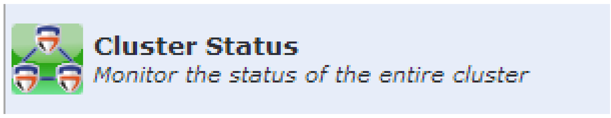
 Failed Authentications Track the latest failed authentications	This shows a table of the last few failed authentications. Clicking on a row drills down into the Access Tracker and shows failed requests sorted by timestamp with the latest request showing first.
 Service Categorization Monitor Service Categorization of authentications	This shows a bar chart with each bar representing a Policy Manager service requests were categorized into. Clicking on a bar drills down into the Access Tracker and shows the requests that were categorized into that specific service.
 Alerts Latest Alerts	This shows a table of the last few system level events. Clicking on a row drills down into the Event Viewer
 Quick Links Launch configuration interfaces with a single click	Quick Links shows links to common configuration tasks: • **Start Configuring Policies** links to the Start Here Page under the Configuration menu. Start configuring Policy Manager Services from here. • **Manage Services** links to the Services page under the Configuration menu. Shows a list of configured services. • **Access Tracker** links to the Access Tracker screen under Reporting & Monitoring menu. • **Analysis & Trending** links to the Analysis & Trending screen under Reporting & Monitoring menu. • **Network Devices** links to the Network Devices screen under the Configuration menu. Configure network devices from here. • **Server Manager** links to the Server Configuration screen under the Administration menu. • **ClearPass Guest** links to the ClearPass Guest application. This application opens in a new tab. • **ClearPass Onboard + WorkSpace** links to the ClearPass Onboard + Workspace screen within the ClearPass Guest application. This application opens in a new tab.

Table 3: *Dashboard Layout Parameters (Continued)*

 **Applications** *Launch other ClearPass Applications*	This shows links to the Dell Insight, Guest and Onboard + WorkSpace applications that are integrated with Policy Manager.
 **Cluster Status** *Monitor the status of the entire cluster*	This shows the status of all nodes in the 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** Host name and IP address of the node ● **CPU Util** Snapshot of the CPU utilization in percentage ● **Mem Util** Snapshot of the memory utilization in percentage ● **Server Role** Publisher or subscriber

The Policy Manager Monitoring feature provides access to live monitoring of components and other functions.

For more information, see:

- "Live Monitoring" on page 33
- "Audit Viewer" on page 58
- "Event Viewer" on page 63
- "Data Filters" on page 65
- "Blacklisted Users" on page 68

Live Monitoring

The live monitoring link provides access to six monitoring features.

For more information, see:

- "Access Tracker" on page 33
- "Accounting" on page 39
- "Analysis and Trending" on page 51
- "Endpoint Profiler" on page 51
- "OnGuard Activity" on page 47
- "System Monitor" on page 53

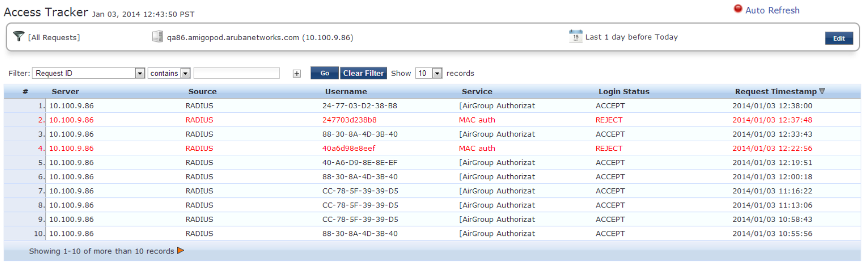
Access Tracker

The Access Tracker feature provides a real-time display of system activity.

For more information, see:

- "Editing the Access Tracker" on page 35
- "Viewing Access Tracker Session Details" on page 35

Figure 4: *Access Tracker Page*



Access Tracker Jan 03, 2014 12:43:50 PST

Auto Refresh

[All Requests] qa86.amigopod.arubanetworks.com (10.100.9.86) Last 1 day before Today

Filter: Request ID contains Show 10 records

#	Server	Source	Username	Service	Login Status	Request Timestamp ▽
1.	10.100.9.86	RADIUS	24-77-03-D2-38-B8	[AirGroup Authorizat	ACCEPT	2014/01/03 12:38:00
2.	10.100.9.86	RADIUS	247703d238b8	MAC auth	REJECT	2014/01/03 12:37:48
3.	10.100.9.86	RADIUS	88-30-8A-4D-3B-40	[AirGroup Authorizat	ACCEPT	2014/01/03 12:33:43
4.	10.100.9.86	RADIUS	40a6d98e8eef	MAC auth	REJECT	2014/01/03 12:22:56
5.	10.100.9.86	RADIUS	40-A6-D9-8E-8E-EF	[AirGroup Authorizat	ACCEPT	2014/01/03 12:19:51
6.	10.100.9.86	RADIUS	88-30-8A-4D-3B-40	[AirGroup Authorizat	ACCEPT	2014/01/03 12:00:18
7.	10.100.9.86	RADIUS	CC-78-5F-39-39-D5	[AirGroup Authorizat	ACCEPT	2014/01/03 11:16:22
8.	10.100.9.86	RADIUS	CC-78-5F-39-39-D5	[AirGroup Authorizat	ACCEPT	2014/01/03 11:13:06
9.	10.100.9.86	RADIUS	CC-78-5F-39-39-D5	[AirGroup Authorizat	ACCEPT	2014/01/03 10:58:43
10.	10.100.9.86	RADIUS	88-30-8A-4D-3B-40	[AirGroup Authorizat	ACCEPT	2014/01/03 10:55:56

Showing 1-10 of more than 10 records

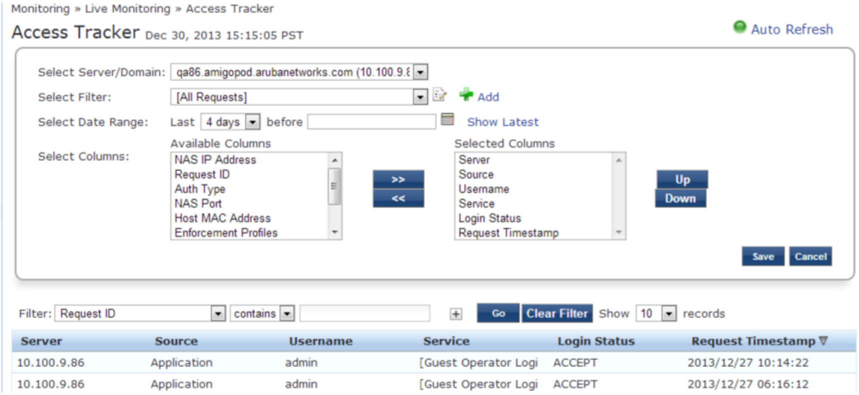
Table 4: *Access Tracker Page Parameters*

Parameter	Description
[All Requests]	Current filter setting. See "Data Filters" on page 65 to modify this setting.
🖥	IP address or domain name of the server.
15 Last 1 day before Today	A setting of Last 1 day before Today displays information for the past 24 hours. Shows the current setting for the number of days prior to the configured date for which Access Tracker data is to be displayed.
Auto Refresh	Click to enable or disable automatic page refresh.
Filter	Select filter to constrain data display. The filters provided for Access Tracker are: ● Request ID ● Source ● Username ● NAS IP Address ● NAS Port ● Service ● Login Status ● Error Code ● Host MAC Address ● Alerts ● Monitor Mode ● Auth Type ● Roles ● Enforcement Profiles ● System Posture Token ● Audit Posture Token ● Request ID
contains or equals	Select either contains or equals.
Show *n* Records	Select 10, 20, 50 or 100 records to display on one report page. This setting is saved and available in subsequent logins.
✎	Modify the currently displayed data filter.
Go Clear Filter	Click **Go** to generate a new report. Click **Clear Filter** to delete all filters except for the first filter.
⊞	Click to add a data filter to the report page. After you click the icon, a second set of filter parameters is displayed. Data filters with more detailed parameters can also be created if you click the Edit button. For more information, see "Data Filters" on page 65.

Editing the Access Tracker

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

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



Monitoring » Live Monitoring » Access Tracker

Access Tracker Dec 30, 2013 15:15:05 PST

Select Server/Domain: qa86.amigopod.arubanetworks.com (10.100.9.8

Select Filter: [All Requests]

Select Date Range: Last 4 days before

Select Columns:

Available Columns: NAS IP Address, Request ID, Auth Type, NAS Port, Host MAC Address, Enforcement Profiles

Selected Columns: Server, Source, Username, Service, Login Status, Request Timestamp

Filter: Request ID contains

Show 10 records

Server	Source	Username	Service	Login Status	Request Timestamp ▽
10.100.9.86	Application	admin	[Guest Operator Logi	ACCEPT	2013/12/27 10:14:22
10.100.9.86	Application	admin	[Guest Operator Logi	ACCEPT	2013/12/27 06:16:12

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

Parameter	Description
Select Server/Domain:	Select the server for which to display dashboard data. Select All to display transactions from all nodes in the Policy Manager cluster.
Auto Refresh:	Click to enable or disable the automatic page refresh feature.
Select Filter:	Select a filter category to constrain data display. For a description of available filters, see Data Filters on page 65.
📝	Click to modify the current data filter. For more information, see Data Filters on page 65.
✚ Add	Click to add a data filter. The Data Filters page opens to the Filter tab. For more information, see Data Filters on page 65.
Select Date Range:	Select the number of days prior to the configured date for which Access Tracker data is to be displayed. Select 1-6 days or 1 week.
📅	Click to select a before date.
Show Latest:	Click to set the before date to Today.
Select Columns:	Available Columns: Displays column names that you can select for display in an Access Tracker report.
	Selected Columns: Displays the column names selected to display in an Access Tracker report.

Viewing Access Tracker Session Details

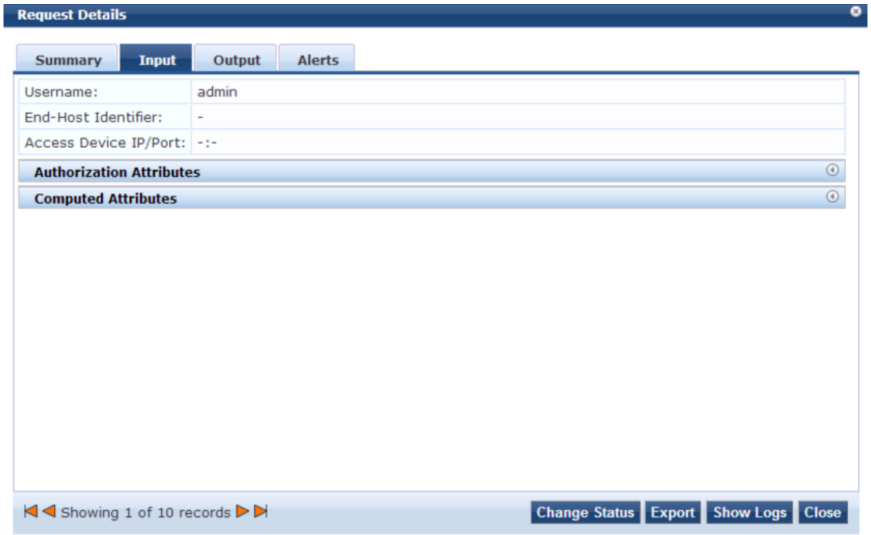
This topic includes examples of the tabs displayed on a typical Request Details page. To view details about a session, click a row containing any entry. The actions available depend on the type of device. The Disconnect or Terminate

Section action is supported by all devices. Some devices support setting a session timeout, changing the VLAN for the session, applying an ACL, etc.

Summary tab

This tab shows a summary view of the transaction, including policies that have been applied.

Figure 6: *Request Details Summary tab Parameters*



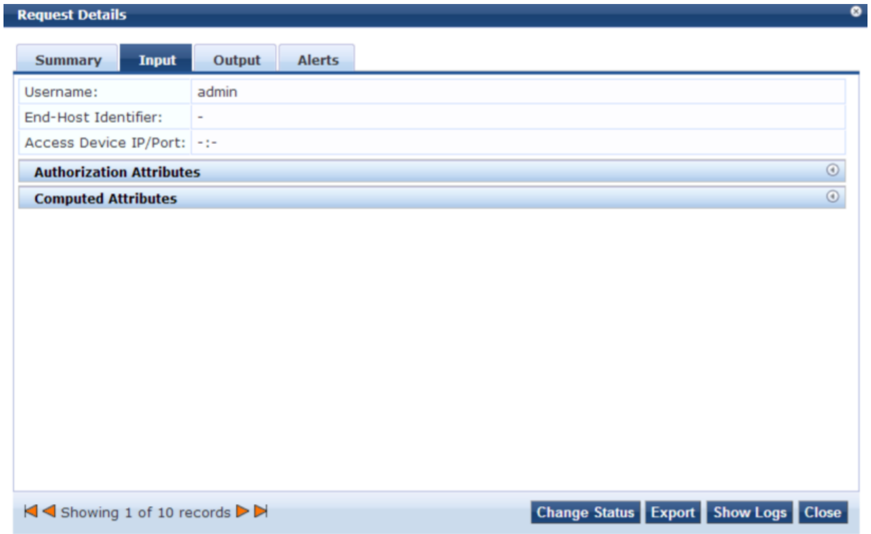
Username:	admin
End-Host Identifier:	-
Access Device IP/Port:	-:-

Showing 1 of 10 records

Input tab

This tab shows protocol specific attributes that Policy Manager received in the transaction request; this includes authentication and posture details (if available). It also shows Compute Attributes, which are attributes that were derived from the request attributes. All of the attributes can be used in role mapping rules.

Figure 7: *Request Details Input tab Parameters*



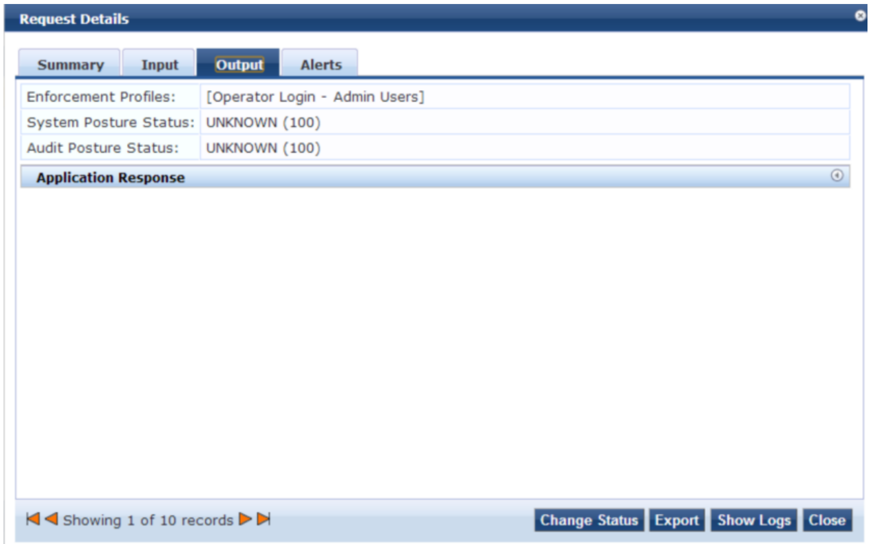
Username:	admin
End-Host Identifier:	-
Access Device IP/Port:	-:-

Showing 1 of 10 records

Output tab

This tab shows the attributes that were sent to the network device and the posture-capable endpoint.

Figure 8: *Output tab Parameters*

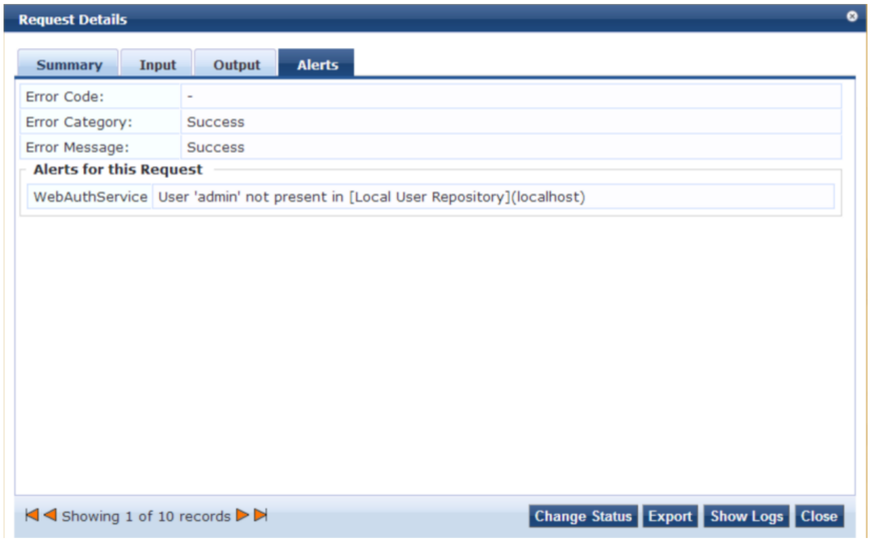


Enforcement Profiles:	[Operator Login - Admin Users]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

Alerts tab

This tab is displayed if there was an error in the Login Status. For example, if you select a row in a report where the Login Status displays TIMEOUT or REJECT, an Alerts tab will be displayed.

Figure 9: *Alerts tab Parameters*



Error Code:	-
Error Category:	Success
Error Message:	Success

Alerts for this Request

WebAuthService	User 'admin' not present in [Local User Repository](localhost)

Table 6: *Request Details Page Control Parameters*

Parameter	Description
Change Status	The button is only enabled if you use the RADIUS and WebAuth authentication types. After you click this button, the Access Control Capabilities tab opens. You can view or change the Access Control Type. Click this button to change the access control status of a session. ● **Agent** This control is available for a session where the endpoint has the OnGuard Agent installed. Actions allowed are: ● Bounce ● Send Message ● 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 attached, via SNMP. **NOTE:** For this type of control, SNMP read and write community strings must be configured for the network device, and Policy Manager must be configured 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 must be 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, applying an ACL, etc.
Export	Export this transaction and download as a compressed (.zip extension) file. The compressed file contains the session-specific logs, the policy XML for the transaction, and a text file containing the Access Tracker session details.
Show Logs	Show logs of this session. Error messages are red, and Warning messages are orange.
Close	RADIUS response attributes sent to the device.

Depending on the type of authentication - RADIUS, WebAuth, TACACS, Application - the view might contain different tabs. A sample of available tabs appears below.

Accounting tab

The Accounting tab is only available for RADIUS sessions. It shows the RADIUS accounting details, including re authentication details for the session.

Authorizations tab

This tab is only available for TACACS+ sessions. This shows the commands entered at the network device, and the authorization status.

RADIUS CoA tab

This tab is only available for RADIUS transactions for which a RADIUS Change of Authorization command was sent to the network device by Policy Manager. The view shows the RADIUS CoA actions sent to the network device in chronological order.

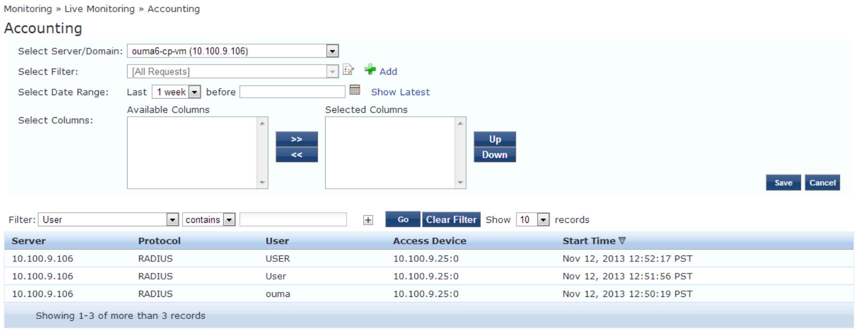
Accounting

The Accounting display provides a dynamic report that describes accesses (as reported by the network access device by means of RADIUS/TACACS+ accounting records), at: **Monitoring > Live Monitoring > Accounting.** Click a row to display the corresponding Accounting Record Details.

For more information, see:

- "RADIUS Accounting Record Details (Auth Sessions tab)" on page 40
- "RADIUS Accounting Record Details (Details tab)" on page 41
- "RADIUS Accounting Record Details (Summary tab)" on page 41
- "RADIUS Accounting Record Details (Utilization tab)" on page 43
- "TACACS+ Accounting Record Details (Auth Sessions tab)" on page 44
- "TACACS+ Accounting Record Details (Details tab)" on page 45
- "TACACS+ Accounting Record Details (Request tab)" on page 46

Figure 10: *Accounting Page (Edit Mode)*



Monitoring » Live Monitoring » Accounting

Accounting

Select Server/Domain: ouma6-cp-vm (10.100.9.106)

Select Filter: [All Requests]

Select Date Range: Last 1 week before

Select Columns: Available Columns / Selected Columns

Filter: User contains

Server	Protocol	User	Access Device	Start Time ▽
10.100.9.106	RADIUS	USER	10.100.9.25:0	Nov 12, 2013 12:52:17 PST
10.100.9.106	RADIUS	User	10.100.9.25:0	Nov 12, 2013 12:51:56 PST
10.100.9.106	RADIUS	ouma	10.100.9.25:0	Nov 12, 2013 12:50:19 PST

Showing 1-3 of more than 3 records

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

Parameter	Description
Select Server/Domain:	Select server for which to display dashboard data.
Select Filter:	Select filter to constrain data display.
Modify:	Modify the currently displayed data filter.
Add: ✚ Add	Go to Data Filters page to create a new data filter.

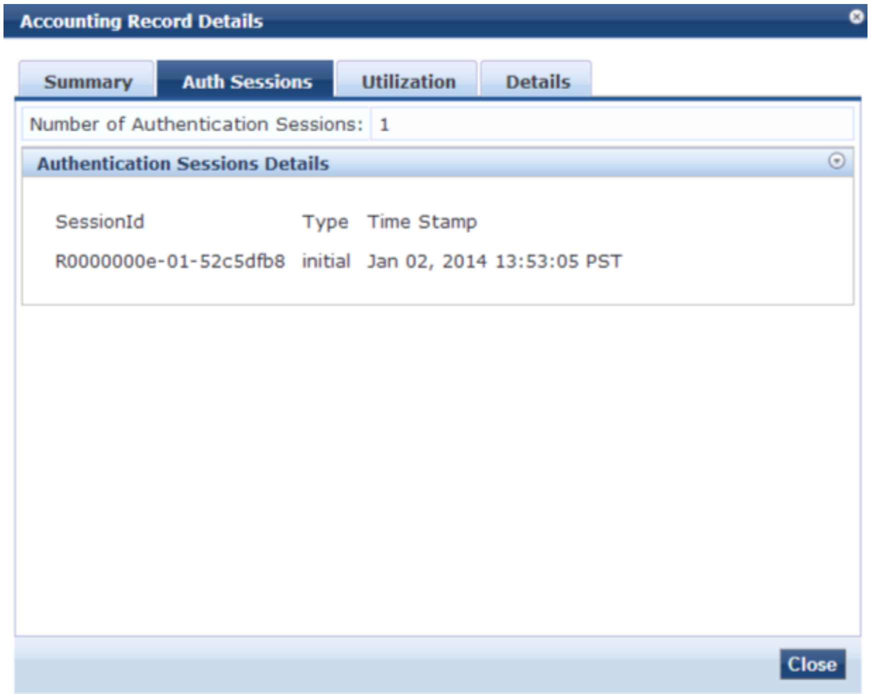
Table 7: *Accounting Page (Edit Mode) Parameters (Continued)*

Parameter	Description
Select Date Range:	Select the number of days prior to the configured date for which Accounting data is to be displayed. Valid number of days is 1 day to a week.
Show Latest:	Sets the date to Today in the previous step to Today.
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 in either column.
Show <*n*> records:	Show 10, 20, 50 or 100 rows. After being selected, this setting is saved and available in subsequent sessions.

RADIUS Accounting Record Details (Auth Sessions tab)

This topic describes the parameters of the Accounting Record Details Auth Sessions tab for the RADIUS Protocol.

Figure 11: *RADIUS Accounting Record Details (Auth Sessions tab)*



Number of Authentication Sessions: 1

SessionId	Type	Time Stamp
R0000000e-01-52c5dfb8	initial	Jan 02, 2014 13:53:05 PST

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

Parameter	Description
Session ID:	Policy Manager session ID.
Type:	Initial authentication or a re-authentication.

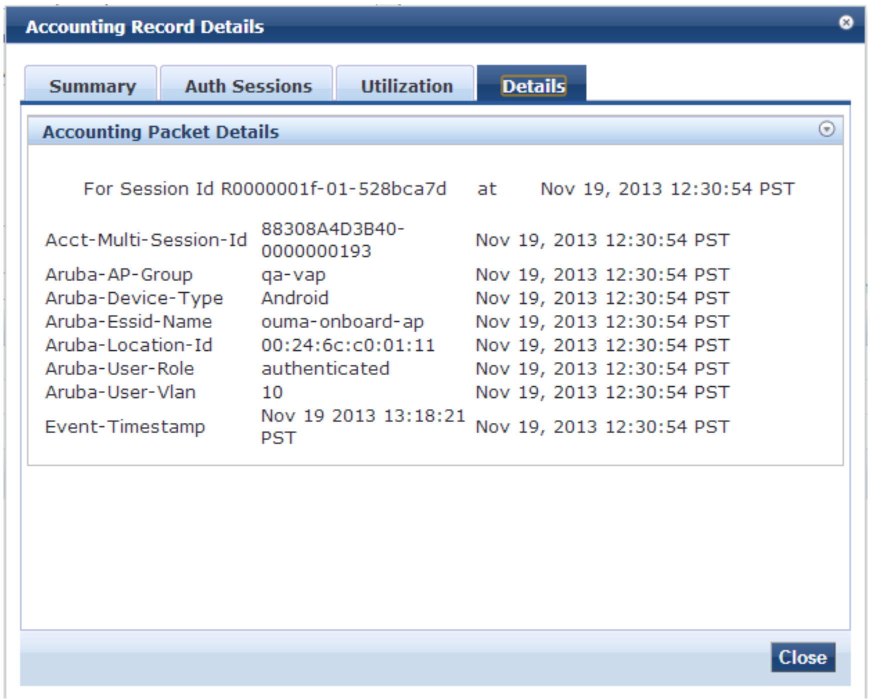
Table 8: *RADIUS Accounting Record Details Auth Sessions tab Parameters (Continued)*

Parameter	Description
Time Stamp:	When the event occurred.

RADIUS Accounting Record Details (Details tab)

This topic describes the parameters of the Accounting Record Details Details tab for the RADIUS Protocol.

Figure 12: *RADIUS Accounting Details tab*



Accounting Packet Details

For Session Id R0000001f-01-528bca7d at Nov 19, 2013 12:30:54 PST

Acct-Multi-Session-Id	88308A4D3B40-0000000193	Nov 19, 2013 12:30:54 PST
Aruba-AP-Group	qa-vap	Nov 19, 2013 12:30:54 PST
Aruba-Device-Type	Android	Nov 19, 2013 12:30:54 PST
Aruba-Essid-Name	ouma-onboard-ap	Nov 19, 2013 12:30:54 PST
Aruba-Location-Id	00:24:6c:c0:01:11	Nov 19, 2013 12:30:54 PST
Aruba-User-Role	authenticated	Nov 19, 2013 12:30:54 PST
Aruba-User-Vlan	10	Nov 19, 2013 12:30:54 PST
Event-Timestamp	Nov 19 2013 13:18:21 PST	Nov 19, 2013 12:30:54 PST

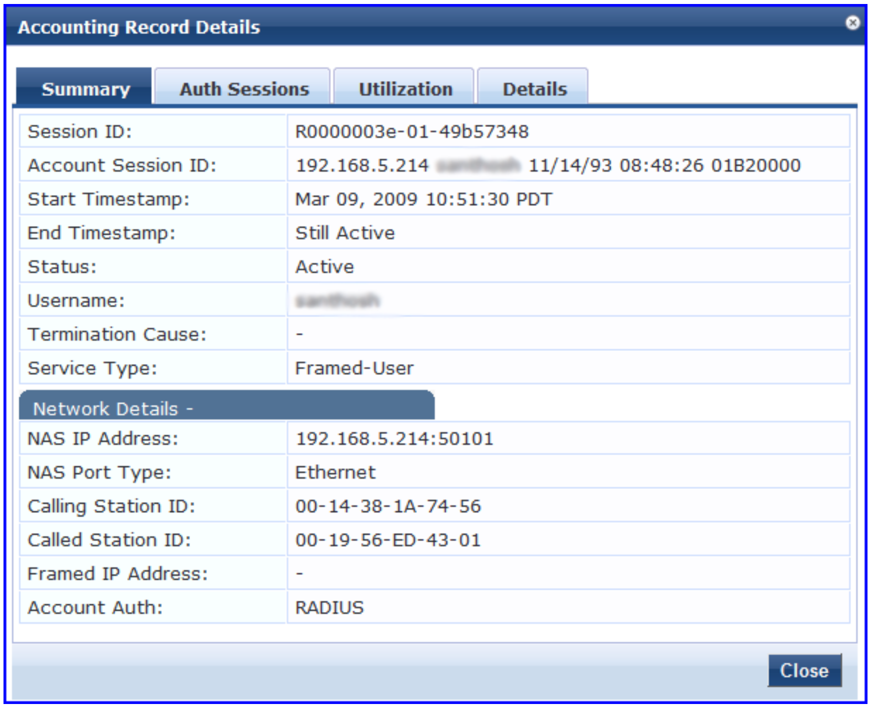
Table 9: *RADIUS Accounting Record Details tab Parameters*

Parameter	Description
Details tab	Shows details of RADIUS attributes sent and received from the network device during the 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 topic describes the parameters of the Accounting Record Details Summary tab for the RADIUS Protocol.

Figure 13: *RADIUS Accounting Record Details (Summary tab)*



Session ID:	R0000003e-01-49b57348
Account Session ID:	192.168.5.214 [redacted] 11/14/93 08:48:26 01B20000
Start Timestamp:	Mar 09, 2009 10:51:30 PDT
End Timestamp:	Still Active
Status:	Active
Username:	[redacted]
Termination Cause:	-
Service Type:	Framed-User

Network Details -

NAS IP Address:	192.168.5.214:50101
NAS Port Type:	Ethernet
Calling Station ID:	00-14-38-1A-74-56
Called Station ID:	00-19-56-ED-43-01
Framed IP Address:	-
Account Auth:	RADIUS

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

Parameter	Description
Session ID:	Policy Manager session identifier (you can correlate this record with a record in Access Tracker).
Account Session ID:	A unique ID for this accounting record.
Start and End Timestamp:	Start and end time of the session.
Status:	Current connection status of the session.
Username:	Username associated with this record.
Termination Cause:	The reason for termination of this session.

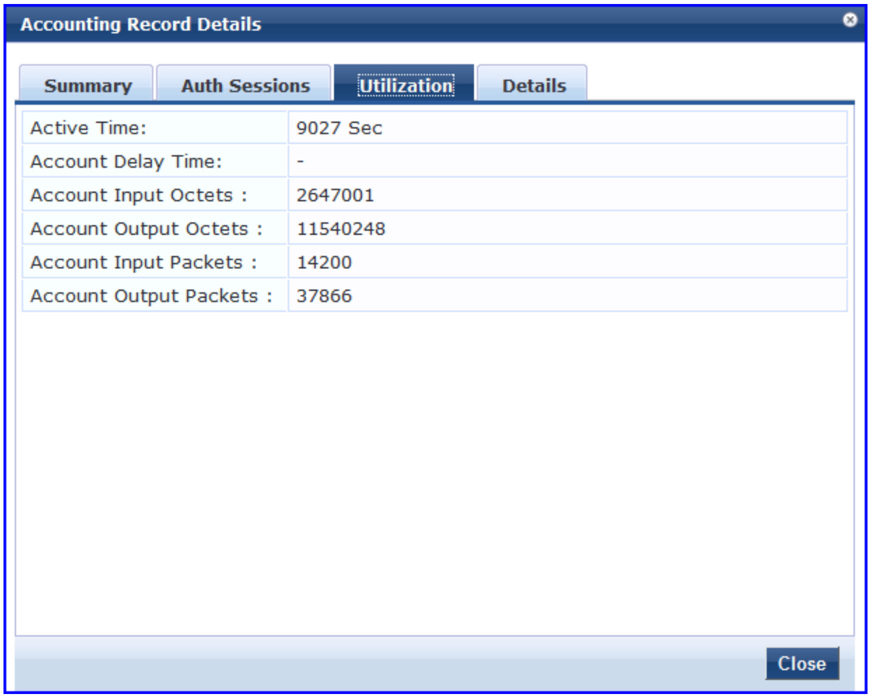
Table 10: *RADIUS Accounting Record Details Summary tab Parameters (Continued)*

Parameter	Description
Service Type:	The value of the standard RADIUS attribute ServiceType.
NAS IP Address:	IP address of the network device.
NAS Port Type:	The access method - For example, Ethernet, 802.11 Wireless, etc.
Calling Station ID:	In most use cases supported by Policy Manager this is the MAC address of the client.
Called Station ID:	MAC Address of the network device.
Framed IP Address:	IP Address of the client (if available).
Account Auth:	Type of authentication - In this case, RADIUS.

RADIUS Accounting Record Details (Utilization tab)

This topic describes the parameters of the Accounting Record Details Utilization tab for the RADIUS Protocol.

Figure 14: *RADIUS Accounting Record Details (Utilization tab)*



Active Time:	9027 Sec
Account Delay Time:	-
Account Input Octets :	2647001
Account Output Octets :	11540248
Account Input Packets :	14200
Account Output Packets :	37866

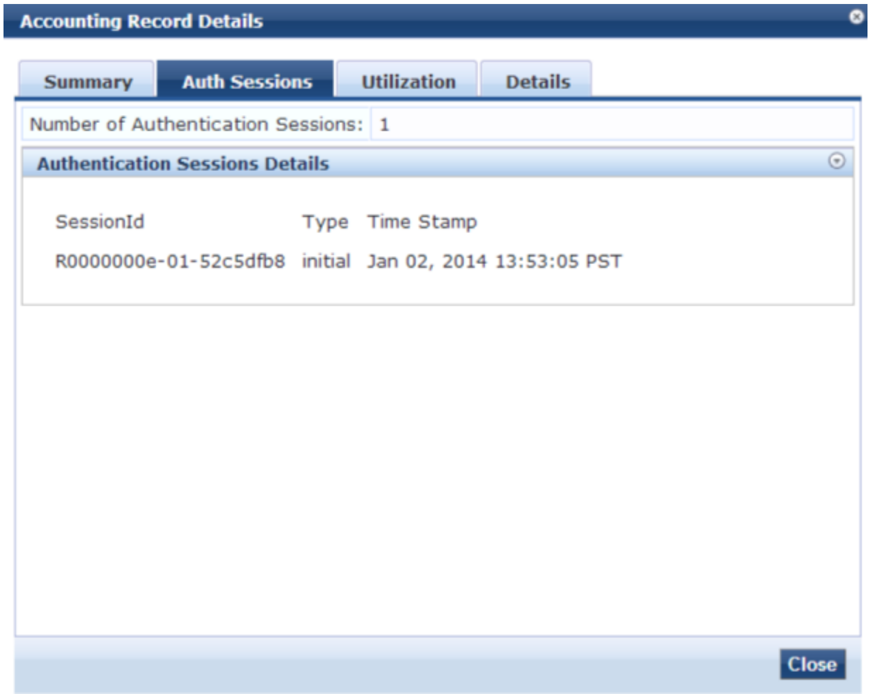
Table 11: *RADIUS Accounting Record Details Utilization tab Parameters*

Parameter	Description
Active Time:	How long the session was active.
Account Delay Time:	How many seconds the network device has been trying to send this record for (subtract from record time stamp to arrive at the time this record was actually generated by the device).
Account Input Octets:	Quantity of octets sent to and received from the device port over the course of the session.
Account Output Octets:	
Account Input Packets:	Packets sent and received from the device port over the course of the session.
Account Output Packets:	

TACACS+ Accounting Record Details (Auth Sessions tab)

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

Figure 15: *TACACS+ Accounting Record Details (Auth Sessions tab)*



Number of Authentication Sessions: 1

Authentication Sessions Details

SessionId	Type	Time Stamp
R0000000e-01-52c5dfb8	initial	Jan 02, 2014 13:53:05 PST

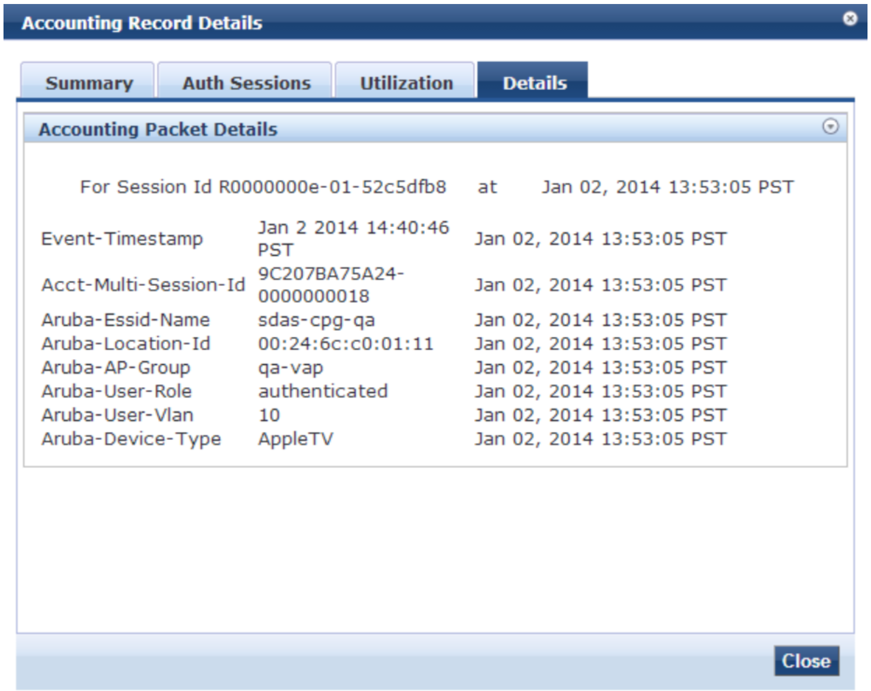
Table 12: *TACACS+ Accounting Record Details Auth Sessions tab Parameters*

Parameter	Description
Number of Authentication Sessions:	Total number of authentications (always 1) and authorizations in this session.
Authentication Sessions Details:	For each request ID, denotes whether it is an authentication or authorization request, and the time at which the request was sent.

TACACS+ Accounting Record Details (Details tab)

This topic describes the parameters of the Accounting Record Details Details tab for the TACACS+ Protocol.

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



Accounting Packet Details

For Session Id R0000000e-01-52c5dfb8 at Jan 02, 2014 13:53:05 PST

Event-Timestamp	Jan 2 2014 14:40:46 PST	Jan 02, 2014 13:53:05 PST
Acct-Multi-Session-Id	9C207BA75A24-0000000018	Jan 02, 2014 13:53:05 PST
Aruba-Essid-Name	sdas-cpg-qa	Jan 02, 2014 13:53:05 PST
Aruba-Location-Id	00:24:6c:c0:01:11	Jan 02, 2014 13:53:05 PST
Aruba-AP-Group	qa-vap	Jan 02, 2014 13:53:05 PST
Aruba-User-Role	authenticated	Jan 02, 2014 13:53:05 PST
Aruba-User-Vlan	10	Jan 02, 2014 13:53:05 PST
Aruba-Device-Type	AppleTV	Jan 02, 2014 13:53:05 PST

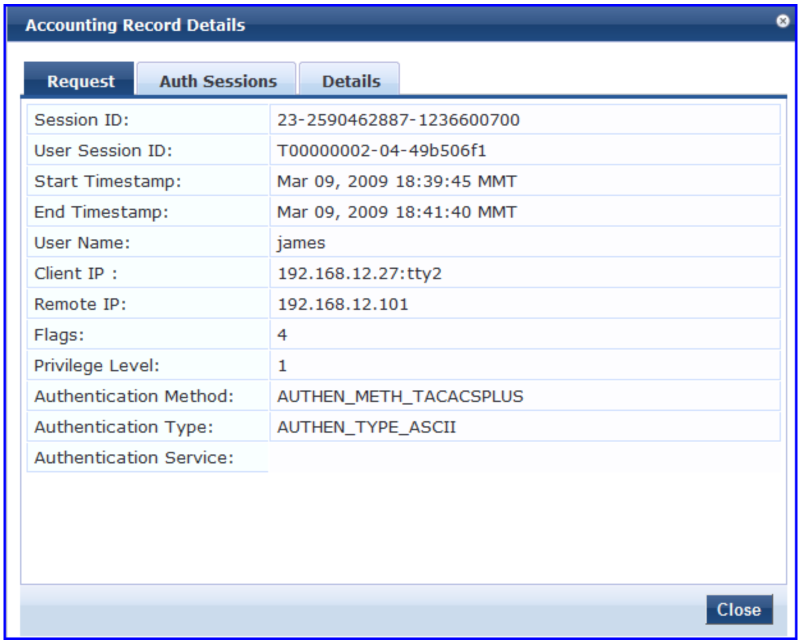
Table 13: *TACACS+ Accounting Record Details tab Parameters*

Parameter	Description
Details tab	For each authorization request, shows: cmd (command typed), priv-lvl (privilege level of the administrator executing the command), service (shell), etc.

TACACS+ Accounting Record Details (Request tab)

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

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



Session ID:	23-2590462887-1236600700
User Session ID:	T00000002-04-49b506f1
Start Timestamp:	Mar 09, 2009 18:39:45 MMT
End Timestamp:	Mar 09, 2009 18:41:40 MMT
User Name:	james
Client IP :	192.168.12.27:tty2
Remote IP:	192.168.12.101
Flags:	4
Privilege Level:	1
Authentication Method:	AUTHEN_METH_TACACSPLUS
Authentication Type:	AUTHEN_TYPE_ASCII
Authentication Service:	

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

Parameter	Description
Session ID:	The Session ID is a Unique ID associated with a request.
User Session ID:	A session ID that correlates authentication, authorization and accounting records.
Start and End Timestamp:	Start and end time of the session.
Username:	Username associated with this record.
Client IP:	The IP address and tty of the device interface.
Remote IP:	The IP address from which Admin is logged in.
Flags:	Identifier corresponding to start, stop or update accounting record.
Privilege Level:	Privilege level of administrator: 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 screen shows the realtime status of all endpoints that have DellW-OnGuard persistent or dissolvable agent, at: **Monitoring** > **Live Monitoring** > **OnGuard Activity**. This screen also presents configuration tools to bounce an endpoint and to send unicast or broadcast messages to all endpoints running the OnGuard agent.

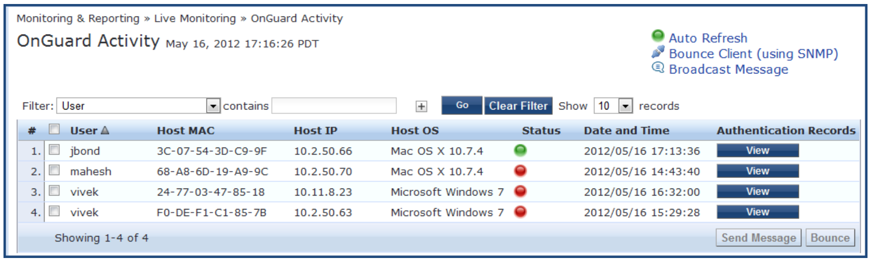
NOTE

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

For more information, see:

- "Bounce an Agent (non-SNMP)" on page 48
- "Bounce a Client Using SNMP" on page 49
- "Broadcast Message" on page 50
- "Send a Message" on page 50

Figure 18: *OnGuard Activity*



Monitoring & Reporting » Live Monitoring » OnGuard Activity

OnGuard Activity May 16, 2012 17:16:26 PDT

Filter: User contains

Show 10 records

#	☐	User	Host MAC	Host IP	Host OS	Status	Date and Time	Authentication Records
1.	☐	jbond	3C-07-54-3D-C9-9F	10.2.50.66	Mac OS X 10.7.4	🟢	2012/05/16 17:13:36	View
2.	☐	mahesh	68-A8-6D-19-A9-9C	10.2.50.70	Mac OS X 10.7.4	🔴	2012/05/16 14:43:40	View
3.	☐	vivek	24-77-03-47-85-18	10.11.8.23	Microsoft Windows 7	🔴	2012/05/16 16:32:00	View
4.	☐	vivek	F0-DE-F1-C1-85-7B	10.2.50.63	Microsoft Windows 7	🔴	2012/05/16 15:29:28	View

Showing 1-4 of 4

Table 15: *OnGuard Activity*

Parameter	Description
Auto Refresh	Toggle auto-refresh. If this is turned on, all endpoint activities are refreshed automatically.
Send Message	Send a message to the selected endpoints.

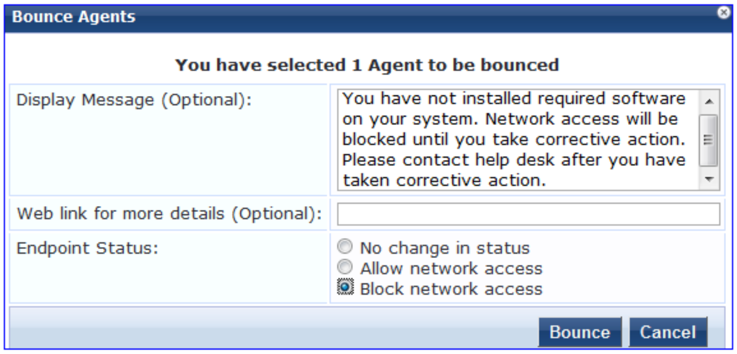
Bounce an Agent (non-SNMP)

This page is used to initiate a bounce on the managed interface on the endpoint. Initiating a bounce on the managed interface on the endpoint results in tags being created 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.

Figure 19: *Bounce Agents Page*



Bounce Agents

You have selected 1 Agent to be bounced

Display Message (Optional): You have not installed required software on your system. Network access will be blocked until you take corrective action. Please contact help desk after you have taken corrective action.

Web link for more details (Optional):

Endpoint Status:
○ No change in status
○ Allow network access
● Block network access

Table 16: *Bounce Agents Page Parameters*

Parameter	Description
Display Message (Optional):	An optional message to display on the endpoint via 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 endpoint’s existing status. **Allow network access** - Always allow network access. Whitelist 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 “Known” endpoints. **Block network access** - Always block network access. Blacklist 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 “Disabled” endpoints.

Bounce a Client Using SNMP

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

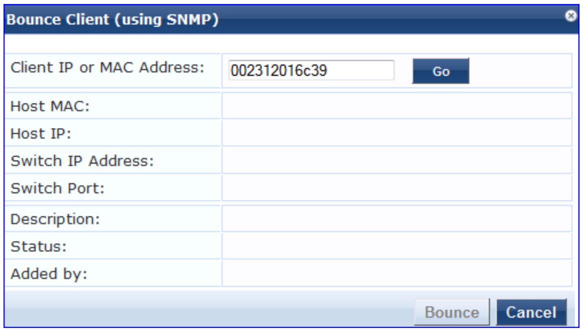
Requirements

To successfully bounce a client using SNMP, the following conditions must exist:

- 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.
- In order to specify the IP address of the endpoint to bounce, the DHCP snooper service on Policy Manager must receive DHCP packets from the endpoint. Refer to your network device documentation to find out how to configure IP helper address.

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

Figure 20: *Bounce Client (Using SNMP) Page*



Client IP or MAC Address:	002312016c39
Host MAC:	
Host IP:	
Switch IP Address:	
Switch Port:	
Description:	
Status:	
Added by:	

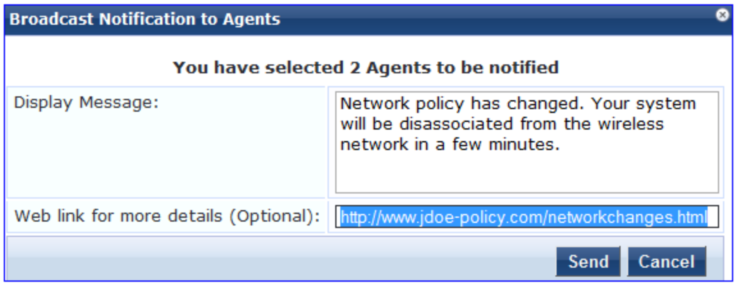
Table 17: *Bounce Client (Using SNMP) Page Parameters*

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

Broadcast Message

After you click the Broadcast Message link on the main page, a page appears where you can write and send a message to all active endpoints.

Figure 21: *Broadcast Notification to Agents Page*



Broadcast Notification to Agents

You have selected 2 Agents to be notified

Display Message: Network policy has changed. Your system will be disassociated from the wireless network in a few minutes.

Web link for more details (Optional): http://www.jdoe-policy.com/networkchanges.html

Table 18: *Broadcast Notification to Agents Page Parameters*

Parameter	Description
Display Message:	Enter the message text in this field.
Web link for more details (Optional):	An optional clickable URL that is displayed along with the Display Message.
Send	Click to send the message to all active endpoints.

Send a Message

To send a message to a selected endpoint, select one or more rows on the OnGuard Activity page. Write the message and click **Send Message**.

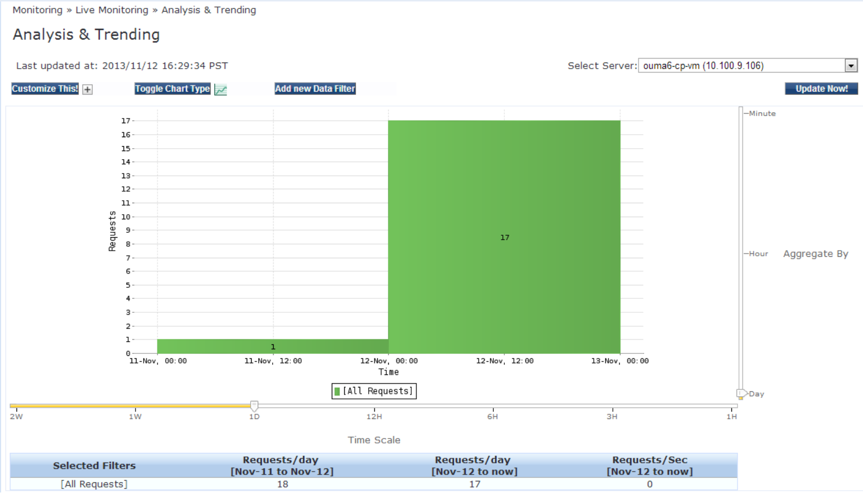
Analysis and Trending

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 topic shows the per-filter count for the aggregated data.

Each bar corresponding to each filter in the bar graph is clickable. Click the bar drills down into the "Access Tracker" on page 33, showing session data for that time slice (and for that many requests).

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

Figure 22: *Analysis and Trending*



Monitoring » Live Monitoring » Analysis & Trending

Analysis & Trending

Last updated at: 2013/11/12 16:29:34 PST

Select Server: ouma6-cp-vm (10.100.9.106)

Selected Filters	Requests/day [Nov-11 to Nov-12]	Requests/day [Nov-12 to now]	Requests/Sec [Nov-12 to now]
[All Requests]	18	17	0

To add filters, refer to "Data Filters" on page 65.

- **Select Server** - Select a node from the cluster for which data is 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 (up to a maximum of 4 filters).
- **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.

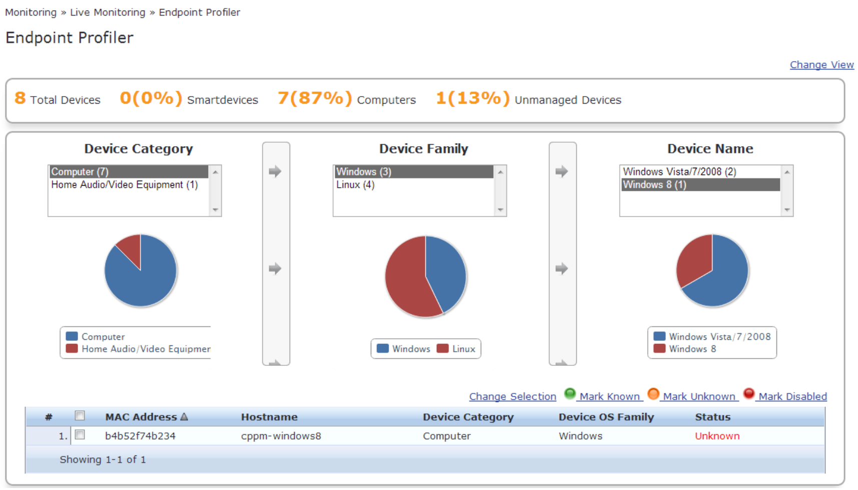
Endpoint Profiler

If the Profile license is enabled, a list of the profiled endpoints will be visible in the Endpoints Profiler table. The list of endpoints you see is based on the Category, OS 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 23: *Endpoint Profiler (view 1)*



Monitoring » Live Monitoring » Endpoint Profiler

Endpoint Profiler

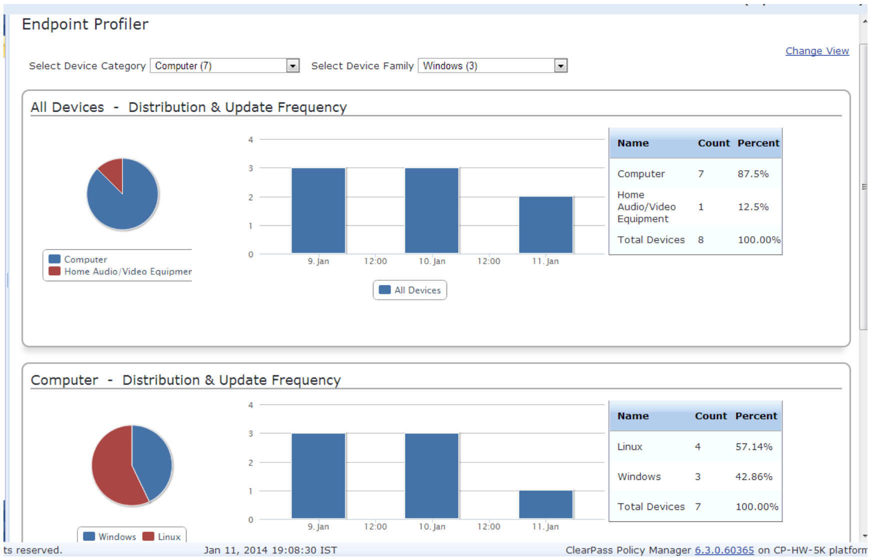
8 Total Devices 0(0%) Smartdevices 7(87%) Computers 1(13%) Unmanaged Devices

Device Category	Device Family	Device Name
Computer (7) Home Audio/Video Equipment (1)	Windows (3) Linux (4)	Windows Vista/7/2008 (2) Windows 8 (1)

#	□	MAC Address ▲	Hostname	Device Category	Device OS Family	Status
1.	□	b4b52f74b234	cppm-windows8	Computer	Windows	Unknown

Showing 1-1 of 1

Figure 24: *Endpoint Profiler (view 2)*



Endpoint Profiler

Select Device Category Computer (7) Select Device Family Windows (3)

All Devices - Distribution & Update Frequency

Name	Count	Percent
Computer	7	87.5%
Home Audio/Video Equipment	1	12.5%
Total Devices	8	100.00%

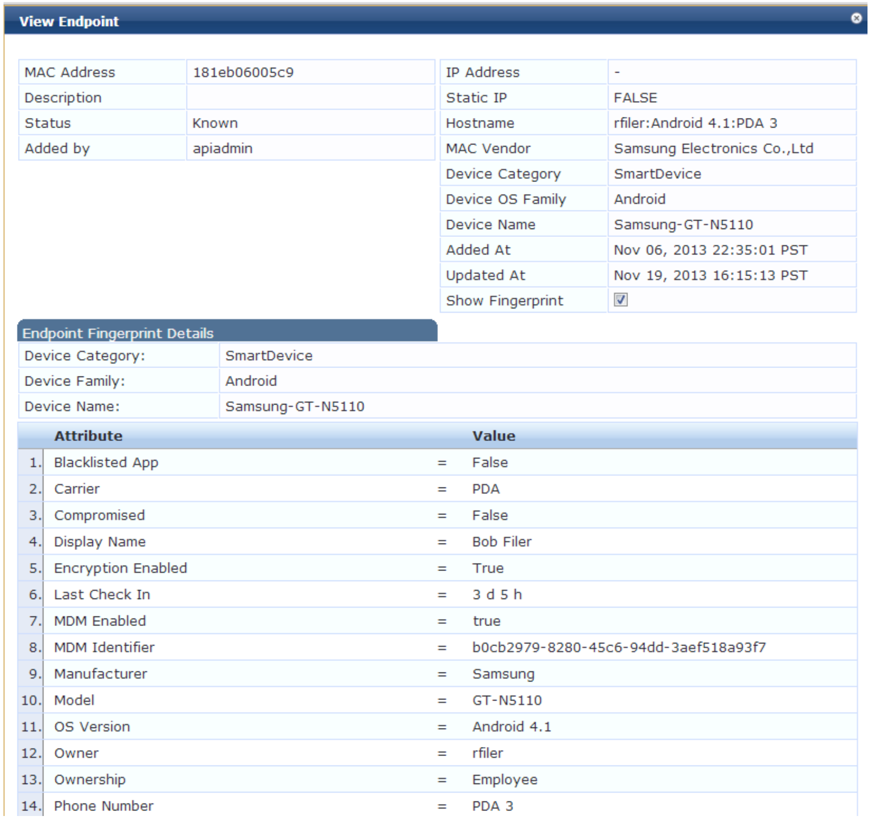
Computer - Distribution & Update Frequency

Name	Count	Percent
Linux	4	57.14%
Windows	3	42.86%
Total Devices	7	100.00%

ts reserved. Jan 11, 2014 19:08:30 IST ClearPass Policy Manager 6.3.0.60365 on CP-HW-5K platform

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 25: *Endpoint Profiler Details*



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 gives real-time information about various components. Click the Update Now! button to refresh the information.

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 more.

Network tab - Displays a graph about a selected network parameter, such as Web Traffic, SSH, and more.

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

- Service Categorization
- Authentication
- Authorization
- Posture Validation
- Enforcement
- End to End request processing

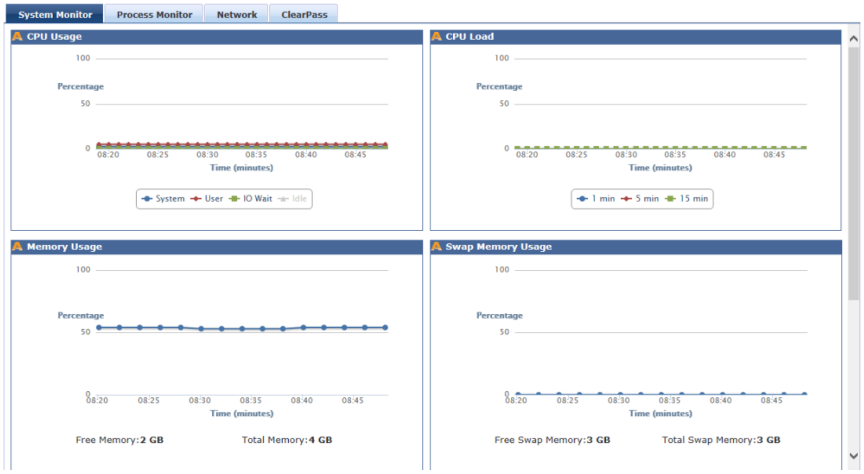
These components are actively monitored and the ClearPass tab displays the past 30 minutes of the data found during the monitoring process.

For more information, see:

- "System Monitor tab" on page 54

- "Process Monitor tab" on page 56
- "Network tab" on page 57
- "ClearPass tab" on page 58

Figure 26: *System Monitor Page*



Free Memory:**2 GB** Total Memory:**4 GB**

Free Swap Memory:**3 GB** Total Swap Memory:**3 GB**

System Monitor tab

The system monitor tab displays information about component usage and load.

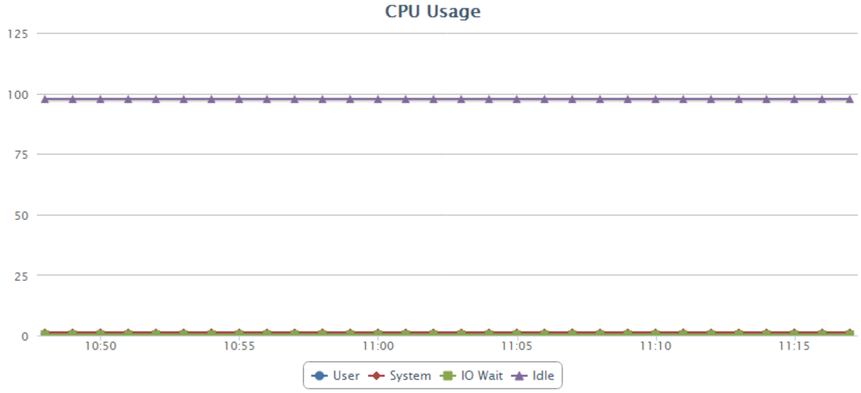
For more information, see:

- "Monitoring CPU Usage" on page 54
- "Monitoring CPU Load" on page 54
- "Monitoring Memory Usage" on page 55
- "Monitoring Swap Memory Usage" on page 55
- "Monitoring Disk - / Usage" on page 56
- "Monitoring Disk Swap Usage" on page 56

Monitoring CPU Usage

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

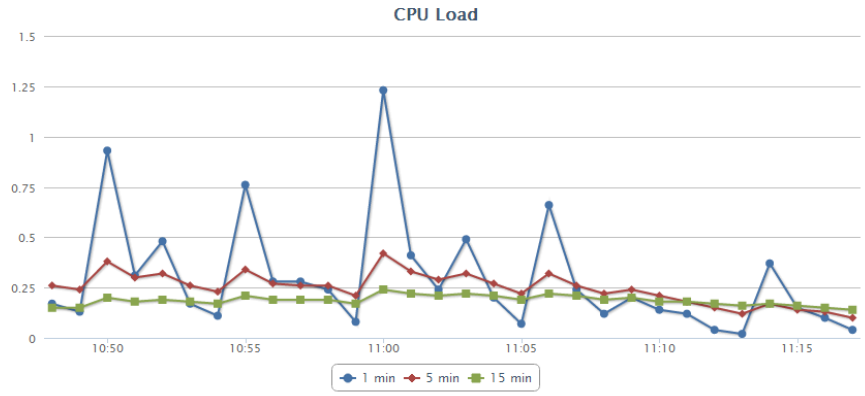
Figure 27: *CPU Usage Graph Example*



Monitoring CPU Load

This graph shows the percentage of CPU Load in increments of one-, five- and 15 minutes.

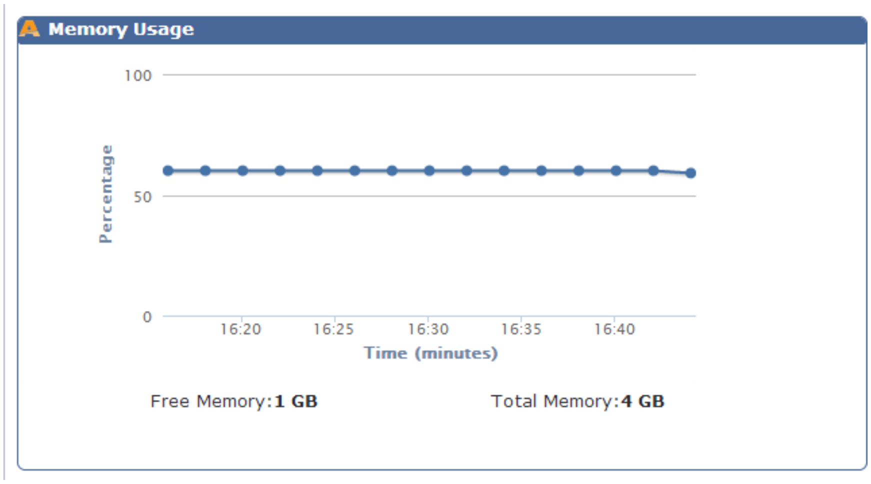
Figure 28: *CPU Load Graph Example*



Monitoring Memory Usage

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

Figure 29: *Memory Usage Graph Example*

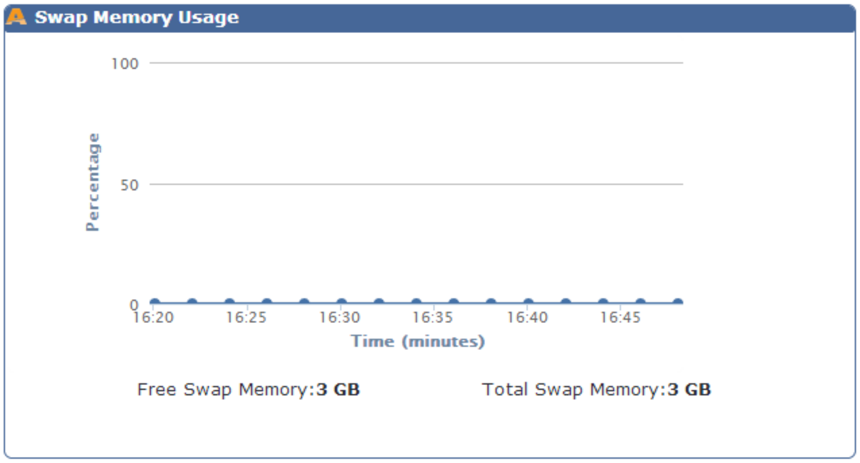


Free Memory:**1 GB** Total Memory:**4 GB**

Monitoring Swap Memory Usage

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

Figure 30: *Used and Free Memory Graph Example*

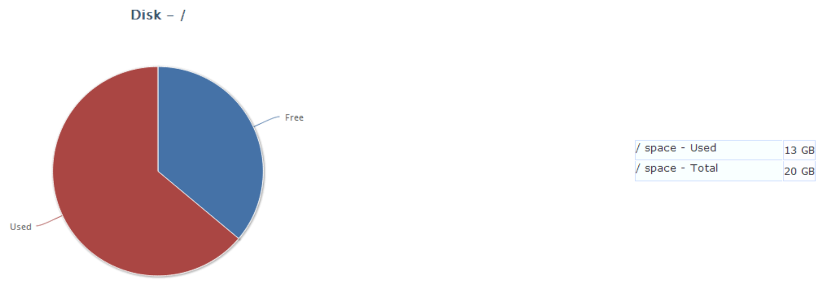


Free Swap Memory:**3 GB** Total Swap Memory:**3 GB**

Monitoring Disk - / Usage

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

Figure 31: *Used and Free Disk Space Graph Example*

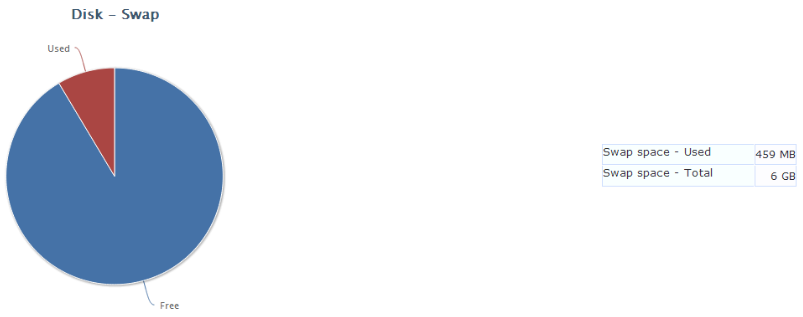


/ space - Used	13 GB
/ space - Total	20 GB

Monitoring Disk Swap Usage

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

Figure 32: *Used and Free Disk Swap Chart Example*



Swap space - Used	459 MB
Swap space - Total	6 GB

Process Monitor tab

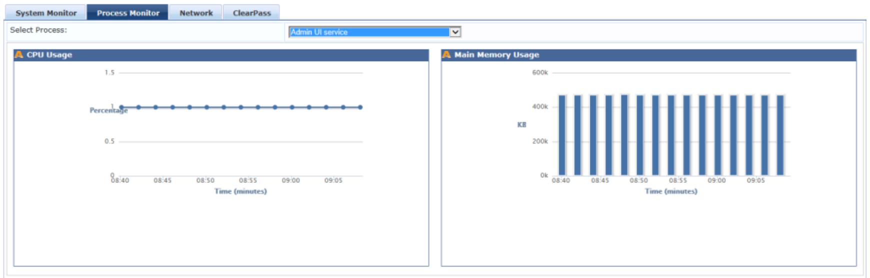
Click this tab to view graphs that show data about CPU Usage and Main Memory Usage on the selected process or service.

The CPU Usage graph on this tab shows only the percentage used and time in minutes for the selected process.

Select a Process name to view CPU and Main Memory usage graphs.

- Admin UI service
- AirGroup notification 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 33: *Process Monitor tab Page Example*

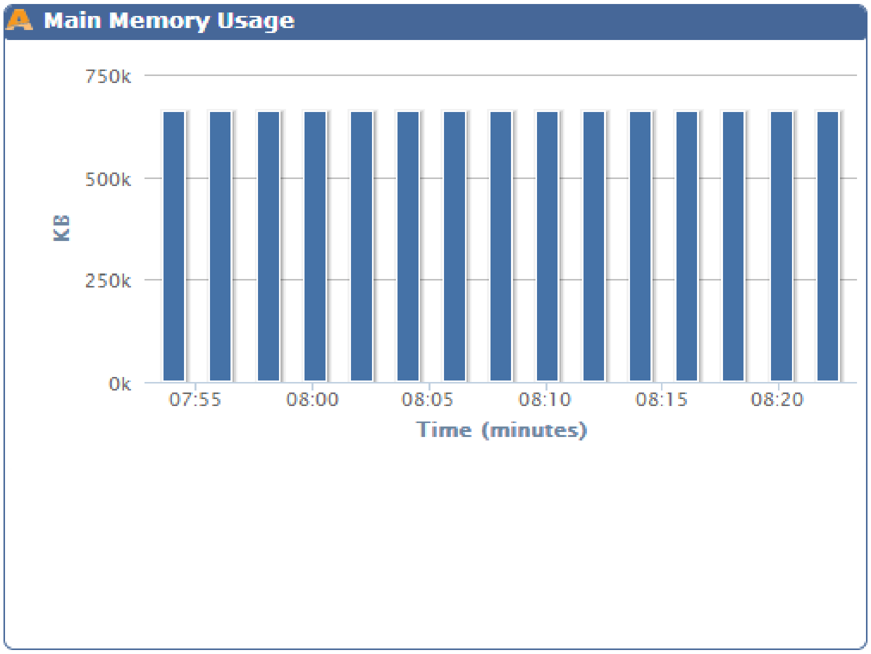


Select Process: Admin UI service

Monitoring Main Memory Usage

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

Figure 34: *Main Memory Usage Graph Example*

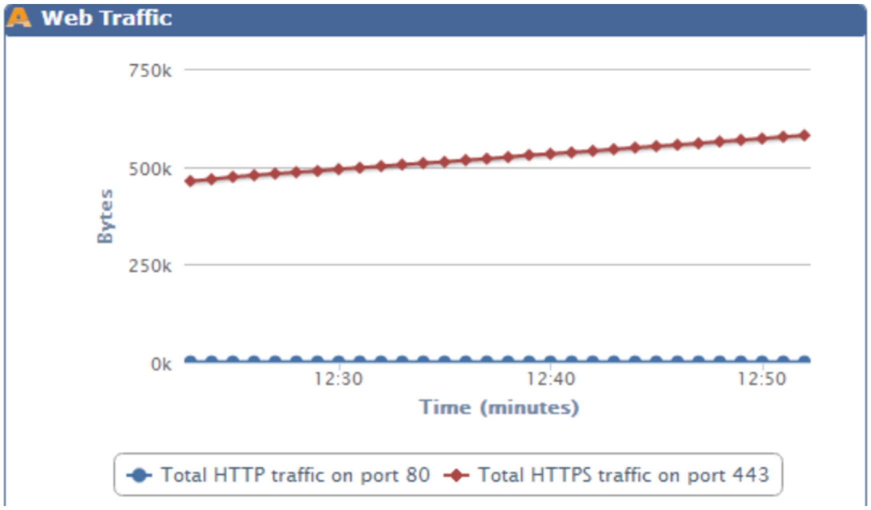


Network tab

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

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

Figure 35: *Network Monitor Tab Graph Example (Web Traffic)*



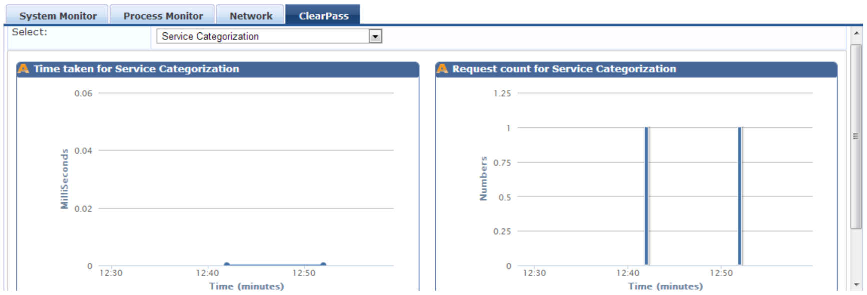
ClearPass tab

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

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

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

Figure 36: *Service Categorization Graph Example*



Select: Service Categorization

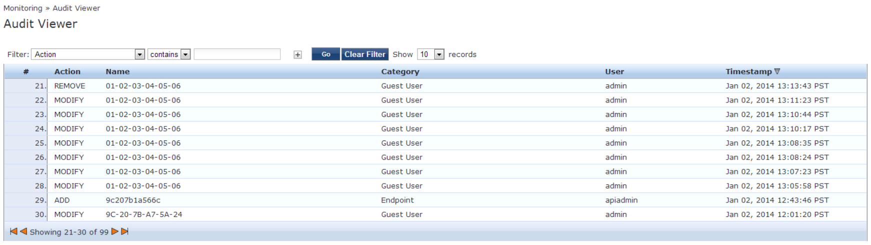
Audit Viewer

The Audit Viewer display page provides a dynamic report about Actions, filterable by Action, Name, Category of policy component, and User.

For more information, see:

- "Viewing Audit Row Details (Add Page)" on page 59
- "Viewing Audit Row Details (Modify Page)" on page 60
- "Viewing Audit Row Details (Remove Page)" on page 62

Figure 37: *Audit Viewer Page*



Monitoring » Audit Viewer

Audit Viewer

Filter: Action contains Show 10 records

#	Action	Name	Category	User	Timestamp ▽
21.	REMOVE	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:13:43 PST
22.	MODIFY	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:11:23 PST
23.	MODIFY	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:10:44 PST
24.	MODIFY	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:10:17 PST
25.	MODIFY	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:08:35 PST
26.	MODIFY	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:08:24 PST
27.	MODIFY	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:07:23 PST
28.	MODIFY	01-02-03-04-05-06	Guest User	admin	Jan 02, 2014 13:05:58 PST
29.	ADD	9c207b1a566c	Endpoint	apiadmin	Jan 02, 2014 12:43:46 PST
30.	MODIFY	9C-20-7B-A7-5A-24	Guest User	admin	Jan 02, 2014 12:01:20 PST

Showing 21-30 of 99

Table 19: *Audit Viewer Page Parameters*

Parameter	Description
Select Filter	Select the filter by which to constrain the display of audit data.
Show <n> records	Show 10, 20, 50 or 100 rows. After being selected, this setting is saved and available in subsequent logins.

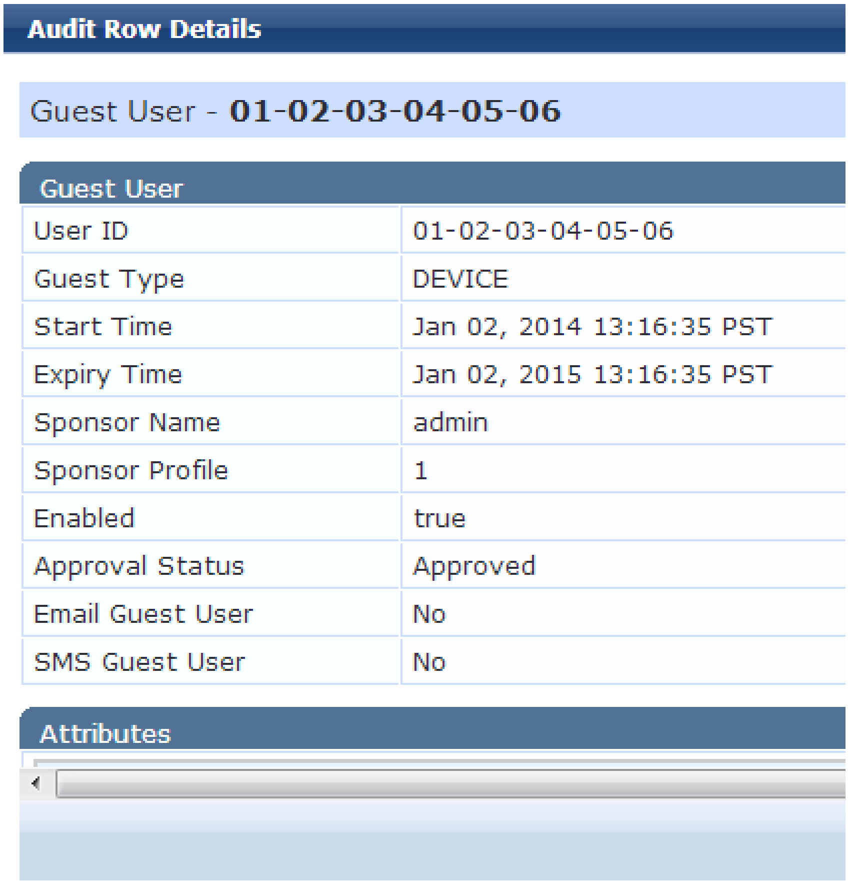
Viewing Audit Row Details (Add Page)

If you click a row on the main page where the Action was ADD, an Audit Row Details page opens. The page gives details that are specific to the Action category.

The top figure shows an example of the Audit Row Details page displayed after a guest user was added.

The bottom figure shows an example of the Audit Row Details page displayed after a virtual IP server was added.

Figure 38: *Audit Row Details Page Example 1 (Guest User Added)*



Audit Row Details

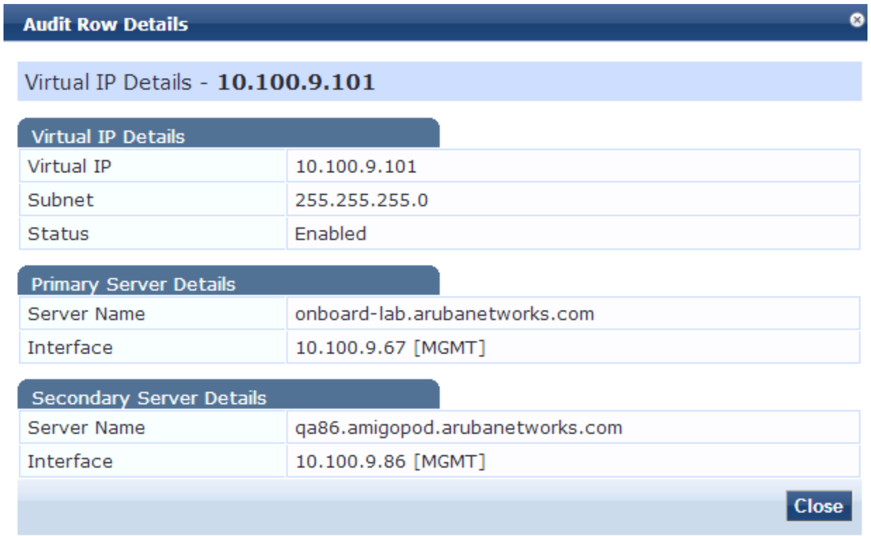
Guest User - **01-02-03-04-05-06**

Guest User

User ID	01-02-03-04-05-06
Guest Type	DEVICE
Start Time	Jan 02, 2014 13:16:35 PST
Expiry Time	Jan 02, 2015 13:16:35 PST
Sponsor Name	admin
Sponsor Profile	1
Enabled	true
Approval Status	Approved
Email Guest User	No
SMS Guest User	No

Attributes

Figure 39: *Audit Row Details Page Example 2 (Virtual IP Server Added)*



Virtual IP Details - **10.100.9.101**

Virtual IP Details	
Virtual IP	10.100.9.101
Subnet	255.255.255.0
Status	Enabled

Primary Server Details	
Server Name	onboard-lab.arubanetworks.com
Interface	10.100.9.67 [MGMT]

Secondary Server Details	
Server Name	qa86.amigopod.arubanetworks.com
Interface	10.100.9.86 [MGMT]

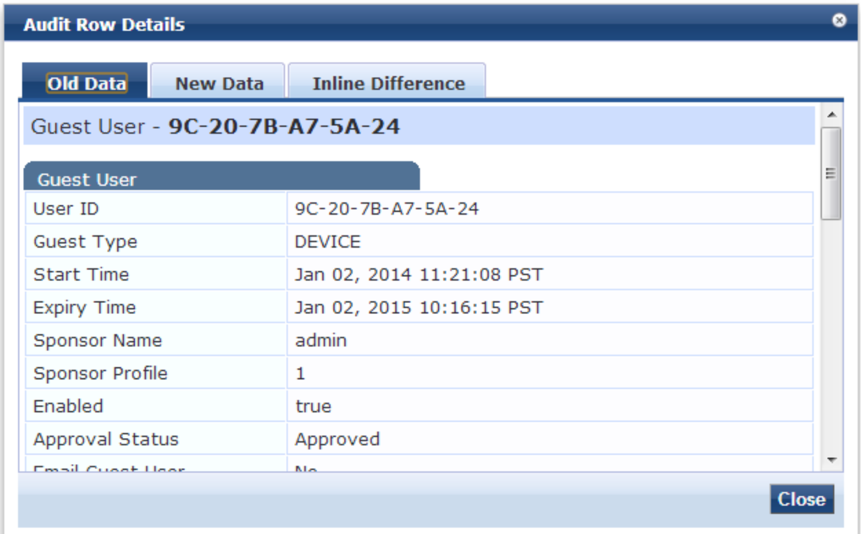
Viewing Audit Row Details (Modify Page)

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

Old Data Tab

The top section of the old data tab is a summary of details about the original data values. The bottom section shows data about the original attributes and values. The figures show an example of a MODIFY action that was taken in the category Guest User.

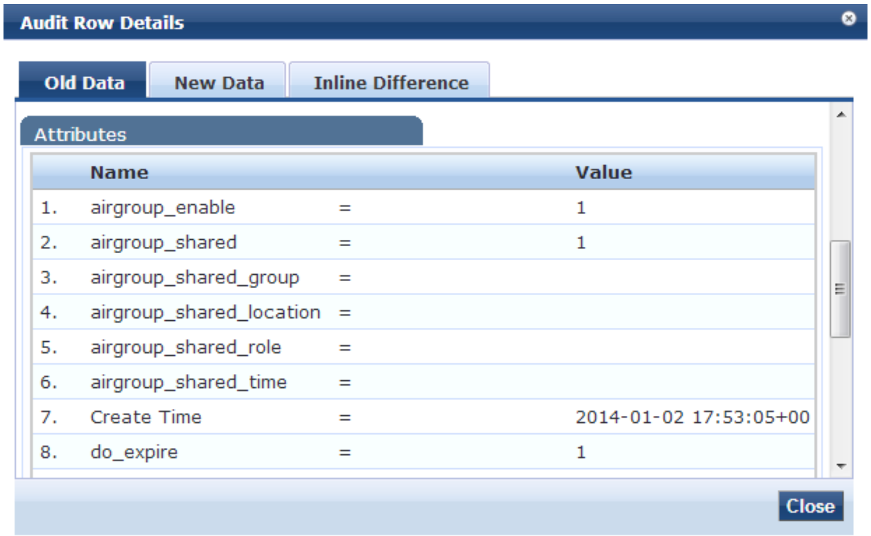
Figure 40: *Old Data tab*



Guest User - **9C-20-7B-A7-5A-24**

Guest User	
User ID	9C-20-7B-A7-5A-24
Guest Type	DEVICE
Start Time	Jan 02, 2014 11:21:08 PST
Expiry Time	Jan 02, 2015 10:16:15 PST
Sponsor Name	admin
Sponsor Profile	1
Enabled	true
Approval Status	Approved
Email Guest User	No

Figure 41: *Old Data tab Attributes Section*

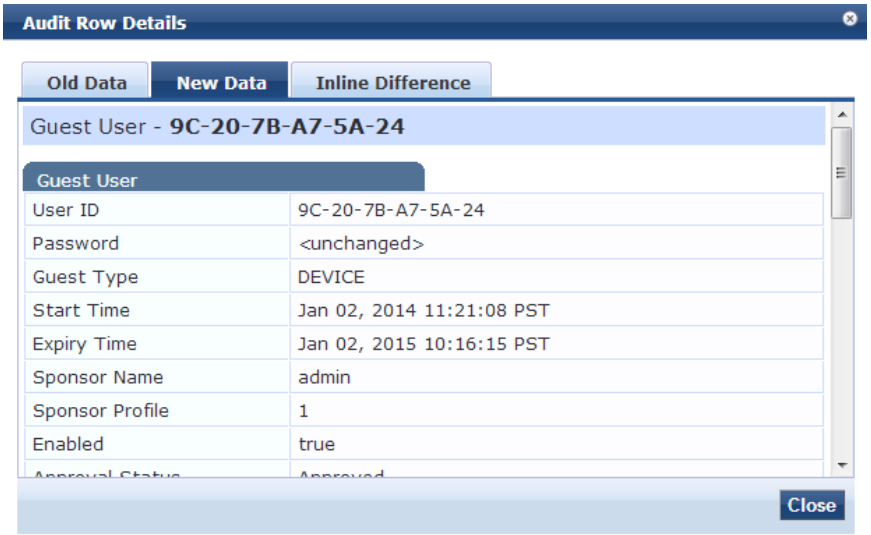


	Name		Value
1.	airgroup_enable	=	1
2.	airgroup_shared	=	1
3.	airgroup_shared_group	=	
4.	airgroup_shared_location	=	
5.	airgroup_shared_role	=	
6.	airgroup_shared_time	=	
7.	Create Time	=	2014-01-02 17:53:05+00
8.	do_expire	=	1

New Data tab

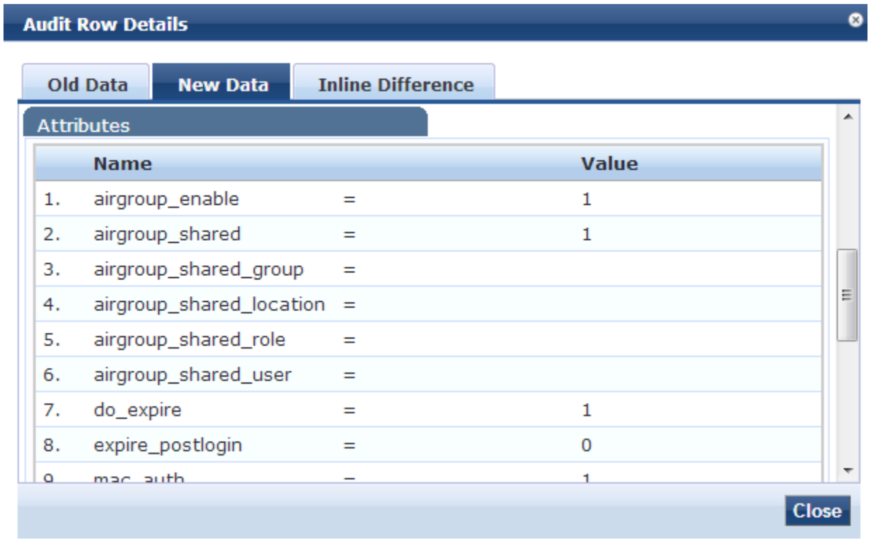
The top section of the old data tab is a summary of details about the original data values. The top section is a summary of the new data values, such as User ID, Password and Guest Type. The bottom section displays new and changed Attributes. The figures show a MODIFY action that was taken in the category Guest User.

Figure 42: *New Data tab*



User ID	9C-20-7B-A7-5A-24
Password	<unchanged>
Guest Type	DEVICE
Start Time	Jan 02, 2014 11:21:08 PST
Expiry Time	Jan 02, 2015 10:16:15 PST
Sponsor Name	admin
Sponsor Profile	1
Enabled	true
Approval Status	Approved

Figure 43: *New Data tab Attributes Section*

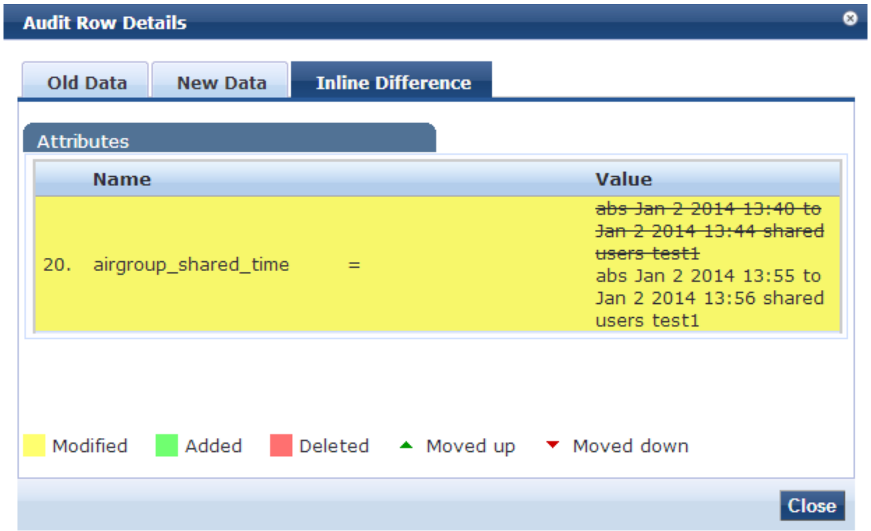


	Name		Value
1.	airgroup_enable	=	1
2.	airgroup_shared	=	1
3.	airgroup_shared_group	=	
4.	airgroup_shared_location	=	
5.	airgroup_shared_role	=	
6.	airgroup_shared_user	=	
7.	do_expire	=	1
8.	expire_postlogin	=	0
9.	mac_auth	=	1

Inline Difference tab

This tab is a summary of the difference(s) between the old and new data. The example shows the modification made to the value on Line 20 of the Old Data Attribute named airgroup_shared_time. Modifications are highlighted in yellow. Additions are highlighted in green. 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 44: *Inline Difference tab*



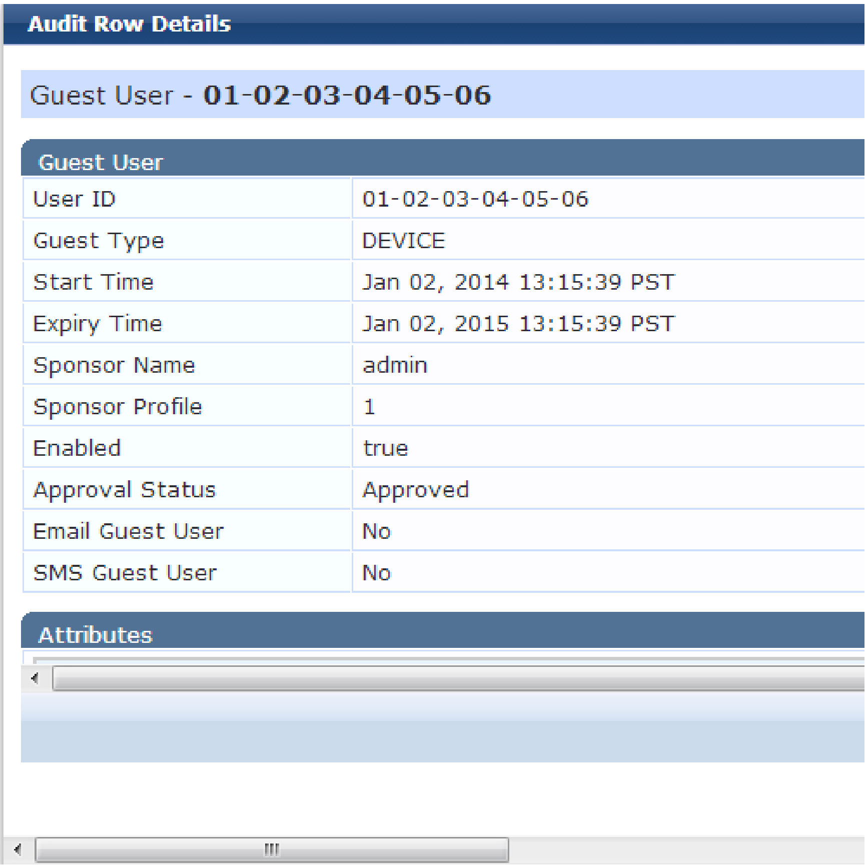
	Name		Value
20.	airgroup_shared_time	=	~~abs Jan 2 2014 13:40 to Jan 2 2014 13:44 shared users test1~~ abs Jan 2 2014 13:55 to Jan 2 2014 13:56 shared users test1

🟨 Modified 🟩 Added 🟥 Deleted ▲ Moved up ▼ Moved down

Viewing Audit Row Details (Remove Page)

If you click on a row that has had an item removed, a popup displays the details and attributes that were removed.

Figure 45: *Audit Row Details (Remove Page)*



Audit Row Details

Guest User - **01-02-03-04-05-06**

Guest User

User ID	01-02-03-04-05-06
Guest Type	DEVICE
Start Time	Jan 02, 2014 13:15:39 PST
Expiry Time	Jan 02, 2015 13:15:39 PST
Sponsor Name	admin
Sponsor Profile	1
Enabled	true
Approval Status	Approved
Email Guest User	No
SMS Guest User	No

Attributes

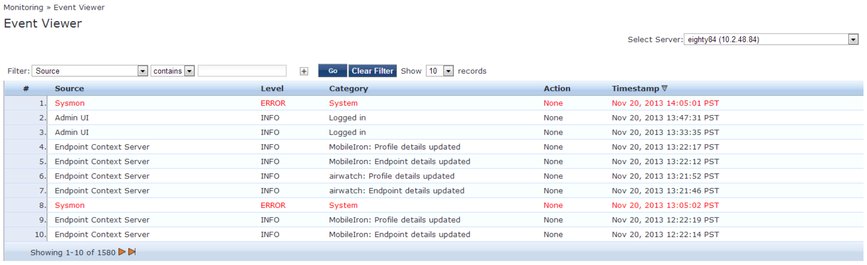
Event Viewer

The Event Viewer page provides reports about system-level events.

For more information, see:

- "Creating an Event Viewer Report Using Default Values" on page 64
- "Creating an Event Viewer Report Using Custom Values" on page 64
- "Viewing Report Details" on page 65

Figure 46: *Event Viewer Report Page (Default Values)*



Monitoring » Event Viewer

Event Viewer

Select Server: eighty84 (10.2.48.84)

Filter: Source contains

Show 10 records

#	Source	Level	Category	Action	Timestamp ▽
1.	Sysmon	ERROR	System	None	Nov 20, 2013 14:05:01 PST
2.	Admin UI	INFO	Logged in	None	Nov 20, 2013 13:47:31 PST
3.	Admin UI	INFO	Logged in	None	Nov 20, 2013 13:33:35 PST
4.	Endpoint Context Server	INFO	MobileIron: Profile details updated	None	Nov 20, 2013 13:22:17 PST
5.	Endpoint Context Server	INFO	MobileIron: Endpoint details updated	None	Nov 20, 2013 13:22:12 PST
6.	Endpoint Context Server	INFO	airwatch: Profile details updated	None	Nov 20, 2013 13:21:52 PST
7.	Endpoint Context Server	INFO	airwatch: Endpoint details updated	None	Nov 20, 2013 13:21:46 PST
8.	Sysmon	ERROR	System	None	Nov 20, 2013 13:05:02 PST
9.	Endpoint Context Server	INFO	MobileIron: Profile details updated	None	Nov 20, 2013 12:22:19 PST
10.	Endpoint Context Server	INFO	MobileIron: Endpoint details updated	None	Nov 20, 2013 12:22:14 PST

Showing 1-10 of 1580

Table 20: *Event Viewer Report Page Parameters (Default Values)*

Parameter	Description
Select Server	Shows the name and IP address of the server you are logged into. Click to select a new server.
Filter	Select a topic to filter for. The options are: ● Source ● Level ● Category ● Action ● Description
Go	Click to create the report.
Clear Filter	Click to restore the default filter settings.
⊞	Click to add up to four filter fields.
⊟	If you added filter fields, click to delete one or more of the added fields.
Select ALL matches	If you added filter fields, click to receive a report that matches all filter parameters.
Select ANY match	If you added filter fields, click to receive a report that matches any filter parameters.
Textboxes	Enter the text you want to search for into the text boxes. For example, if you want to search for a Source that contains Sysmon, you would enter Sysmon in the text field (see "Event Viewer" on page 63).

Creating an Event Viewer Report Using Default Values

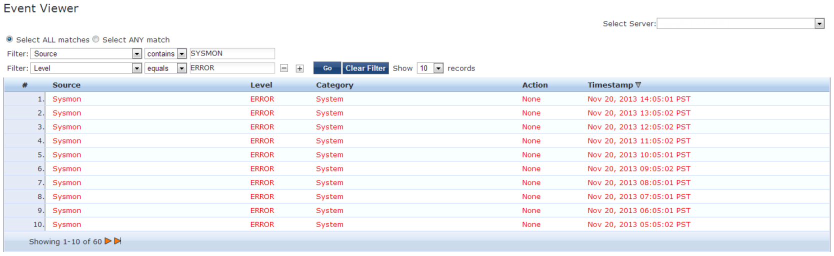
1. In the Filter field, select **Source** as the Filter parameter.
2. Leave **contains** as the search term.
3. Leave the text field blank.
4. Leave the Show records value at 10.
5. Click **Go**. The systems returns all event records.

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 parameter field to **equals**.
8. Enter **SYSMON** in the text field.

9. Change the Show records value to 20.
10. Click **Go**.

Figure 47: *Event Viewer Report Example (Custom Values)*



● Select ALL matches ○ Select ANY match

Filter: Source contains SYSMON

Filter: Level equals ERROR

Show 10 records

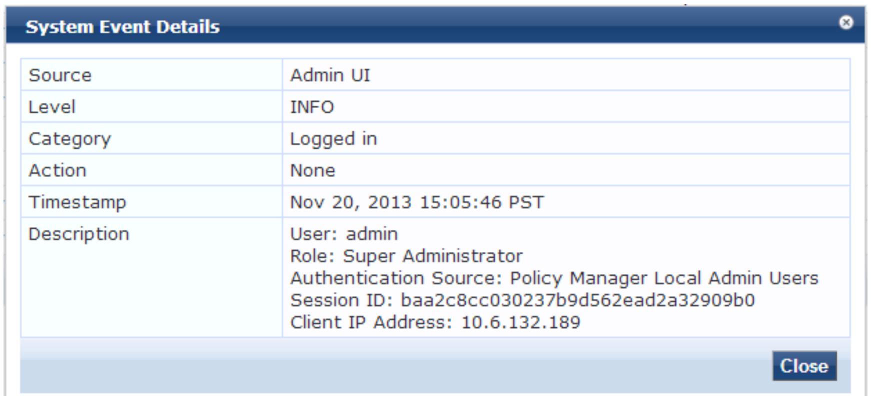
#	Source	Level	Category	Action	Timestamp ▽
1.	Sysmon	ERROR	System	None	Nov 20, 2013 14:05:01 PST
2.	Sysmon	ERROR	System	None	Nov 20, 2013 13:05:02 PST
3.	Sysmon	ERROR	System	None	Nov 20, 2013 12:05:02 PST
4.	Sysmon	ERROR	System	None	Nov 20, 2013 11:05:02 PST
5.	Sysmon	ERROR	System	None	Nov 20, 2013 10:05:01 PST
6.	Sysmon	ERROR	System	None	Nov 20, 2013 09:05:02 PST
7.	Sysmon	ERROR	System	None	Nov 20, 2013 08:05:01 PST
8.	Sysmon	ERROR	System	None	Nov 20, 2013 07:05:01 PST
9.	Sysmon	ERROR	System	None	Nov 20, 2013 06:05:01 PST
10.	Sysmon	ERROR	System	None	Nov 20, 2013 05:05:02 PST

Showing 1-10 of 60

Viewing Report Details

Click a row in the Event View report to display System Event Details.

Figure 48: *System Event Details Page*



Source	Admin UI
Level	INFO
Category	Logged in
Action	None
Timestamp	Nov 20, 2013 15:05:46 PST
Description	User: admin Role: Super Administrator Authentication Source: Policy Manager Local Admin Users Session ID: baa2c8cc030237b9d562ead2a32909b0 Client IP Address: 10.6.132.189

Data Filters

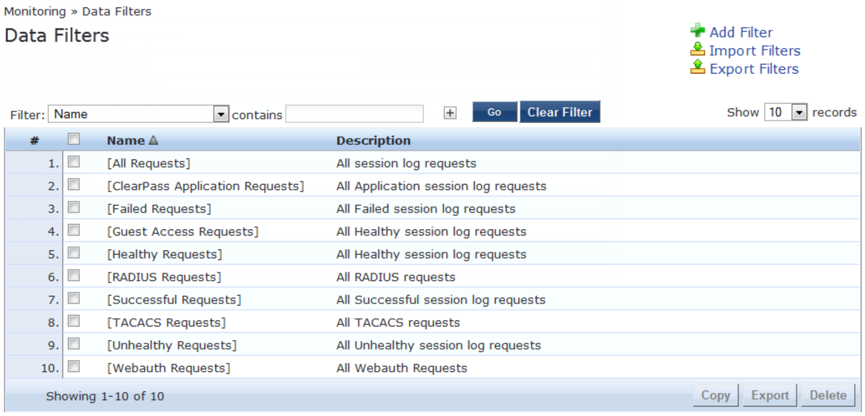
The Data Filters provide a way to filter data (limit the number of rows of data shown by defining custom criteria or rules) that is shown in the "Access Tracker" on page 33, "Syslog Export Filters" on page 368, "Analysis and Trending" on page 51, and "Accounting" on page 39 components in Policy Manager. It is available at: **Monitoring > Data Filters**.

Policy Manager comes 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; includes RADIUS, TACACS+ and Web Authentication results.
- **Guest Access Requests** - All requests - RADIUS or Web Authentication - where the user was assigned the built-in role called Guest.
- **Healthy Requests** - All requests that were deemed healthy per policy.
- **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 per policy.
- WebAuth Requests - All Web Authentication requests (requests originated from the Dell Guest Portal).

For more information, see "Add a Filter " on page 66.

Figure 49: *Data Filters Page*



Monitoring » Data Filters

Data Filters

#		Name	Description
1.	□	[All Requests]	All session log requests
2.	□	[ClearPass Application Requests]	All Application session log requests
3.	□	[Failed Requests]	All Failed session log requests
4.	□	[Guest Access Requests]	All Healthy session log requests
5.	□	[Healthy Requests]	All Healthy session log requests
6.	□	[RADIUS Requests]	All RADIUS requests
7.	□	[Successful Requests]	All Successful session log requests
8.	□	[TACACS Requests]	All TACACS requests
9.	□	[Unhealthy Requests]	All Unhealthy session log requests
10.	□	[Webauth Requests]	All Webauth Requests

Showing 1-10 of 10

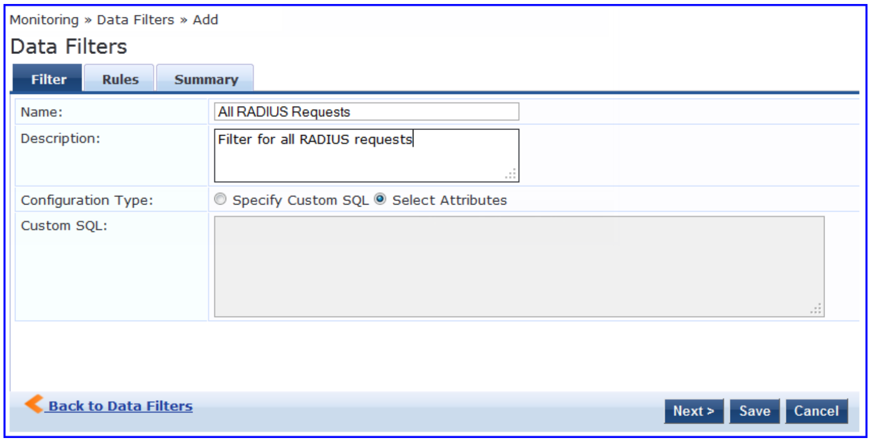
Table 21: *Data Filters Page Parameters*

Parameter	Description
Add Filter	Click to open the Add Filter wizard.
Import Filters	Click to open the **Import Filters** popup.
Export Filters	Click to open the **Export Filters** popup. This exports all configured filters.
Copy	Copy the selected filters.
Export	Click to open the **Export** popup to export selected reports.
Delete	Click to delete the selected filters.

Add a Filter

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

Figure 50: *Add Filter (Filter tab)*



Monitoring » Data Filters » Add

Data Filters

Name: All RADIUS Requests

Description: Filter for all RADIUS requests

Configuration Type: ○ Specify Custom SQL ● Select Attributes

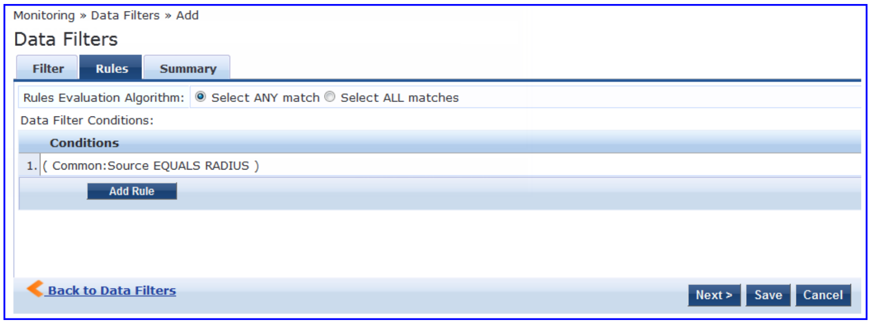
Custom SQL:

Table 22: *Add Filter (Filter tab)*

Parameter	Description
Name/Description	Name and description of the filter (freeform).
Configuration Type	Choose one of the following configuration types: ● **Specify Custom SQL** - Selecting this option allows you to specify a custom SQL entry for the filter. If this is specified, then the Rules tab disappears, and a SQL template displays in the Custom SQL field. **NOTE:** Selecting this option is not recommended. For users who need to utilize this, however, we recommend contacting Support. ● **Select Attributes** - This option is selected by default and enables the Rules tab. If this option is selected, 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:** We recommend that users who choose this method contact Support. 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 51: *Add Filter (Rules tab)*



Monitoring » Data Filters » Add

Data Filters

Rules Evaluation Algorithm: ● Select ANY match ○ Select ALL matches

Data Filter Conditions:

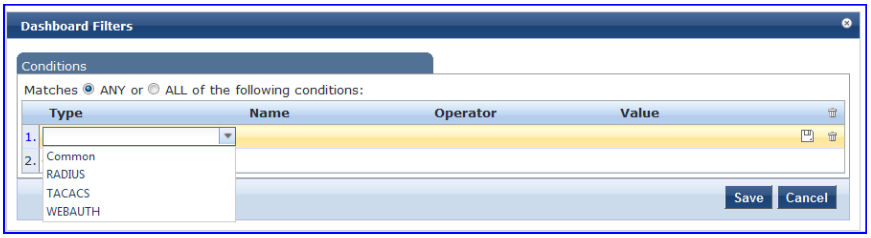
	Conditions
1.	(Common:Source EQUALS RADIUS)

Table 23: *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.
Edit/Remove Rule	Edit or remove a rule.
Save	Save this filter.
Cancel	Cancel edit operation.

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

Figure 52: *Add Filter (Rules tab) - Rules Editor*



Matches ● ANY or ○ ALL of the following conditions:

Table 24: *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 - These are attributes common to RADIUS, TACACS, and WebAuth requests and responses. • RADIUS - Attributes associated with RADIUS authentication and accounting requests and responses. • TACACS - Attributes associated with TACACS authentication, accounting, and policy requests and responses. • Web Authentication Policy - Policy Manager policy objects assigned after evaluation of policies associated with Web Authentication requests. Example: Auth Method, Auth Source, Enforcement Profiles.
Name	Name of the attributes corresponding to the selected namespace (Type).
Operator	A subset of string data type operators (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.

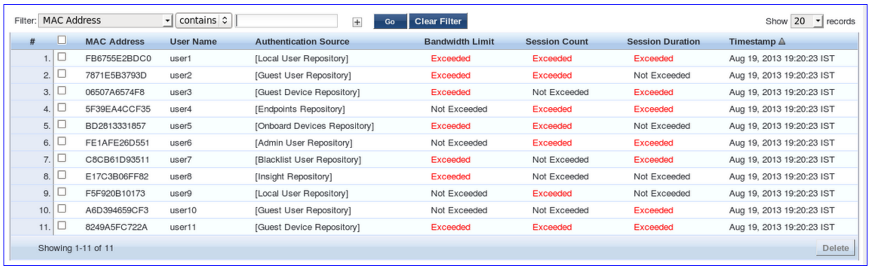
Blacklisted Users

The Blacklisted Users page lists all blacklisted users and the reason(s) why they have been blacklisted. This monitoring page shows whether the following attributes have been exceeded:

- Bandwidth limit
- Session count
- Session duration

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

Figure 53: *Monitoring Blacklisted Users*



Filter: MAC Address contains

Show 20 records

#	□	MAC Address	User Name	Authentication Source	Bandwidth Limit	Session Count	Session Duration	Timestamp ▲
1.	□	FB6755E2BDC0	user1	[Local User Repository]	Exceeded	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
2.	□	7871E5B3793D	user2	[Guest User Repository]	Exceeded	Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
3.	□	06507A6574F8	user3	[Guest Device Repository]	Exceeded	Not Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
4.	□	5F39EA4CCF35	user4	[Endpoints Repository]	Not Exceeded	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
5.	□	BD2813331857	user5	[Onboard Devices Repository]	Exceeded	Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
6.	□	FE1AFE26D551	user6	[Admin User Repository]	Not Exceeded	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
7.	□	C8CB61D93511	user7	[Blacklist User Repository]	Exceeded	Not Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
8.	□	E17C3B06FF82	user8	[Insight Repository]	Exceeded	Not Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
9.	□	F5F920B10173	user9	[Local User Repository]	Not Exceeded	Exceeded	Not Exceeded	Aug 19, 2013 19:20:23 IST
10.	□	A6D394659CF3	user10	[Guest User Repository]	Not Exceeded	Not Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST
11.	□	8249A5FC722A	user11	[Guest Device Repository]	Exceeded	Exceeded	Exceeded	Aug 19, 2013 19:20:23 IST

Showing 1-11 of 11

Chapter 5
Policy Manager Policy Model

From the point of view of network devices or other entities that need authentication and authorization services, Policy Manager appears as a RADIUS, TACACS+ or HTTP/S based Authentication server; however, its 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 the Enterprise.

For more information, see:

- "Services Paradigm" on page 71
- "Policy Simulation" on page 77

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.

NOTE

Policy Manager ships configured with a number of basic Service types. You can flesh out these Service types, copy them for 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 determination of enforcement parameters for network access.

For more information, see:

- "Viewing Existing Services" on page 75
- "Adding and Removing Services" on page 75
- "Links to Use Cases and Configuration Instructions" on page 76

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

Figure 54: *Generic Policy Manager Service Flow of Control*

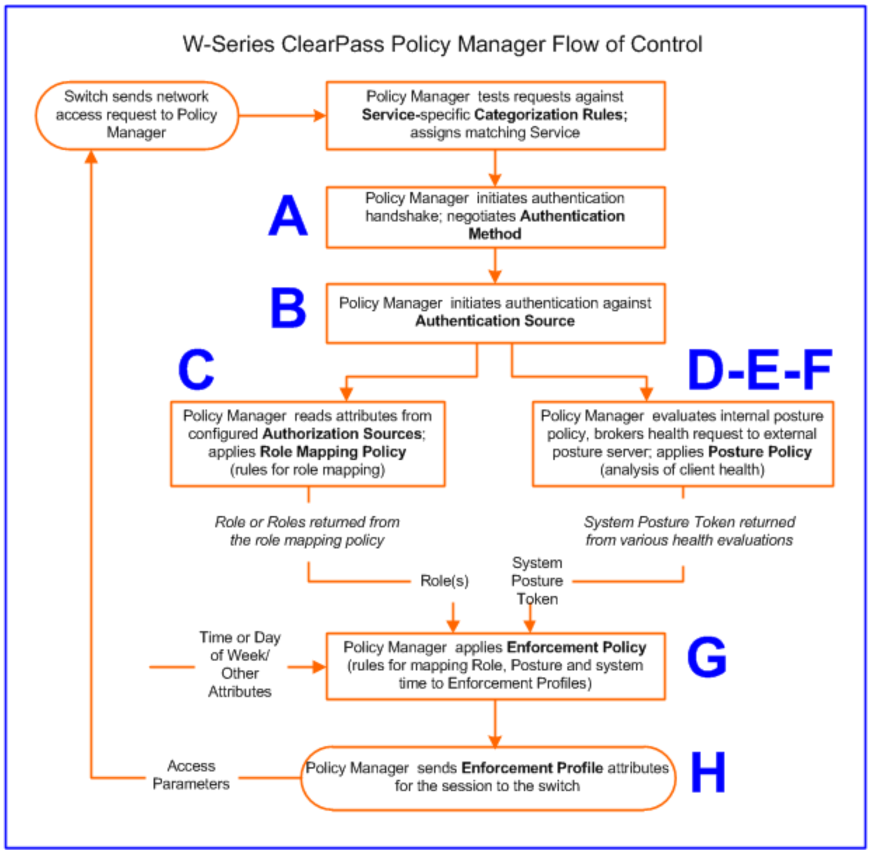

W-Series ClearPass Policy Manager Flow of Control
Switch sends network access request to Policy Manager
Policy Manager tests requests against Service-specific Categorization Rules; assigns matching Service
A
Policy Manager initiates authentication handshake; negotiates Authentication Method
B
Policy Manager initiates authentication against Authentication Source
C
D-E-F
Policy Manager reads attributes from configured Authorization Sources; applies Role Mapping Policy (rules for role mapping)
Policy Manager evaluates internal posture policy, brokers health request to external posture server; applies Posture Policy (analysis of client health)
Role or Roles returned from the role mapping policy
System Posture Token returned from various health evaluations
Role(s)
System Posture Token
Time or Day of Week/ Other Attributes
Policy Manager applies Enforcement Policy (rules for mapping Role, Posture and system time to Enforcement Profiles)
G
Access Parameters
Policy Manager sends Enforcement Profile attributes for the session to the switch
H

Table 25: *Policy Manager Service Components*

Component	Service: component ratio	Description
A - Authentication Method	Zero or more per service	EAP or non-EAP method for client authentication. Policy Manager supports four broad 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: (1) makes internal checks to verify that the request is indeed a *MAC Authentication* request (and not a spoofed request) and (2) makes sure 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 tab available.
B - Authentication Source	Zero or more per service	An Authentication Source is the identity repository against which Policy Manager verifies identity. It supports these 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 the 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. You specify the attributes you want to collect when you configure the authentication source. Policy Manager supports the following authorization source types: • Microsoft Active Directory • any LDAP compliant directory • RSA or other RADIUS-based token servers • SQL database, including the local user store.

Table 25: *Policy Manager Service Components (Continued)*

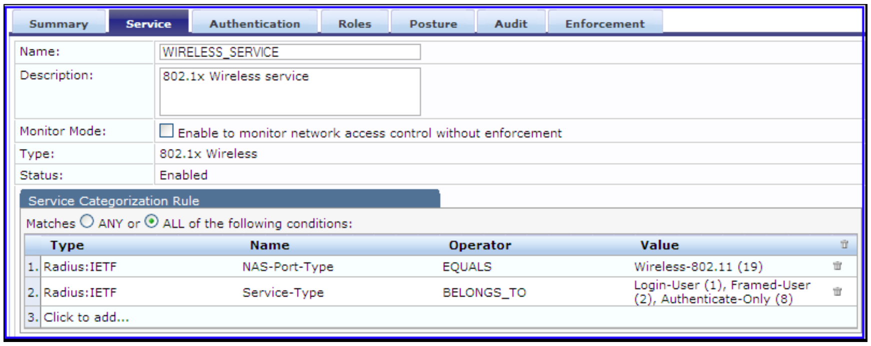
Component	Service: component ratio	Description
C - Role Mapping Policy	Zero or one per service	Policy Manager evaluates Requests against Role Mapping Policy rules to match Clients to Role(s). All rules are evaluated and Policy Manager may return more than one Role. If no rules match, the request takes the configured Default Role. 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 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 can 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, typically posture credentials that cannot be evaluated internally by Policy Manager (that is, not by internal posture policies). Currently, Policy Manager supports two forms of posture server interfaces: *HCAP*, *RADIUS*, and *GAMEv2* posture servers.
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 in lieu 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 Enforcement Policy rules to return one or more matching 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 Policy 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 into individual services:

In the menu panel, click **Services** to view a list of services that you can filter by phrase or sort by order.

Figure 55: *List of services with sorting tool*



Name:	WIRELESS_SERVICE
Description:	802.1x Wireless service
Monitor Mode:	□ Enable to monitor network access control without enforcement
Type:	802.1x Wireless
Status:	Enabled

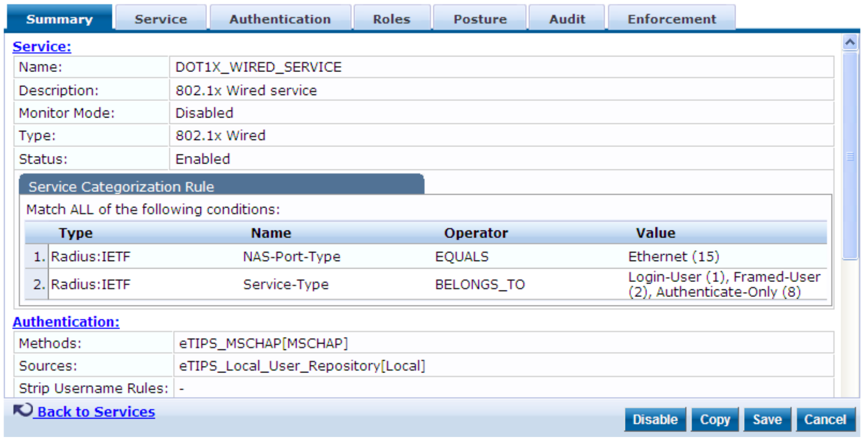
Service Categorization Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			

In the **Services** page, click the name of a Service to display its details.

Figure 56: *Details for an individual service*



Service:

Name:	DOT1X_WIRED_SERVICE
Description:	802.1x Wired service
Monitor Mode:	Disabled
Type:	802.1x Wired
Status:	Enabled

Service Categorization Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)

Authentication:

Methods:	eTIPS_MSCHAP[MSCHAP]
Sources:	eTIPS_Local_User_Repository[Local]
Strip Username Rules:	-

Adding and Removing Services

You can add to the list of services by working from a copy, importing from another configuration, or creating a service from scratch:

- **Create a template** by copying an existing service.

  In the **Services** page, click a service's check box, then click **Copy**.

- **Clone a service** by import (of a previously exported named file from this or another configuration).

  In the **Services** page, click a service's check box, then click the **Export a Service** link and provide the output file path. Later, you can import this service by clicking **Import a Service** and providing the file path.

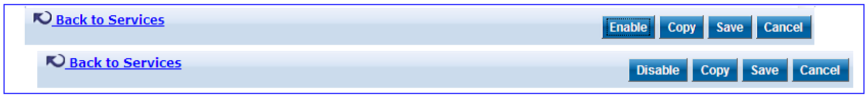
- **Create a new service** that you will configure from scratch.

  In the **Services** page, click **Add a Service**, then follow the configuration wizard from component to component by clicking **Next** as you complete each tab.

- **Remove a service**.

  In the **Services** page, fill the check box for a service, then click the **Delete** button. You can also disable/enable a service from the service detail page by clicking **Disable/Enable** (lower right of page).

Figure 57: *Disable/Enable toggle for a Policy Manager Service*



Links to Use Cases and Configuration Instructions

For each of a Service's policy components that you can configure, the following table references an illustrative Use Case and detailed Configuration Instructions.

Table 26: *Policy Component Use Cases and Configuration Instructions*

Policy Component	Illustrative Use Cases	Configuration Instructions
Service	● "802.1X Wireless Use Case" on page 479 ● "Web Based Authentication Use Case" on page 485. ● "MAC Authentication Use Case" on page 492. ● "TACACS+ Use Case" on page 495.	"Adding Services" on page 123
Authentication Method	"802.1X Wireless Use Case" on page 479 demonstrates the principle of multiple authentication methods in a list. When Policy Manager initiates the authentication handshake, it tests the methods in priority order until one is accepted by the client. "Web Based Authentication Use Case" on page 485 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 131
Authentication Source	● "802.1X Wireless Use Case" on page 479 demonstrates the principle of multiple authentication sources in a list. Policy Manager tests the sources in priority order until the client can be authenticated. In this case Active Directory is listed first. ● "Web Based Authentication Use Case" on page 485 uses the local Policy Manager repository, as this is common practice among administrators configuring Guest Users. ● "MAC Authentication Use Case" on page 492 uses a Static Host List for authentication of the MAC address sent by the switch as the device's username. ● "TACACS+ Use Case" on page 495 uses the local Policy Manager repository. Other authentication sources would also be fine.	"Adding and Modifying Authentication Sources" on page 149

Table 26: *Policy Component Use Cases and Configuration Instructions (Continued)*

Policy Component	Illustrative Use Cases	Configuration Instructions
Role Mapping	"802.1X Wireless Use Case" on page 479 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 190 - "Adding and Modifying Roles" on page 189 - "Adding and Modifying Local Users" on page 183 - "Adding and Modifying Static Host Lists" on page 187
Posture Policy	"Web Based Authentication Use Case" on page 485 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 198
Posture Server	"802.1X Wireless Use Case" on page 479 appends a third-party posture server to evaluate health policies based on vendor-specific posture credentials.	"Adding and Modifying Posture Servers" on page 230
Audit Server	"MAC Authentication Use Case" on page 492, uses an Audit Server to provide port scanning for health.	"Configuring Audit Servers" on page 233
Enforcement Policy and Profiles	All Use Cases have an assigned Enforcement Policy and corresponding Enforcement Rules.	- "Configuring Enforcement Profiles " on page 246 - "Configuring Enforcement Policies" on page 277

Policy Simulation

After the policies have been set up, the Policy Simulation utility can be used to evaluate these policies - before deployment. The Policy Simulation utility applies a set of request parameters as input against a given policy component and displays the outcome, at: **Configuration > Policy Simulation**.

The following types of simulations are supported:

- **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.
- **Role Mapping** - Given the service name (and associated role mapping policy), the authentication source and the user name, the role mapping simulation maps the user into a role or set of roles. You can also use the role mapping simulation to test whether the specified authentication source is reachable.
- **Posture Validation** - A 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** - An audit simulation allows you to specify an audit server (Nessus- or NMAP-based) and the IP address of the device you want to audit. An audit simulation triggers an audit on the specified device and displays the results.
- **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.
- **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.

For more information, see:

- "Adding Simulation Test" on page 79
- "Import and Export Simulations" on page 84

Figure 58: *Policy Simulation Page*

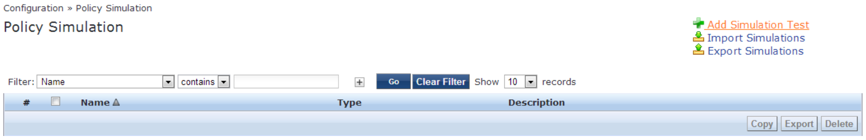


Table 27: *Policy Simulation Page Parameters*

Parameter	Description
Add Simulation Test	Opens the **Add Simulation Test** page.
Import Simulations	Opens the **Import Simulations** popup.
Export Simulations	Opens the **Export Simulations** popup.
Filter	Select the filter by which to constrain the display of simulation data.

Table 27: *Policy Simulation Page Parameters (Continued)*

Parameter	Description
Copy	Make a copy 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.

Adding Simulation Test

Navigate to **Configuration** > **Policy Simulation** and click on the **Add Simulation** link. Depending on the simulation type selected the contents of the **Simulation** tab changes.

Table 28: *Add Policy Simulation (Simulation tab)*

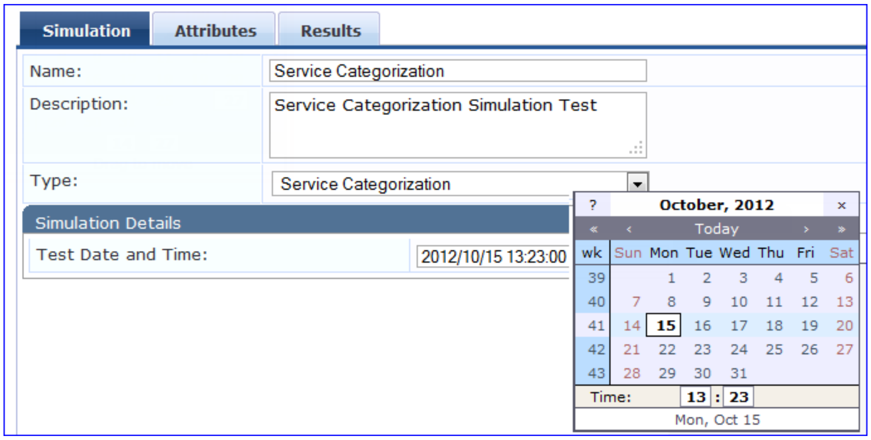
Parameter	Description
Name/Description	Specify name and description (freeform).
Type **Service Categorization.**	• Input (**Simulation** tab): Select **Date** and **Time**. (optional - use if you have time based service rules)  Name: Service Categorization Description: Service Categorization Simulation Test Type: Service Categorization Simulation Details Test Date and Time: 2012/10/15 13:23:00 ? October, 2012 × « ‹ Today › » wk Sun Mon Tue Wed Thu Fri Sat 39 1 2 3 4 5 6 40 7 8 9 10 11 12 13 41 14 15 16 17 18 19 20 42 21 22 23 24 25 26 27 43 28 29 30 31 Time: 13 : 23 Mon, Oct 15 • Input (**Attributes** tab): Use the **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)

Table 28: *Add Policy Simulation (Simulation tab) (Continued)*

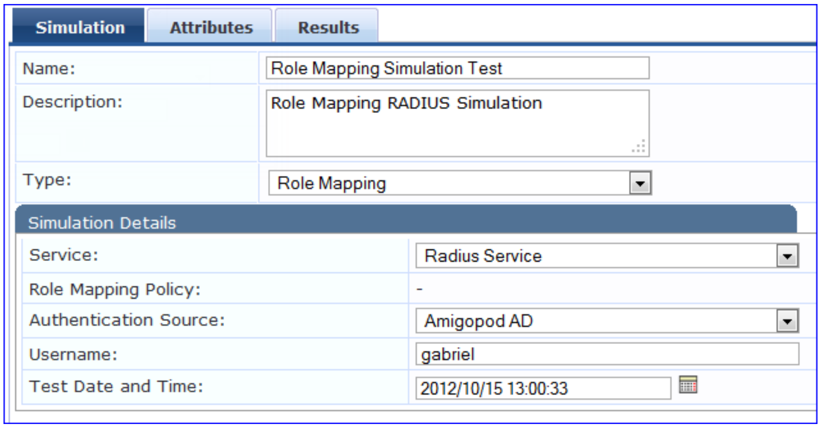
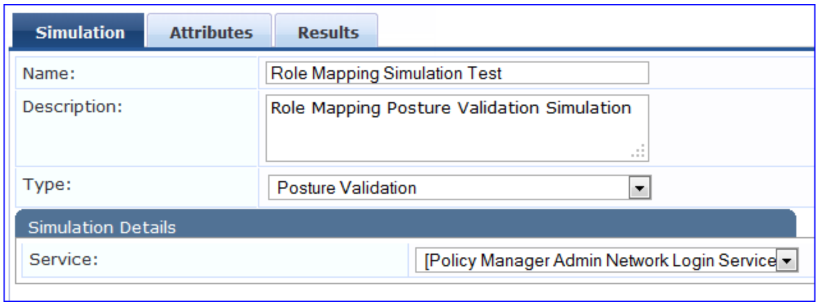
Parameter	Description
Type **Role Mapping.**	● Input (**Simulation** tab): Select **Service** (**Role Mapping Policy** is implicitly selected, because there is only one such policy associated with a service), **Authentication Source**, **User Name**, and **Date/Time**.  Name: Role Mapping Simulation Test Description: Role Mapping RADIUS Simulation Type: Role Mapping Simulation Details Service: Radius Service Role Mapping Policy: - Authentication Source: Amigopod AD Username: gabriel Test Date and Time: 2012/10/15 13:00:33 ● Input (**Attributes** tab): Use the **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)* - including authorization source attributes fetched as roles.
Type **Posture Validation.**	● Input (**Simulation** tab): Select **Service** (Posture policies are implicitly selected by their association with the service).  Name: Role Mapping Simulation Test Description: Role Mapping Posture Validation Simulation Type: Posture Validation Simulation Details Service: [Policy Manager Admin Network Login Service ● Input (**Attributes** tab): Use the **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*.

Table 28: *Add Policy Simulation (Simulation tab) (Continued)*

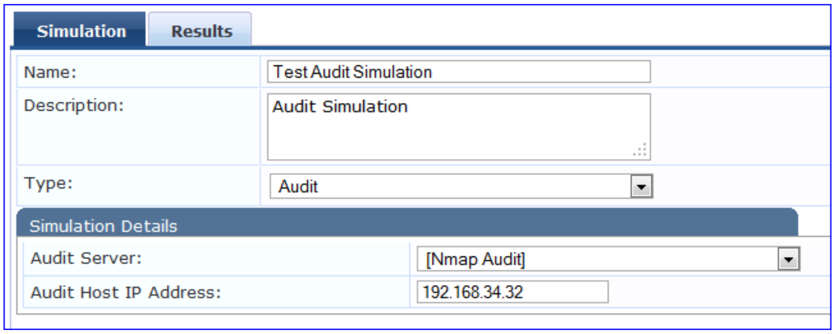
Parameter	Description
Type **Audit.**	- Input (**Simulation** tab): Select the **Audit Server** and host to be Audited (IP address or hostname)  Name: Test Audit Simulation Description: Audit Simulation Type: Audit Simulation Details Audit Server: [Nmap Audit] Audit Host IP Address: 192.168.34.32 - Returns (**Results** tab): *Summary Posture Status*, *Audit Attributes* and *Status* **NOTE:** Audit simulations can take a while; an AuditInProgress status is shown until the audit completes.

Table 28: *Add Policy Simulation (Simulation tab) (Continued)*

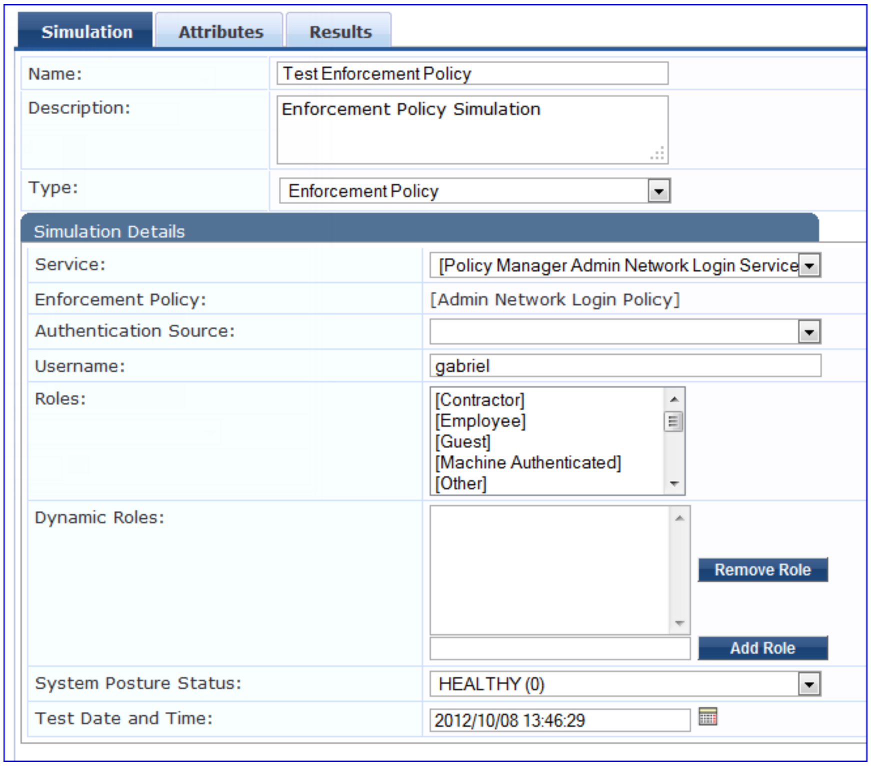
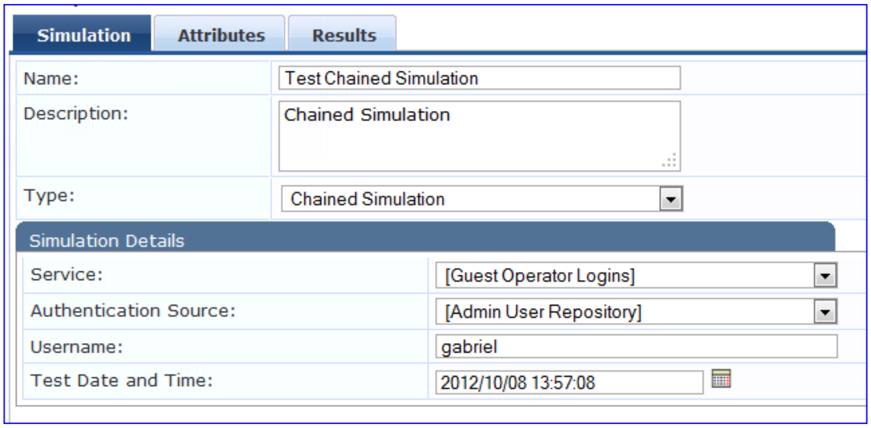
Parameter	Description
Type **Enforcement Policy.**	- Input (**Simulation** tab): Select **Service** (Enforcement Policy is implicit by its association with the Service), Authentication Source (optional), User Name (optional), Roles, Dynamic Roles (optional), System Posture Status, and Date/Time (optional).  Name: Test Enforcement Policy Description: Enforcement Policy Simulation Type: Enforcement Policy Simulation Details Service: [Policy Manager Admin Network Login Service Enforcement Policy: [Admin Network Login Policy] Authentication Source: Username: gabriel Roles: [Contractor] [Employee] [Guest] [Machine Authenticated] [Other] Dynamic Roles: System Posture Status: HEALTHY (0) Test Date and Time: 2012/10/08 13:46:29 - 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, refer to "Adding and Modifying Authentication Sources" on page 149for more information.

Table 28: *Add Policy Simulation (Simulation tab) (Continued)*

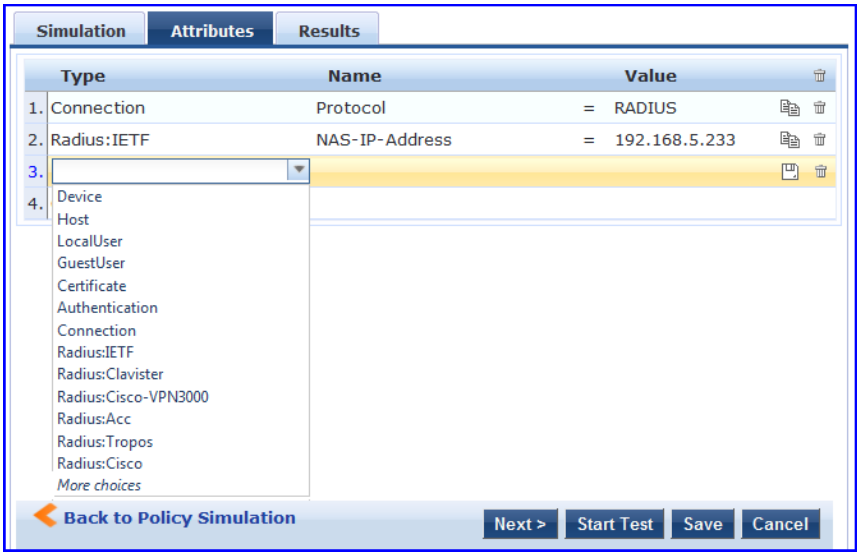
Parameter	Description
Type **Chained Simulations.**	- Input (**Simulation** tab): Select **Service**, **Authentication Source**, **User Name**, and **Date/Time**.  Name: Test Chained Simulation Description: Chained Simulation Type: Chained Simulation Simulation Details Service: [Guest Operator Logins] Authentication Source: [Admin User Repository] Username: gabriel Test Date and Time: 2012/10/08 13:57:08 - Input (**Attributes** tab): Use the **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	Upon completion of your work in this tab, click Next to open the **Attributes** tab.
Start Test	Run test. Outcome is displayed in the **Results** tab.
Save/Cancel	Click **Save** to commit or **Cancel** to dismiss the popup.

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

NOTE

The **Attributes** tab will not display if you select the **Audit Policy** component in the **Simulation** tab.

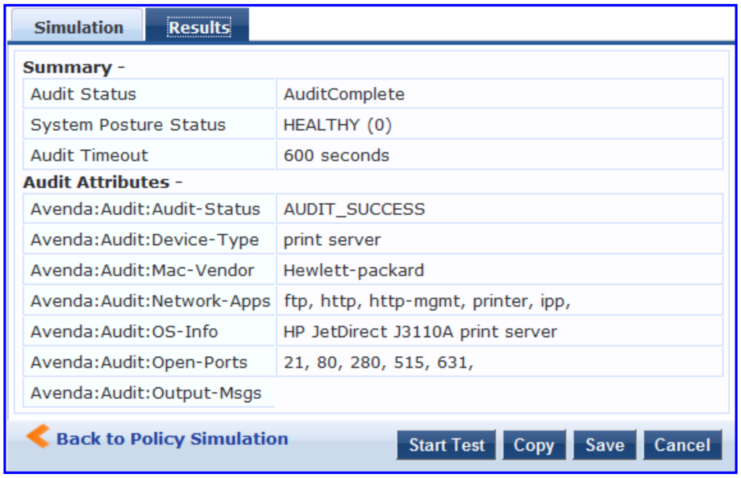
Figure 59: *Add Simulation (Attributes Tab)*



	Type	Name		Value
1.	Connection	Protocol	=	RADIUS
2.	Radius:IETF	NAS-IP-Address	=	192.168.5.233
3.				
4.				

In the **Results** tab, Policy Manager displays the outcome of applying the test request parameters against the specified policy component(s). What is shown in the results tab again depends on the type of simulation.

Figure 60: *Add Simulation (Results Tab)*



Summary -

Audit Status	AuditComplete
System Posture Status	HEALTHY (0)
Audit Timeout	600 seconds

Audit Attributes -

Avenda:Audit:Audit-Status	AUDIT_SUCCESS
Avenda:Audit:Device-Type	print server
Avenda:Audit:Mac-Vendor	Hewlett-packard
Avenda:Audit:Network-Apps	ftp, http, http-mgmt, printer, ipp,
Avenda:Audit:OS-Info	HP JetDirect J3110A print server
Avenda:Audit:Open-Ports	21, 80, 280, 515, 631,
Avenda:Audit:Output-Msgs	

Import and Export Simulations

Navigate to **Configuration > Policy Simulation** and select the **Import Simulations** link.

Figure 61: *Import Simulations*

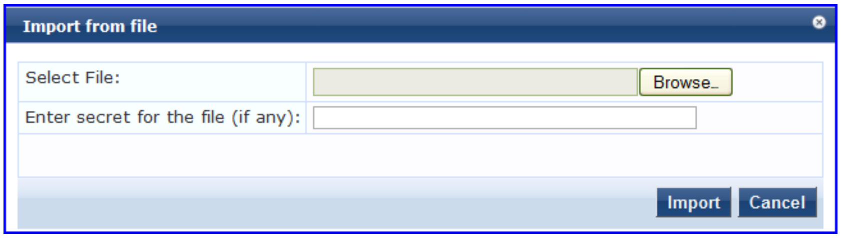


Table 29: *Import Simulations*

Parameter	Description
Select file	Browse to select name of simulations import file.
Import/Cancel	**Import** to commit or **Cancel** to dismiss popup.

Export Simulations

Click the **Export Simulations** link. This task exports all simulations. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Export

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

Services

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

For more information, see:

- "Architecture and Flow" on page 87
- "Start Here" on page 87
- "Policy Manager Service Types" on page 99
- "Services" on page 122
- "Identity" on page 181

Architecture and Flow

Architecturally, Policy Manager Services are:

- **Parents** of their policy components, which they wrap (hierarchically) and coordinate in processing requests.
- **Siblings** of other Policy Manager Services, within an ordered priority that determines the sequence in which they are tested against requests.
- **Children** of Policy Manager, which tests requests against their Rules, to find a matching Service for each request.

The flow-of-control for requests parallels 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 Approach - Create all policy components (Authentication Method, Authentication Source, Role Mapping Policy, Posture Policy, Posture Servers, Audit Servers, Enforcement Profiles, Enforcement Policy) first, as needed, and then create the Service from using the Service creation Wizard.
- Top-Down Approach - Start with the Service creation wizard, and create the associated policy components as and when you need them, 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

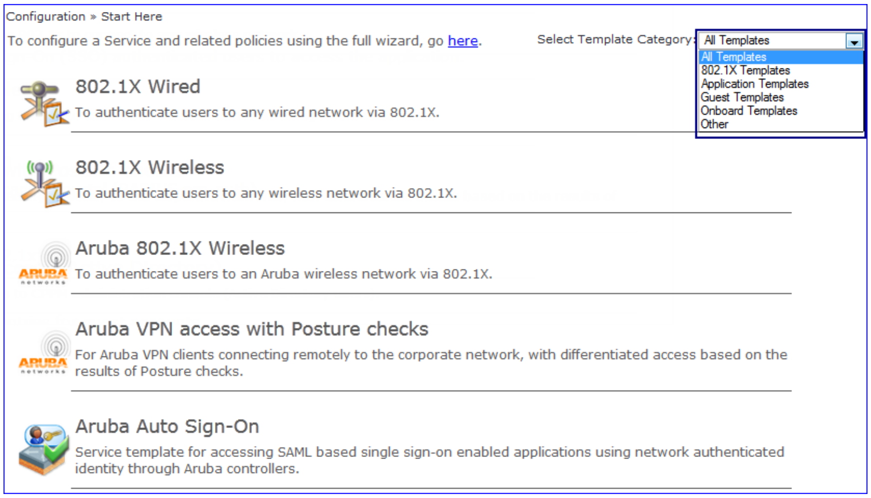
The Dell Networking W-ClearPass Policy Manager Start Here page provides the ability to create templates for services where you can define baseline policies and require specific data when you create services. Service templates create services and define components such as role-mapping policies, enforcement policies, and network devices with a "fill-in-the-blanks" approach. You fill in various fields, and 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, Wireless, and Dell Wireless" on page 88
- "Dell VPN Access with Posture Checks" on page 89

- "Aruba Auto Sign-On" on page 91
- "ClearPass Admin Access" on page 92
- "ClearPass Admin SSO Login (SAML SP Service)" on page 92
- "ClearPass Identity Provider (SAML IdP Service)" on page 93
- "EDUROAM Service" on page 93
- "Guest Access Web Login" on page 95
- "Guest Access" on page 95
- "Guest MAC Authentication" on page 96
- "Onboard" on page 97
- "WorkSpace Authentication" on page 98

Figure 62: *Service Templates page (partial view)*



Configuration » Start Here

To configure a Service and related policies using the full wizard, go here.

Select Template Category: All Templates

802.1X Wired

To authenticate users to any wired network via 802.1X.

802.1X Wireless

To authenticate users to any wireless network via 802.1X.

Aruba 802.1X Wireless

To authenticate users to an Aruba wireless network via 802.1X.

Aruba VPN access with Posture checks

For Aruba VPN clients connecting remotely to the corporate network, with differentiated access based on the results of Posture checks.

Aruba Auto Sign-On

Service template for accessing SAML based single sign-on enabled applications using network authenticated identity through Aruba controllers.

802.1X Wired, Wireless, and Dell Wireless

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

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

All three templates are configured using identical parameters.

Table 30: *802.1X Wired, 802.1X Wireless, and Dell 802.1X Wireless Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Authentication	
AD Name	Enter your active directory name.

Table 30: *802.1X Wired, 802.1X Wireless, and Dell 802.1X Wireless Service Template Parameters (Continued)*

Parameter	Description
Description	Enter a description that will help you 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.
Enforcement Details	
Attribute Name	The active directory attribute name.
Attribute Value	The active directory attribute value.
VLAN ID	Standard RADIUS-IETF VLAN ID.
Wireless Network Settings	
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 Change of Authorization on the network device.
RADIUS CoA Port	By default this is 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.

Table 31: *Dell VPN Access with Posture Checks Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Authentication	
AD Name	Enter your active directory name.
Description	Enter a description that will help you 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	
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 Change of Authorization on the network device.
RADIUS CoA Port	By default this is 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	
Initial Role	Enter the initial role of the client before posture checks are performed.
Quarantined Role	Enter the role of clients that fail posture checks.
Healthy Role	Enter the role of the client after it has passed a posture check and is deemed healthy.

Aruba Auto Sign-On

This application service template allows access to SAML-based, single-sign-on-enabled applications (such as Policy Manager, Guest, and Insight) using Aruba controllers for network authentication.

Table 32: *ClearPass Aruba Auto Sign-On Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Authentication	
AD Name	Enter the hostname or the IP address of the Active Directory server.
Description	Enter a description that will help you 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 the Distinguished Name of the administrator account.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection. This value defaults to 389.
Enforcement Details	
Create new Enforcement Policy	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 specifying that "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 will be included in SAML responses.
Attribute Value	

ClearPass Admin Access

This template is designed for services that authenticate users against Active Directory (AD) and use AD attributes to determine appropriate privilege levels for Dell Networking W-ClearPass Policy Manager admin access.

Table 33: *ClearPass Admin Access Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Authentication	
AD Name	Enter the hostname or the IP address of the Active Directory server.
Description	Enter a description that will help you 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 the Distinguished Name of the administrator account.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
Role Mapping	
Attribute Name	Select the active directory attribute.
Super Admin Condition	Defines the 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 screens.

Table 34: *ClearPass Admin SSO Login Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.

Parameter	Description
Service Rule	
Application	Select the application that single-sign-on-authenticated administrative users will be able to access.

ClearPass Identity Provider (SAML IdP Service)

This template is designed for services that act as an Identity Provider (IdP). This IdP feature provides a way for the layer-2 device, RADIUS server, and Security Asserting Markup Language (SAML) IdP to work together to deliver application-based single sign-on using network authentication information.

Table 35: *ClearPass Admin Access Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Authentication	
AD Name	Enter the hostname or the IP address of the Active Directory server.
Description	Enter a description that will help you 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 the Distinguished Name of the administrator account.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
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 will be 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.

Table 36: *EDUROAM Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Service Rule	**Service Rule**
Enter domain details	Enter the domain name of the network.
Select Vendor	Select the vendor of the network device.
Authentication	
AD Name	Enter the hostname or the IP address of the Active Directory server.
Description	Enter a description that will help you 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 the Distinguished Name of the administrator account.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
Wireless Network Settings	
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 Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device.
FLRs	
Host Name	The hostname of the federation RADIUS server.

Table 36: *EDUROAM Service Template Parameters (Continued)*

Parameter	Description
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 Change of Authorization on the network device.
RADIUS CoA Port	By default this is 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.

Guest Access Web Login

This service authenticates guests logging in via 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."

Table 37: *Guest Web Login Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended 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 days on which access is allowed.

Guest Access

This template is designed for authenticating guest users who login via 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.

Table 38: *Guest Access Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended 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.
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 Change of Authorization on the network device.
RADIUS CoA Port	By default this is 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 days on which access is allowed.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data, in megabytes, 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.

Table 39: *Guest MAC Authentication Service Template Parameters.*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Wireless Network Settings	**Wireless Network Settings**

Table 39: *Guest MAC Authentication Service Template Parameters. (Continued)*

Parameter	Description
Wireless SSID for Guest access	Enter the SSID name of your network.
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 Change of Authorization on the network device.
RADIUS CoA Port	By default this is 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 number of days the MAC account will remain valid for Guest Role. After this the guest will need to re-authenticate via captive portal.
Cache duration for Employee role	Enter the number of days the MAC account will remain valid for Employee Role. After this the guest will need to re-authenticate via captive portal.
Cache duration for Contractor role	Enter the number of days the MAC account will remain valid for Contractor Role. After this the guest will need to re-authenticate via captive portal.
Guest Access Restrictions	
Days allowed for access	Select the days on which access is allowed.
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, a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

Onboard

This template is designed for configuration that allows checks to be performed before allowing Onboard provisioning for BYOD use-cases. This service creates an Onboard Pre-Auth service to check the user's credentials prior to 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 also after device provisioning is complete.

Table 40: *Onboard Authorization Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
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 Change of Authorization on the network device.
RADIUS CoA Port	By default this is 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 days on which access is allowed.
Provisioning Wireless Network Settings	
Wireless SSID for Onboard Provisioning	Enter the SSID of your network.

WorkSpace Authentication

This template authenticates users against an Active Directory (AD) and enforces selected WorkSpace device provisioning settings.

Table 41: *WorkSpace Authorization Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
Authentication	
AD Name	Enter the hostname or the IP address of the Active Directory server.
Description	Enter a description that will help you identify the characteristics of this template.
Server	Enter the hostname or the IP address of the Active Directory server.

Table 41: *WorkSpace Authorization Service Template Parameters (Continued)*

Parameter	Description
Identity	Enter the Distinguished Name of the administrator account.
NETBIOS	Enter the server Active Directory domain name.
Base DN	Enter the Distinguished Name of the administrator account.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
Device Access Restrictions	
Days allowed for access	Select the days on which access is allowed.
Provisioning Settings	
Select Provisioning Settings	Select a provisioning setting.

Policy Manager Service Types

The following service types are available in Policy Manager:

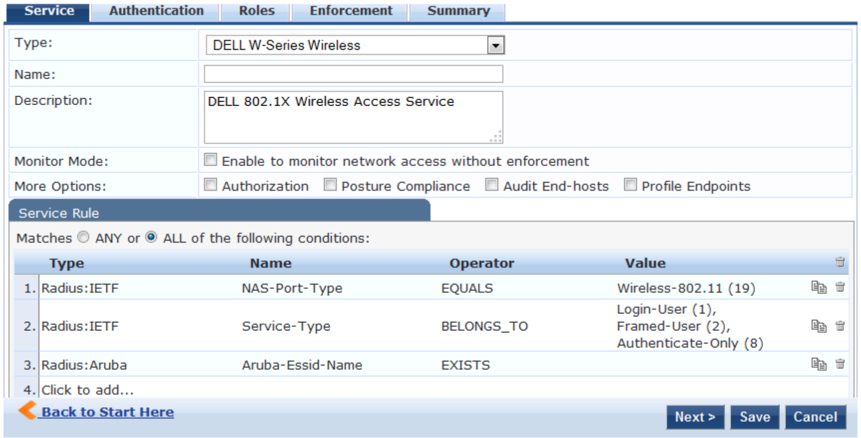
- "Dell 802.1X Wireless" on page 99
- "802.1X Wireless" on page 103
- "802.1X Wired" on page 105
- "MAC Authentication" on page 106
- "Web-based Authentication" on page 109
- "Web-based Health Check Only" on page 111
- "Web-based Open Network Access" on page 111
- "802.1X Wireless - Identity Only" on page 112
- "802.1X Wired - Identity Only" on page 112
- "RADIUS Enforcement (Generic)" on page 112
- "RADIUS Proxy" on page 115
- "RADIUS Authorization" on page 116
- "TACACS+ Enforcement" on page 116
- "Dell W-Series Application Authentication" on page 118
- "Dell W-Series Application Authorization" on page 119
- "Cisco Web Authentication Proxy" on page 120

Dell 802.1X Wireless

Configure this service for wireless hosts connecting through a DellW-Series 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Service rules are customized for a typical Dell W-Series Mobility Controller deployment. This service by default includes a rule that specifies that a Dell ESSID exists.

The default, configuration tabs are Service, Authentication, Roles, and Enforcement. You can also select Authorization, Posture Compliance, Audit End Hosts, and Profile Endpoints in the **More Options** section to access those configuration tabs.

Figure 63: *Dell 802.1X Wireless Service*



Type:	DELL W-Series Wireless
Name:	
Description:	DELL 802.1X Wireless Access Service
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EXISTS	
4.	Click to add...			

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of its options.

NOTE

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 sources.

- **Authentication Methods:** The authentication methods 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:
  - EAP PEAP
  - EAP FAST
  - EAP TLS
  - EAP TTLS

  Non-tunneled EAP methods such as EAP-MD5 can also be used as authentication methods.
- **Authentication Sources**: The Authentication Sources used for this type of service can be one or more instances of the following: Active Directory, LDAP Directory, SQL DB, Token Server or the Policy Manager local DB.

For both Authentication Methods and Authentication Sources, you can select one item in the list and use the buttons on the right to:

- Move it up or down

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged.

- Remove it
- View its details
- Modify it. See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.

You can also use the links on the right to add a new authentication method or source.

Select the **Strip Username Rules** checkbox to pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

The Authorization tab is not visible by default. To access it, select the **Authorization** check box on the Services tab.

The Authorization tab is where you select 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:

- The authorization sources associated with the authentication source.
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 131.

To add an authorization source, select it from the drop-down list.

For authorization sources in the list, you can select one and use the buttons on the right to:

- Remove it.
- View its details.
- Modify it.

For more information on configuring authorization sources, see "Adding and Modifying Authentication Methods" on page 131.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Posture Tab

This type of service does not have Posture checking enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box on the Service tab.

You can enable posture checking for this kind of service if you are deploying Policy Manager in a Microsoft NAP or Cisco NAC framework environment, or if you are deploying a Dell hosted captive portal that does posture checks through a dissolvable agent. You can also choose to **Enable auto-remediation of non-compliant end-hosts** and enter the **Remediation URL** of a server resource that can perform remediation action (when a client is quarantined).

NOTE

When you configure posture policies, only those that are configured for the OnGuard Agent are shown in a list of posture policies.

For more information on configuring Posture Polices and Posture Servers, see "Adding a Posture Policy" on page 198 and "Adding and Modifying Posture Servers" on page 230.

Enforcement Tab

The Enforcement tab is where you select an enforcement policy for a service. You must select one.

See "Configuring Enforcement Policies" on page 277 for more information.

Audit Tab

By default, this type of service does not have Audit checking enabled and the Audit tab is not visible. To access it and enable posture checking for this service select the **Audit End-hosts** check box on the Service tab.

- Select an **Audit Server** - either built-in or customized. See "Configuring Audit Servers" on page 233 for audit server configuration steps.
- Select an Audit Trigger Condition:
  - **Always**
  - **When posture is not available**
  - **For MAC authentication requests**. If you select this, then select also one of:
    - For known end-hosts only
    - For unknown end hosts only
    - For all end hosts

Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service.

- Select an **Action after audit**. 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, there should be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways:
  - **No Action:** The audit will not apply policies on the network device after this audit.
  - **Do SNMP bounce:** This option will bounce the switch port or force an 802.1X reauthentication (both done via SNMP).
  - 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.
  - **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.

Profiler Tab

The Profiler tab is not visible by default. To access it, select the **Profile Endpoints** check box on the Services tab.

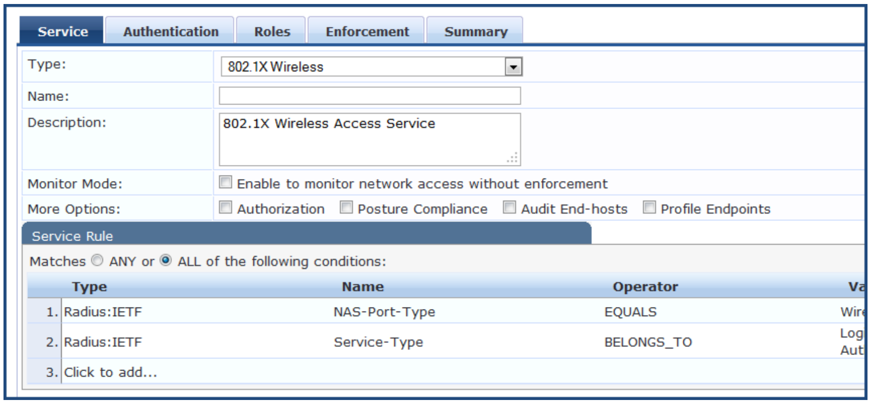
Select one or more Endpoint Classification items from the drop-down list, then select the RADIUS CoA action. You can also create a new action by selecting the **Add new RADIUS CoA Action** link.

802.1X Wireless

Configure the 802.1X Wireless service for wireless clients connecting through an 802.11 wireless access device or controller with authentication via IEEE 802.1X.

The default configuration tabs are: Service, Authentication, Roles, and Enforcement. You can also select Authorization, Posture Compliance, Audit End Hosts, and Profile Endpoints in the **More Options** section to access those configuration tabs.

Figure 64: *802.1X Wireless Service*



Type:	802.1X Wireless
Name:	
Description:	802.1X Wireless Access Service
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Va
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wir
2.	Radius:IETF	Service-Type	BELONGS_TO	Log Aut
3.	Click to add...			

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of 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 sources.

- **Authentication Methods:** The authentication methods 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, are
  - EAP PEAP
  - EAP FAST
  - EAP TLS
  - EAP TTLS

  Non-tunneled EAP methods such as EAP-MD5 can also be used as authentication methods.
- **Authentication Sources**: The Authentication Sources used for this type of service can be one or more instances of the following: Active Directory, LDAP Directory, SQL DB, Token Server or the Policy Manager local DB.

For both Authentication Methods and Authentication Sources, you can select one item in the list and use the buttons on the right to:

- Move it up or down

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged.

- Remove it
- View its details
- Modify it. See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.

You can also use the links on the right to add a new authentication method or source.

Select **Strip Username Rules** to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

The Authorization tab is not visible by default. To access it, select the **Authorization** check box on the Services tab.

The Authorization tab is where you select 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:

- The authorization sources associated with the authentication source.
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 131.

To add an authorization source, select it from the drop-down list.

For authorization sources in the list, you can select one and use the buttons on the right to:

- Remove it.
- View its details.
- Modify it.

For more information on configuring authorization sources, see "Adding and Modifying Authentication Methods" on page 131.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Posture Tab

This type of service does not have Posture checking enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box on the Service tab.

You can enable posture checking for this kind of service if you are deploying Policy Manager in a Microsoft NAP or Cisco NAC framework environment, or if you are deploying a Dell hosted captive portal that does posture checks through a dissolvable agent. You can also choose to **Enable auto-remediation of non-compliant end-hosts** and enter the **Remediation URL** of a server resource that can perform remediation action (when a client is quarantined).

NOTE

When you configure posture policies, only those that are configured for the OnGuard Agent are shown in a list of posture policies.

For more information on configuring Posture Polices and Posture Servers, see "Adding a Posture Policy" on page 198 and "Adding and Modifying Posture Servers" on page 230.

Enforcement Tab

The Enforcement tab is where you select an enforcement policy for a service. You must select one.

See "Configuring Enforcement Policies" on page 277 for more information.

Audit Tab

By default, this type of service does not have Audit checking enabled and the Audit tab is not visible. To access it and enable posture checking for this service select the **Audit End-hosts** check box on the Service tab.

- Select an **Audit Server** - either built-in or customized. See "Configuring Audit Servers" on page 233 for audit server configuration steps.
- Select an Audit Trigger Condition:
  - **Always**
  - **When posture is not available**
  - **For MAC authentication requests**. If you select this, then select also one of:
    - For known end-hosts only
    - For unknown end hosts only
    - For all end hosts

Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service.

- Select an **Action after audit**. 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, there should be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways:
  - **No Action:** The audit will not apply policies on the network device after this audit.
  - **Do SNMP bounce:** This option will bounce the switch port or force an 802.1X reauthentication (both done via SNMP).
  - 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.
  - **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.

Profiler Tab

The Profiler tab is not visible by default. To access it, select the **Profile Endpoints** check box on the Services tab.

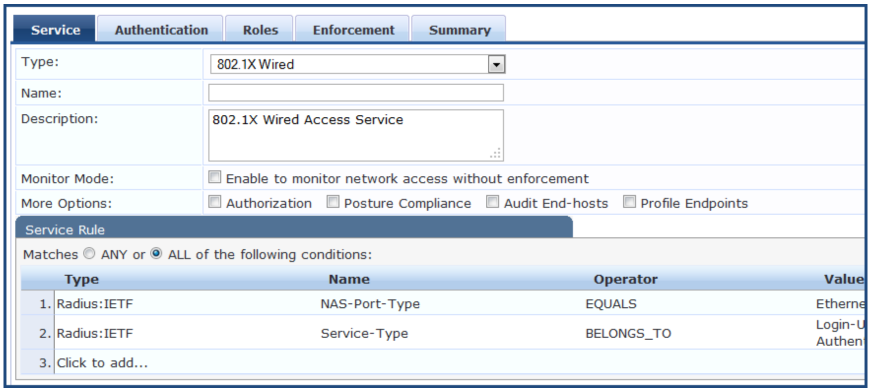
Select one or more Endpoint Classification items from the drop-down list, then select the RADIUS CoA action. You can also create a new action by selecting the **Add new RADIUS CoA Action** link.

802.1X Wired

Configure this service for clients connecting through an Ethernet LAN, with authentication via 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 802.1X Wireless Service. See "802.1X Wireless" on page 103 for details.

Figure 65: *802.1X Wired Service*



Type:	802.1X Wired
Name:	
Description:	802.1X Wired Access Service
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Etherne
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-U Authen
3.	Click to add...			

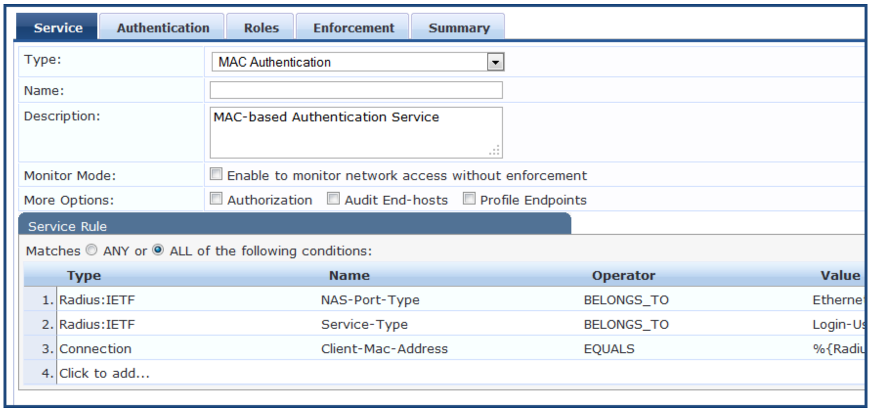
MAC Authentication

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.

Figure 66: *MAC Authentication Service*



Type:	MAC Authentication
Name:	
Description:	MAC-based Authentication Service
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Etherne
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-U
3.	Connection	Client-Mac-Address	EQUALS	%{Radiu
4.	Click to add...			

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of its options.

Authentication Tab

The **Authentication** tab contains options for configuring authentication methods and sources. The default Authentication method used for this type of service is [MAC AUTH], which is a special type of method called MAC-AUTH. When this authentication method is selected, Policy Manager does stricter checking of the MAC Address of the client. This type of service can use either a built-in static host list (see "Adding and Modifying Static Host Lists" on page 187), or any other authentication source for the purpose of white-listing or black-listing the client. You can also specify the role mapping policy, based on categorization of the MAC addresses in the authorization sources.

- **Authentication Methods:** The authentication methods 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. For this service, MAC AUTH is automatically selected. Non-tunneled EAP methods such as EAP-MD5 can also be used as authentication methods.
- **Authentication Sources**: The Authentication Sources used for this type of service can be one or more instances of the following: Active Directory, LDAP Directory, SQL DB, Token Server or the Policy Manager local DB.

For both Authentication Methods and Authentication Sources, you can select one item in the list and use the buttons on the right to:

- Move it up or down.

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged.

- Remove it.
- View its details.
- Modify it. (See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.)

You can also use the links on the right to add a new authentication method or source.

Select **Strip Username Rules** to pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

The Authorization tab is not visible by default. To access it, select the **Authorization** check box on the Services tab.

The Authorization tab is where you select 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:

- The authorization sources associated with the authentication source.
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 131.

To add an authorization source, select it from the drop-down list.

For authorization sources in the list, you can select one and use the buttons on the right to:

- Remove it.
- View its details.

- Modify it.

For more information on configuring authorization sources, see "Adding and Modifying Authentication Methods" on page 131.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Enforcement Tab

The Enforcement tab is where you select an enforcement policy for a service. You must select one.

See "Configuring Enforcement Policies" on page 277 for more information.

Audit Tab

By default, this type of service does not have Audit checking enabled and the Audit tab is not visible. To access it and enable posture checking for this service select the **Audit End-hosts** check box on the Service tab.

- Select an **Audit Server** - either built-in or customized. See "Configuring Audit Servers" on page 233 for audit server configuration steps.
- Select an Audit Trigger Condition:
  - **Always**
  - **When posture is not available**
  - **For MAC authentication requests**. If you select this, then select also one of:
    - For known end-hosts only
    - For unknown end hosts only
    - For all end hosts

Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service.

- Select an **Action after audit**. 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, there should be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways:
  - **No Action:** The audit will not apply policies on the network device after this audit.
  - **Do SNMP bounce:** This option will bounce the switch port or force an 802.1X reauthentication (both done via SNMP).
  - 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.
  - **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.

Profiler Tab

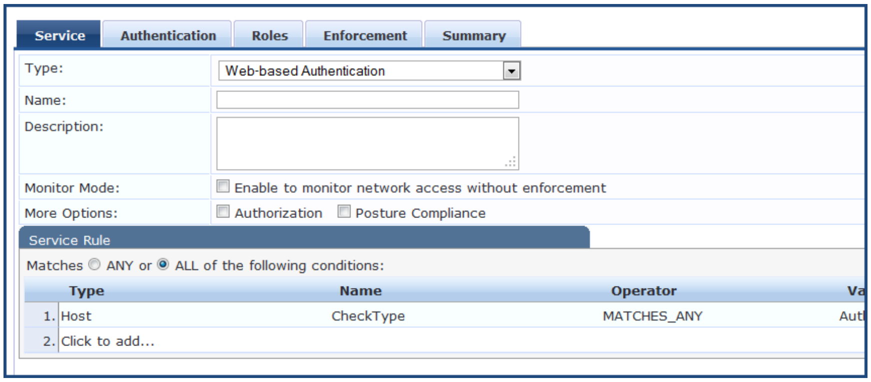
The Profiler tab is not visible by default. To access it, select the **Profile Endpoints** check box on the Services tab.

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.

Web-based Authentication

Configure this service for guests or agentless hosts that connect via 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 Windows 7, Windows Vista, Windows XP, Windows Server 2008, Windows Server 2003, and popular Linux systems). There is an internal service rule (*Connection:Protocol EQUALS WebAuth*) that categorizes requests into this type of service. You can add additional rules, if needed.

Figure 67: *Web-based Authentication Service*



Type:	Web-based Authentication
Name:	
Description:	
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Va
1.	Host	CheckType	MATCHES_ANY	Aut
2.	Click to add...			

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of its options.

Authentication Tab

The **Authentication** tab contains options for configuring authentication sources.

- **Authentication Sources**: Select the Authentication Sources used for this type of service.

You can select one item in the list and use the buttons on the right to:

- Move it up or down.

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packet exchanged.

- Remove it.
- View its details.
- Modify it. (See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.)

You can also use the links on the right to add a new authentication method or source.

Select **Strip Username Rules** to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

NOTE

There is no authentication method associated with this type of service. Authentication methods are only relevant for RADIUS requests.

Authorization Tab

The Authorization tab is not visible by default. To access it, select the **Authorization** check box on the Services tab.

The Authorization tab is where you select 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:

- The authorization sources associated with the authentication source.
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 131.

To add an authorization source, select it from the drop-down list.

For authorization sources in the list, you can select one and use the buttons on the right to:

- Remove it.
- View its details.
- Modify it.

For more information on configuring authorization sources, see "Adding and Modifying Authentication Methods" on page 131.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Posture Tab

This type of service does not have Posture checking enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box on the Service tab.

You can enable posture checking for this kind of service if you are deploying Policy Manager in a Microsoft NAP or Cisco NAC framework environment, or if you are deploying a Dell hosted captive portal that does posture checks through a dissolvable agent. You can also choose to **Enable auto-remediation of non-compliant end-hosts** and enter the **Remediation URL** of a server resource that can perform remediation action (when a client is quarantined).

NOTE

When you configure posture policies, only those that are configured for the OnGuard Agent are shown in a list of posture policies.

For more information on configuring Posture Polices and Posture Servers, see "Adding a Posture Policy" on page 198 and "Adding and Modifying Posture Servers" on page 230.

Enforcement Tab

The Enforcement tab is where you select an enforcement policy for a service. You must select one.

See "Configuring Enforcement Policies" on page 277 for more information.

Web-based Health Check Only

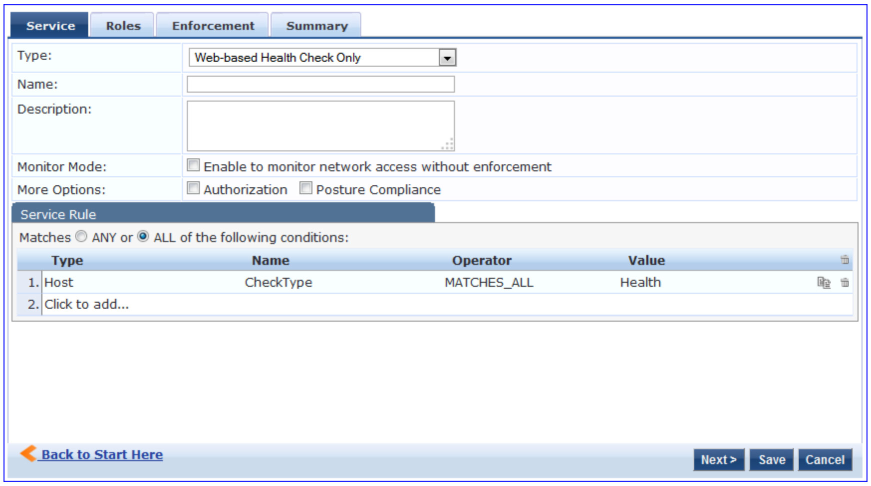
This type of service is the same as the Web-based Authentication service, except that there is no authentication performed; only health checking is done. There is an internal service rule (*Connection:Protocol EQUALS WebAuth*) that categorizes requests into this type of service. There is also an external service rule that is automatically added when you select this type of service: *Host:CheckType EQUALS Health*.

Configuration for this service is the same as Web-based Authentication except that Authentication is not performed. Refer to Web-based Authentication for more information.

NOTE

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

Figure 68: *Web-Based Health Check Only Service*



Type: Web-based Health Check Only

Name:

Description:

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: □ Authorization □ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

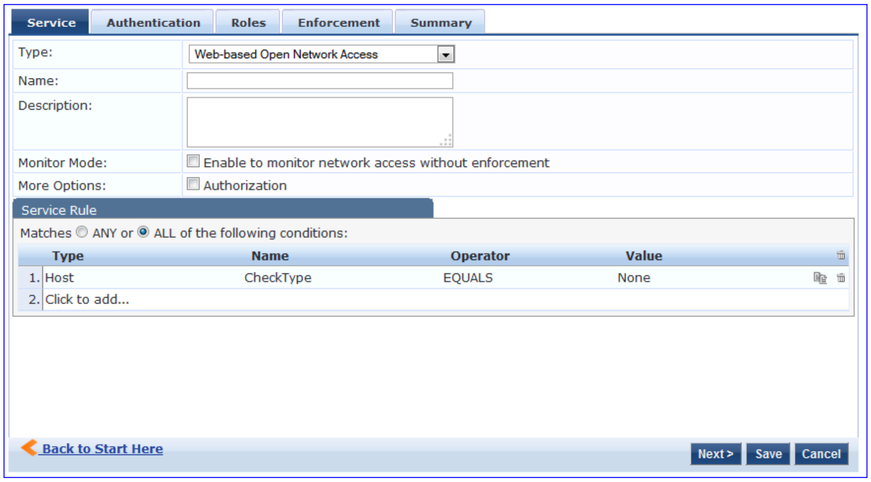
	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ALL	Health
2.	Click to add...			

Web-based Open Network Access

This type of service is similar to other Web-based services, except that health checking is not performed on the endpoint. A "Terms of Service" page (as configured on the Guest Portal page) is presented to the user. Network access is granted when the user clicks the submit action on the page.

Configuration for this service is the same as Web-based Authentication except that Posture options are not available. Refer to Web-based Authentication for more information.

Figure 69: *Web-based Open Network Access Service*



Type: Web-based Open Network Access

Name:

Description:

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: □ Authorization

Service Rule

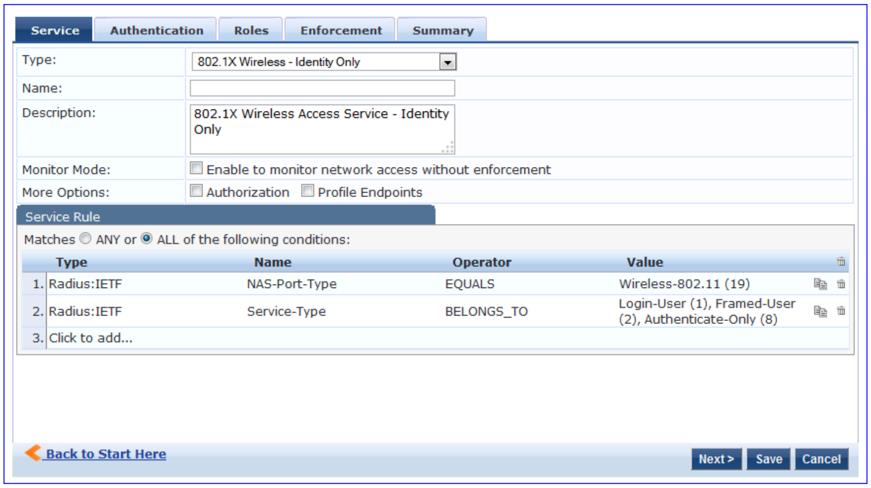
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	EQUALS	None
2.	Click to add...			

802.1X Wireless - Identity Only

Configuration for this type of service is the same as regular 802.1X Wireless Service, except that posture and audit policies are not configurable when you use this template. Refer to "802.1X Wireless" on page 103 for more information.

Figure 70: *802.1X Wireless - Identity Only Service*



Type:	802.1X Wireless - Identity Only
Name:	
Description:	802.1X Wireless Access Service - Identity Only
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Profile Endpoints

Service Rule

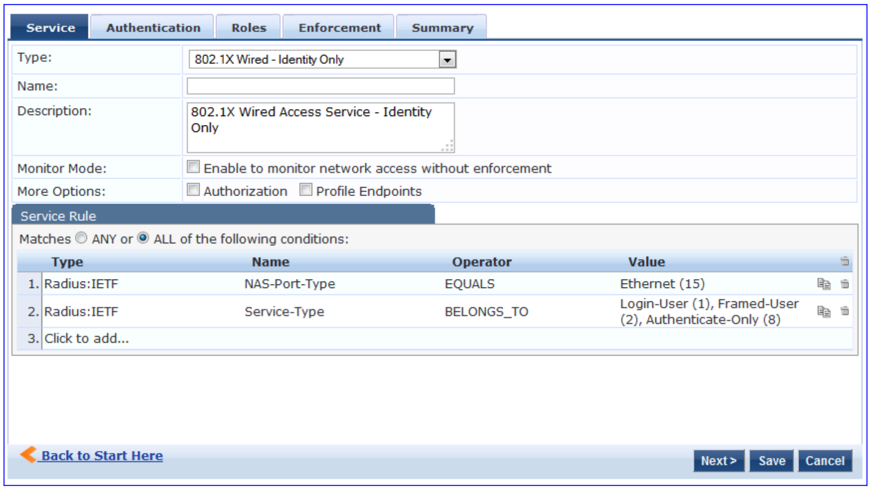
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			

802.1X Wired - Identity Only

Configure this service for clients connecting through an Ethernet LAN, with authentication via IEEE 802.1X. Configuration for the 802.1X Wired - Identity Only service is the same as regular 802.1X Wired, except that posture and audit policies are not configurable when you use this template. Refer to "802.1X Wired" on page 105.

Figure 71: *802.1X Wired - Identity Only Service*



Type:	802.1X Wired - Identity Only
Name:	
Description:	802.1X Wired Access Service - Identity Only
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Click to add...			

RADIUS Enforcement (Generic)

Configure this service for any kind of RADIUS requests.

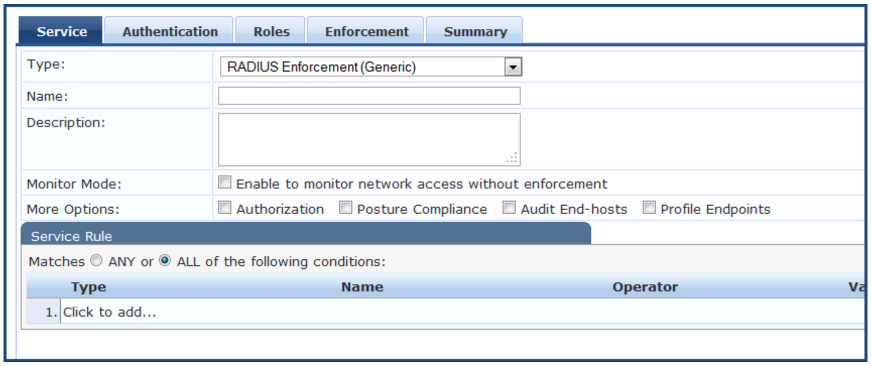
NOTE

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** section.

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.

Figure 72: *RADIUS Enforcement (Generic) Service*



Type: RADIUS Enforcement (Generic)

Name:

Description:

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: □ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Va
1.	Click to add...			

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of its options.

The **Authentication** tab contains options for configuring authentication methods and sources.

- **Authentication Methods:** The authentication methods used for this service depend on the type of authentication methods you choose to deploy. Policy Manager automatically selects the appropriate method for authentication when a user attempts to connect.
- **Authentication Sources**: Specify the Authentication Sources used for this type of service.

For both Authentication Methods and Authentication Sources, you can select one item in the list and use the buttons on the right to:

- Move it up or down.

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged.

- Remove it.
- View its details.
- Modify it. (See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.)

You can also use the links on the right to add a new authentication method or source.

Select **Strip Username Rules** to pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

The Authorization tab is not visible by default. To access it, select the **Authorization** check box on the Services tab.

The Authorization tab is where you select 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:

- The authorization sources associated with the authentication source.
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 131.

To add an authorization source, select it from the drop-down list.

For authorization sources in the list, you can select one and use the buttons on the right to:

- Remove it.
- View its details.
- Modify it.

For more information on configuring authorization sources, see "Adding and Modifying Authentication Methods" on page 131.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Posture Tab

This type of service does not have Posture checking enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box on the Service tab.

You can enable posture checking for this kind of service if you are deploying Policy Manager in a Microsoft NAP or Cisco NAC framework environment, or if you are deploying a Dell hosted captive portal that does posture checks through a dissolvable agent. You can also choose to **Enable auto-remediation of non-compliant end-hosts** and enter the **Remediation URL** of a server resource that can perform remediation action (when a client is quarantined).

NOTE

When you configure posture policies, only those that are configured for the OnGuard Agent are shown in a list of posture policies.

For more information on configuring Posture Polices and Posture Servers, see "Adding a Posture Policy" on page 198 and "Adding and Modifying Posture Servers" on page 230.

Enforcement Tab

The Enforcement tab is where you select an enforcement policy for a service. You must select one.

See "Configuring Enforcement Policies" on page 277 for more information.

Audit Tab

By default, this type of service does not have Audit checking enabled and the Audit tab is not visible. To access it and enable posture checking for this service select the **Audit End-hosts** check box on the Service tab.

- Select an **Audit Server** - either built-in or customized. See "Configuring Audit Servers" on page 233 for audit server configuration steps.
- Select an Audit Trigger Condition:
  - **Always**
  - **When posture is not available**
  - **For MAC authentication requests**. If you select this, then select also one of:
    - For known end-hosts only
    - For unknown end hosts only
    - For all end hosts

Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service.

- Select an **Action after audit**. 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, there should be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways:
  - **No Action:** The audit will not apply policies on the network device after this audit.
  - **Do SNMP bounce:** This option will bounce the switch port or force an 802.1X reauthentication (both done via SNMP).
  - 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.
  - **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.

Profiler Tab

The Profiler tab is not visible by default. To access it, select the **Profile Endpoints** check box on the Services tab.

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.

RADIUS Proxy

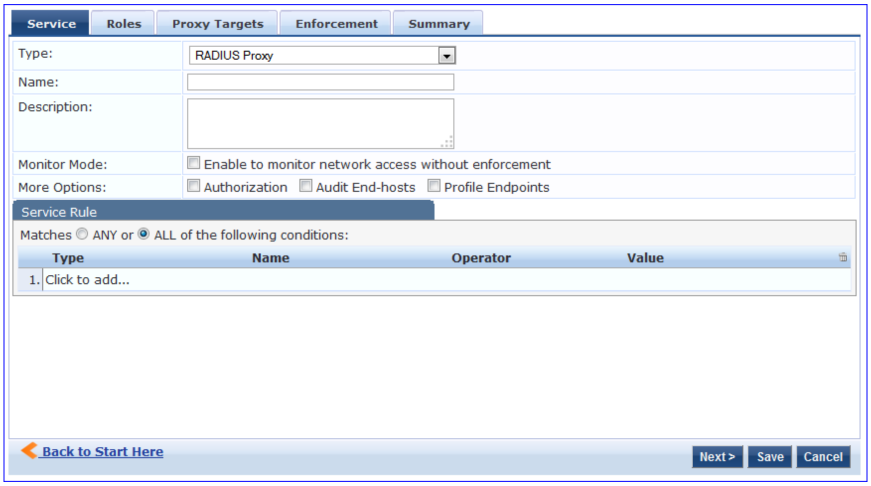
Configure this service for any kind of RADIUS request that needs to be proxied to another RADIUS server (a Proxy Target).

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 for this service is the same as RADIUS Enforcement (Generic), except that you do not configure Authentication or Posture with this service type, but you do configure Proxy Targets – the servers to which requests are proxied. Requests can be dispatched to the proxy targets randomly. Over time these requests are *Load Balanced*. Otherwise, in the Failover mode, requests can be dispatched to the first proxy target in the ordered list of targets, and then subsequently to the other proxy targets if the prior requests failed. When you **Enable proxy for accounting requests** accounting requests are also sent to the proxy targets.

Refer to "RADIUS Enforcement (Generic)" on page 112 for more information.

Figure 73: *RADIUS Proxy Service*



Type:	RADIUS Proxy
Name:	
Description:	
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

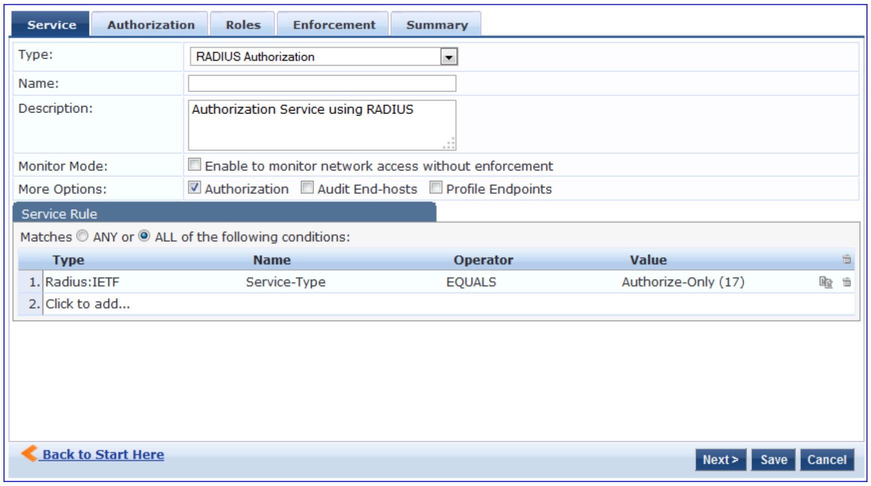
	Type	Name	Operator	Value
1.	Click to add...			

RADIUS Authorization

Configure this service type for services that perform authorization using RADIUS. When selected, the Authorization tab is enabled by default.

Configuration for this service is the same as RADIUS Enforcement (Generic), except that you do not configure Authentication or Posture with this service type. Refer to "RADIUS Enforcement (Generic)" on page 112 for more information.

Figure 74: *RADIUS Authorization Service*



Type:	RADIUS Authorization
Name:	
Description:	Authorization Service using RADIUS
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	☑ Authorization □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	Service-Type	EQUALS	Authorize-Only (17)
2.	Click to add...			

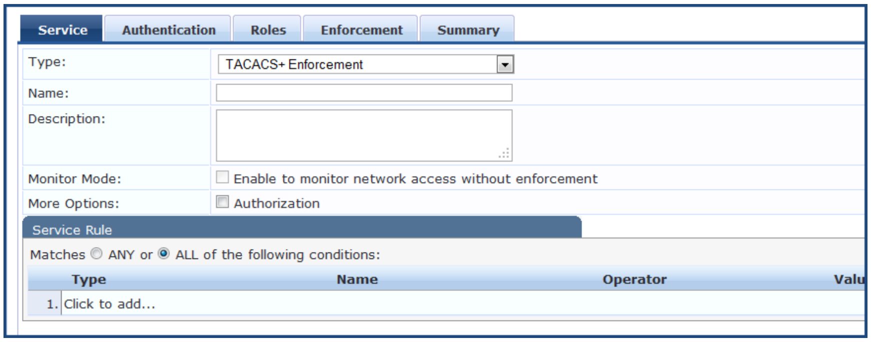
TACACS+ Enforcement

Configure this 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 on the **Service** tab to enable this feature.

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 274 for more information.

Figure 75: *TACACS+ Enforcement Service*



Type:	TACACS+ Enforcement
Name:	
Description:	
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Valu
1.	Click to add...			

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of its options.

Authentication Tab

The **Authentication** tab contains options for configuring authentication sources.

- **Authentication Sources**: Select the Authentication Sources used for this type of service.

You can select one item in the list and use the buttons on the right to:

- Move it up or down.

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged.

- Remove it.
- View its details.
- Modify it. (See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.)

You can also use the links on the right to add a new authentication method or source.

Select **Strip Username Rules** to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

NOTE

There is no authentication method associated with this type of service.

Authorization Tab

The Authorization tab is not visible by default. To access it, select the **Authorization** check box on the Services tab.

The Authorization tab is where you select 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:

- The authorization sources associated with the authentication source.
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 131.

To add an authorization source, select it from the drop-down list.

For authorization sources in the list, you can select one and use the buttons on the right to:

- Remove it.
- View its details.
- Modify it.

For more information on configuring authorization sources, see "Adding and Modifying Authentication Methods" on page 131.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Enforcement Tab

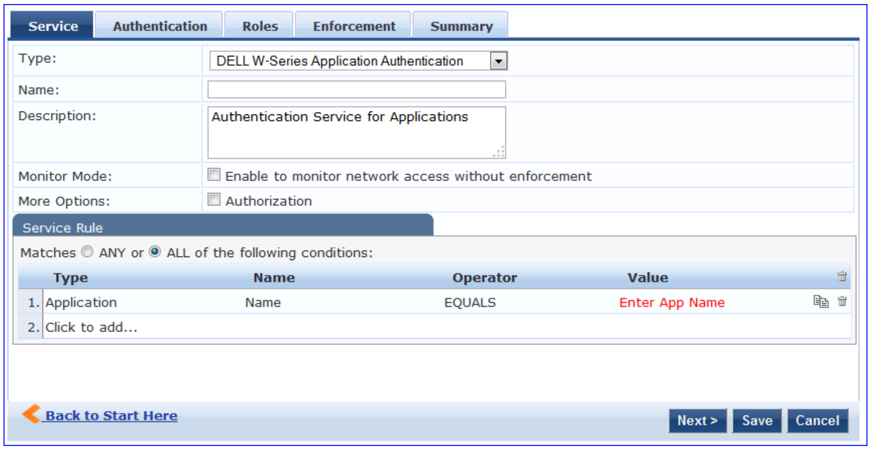
The Enforcement tab is where you select an enforcement policy for a service. You must select one.

See "Configuring Enforcement Policies" on page 277 for more information.

Dell W-Series Application Authentication

This type of service provides authentication and authorization to users of Dell applications: Guest and Insight. "Generic Application Enforcement" on page 265 can be sent to these or other generic applications for authenticating and authorizing the users.

Figure 76: *Dell W-Series Application Authentication*



Type:	DELL W-Series Application Authentication
Name:	
Description:	Authentication Service for Applications
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Application	Name	EQUALS	Enter App Name
2.	Click to add...			

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of its options.

Authentication Tab

The **Authentication** tab contains options for configuring authentication sources.

- **Authentication Sources**: Select the Authentication Sources used for this type of service.

You can select one item in the list and use the buttons on the right to:

- Move it up or down.

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packet exchanged.

- Remove it.
- View its details.
- Modify it.(See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.)

You can also use the links on the right to add a new authentication method or source.

Select **Strip Username Rules** to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

NOTE

There is no authentication method associated with this type of service.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Enforcement Tab

The Enforcement tab is where you select an enforcement policy for a service. You must select one.

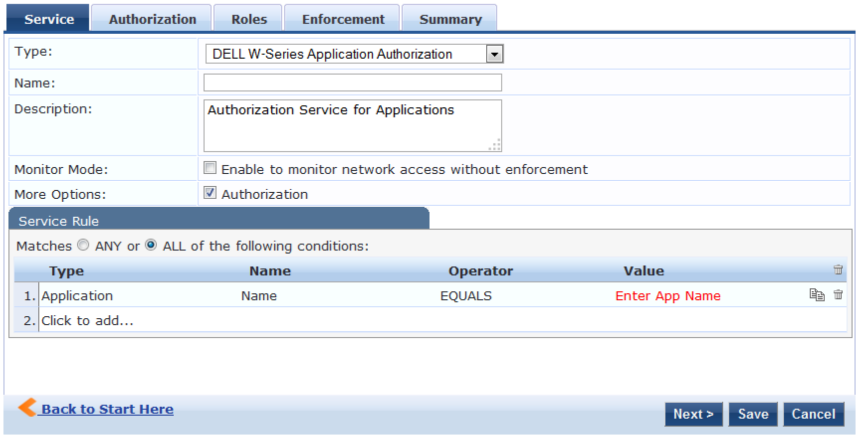
See "Configuring Enforcement Policies" on page 277 for more information.

Dell W-Series Application Authorization

This type of service provides authorization for users of Dell applications: Guest and Insight. "Generic Application Enforcement" on page 265 can be sent to these or other generic applications for authorizing the users.

Configuration options for this service are the same as Dell W-Series Application Authentication, except that authentication options are not available. Refer to "Dell W-Series Application Authentication" on page 118

Figure 77: *Dell W-Series Application Authorization*



Type:	DELL W-Series Application Authorization
Name:	
Description:	Authorization Service for Applications
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Application	Name	EQUALS	Enter App Name
2.	Click to add...			

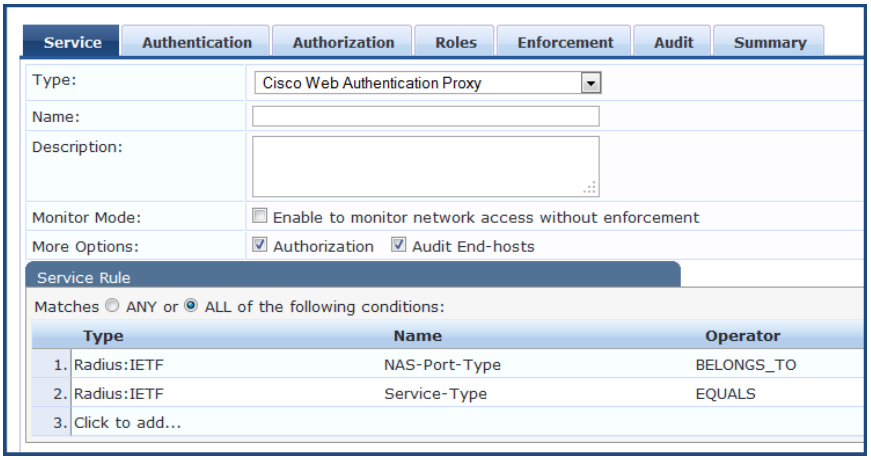
Cisco Web Authentication Proxy

This service is a Web-based authentication service for guests or agentless hosts. The Cisco switch hosts a captive portal, and the portal Web page collects username and password information. The switch then sends a RADIUS request in the form of a 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. Refer to the "Cisco Web Authentication Proxy" on page 120 service type for a description of these tabs.

Figure 78: *Cisco Web Authentication Proxy Service*



Type:	Cisco Web Authentication Proxy
Name:	
Description:	
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☑ Audit End-hosts

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO
2.	Radius:IETF	Service-Type	EQUALS
3.	Click to add...		

Service Tab

The Service tab includes basic information about the service including: Name, Description, and Service Type. When adding a service, enter a **Name** and **Description** that will help you know what the service does without looking at its details. The **Service Type** defines what can be configured.

Select the **Monitor Mode** check box to exclude enforcement.

Select any of the **More Options** check boxes to access that category of configuration options.

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 any of its options.

Authentication Tab

The **Authentication** tab contains options for configuring authentication methods and sources.

- **Authentication Methods:** The authentication methods used for this service depend on the authentication methods you choose to deploy. Policy Manager automatically selects the appropriate method for authentication when a user attempts to connect. In this case, PAP is selected by default.
- **Authentication Sources**: The Authentication Sources used for this type of service.

For both Authentication Methods and Authentication Sources, you can select one item in the list and use the buttons on the right to:

- Move it up or down

  The order of authentication matters. When a client tries to do 802.1X authentication, Policy Manager proposes the first authentication method configured. The client can accept the authentication method proposed by Policy Manager and continue authentication or send a NAK and propose a different authentication method. If this authentication method is also configured, then authentication will proceed. Otherwise authentication will fail.

NOTE

If most of the clients in the network use a particular authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged.

- Remove it.
- View its details.
- Modify it. See "Adding and Modifying Authentication Methods" on page 131 and "Adding and Modifying Authentication Sources" on page 149.

You can also use the links on the right to add a new authentication method or source.

Select **Strip Username Rules** to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Tab

The Authorization tab is not visible by default. To access it, select the **Authorization** check box on the Services tab.

The Authorization tab is where you select 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:

- The authorization sources associated with the authentication source.
- The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 131.

To add an authorization source, select it from the drop-down list.

For authorization sources in the list, you can select one and use the buttons on the right to:

- Remove it.
- View its details.
- Modify it.

For more information on configuring authorization sources, see "Adding and Modifying Authentication Methods" on page 131.

Roles Tab

To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, see "Configuring a Role Mapping Policy" on page 189.

Enforcement Tab

The Enforcement tab is where you select an enforcement policy for a service. You must select one.

See "Configuring Enforcement Policies" on page 277 for more information.

Audit Tab

By default, this type of service does not have Audit checking enabled and the Audit tab is not visible. To access it and enable posture checking for this service select the **Audit End-hosts** check box on the Service tab.

- Select an **Audit Server** - either built-in or customized. See "Configuring Audit Servers" on page 233 for audit server configuration steps.
- Select an Audit Trigger Condition:
  - **Always**
  - **When posture is not available**
  - **For MAC authentication requests**. If you select this, then select also one of:
    - For known end-hosts only
    - For unknown end hosts only
    - For all end hosts

Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service.

- Select an **Action after audit**. 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, there should be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways:
  - **No Action:** The audit will not apply policies on the network device after this audit.
  - **Do SNMP bounce:** This option will bounce the switch port or force an 802.1X reauthentication (both done via SNMP).
  - 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.
  - **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.

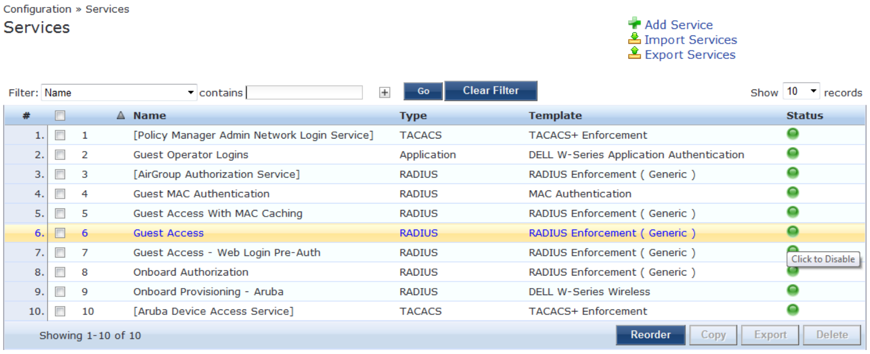
Services

The Services page shows the current list and order of services that CPPM follows during authentication and authorization. You can use the default service types as configured, or you can add additional services. Services included in "[ ]" indicate default services.

For more information, see:

- "Adding Services" on page 123
- "Modifying Services" on page 126
- "Reordering Services" on page 128

Figure 79: *Service Listing Page*



Configuration » Services

Services

Filter: Name contains

Show 10 records

#	□		Name	Type	Template	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	□	2	Guest Operator Logins	Application	DELL W-Series Application Authentication	●
3.	□	3	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
4.	□	4	Guest MAC Authentication	RADIUS	MAC Authentication	●
5.	□	5	Guest Access With MAC Caching	RADIUS	RADIUS Enforcement (Generic)	●
6.	□	6	Guest Access	RADIUS	RADIUS Enforcement (Generic)	●
7.	□	7	Guest Access - Web Login Pre-Auth	RADIUS	RADIUS Enforcement (Generic)	●
8.	□	8	Onboard Authorization	RADIUS	RADIUS Enforcement (Generic)	●
9.	□	9	Onboard Provisioning - Aruba	RADIUS	DELL W-Series Wireless	●
10.	□	10	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●

Showing 1-10 of 10

Table 42: *Services page*

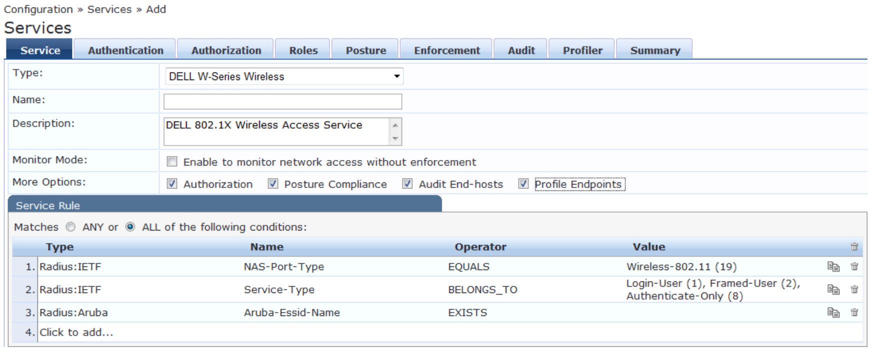
Parameter	Description
Add Service:	Add a service.
Import Services:	Import previously exported services.
Export Service:	Export all currently defined services, including all associated policies.
Filter:	Filter the service listing by specifying values for different listing fields: ● Name ● Type ● Template ● Status
Status:	The status displays in the last column of the table. A green/red icon indicates enabled/disabled state. Clicking on the icon allows you 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.
Reorder:	The Reorder button below the table is used for reorder services.
Copy:	Create a copy of the service. An instance of the name prefixed with Copy_of_ is created.
Export:	Export the selected services.
Delete:	Delete the selected services.

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 Service** in the upper-right corner to add a new service.

Figure 80: *Add Service Page (all options enabled)*



Type: DELL W-Series Wireless

Name:

Description: DELL 802.1X Wireless Access Service

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: ☑ Authorization ☑ Posture Compliance ☑ Audit End-hosts ☑ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

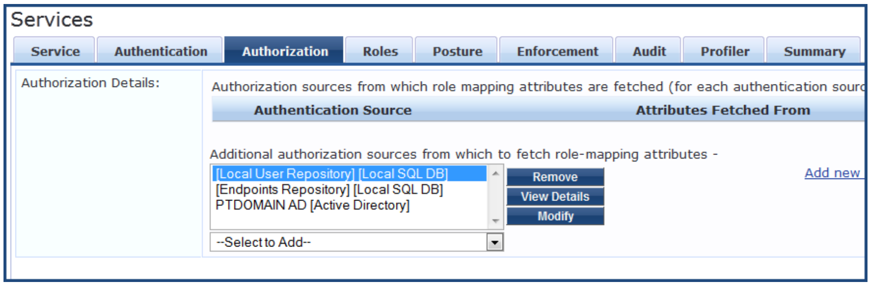
	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EXISTS	
4.	Click to add...			

The **Add Service** tab includes the following fields.

Table 43: *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 Dictionary** (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 when the request type is RADIUS. - Any other supported namespace. See "Rules Editing and Namespaces" on page 445 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 from scratch.
Name	Label for a Service.
Description	Description for a Service (optional).

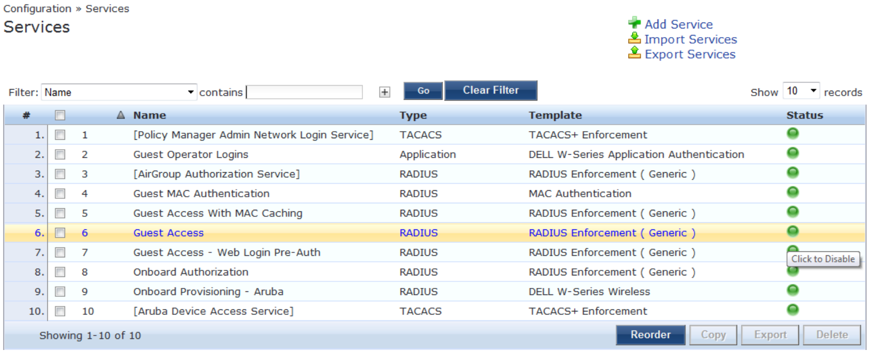
Table 43: *Service Page (General Parameters) (Continued)*

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 for 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. Finally, specify the Posture Server from the drop-down list or add a new server by clicking the **Add new Posture Server** link.  Services Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Authorization Details: Authentication Source Attributes Fetched From Remove View Details Modify Add new Authorization sources from which role mapping attributes are fetched (for each authentication sourc Additional authorization sources from which to fetch role-mapping attributes - [Local User Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] PTDOMAIN AD [Active Directory] --Select to Add-- ● **Audit End-hosts:** Select an Audit Server, either built-in or customized. Refer to "Configuring Audit Servers" on page 233 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, there should be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways: ■ **No Action:** The audit will not apply policies on the network device after this audit. ■ **Do SNMP bounce:** This option will bounce the switch port or force an 802.1X re authentication (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. ■ **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager. ● 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.

Figure 81: *Service Listing Page*



Configuration » Services

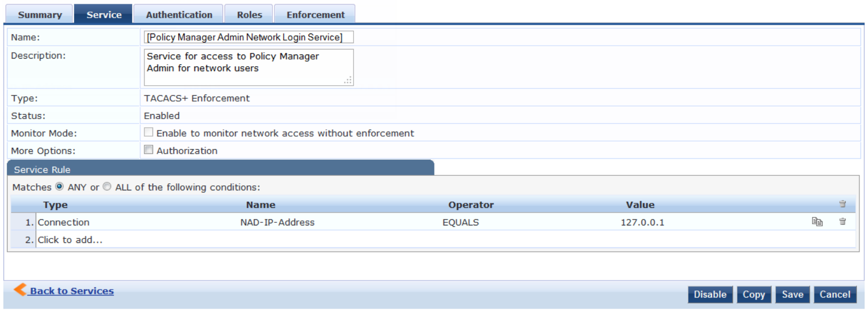
Services

#		Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	2	Guest Operator Logins	Application	DELL W-Series Application Authentication	●
3.	3	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
4.	4	Guest MAC Authentication	RADIUS	MAC Authentication	●
5.	5	Guest Access With MAC Caching	RADIUS	RADIUS Enforcement (Generic)	●
6.	6	Guest Access	RADIUS	RADIUS Enforcement (Generic)	●
7.	7	Guest Access - Web Login Pre-Auth	RADIUS	RADIUS Enforcement (Generic)	● Click to Disable
8.	8	Onboard Authorization	RADIUS	RADIUS Enforcement (Generic)	●
9.	9	Onboard Provisioning - Aruba	RADIUS	DELL W-Series Wireless	●
10.	10	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●

Showing 1-10 of 10

To modify an existing service, click on its name 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.

Figure 82: *Services Configuration*



Name:	[Policy Manager Admin Network Login Service]
Description:	Service for access to Policy Manager Admin for network users
Type:	TACACS+ Enforcement
Status:	Enabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization

Service Rule

Matches ● ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	NAD-IP-Address	EQUALS	127.0.0.1
2.	Click to add...			

The following fields are available on the **Service** tab.

Table 44: *Service Page (General Parameters)*

Parameter	Description
Name	Enter or modify the label for a service.
Description	Enter or modify the service description (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. This button will 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 will 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.

Table 44: *Service Page (General Parameters) (Continued)*

Parameter	Description
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.

Table 45: *Service Page (Rules Editor)*

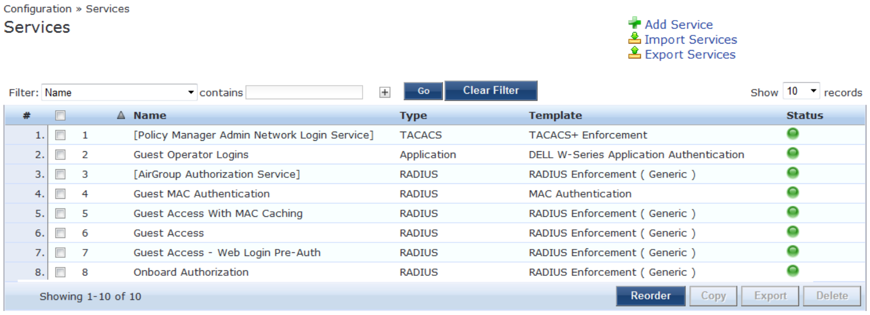
Label	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on Service type. When working with service rules, you can select from the following namespace dictionaries: ● **Application**: The type of application for this 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, 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 Dictionary** (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 when the request type is RADIUS. ● Any other supported namespace. See "Rules Editing and Namespaces" on page 445 for an exhaustive list of namespaces and their descriptions.
Name (of attribute)	Drop-down list of attributes present in the selected namespace.
Operator	Drop-down list of context-appropriate (with respect to the attribute) operators. See "Rules Editing and Namespaces" on page 445 for an exhaustive list of operators and their descriptions.
Value of attribute	Depending on attribute data type, this can be a free-form (one or many lines) edit box, a drop-down list, or a time/date widget.

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 Reordering Services form.

Figure 83: *Service Reorder Button*



Configuration » Services

Services

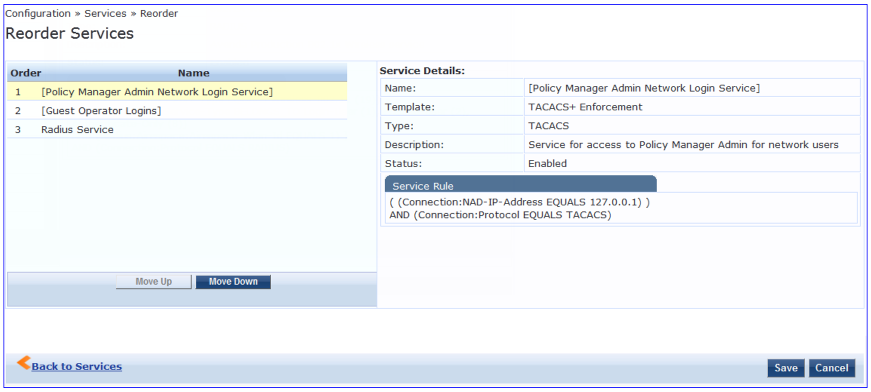
Add Service
Import Services
Export Services

Filter: Name contains Go Clear Filter Show 10 records

#	☐		Name	Type	Template	Status
1.	☐	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	☐	2	Guest Operator Logins	Application	DELL W-Series Application Authentication	●
3.	☐	3	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
4.	☐	4	Guest MAC Authentication	RADIUS	MAC Authentication	●
5.	☐	5	Guest Access With MAC Caching	RADIUS	RADIUS Enforcement (Generic)	●
6.	☐	6	Guest Access	RADIUS	RADIUS Enforcement (Generic)	●
7.	☐	7	Guest Access - Web Login Pre-Auth	RADIUS	RADIUS Enforcement (Generic)	●
8.	☐	8	Onboard Authorization	RADIUS	RADIUS Enforcement (Generic)	●

Showing 1-10 of 10

Figure 84: *Reordering Services*



Configuration » Services » Reorder

Reorder Services

Order	Name
1	[Policy Manager Admin Network Login Service]
2	[Guest Operator Logins]
3	Radius Service

Service Details:

Name:	[Policy Manager Admin Network Login Service]
Template:	TACACS+ Enforcement
Type:	TACACS
Description:	Service for access to Policy Manager Admin for network users
Status:	Enabled

Service Rule

((Connection:NAD-IP-Address EQUALS 127.0.0.1))
AND (Connection:Protocol EQUALS TACACS)

Table 46: *Reordering Services*

Label	Description
Move Up/Move Down:	Select a service from the list and move it up or down
Save:	Save the reorder operation
Cancel:	Cancel the reorder operation

Authentication and Authorization

As the 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 129
- "Configuring Authentication Components" on page 130
- "Adding and Modifying Authentication Methods" on page 131
- "Adding and Modifying Authentication Sources" on page 149

Authentication and Authorization Architecture and Flow

Policy Manager divides the architecture of authentication and authorization into three components: Authentication Methods, Authentication Source, and 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 NAKs the last method, 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.

NOTE

An Authentication Method is only configurable for some service types (Refer to "Policy Manager Service Types" on page 99). 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 is to collect role mapping attributes from the authorization sources.

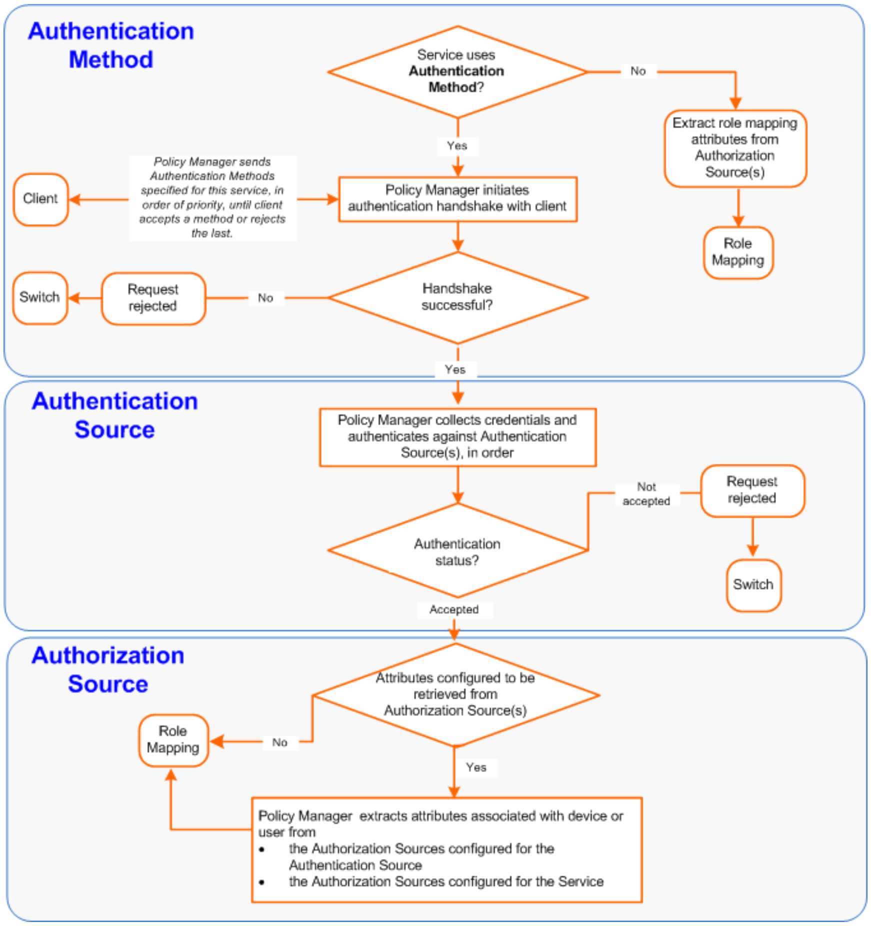
Where no authentication source is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this Service.

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 85: *Authentication and Authorization Flow of Control*


Authentication Method
Service uses Authentication Method?
No
Extract role mapping attributes from Authorization Source(s)
Role Mapping
Yes
Policy Manager sends Authentication Methods specified for this service, in order of priority, until client accepts a method or rejects the last.
Client
Policy Manager initiates authentication handshake with client
Switch
Request rejected
No
Handshake successful?
Yes
Authentication Source
Policy Manager collects credentials and authenticates against Authentication Source(s), in order
Not accepted
Request rejected
Authentication status?
Switch
Accepted
Authorization Source
Attributes configured to be retrieved from Authorization Source(s)
Role Mapping
No
Yes
Policy Manager extracts attributes associated with device or user from
the Authorization Sources configured for the Authentication Source
the Authorization Sources configured for the Service

Configuring Authentication Components

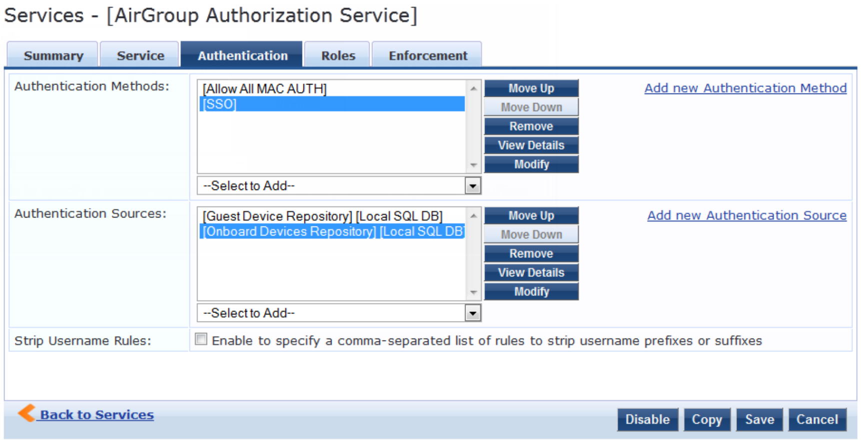
The following summarizes the methods for configuring authentication:

For an existing Service, you can add or modify an authentication method or source by opening the Service (**Configuration** > **Services**, then select), then opening the **Authentication** tab.

For a new Service, the Policy Manager wizard automatically opens the **Authentication** tab for configuration.

Outside of the context of a particular service, you can open an authentication method or source: **Configuration** > **Authentication** > **Methods or Configuration** > **Authentication** > **Sources**.

Figure 86: *Authentication Components*



Services - [AirGroup Authorization Service]

Authentication Methods: [Allow All MAC AUTH]
[SSO] --Select to Add--

Authentication Sources: [Guest Device Repository] [Local SQL DB]
[Onboard Devices Repository] [Local SQL DB] --Select to Add--

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

From the **Authentication** tab of a service, you can configure three features of authentication:

Table 47: *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 launches 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. Refer to "Adding and Modifying Authentication Methods" on page 131 for information about Authentication Methods. **NOTE:** An Authentication Method is only configurable for some service types. Refer to "Policy Manager Service Types" on page 99 for more information.
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 launches 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. Refer to "Adding and Modifying Authentication Sources" on page 149 for additional information about Authentication Sources.
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 and non-EAP, tunneled and non-tunneled, methods.

NOTE

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

Table 48: *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. If the MAC_AUTH method is selected, Policy Manager makes internal checks to verify that the request is indeed a **MAC_Authentication** request (and not a spoofed request).

NOTE

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

From the **Services** page (**Configuration** > **Services**), you can configure authentication for a new service (as part of the flow of the **Add Service** wizard), or modify an existing authentication method directly (**Configuration** > **Authentication** > **Methods**, then click on its name in the Authentication Methods listing).

If you click **Add New Authentication Method** from any of these locations, Policy Manager displays the **Add Authentication Method** popup.

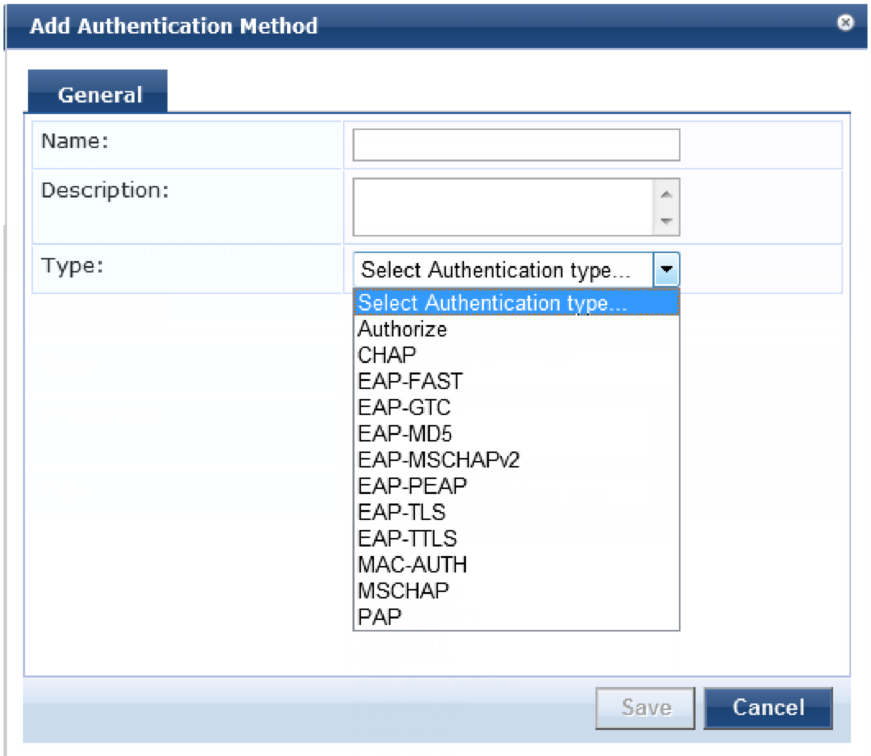
Depending on the **Type** selected, different tabs and fields appear.

For more information, see:

- "Authorize" on page 133
- "CHAP and EAP-MD5" on page 134
- "EAP-FAST " on page 136
- "EAP-GTC" on page 141
- "EAP-MSCHAPv2" on page 142
- "EAP-PEAP" on page 142

- "EAP-TLS" on page 144
- "EAP-TTLS" on page 146
- "MAC-AUTH" on page 147
- "MSCHAP" on page 148
- "PAP" on page 149

Figure 87: *Add Authentication Method dialog box*



Add Authentication Method

General

Name:

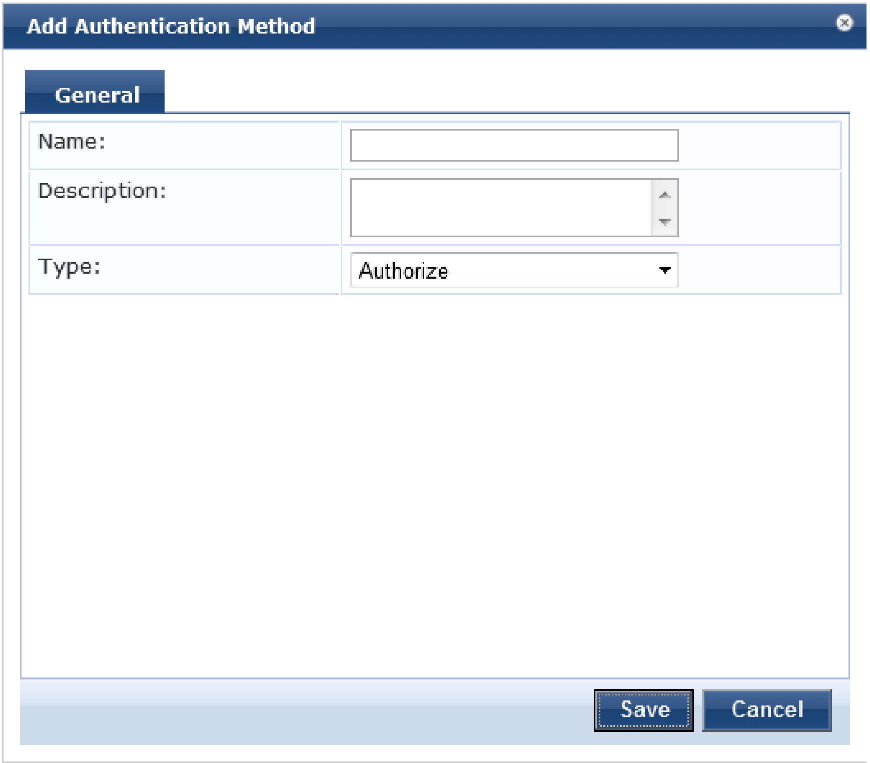
Description:

Type: Select Authentication type...

Authorize

This is an authorization-only method that you can add with a custom name.

Figure 88: *Add Authentication General tab*



Add Authentication Method

General

Name:

Description:

Type: Authorize

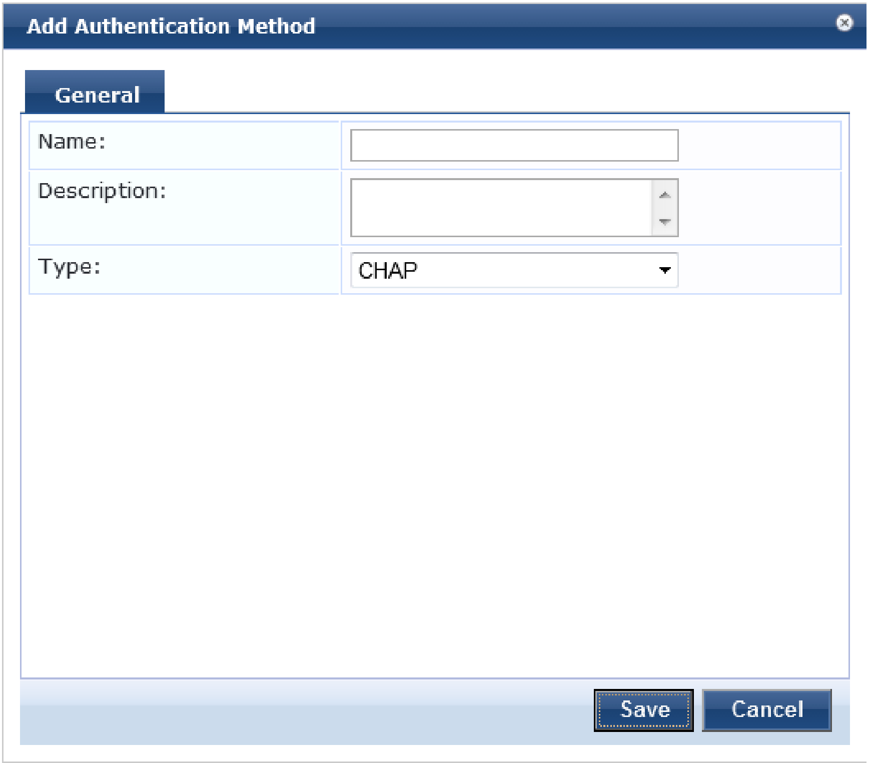
Table 49: *Add Authentication General Tab Parameters*

Parameter	Description
Name/Description:	Freeform label and description.
Type:	In this context, always **Authorize.**

CHAP and EAP-MD5

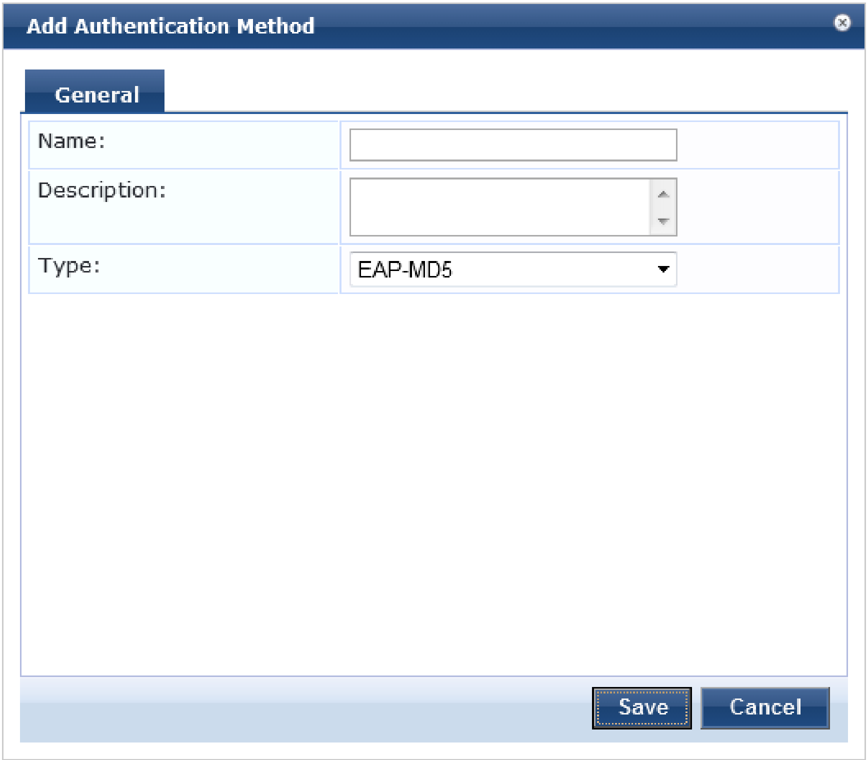
Policy Manager is preconfigured with CHAP and EAP-MD5 authentication methods, You can add CHAP and EAP-MD5 methods, and associate the new methods with a *Service*.

Figure 89: *Add Authentication Method CHAP General tab*



Name:	
Description:	
Type:	CHAP

Figure 90: *Add Authentication Method EAP-MD5 General tab*



Name:	
Description:	
Type:	EAP-MD5

Table 50: *Add Authentication Methods for CHAP and EAP-MD5 General tab Parameters*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **CHAP** or **EAP-MD5**.

EAP-FAST

The EAP-FAST method contains four tabs: General, Inner Methods, PACs, PAC Provisioning.

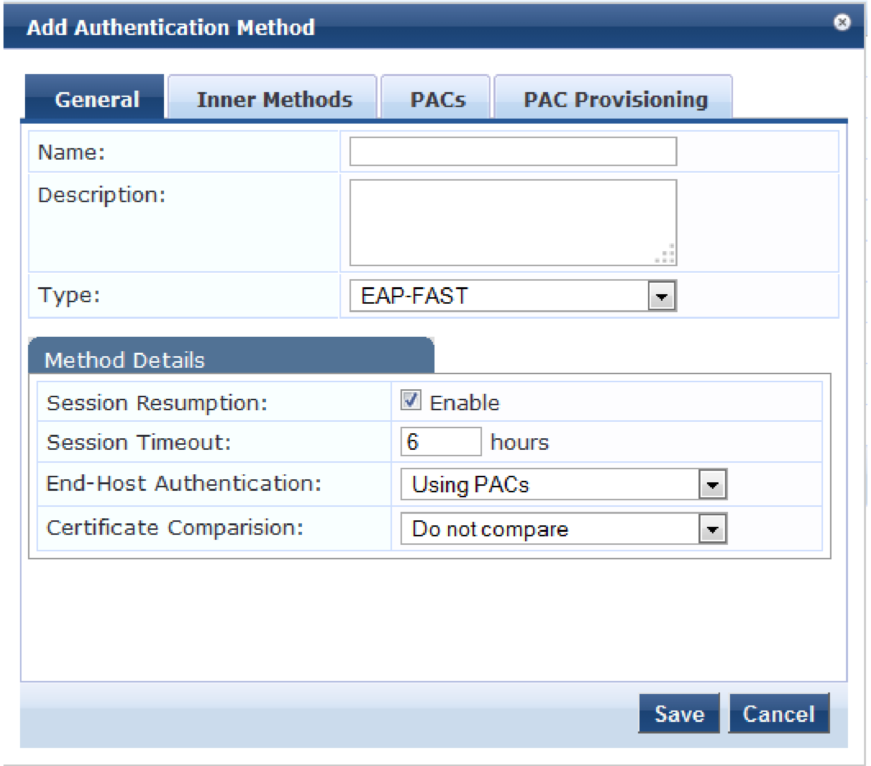
NOTE

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.

Figure 91: *Add Authentication EAP-FAST General tab*



Name:

Description:

Type: EAP-FAST

Session Resumption: ☑ Enable

Session Timeout: 6 hours

End-Host Authentication: Using PACs

Certificate Comparision: Do not compare

Table 51: *EAP_FAST General tab Parameters*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **EAP_FAST**.

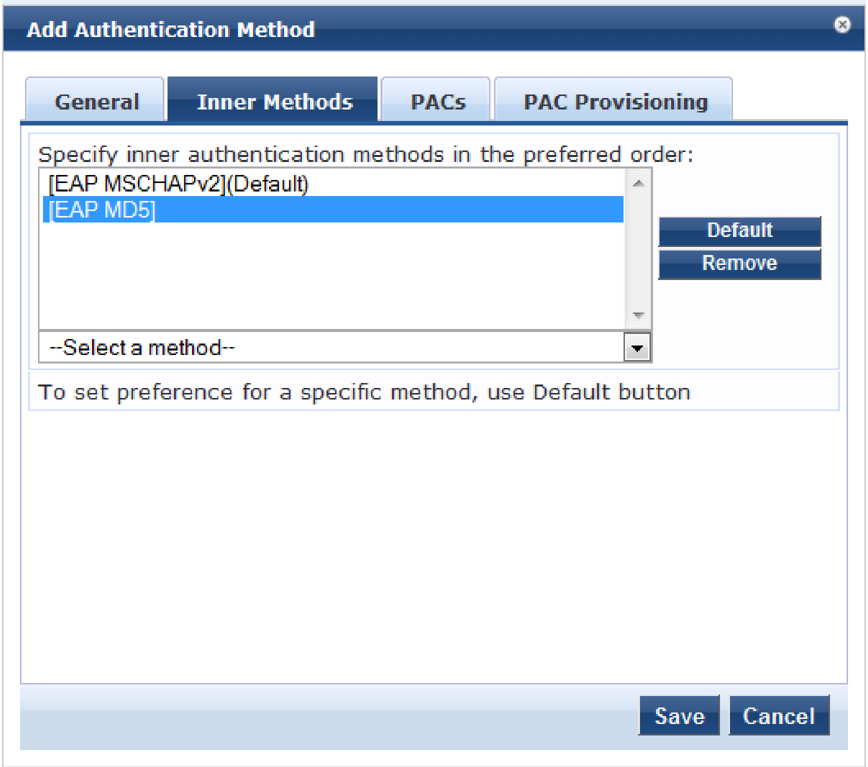
Table 51: *EAP_FAST General tab Parameters (Continued)*

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.
End-Host Authentication	Refers to establishing the EAP-Fast Phase 1 Outer tunnel: ● Choose **Using PACs** to use a strong shared secret. ● Choose **Using Client Certificate** to use a certificate. **NOTE:** The PACs and PAC Provisioning tabs are only available when Using PACs is selected.
Certificate Comparison	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 Distinguished Name (DN)**, **Compare Common Name (CN)**, **Compare Subject Alternate Name (SAN)**, or **Compare CN or SAN**. ● To perform a binary comparison of the *stored* (in the end-host record in Active Directory or another LDAP-compliant directory) and *presented* certificates, choose **Compare Binary**.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the EAP-FAST method

Figure 92: *Add Authentication Inner Methods tab*



Specify inner authentication methods in the preferred order:

[EAP MSCHAPv2](Default)
[EAP MD5]

--Select a method--

To set preference for a specific method, use Default button

To append an inner method to the displayed list, select it from the drop-down list, then click **Add**. The list can contain multiple inner methods, which Policy Manager will send, in priority order, until negotiation succeeds.

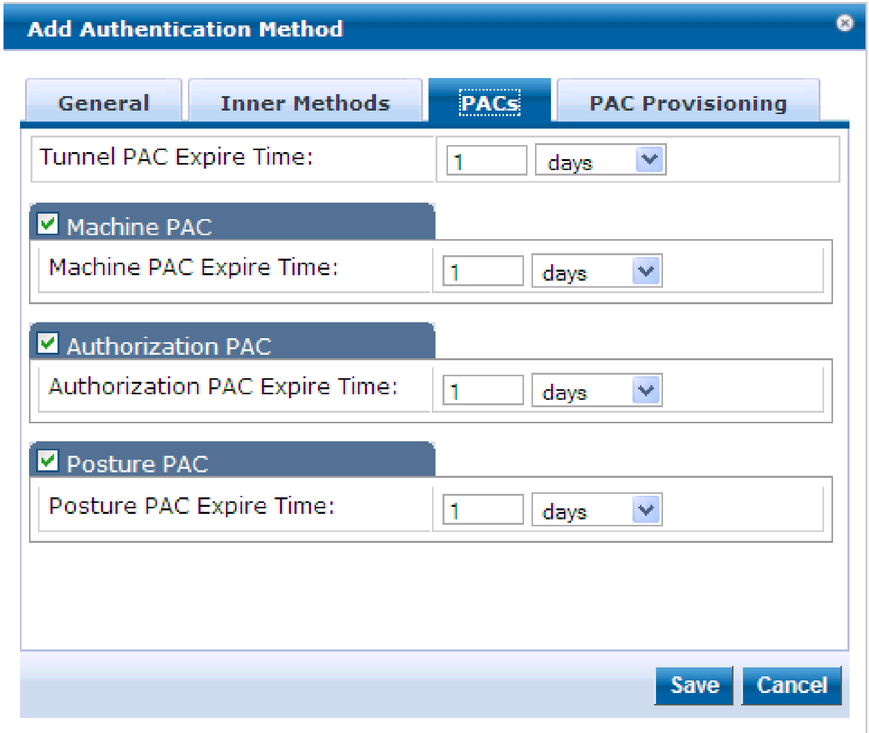
To remove an inner method from the displayed list, select the method and click **Remove.**

To set an inner method as the default (the method tried first), select it and click **Default.**

PACs tab

The Add Authentication Method **PACs** tab enables or disables PAC types:

Figure 93: *EAP_FAST PACs Tab*



Tunnel PAC Expire Time: 1 days

☑ Machine PAC

Machine PAC Expire Time: 1 days

☑ Authorization PAC

Authorization PAC Expire Time: 1 days

☑ Posture PAC

Posture PAC Expire Time: 1 days

To provision a Tunnel PAC on the end-host after initial successful machine authentication, specify the **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. During authentication, Policy Manager can use the Tunnel PAC shared secret to create the outer EAP-FAST tunnel.

To provision a Machine PAC on the end-host after initial successful machine authentication, select the **Machine PAC** check box. 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).

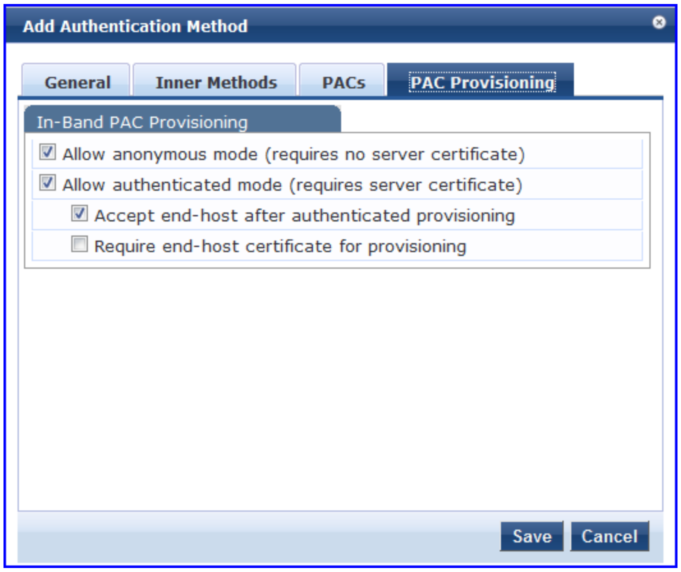
To provision an authorization PAC upon successful user authentication, select the **Authorization PAC** check box. Authorization PAC results from a prior user authentication and authorization. After presentation with a valid Authorization PAC, Policy Manager skips the inner user authentication handshake 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, rather than months and years).

To provision a posture PAC upon successful posture validation, select the **Posture PAC** check box. 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 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, rather than months and years).

PAC Provisioning tab

The **PAC Provisioning** tab controls anonymous and authenticated modes:

Figure 94: *EAP_FAST PAC Provisioning tab*



☑ Allow anonymous mode (requires no server certificate)

☑ Allow authenticated mode (requires server certificate)

☑ Accept end-host after authenticated provisioning

☐ Require end-host certificate for provisioning

Table 52: *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 Policy Manager provisions 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 in Allow Authenticated Mode *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.	

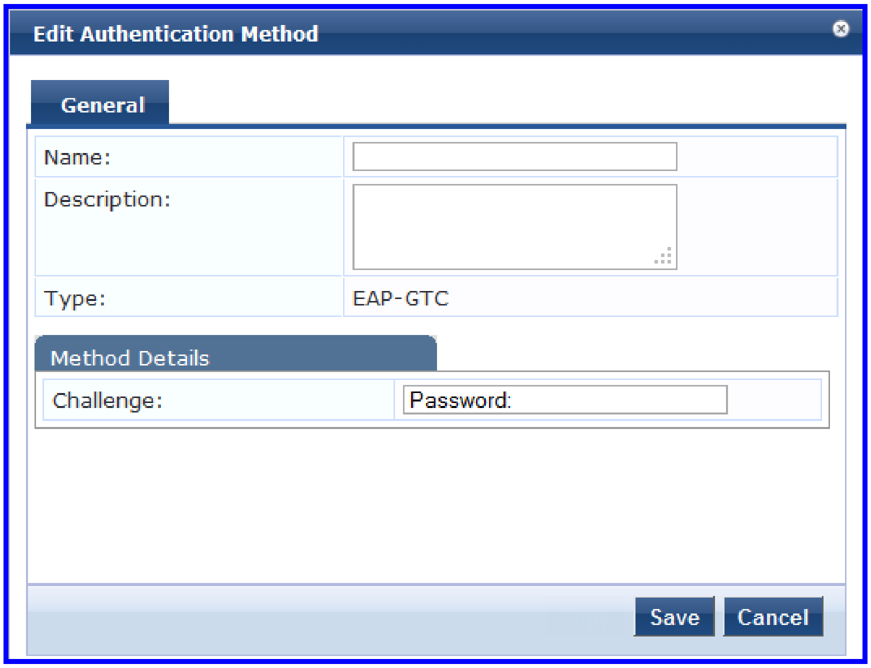
Table 52: *EAP_FAST PAC Provisioning tab Parameters (Continued)*

Parameter	Description	Considerations
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 reauthenticates using the newly provisioned PAC. When enabled, Policy Manager accepts the end-host authentication in the provisioning 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 one tab: General. This tab labels the method, defines session details, and configures the challenge password.

Figure 95: *EAP-GTC General Tab*



Edit Authentication Method

General

Name:	
Description:	
Type:	EAP-GTC

Method Details

Challenge:	Password:

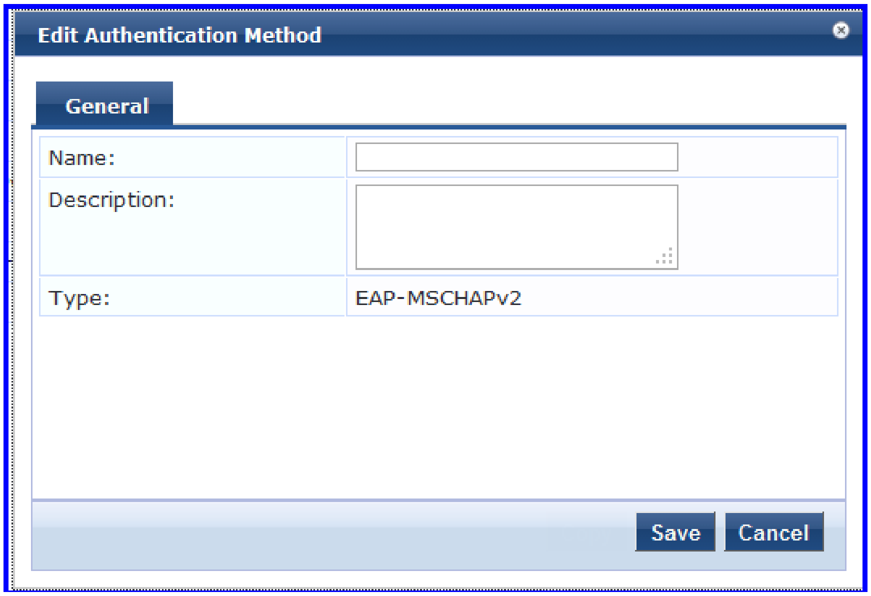
Table 53: *EAP-GTC General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **EAP-GTC**.
Challenge	Specify an optional password.

EAP-MSCHAPv2

The EAP-MSCHAPv2 method contains one tab: General. This tab labels the method and defines session details.

Figure 96: *EAP-MSCHAPv2 General Tab*



Name:	
Description:	
Type:	EAP-MSCHAPv2

Table 54: *EAP-MSCHAPv2 General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **EAP-MSCHAPv2**.

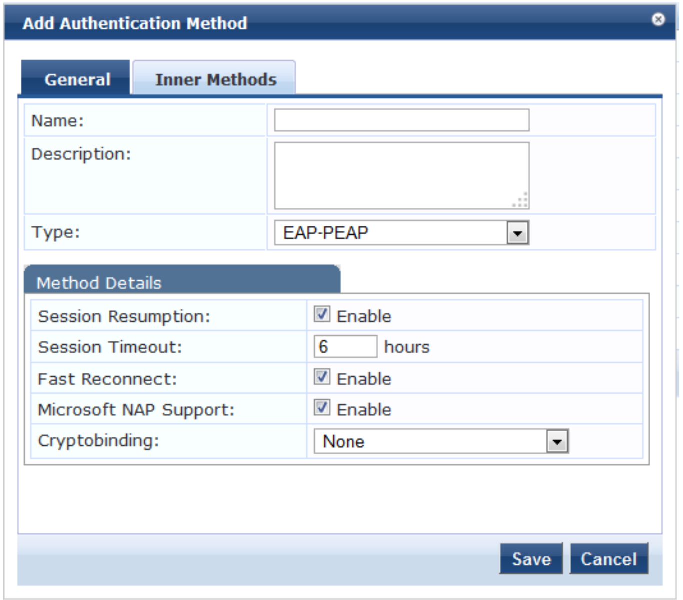
EAP-PEAP

The EAP-PEAP method contains two tabs: General and Inner Methods.

General Tab

The **General** tab labels the method and defines session details.

Figure 97: *EAP-PEAP General Tab*



Name:

Description:

Type: EAP-PEAP

Method Details

Session Resumption: ☑ Enable

Session Timeout: 6 hours

Fast Reconnect: ☑ Enable

Microsoft NAP Support: ☑ Enable

Cryptobinding: None

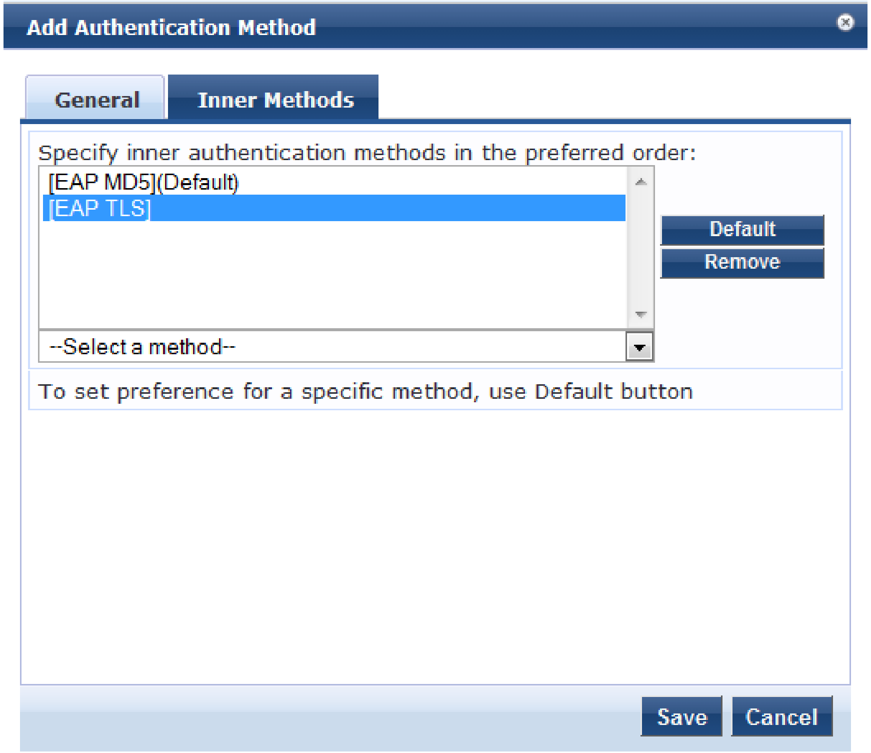
Table 55: *EAP-PEAP General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **EAP-PEAP.**
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 fast reconnect to work, session resumption must be enabled.
Microsoft NAP Support	Enable while Policy Manager establishes the protected PEAP tunnel with a Microsoft NAP-enabled client. If enabled, Policy Manager prompts the client for Microsoft Statement of Health (SoH) credentials.
Cryptobinding	Enabling the cryptobinding setting ensures an extra level of protection for PEAPv0 exchanges. It ensures that the PEAP client and PEAP server (Policy Manager) participated in both the outer and inner handshakes. This is currently valid only for the client PEAP implementations in Windows 7, Windows Vista and Windows XP SP3.

Inner Methods Tab

The **Inner Methods** Tab controls the inner methods for the EAP-PEAP method:

Figure 98: *EAP-PEAP Inner Methods Tab*



Specify inner authentication methods in the preferred order:

[EAP MD5](Default)
[EAP TLS]

--Select a method--

To set preference for a specific method, use Default button

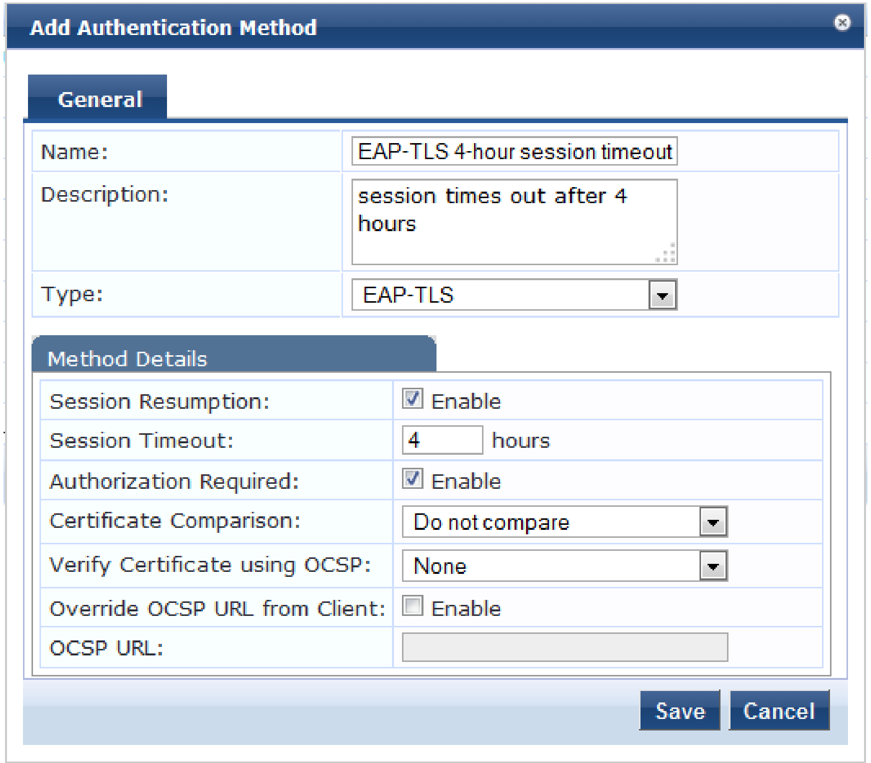
Select any method available in the current context from the drop-down list. Additional functions available in this tab include:

- To append an inner method to the displayed list, select it from the drop-down list, then click **Add**. The list can contain multiple inner methods, which Policy Manager will send, 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 one tab: General. This tab labels the method and defines session details.

Figure 99: *EAP-TLS General Tab*



Name:	EAP-TLS 4-hour session timeout
Description:	session times out after 4 hours
Type:	EAP-TLS
Session Resumption:	☑ Enable
Session Timeout:	4 hours
Authorization Required:	☑ Enable
Certificate Comparison:	Do not compare
Verify Certificate using OCSP:	None
Override OCSP URL from Client:	□ Enable
OCSP URL:	

Table 56: *EAP-TLS General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **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	How long (in hours) to retain cached EAP-TLS sessions.
Authorization Required	Specify whether to perform an authorization check.
Certificate Comparison	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 Distinguished Name (DN)**, **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**.

Table 56: *EAP-TLS General Tab (Continued)*

Parameter	Description
Verify Certificate using OCSP	Select **Optional** or **Required** if the certificate should be verified by the Online Certificate Status Protocol (OCSP). Select **None** to not verify the certificate.
Override OCSP URL from the Client	Select this option if you want to use a different URL for OCSP. After this is enabled, you can enter a new URL in the OCSP URL field.
OCSP URL	If Override OCSP URL from the Client is enabled, then enter the replacement URL here.

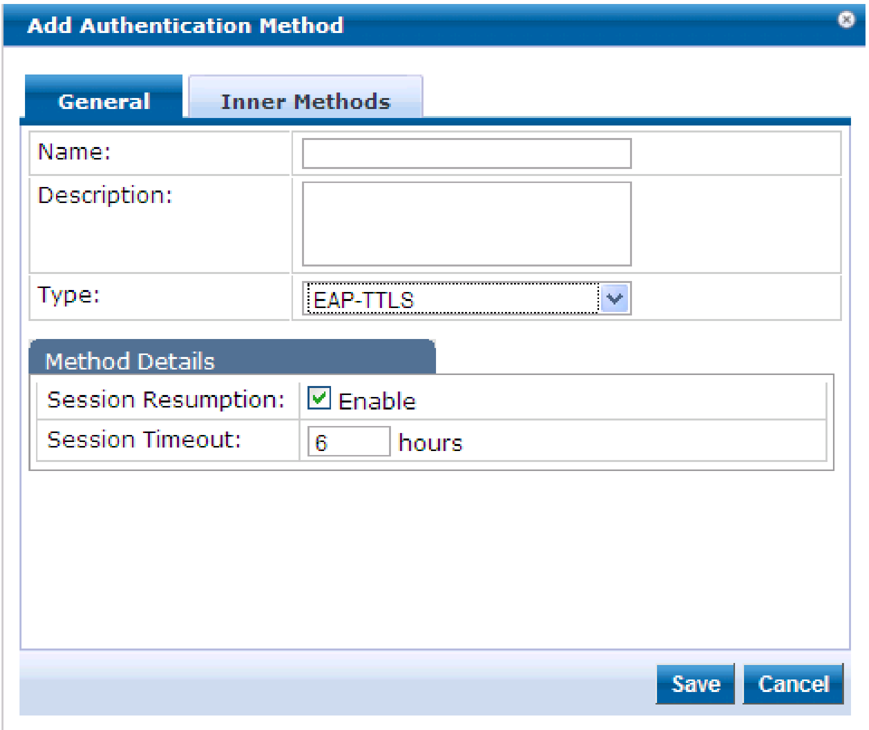
EAP-TTLS

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

General Tab

The **General** tab labels the method and defines session details.

Figure 100: *EAP-TTLS General Tab*



Name:

Description:

Type: EAP-TTLS

Method Details

Session Resumption: ☑ Enable

Session Timeout: 6 hours

Table 57: *EAP-TTLS General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **EAP-TTLS**.

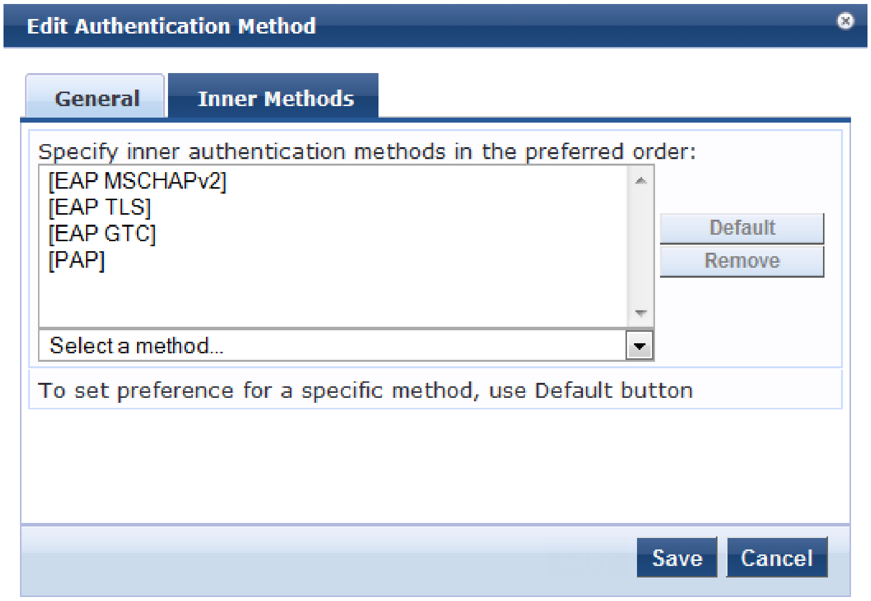
Table 57: *EAP-TTLS General Tab (Continued)*

Parameter	Description
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	How long (in hours) to retain cached EAP-TTLS sessions.

Inner Methods Tab

The **Inner Methods** tab controls the inner authentication methods for the EAP-TTLS method:

Figure 101: *EAP_TTLS Inner Methods Tab*



Specify inner authentication methods in the preferred order:

[EAP MSCHAPv2]
[EAP TLS]
[EAP GTC]
[PAP]

Select a method...

To set preference for a specific method, use Default button

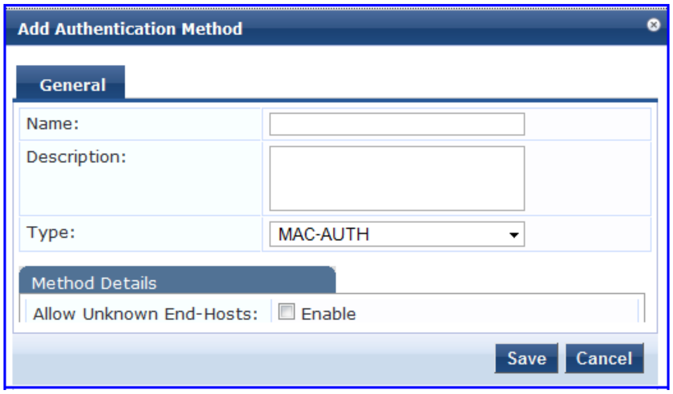
Select any method available from the drop-down list. Additional functions available in this tab include:

- To append an inner method to the displayed list, select it from the drop-down list, then click **Add**. The list can contain multiple inner methods, which Policy Manager will send 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**.

MAC-AUTH

The MAC-AUTH method contains one tab: General. This tab labels the method and defines session details.

Figure 102: *MAC-AUTH General Tab*



Name:

Description:

Type: MAC-AUTH

Allow Unknown End-Hosts: □ Enable

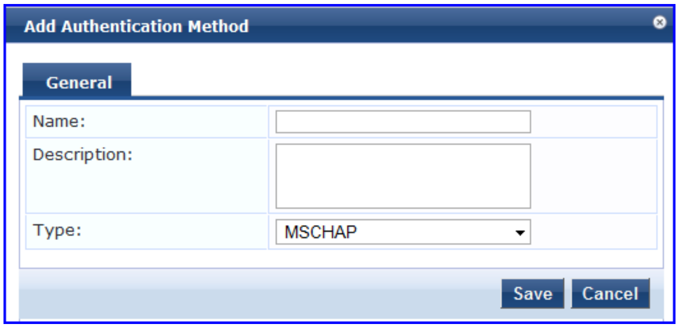
Table 58: *MAC-Auth General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **MAC-AUTH.**
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 turning on this check box and enabling audit (see "Configuring Audit Servers" on page 233), you can trigger an audit of an unknown client.

MSCHAP

The MSCHAP method contains one tab: General. This tab labels the method and defines session details.

Figure 103: *MSCHAP General Tab*



Name:

Description:

Type: MSCHAP

Table 59: *MSCHAP General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **MSCHAP**.

PAP

The PAP method contains one tab: General. This tab labels the method and defines session details. From this tab, you also specify the PAP encryption scheme.

Figure 104: *PAP General Tab*

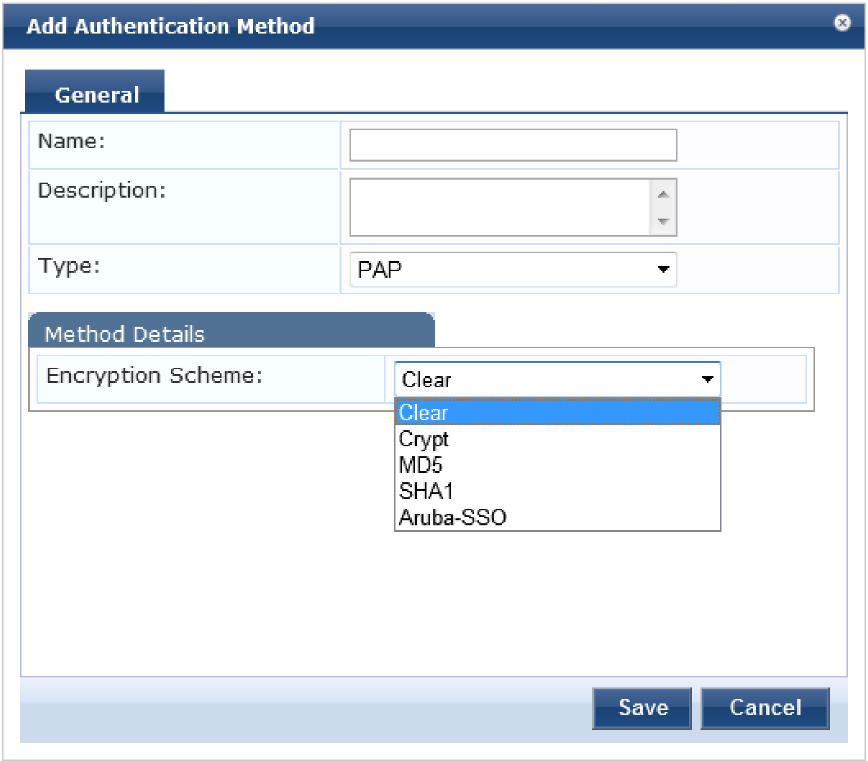


Table 60: *PAP General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **PAP**.
Encryption Scheme	Select the PAP authentication encryption scheme. Supported schemes are: Clear, Crypt, MD5, SHA1 and Aruba-SSO.

Adding and Modifying Authentication Sources

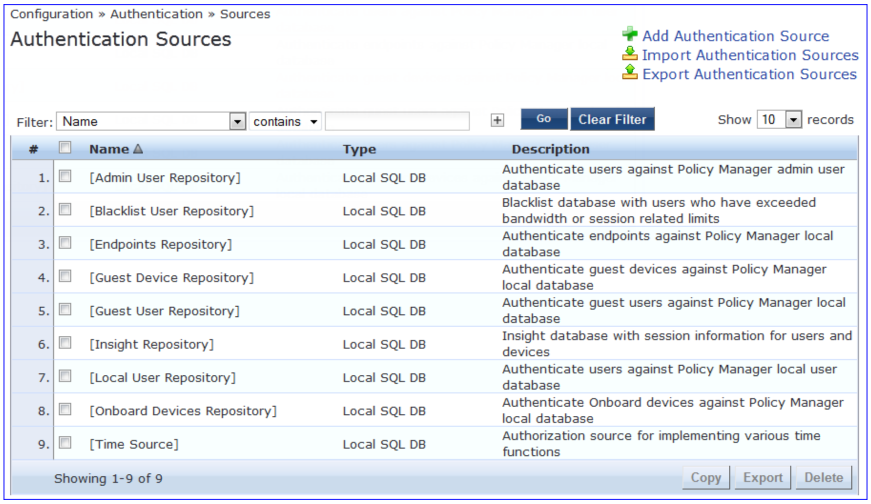
Policy Manager supports multiple authentication sources. From the **Services** page (**Configuration** > **Service**), you can configure the authentication source for a new service, as part of the flow of the **Add Service** wizard), or modify an existing authentication source directly (**Configuration** > **Authentication** > **Sources**, then click on its name in the listing page).

For more information, see:

- "Generic LDAP and Active Directory" on page 150
- "Generic SQL DB" on page 163
- "HTTP" on page 167
- "Kerberos" on page 170

- "Okta" on page 172
- "Static Host List" on page 175
- "Token Server" on page 177

Figure 105: *Authentication Sources Listing Page*



Configuration » Authentication » Sources

Authentication Sources

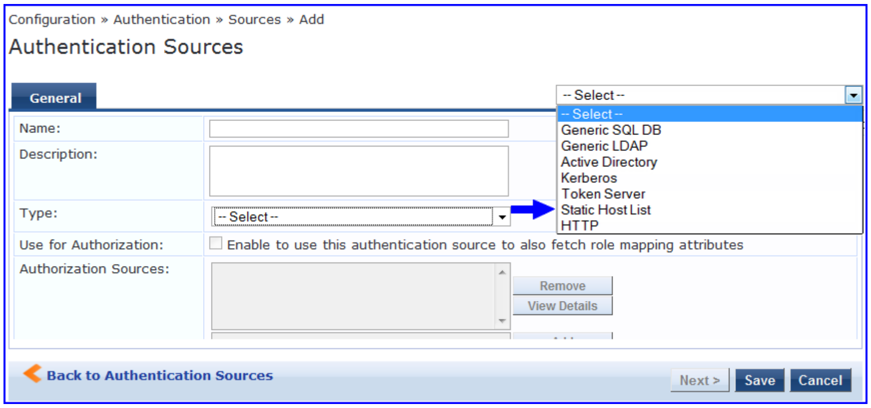
Add Authentication Source
Import Authentication Sources
Export Authentication Sources
Filter: Name
contains
Go
Clear Filter
Show 10 records

#	☐	Name	Type	Description
1.	☐	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	☐	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
3.	☐	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	☐	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	☐	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	☐	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	☐	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	☐	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
9.	☐	[Time Source]	Local SQL DB	Authorization source for implementing various time functions

Showing 1-9 of 9

After you click **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 106: *Add Authentication Source Page*



Configuration » Authentication » Sources » Add

Authentication Sources

Name:	
Description:	
Type:	-- Select --
Use for Authorization:	☐ Enable to use this authentication source to also fetch role mapping attributes
Authorization Sources:	

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 retrieve role mapping attributes by using filters.

NOTE

Click the Summary tab to view configured parameters.

For more information, see "Adding and Modifying Role Mapping Policies" on page 190.

At the top level, there are buttons 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.

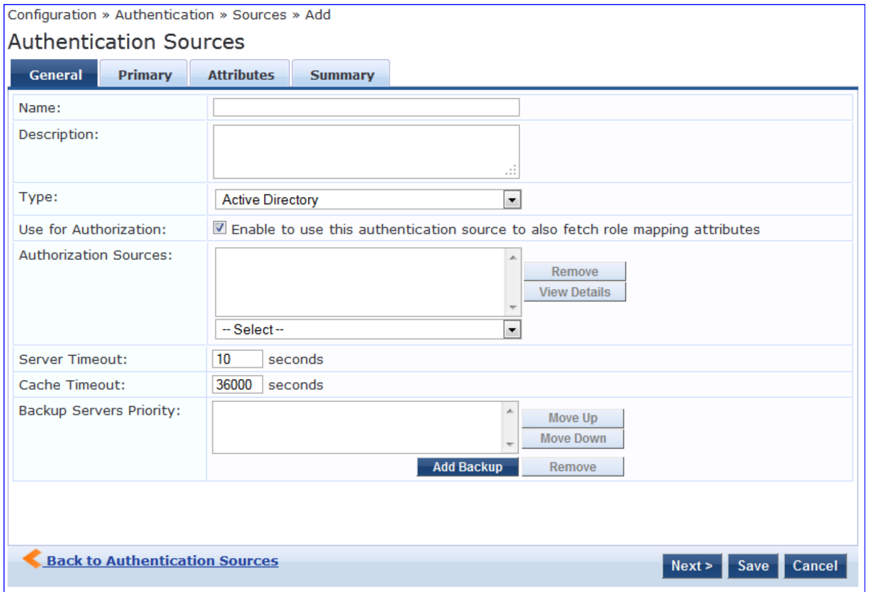
You configure Generic LDAP and Active Directory authentication sources on the following tabs:

- "General Tab" on page 151
- "Primary Tab" on page 152
- "Attributes Tab" on page 155

General Tab

The **General** tab labels the authentication source and defines session details.

Figure 107: *Generic LDAP or Active Directory (General Tab)*



Configuration » Authentication » Sources » Add

Authentication Sources

Name:	
Description:	
Type:	Active Directory
Use for Authorization:	☑ Enable to use this authentication source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	

Table 61: *Generic LDAP or Active Directory (General Tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, **General LDAP** or **Active Directory.**
Use for Authorization	This check box instructs 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 this setting is enabled). This box is checked (enabled) by default.

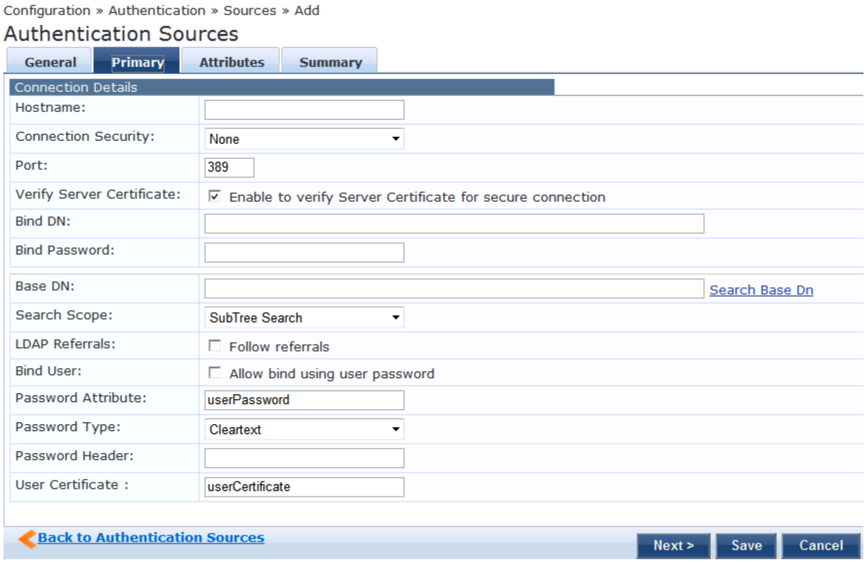
Table 61: *Generic LDAP or Active Directory (General Tab) (Continued)*

Parameter	Description
Authorization Sources	You can 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 87, additional authorization sources can be specified at the Service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.
Server Timeout	The number of seconds that Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the 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 number of seconds for which the attributes are cached.
Backup Servers Priority	To add a backup server, click **Add Backup**. If the **Backup 1** tab appears, you can specify connection details for a backup server (same fields as 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 if the primary server is unreachable.

Primary Tab

The **Primary** tab defines the settings for the primary server.

Figure 108: *Generic LDAP or Active Directory (Primary Tab)*



Hostname:

Connection Security: None

Port: 389

Verify Server Certificate: ☑ Enable to verify Server Certificate for secure connection

Bind DN:

Bind Password:

Base DN:

Search Scope: SubTree Search

LDAP Referrals: □ Follow referrals

Bind User: □ Allow bind using user password

Password Attribute: userPassword

Password Type: Cleartext

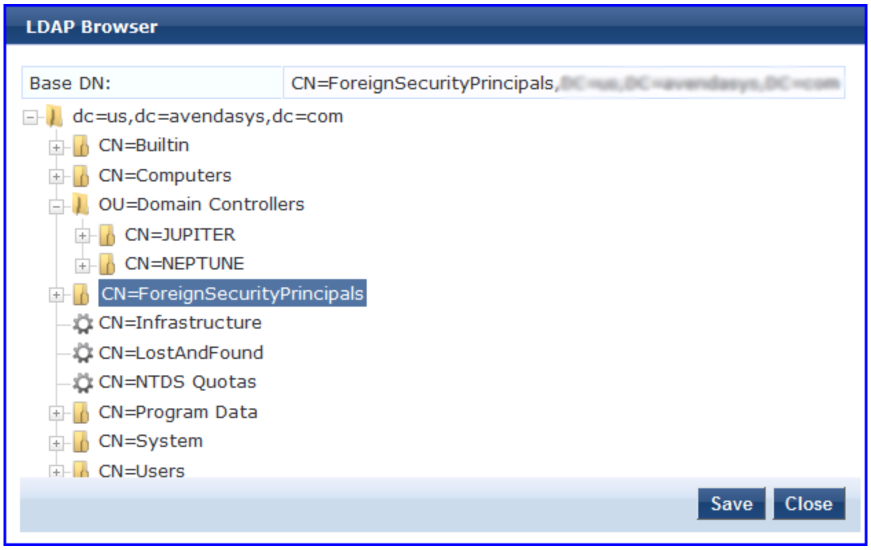
Password Header:

User Certificate : userCertificate

Table 62: *Generic LDAP or active Directory (Primary Tab)*

Parameter	Description
Hostname	Hostname or 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	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 if you want to verify the Server Certificate as part of the authentication.
Bind DN/Password	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 (e.g., administrator@acme.com). Also specify the password for the administrator DN entered in the Bind DN field.
NetBIOS Domain Name	The AD 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 only available for Active Directory.

Parameter	Description

Base DN	Enter DN of the node in your directory tree from which to start searching for records. After you have entered values for the fields described above, click on **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.
	
	LDAP Browser
	Base DN: CN=ForeignSecurityPrincipals,[redacted]
	dc=us,dc=avendasys,dc=com
	CN=Builtin
	CN=Computers
	OU=Domain Controllers
	CN=JUPITER
	CN=NEPTUNE
	CN=ForeignSecurityPrincipals
	CN=Infrastructure
	CN=LostAndFound
	CN=NTDS Quotas
	CN=Program Data
	CN=System
	CN=Users
	
	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 one way to test the connectivity to your LDAP or AD directory. If the values entered for the primary server attributes are correct, you should be able to browse the directory hierarchy by clicking on Search Base DN

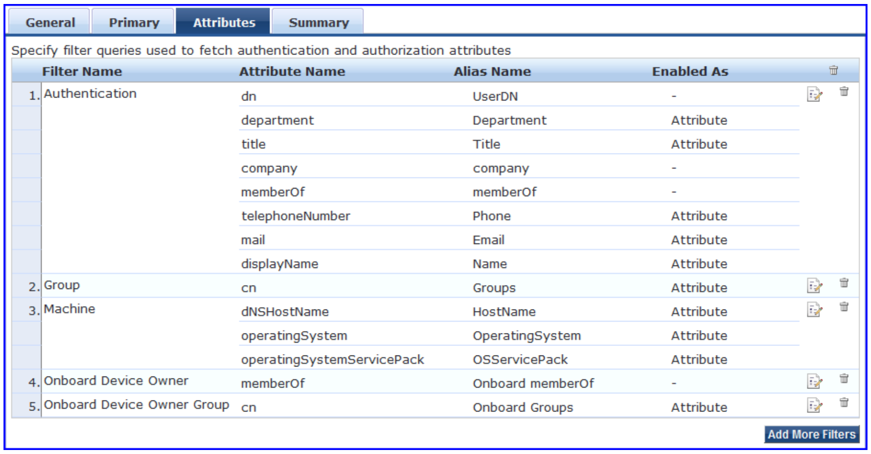
Search Scope	Scope of the search you want to perform, starting at the Base DN. ● **Base Object Search** allows you to search at the level specified by the base DN. ● **One Level Search** allows you to search up to one level below (immediate children of) the base DN. ● **Subtree Search** allows you to 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 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.

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**)	Oracle's LDAP implementation prepends a header to a hashed password string. If using Oracle LDAP, enter the header in this field so the hashed password can be correctly identified and read.
User Certificate	Enter the name of the attribute in the user record from which user certificate can be retrieved.

Attributes Tab

The **Attributes** tab defines the Active Directory or LDAP Directory query filters and the attributes to be fetched by using those filters.

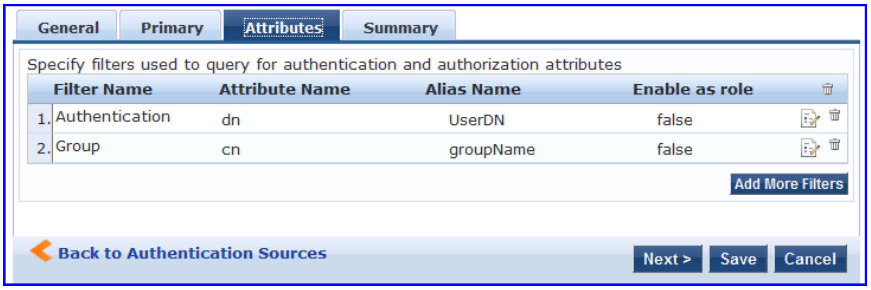
Figure 109: *Active Directory Attributes Tab (with default data)*



Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	dn	UserDN	-
		department	Department	Attribute
		title	Title	Attribute
		company	company	-
		memberOf	memberOf	-
		telephoneNumber	Phone	Attribute
		mail	Email	Attribute
		displayName	Name	Attribute
2.	Group	cn	Groups	Attribute
3.	Machine	dNSHostName	HostName	Attribute
		operatingSystem	OperatingSystem	Attribute
		operatingSystemServicePack	OSServicePack	Attribute
4.	Onboard Device Owner	memberOf	Onboard memberOf	-
5.	Onboard Device Owner Group	cn	Onboard Groups	Attribute

Figure 110: *Generic LDAP Directory Attributes Tab*



Specify filters used to query for authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enable as role
1.	Authentication	dn	UserDN	false
2.	Group	cn	groupName	false

Table 63: *D/LDAP Attributes Tab (Filter Listing Screen)*

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enable as Role	Listing column descriptions: ● **Filter Name**: Name of the filter. ● **Attribute Name**: Name of the LDAP/AD attributes defined for this filter. ● **Alias Name**: For each attribute name selected for the filter, you can specify an alias name. ● **Enabled As**: Specify whether 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.
Add More Filters	Brings up the filter creation popup. Refer to "Add More Filters" on page 158 for more information.

The following table describes the available directories.

Table 64: *AD/LDAP Default Filters Explained*

Directory	Default Filters

Active Directory	● **Authentication**: This is the filter used for authentication. The query searches in 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 set up to fetch the following attributes based on this filter query:
	■ **dn** (aliased to 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

Table 64: *AD/LDAP Default Filters Explained (Continued)*

Directory	Default Filters

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:
	■ **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	Brings up the filter creation popup. Refer to "Add More Filters" on page 158 for more information.

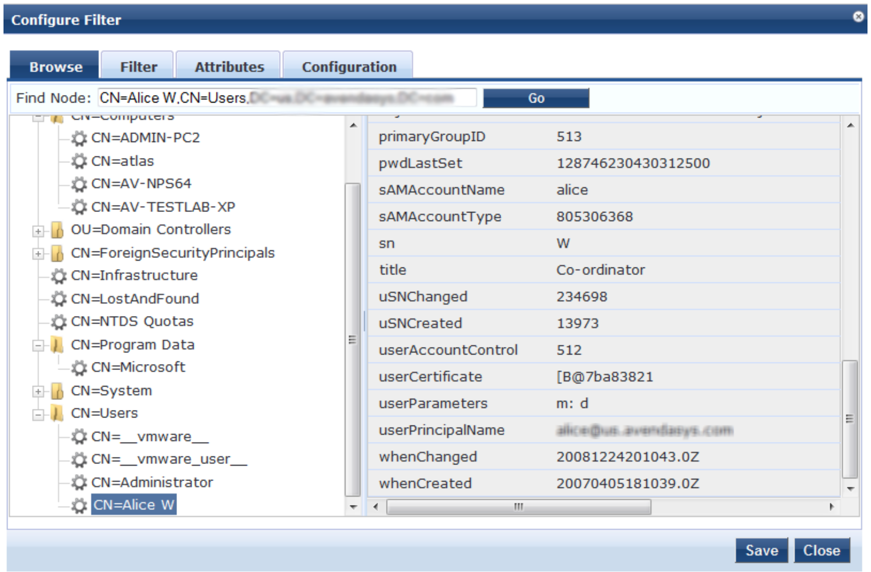
Add More Filters

The **Filter Creation** popup displays when you click the **Add More Filters** button on the **Authentication Sources > Add** page. With this popup, 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) brings up the attributes associated with that node

Figure 111: *AD/LDAP Configure Filter (Browse Tab)*



Find Node: CN=Alice W,CN=Users,[redacted]

CN=Computers
CN=ADMIN-PC2
CN=atlas
CN=AV-NPS64
CN=AV-TESTLAB-XP
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=Infrastructure
CN=LostAndFound
CN=NTDS Quotas
CN=Program Data
CN=Microsoft
CN=System
CN=Users
CN=__vmware__
CN=__vmware_user__
CN=Administrator
CN=Alice W

primaryGroupID	513
pwdLastSet	128746230430312500
sAMAccountName	alice
sAMAccountType	805306368
sn	W
title	Co-ordinator
uSNChanged	234698
uSNCreated	13973
userAccountControl	512
userCertificate	[B@7ba83821
userParameters	m: d
userPrincipalName	[redacted]
whenChanged	20081224201043.0Z
whenCreated	20070405181039.0Z

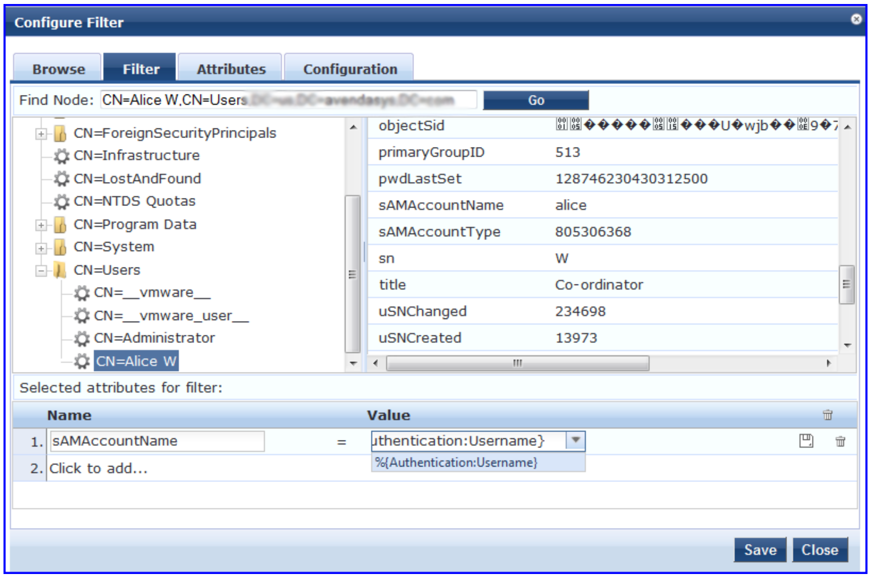
Table 65: *AD/LDAP Configure Filter Popup (Browse Tab)*

Navigation	Description
Find Node / Go	Go directly to a given node by entering its 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. Through this interface you can define the attributes used in the filter query.

Figure 112: *AD/LDAP Create Filter Popup (Filter Tab)*



Find Node: CN=Alice W,CN=Users,[redacted]

- CN=ForeignSecurityPrincipals
- CN=Infrastructure
- CN=LostAndFound
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=Users
  - CN=__vmware__
  - CN=__vmware_user__
  - CN=Administrator
  - CN=Alice W

objectSid	������������U�wjb���9�
primaryGroupID	513
pwdLastSet	128746230430312500
sAMAccountName	alice
sAMAccountType	805306368
sn	W
title	Co-ordinator
uSNChanged	234698
uSNCreated	13973

Selected attributes for filter:

	Name		Value

1.	sAMAccountName	=	uthentication:Username}
			%{Authentication:Username}

2.	Click to add...		

Policy Manager comes pre-populated with filters and selected attributes for Active Directory and generic LDAP directory. New filters need to be created only if you need Policy Manager to fetch role mapping attributes from a new type of record.

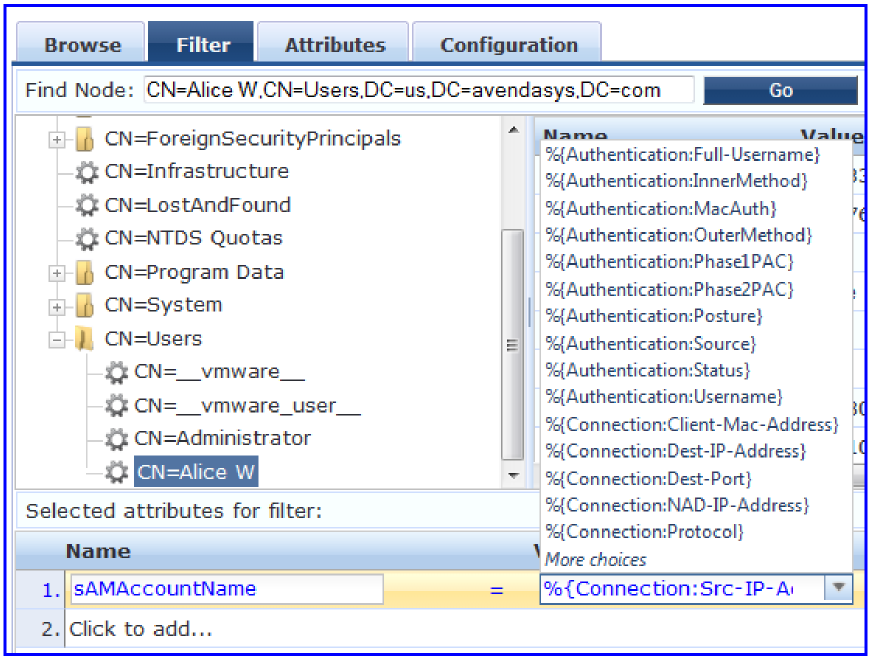
Records of different types can be fetched by specifying multiple filters that use different dynamic session attributes. For example, for a given request Policy Manager can fetch the user record associated with %{Authentication:Username}, and a machine record associated with %{RADIUS:IETF:Calling-Station-ID}.

Table 66: *Configure Filter Popup (Filter Tab)*

Parameter	Description
Find Node / Go	Go directly to a given node by entering its Distinguished Name (DN) and clicking on the Go button.

Table 66: *Configure Filter Popup (Filter Tab) (Continued)*

Parameter	Description

Select the attributes for filter	This table has a name and value column. There are two ways to enter the attribute name
	- By going to a node of interest, inspecting the attributes, and then manually entering the attribute name by clicking on **Click to add...** in the table row.
	- By clicking on 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 has been 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 (See image below).
	
	 Browse
	Filter
	Attributes
	Configuration
	Go
	CN=ForeignSecurityPrincipals
	CN=Infrastructure
	CN=LostAndFound
	CN=NTDS Quotas
	CN=Program Data
	CN=System
	CN=Users
	CN=__vmware__
	CN=__vmware_user__
	CN=Administrator
	CN=Alice W
	Name
	Value
	%{Authentication:Full-Username}
	%{Authentication:InnerMethod}
	%{Authentication:MacAuth}
	%{Authentication:OuterMethod}
	%{Authentication:Phase1PAC}
	%{Authentication:Phase2PAC}
	%{Authentication:Posture}
	%{Authentication:Source}
	%{Authentication:Status}
	%{Authentication:Username}
	%{Connection:Client-Mac-Address}
	%{Connection:Dest-IP-Address}
	%{Connection:Dest-Port}
	%{Connection:NAD-IP-Address}
	%{Connection:Protocol}
	More choices
	Find Node: CN=Alice W,CN=Users,DC=us,DC=avendasys,DC=com
	Selected attributes for filter:
	Name
	1. sAMAccountName = %{Connection:Src-IP-A
	2. Click to add...

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

Table 67: *Filter Creation Steps*

Step	Description
Step 1 Select filter node	The goal of filter creation is to help Policy Manager 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 see attributes associated with that user.
Step 2 Select attribute	Click on attributes that will help Policy Manager to uniquely 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 (along with their values). In this example, if you select sAMAccountName, the row in the filter table will show this attribute with a value of alice (assuming you picked Alice's record as a sample user node).

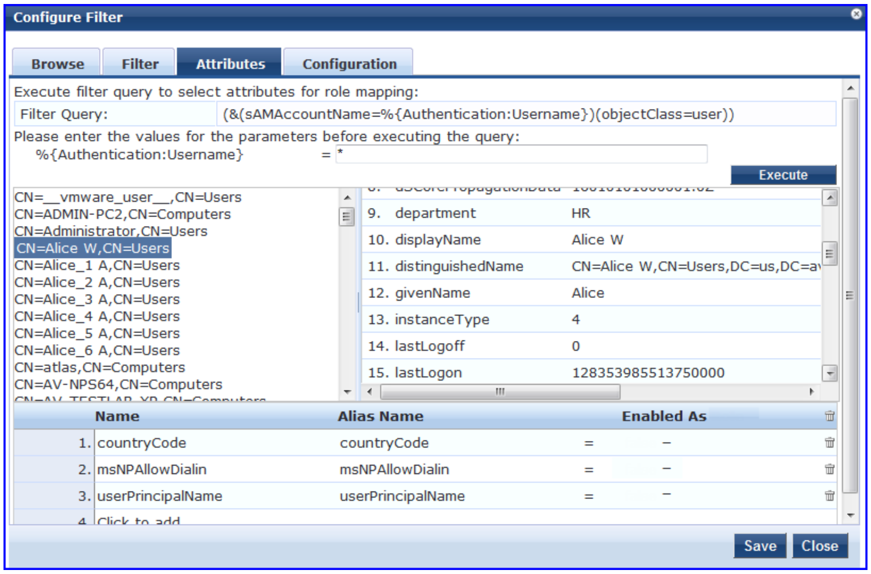
Table 67: *Filter Creation Steps (Continued)*

Step	Description
Step 3 Enter value (optional)	After Step 3, you have values for a specific record (Alice's record, in this case). Change the value to a dynamic session attribute that will help 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 node of interest 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 Role,” which means the value fetched for this attribute can be used directly in Enforcement Policies (See "Configuring Enforcement Policies" on page 277.)

Figure 113: *AD/LDAP Configure Filter Attributes Tab*



Execute filter query to select attributes for role mapping:

Filter Query: (&(sAMAccountName=%{Authentication:Username})(objectClass=user))

Please enter the values for the parameters before executing the query:

%{Authentication:Username} = *

```
CN=__vmware_user__,CN=Users
CN=ADMIN-PC2,CN=Computers
CN=Administrator,CN=Users
CN=Alice W,CN=Users
CN=Alice_1 A,CN=Users
CN=Alice_2 A,CN=Users
CN=Alice_3 A,CN=Users
CN=Alice_4 A,CN=Users
CN=Alice_5 A,CN=Users
CN=Alice_6 A,CN=Users
CN=atlas,CN=Computers
CN=AV-NPS64,CN=Computers
```

```
9.  department         HR
10. displayName        Alice W
11. distinguishedName  CN=Alice W,CN=Users,DC=us,DC=a
12. givenName          Alice
13. instanceType       4
14. lastLogoff         0
15. lastLogon          128353985513750000
```

	Name	Alias Name		Enabled As
1.	countryCode	countryCode	=	–
2.	msNPAllowDialin	msNPAllowDialin	=	–
3.	userPrincipalName	userPrincipalName	=	–
4	Click to add			

Table 68: *AD/LDAP Configure Filter Popup (Attributes Tab)*

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.

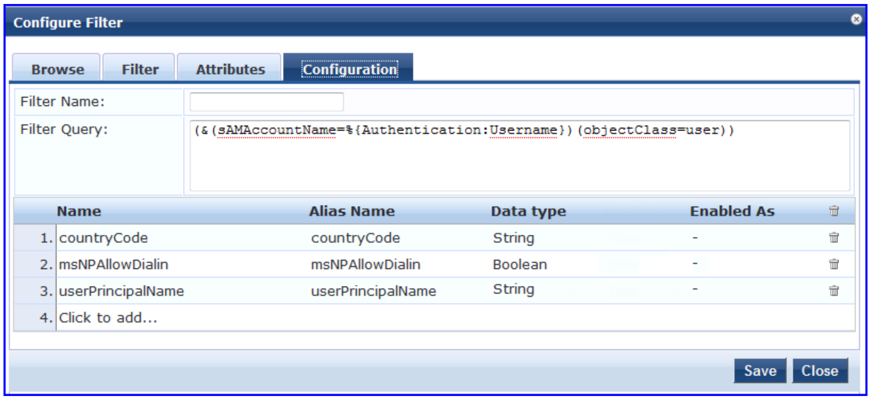
Table 68: *AD/LDAP Configure Filter Popup (Attributes Tab) (Continued)*

Parameter	Description
Execute	After you have entered the values for all dynamic parameters, click **Execute** to execute the filter query. You see all entries that match the filter query. Click on one of the entries (nodes) and you see 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 / Alias Name / Enable as Role	**Name**: This is the name of the attribute **Alias Name**: A friendly name for the attribute. By default, this is the same as the attribute name. **Enabled As**: Click here to enable this attribute value to be used directly as a role in an Enforcement Policy. This bypasses the step of having to assign 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.

Figure 114: *Configure Filter Popup (Configuration Tab)*



Filter Name:

Filter Query: (&(sAMAccountName=%{Authentication:Username})(objectClass=user))

	Name	Alias Name	Data type	Enabled As
1.	countryCode	countryCode	String	-
2.	msNPAllowDialin	msNPAllowDialin	Boolean	-
3.	userPrincipalName	userPrincipalName	String	-
4.	Click to add...			

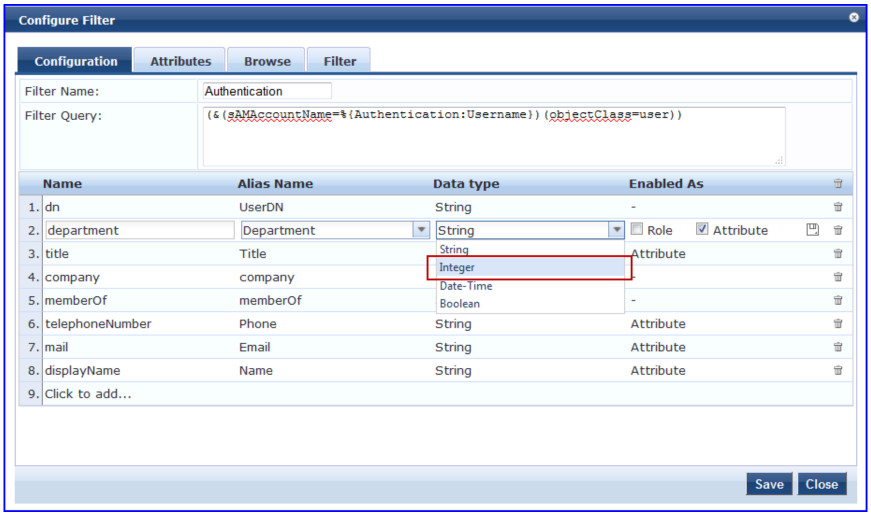
Modify Default Filters

When you add a new authentication source of type Active Directory or LDAP, a few default filters and attributes are pre-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

At least 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 will be rejected.

Figure 115: *Modify Default Filters*



Filter Name:	Authentication
Filter Query:	(&(sAMAccountName=%{Authentication:Username})(objectClass=user))

	Name	Alias Name	Data type	Enabled As
1.	dn	UserDN	String	-
2.	department	Department	String String Integer Date-Time Boolean	□ Role ☑ Attribute
3.	title	Title		Attribute
4.	company	company		-
5.	memberOf	memberOf		-
6.	telephoneNumber	Phone	String	Attribute
7.	mail	Email	String	Attribute
8.	displayName	Name	String	Attribute
9.	Click to add...			

The attributes that are defined for the authentication source show up 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. If, for example, you modify the Active Directory **department** to be an Integer rather than a String, then the list of Operator values will populate with values that are specific to Integers.

NOTE

This functionality that allows you to modify the Data type exists for Generic SQL DB, Generic LDAP, Active Directory, and HTTP authentication source types.

When you are finished editing a filter, click **Save**.

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. You specify a stored procedure to query the relevant tables and retrieve role mapping attributes by using filters.

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

- "General Tab" on page 163
- "Primary Tab" on page 165
- "Attributes Tab" on page 165

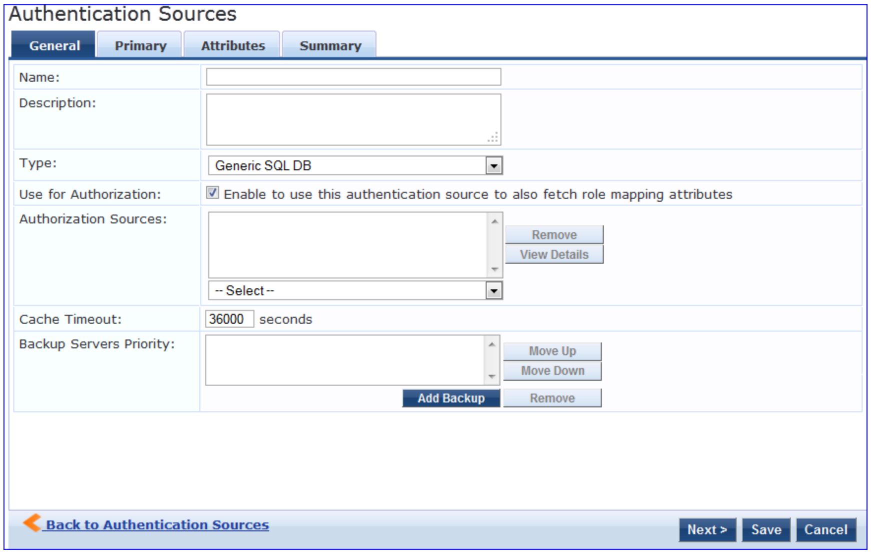
For a configured Generic SQL DB authentication source, buttons on the main page enable you to:

- **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.

Figure 116: *Generic SQL DB (General Tab)*



Name:

Description:

Type: Generic SQL DB

Use for Authorization: ☑ Enable to use this authentication source to also fetch role mapping attributes

Authorization Sources: -- Select --

Cache Timeout: 36000 seconds

Backup Servers Priority:

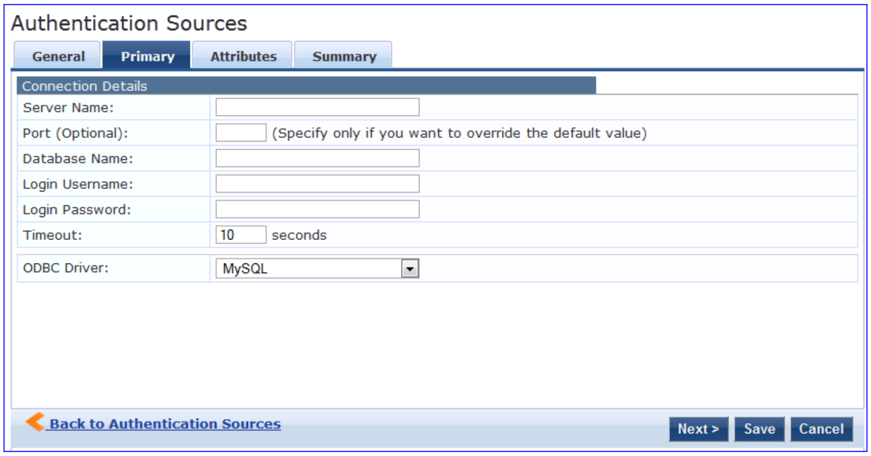
Table 69: *General SQL DB (General Tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, **Generic SQL DB**.
Use for Authorization	This check box instructs 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 this setting is enabled). This check box is enabled by default
Authorization Sources	You can 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,” additional authorization sources can be specified 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**. After the **Backup 1** tab appears, you can specify connection details for a backup server (same fields as 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.
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.

Figure 117: *General SQL DB (Primary Tab)*



Server Name:	
Port (Optional):	(Specify only if you want to override the default value)
Database Name:	
Login Username:	
Login Password:	
Timeout:	10 seconds
ODBC Driver:	MySQL

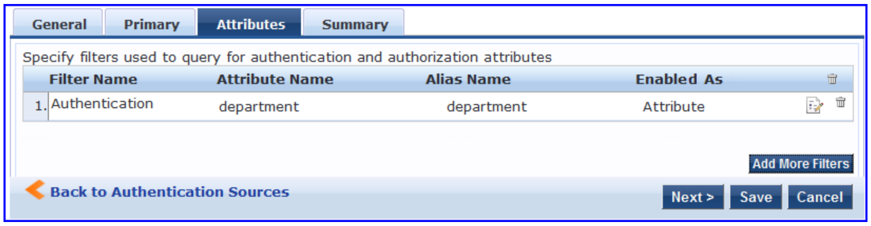
Table 70: *Generic SQL DB (Primary Tab)*

Parameter	Description
Server Name	Enter the hostname or IP address of the database server.
Port (Optional)	Specify a port value if you want to override the default port.
Database Name	Enter the name of the database to retrieve records from.
Login Username/Password	Enter the name of the user used to log into the database. This account should have read access to all the attributes that need to be retrieved by the specified filters. Enter the password for the user account entered in the field above.
Timeout	Enter the time 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 newer. 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, so customers using MySQL should contact support before they upgrade.

Attributes Tab

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

Figure 118: *Generic SQL DB (Attributes Tab)*



Specify filters used to query for authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	department	department	Attribute

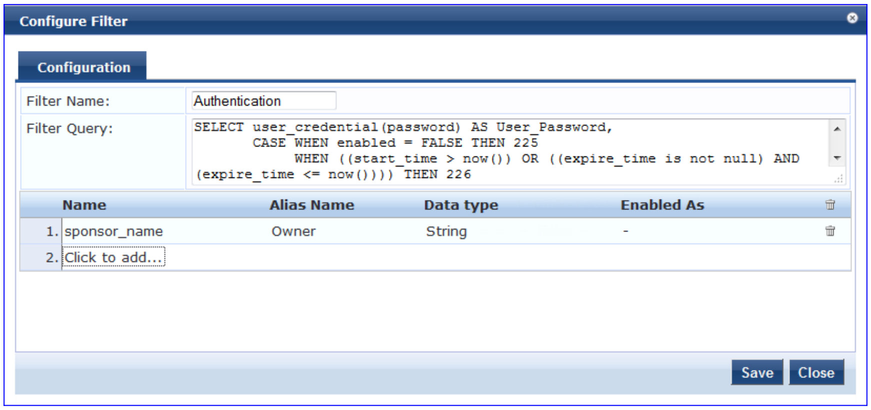
Table 71: *Generic SQL DB Attributes Tab (Filter List)*

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enabled As	Listing column descriptions: ● **Filter Name**: Name of the filter. ● **Attribute Name**: Name of the SQL DB attributes defined for this filter. ● **Alias Name**: For each attribute name selected for the filter, you can specify an alias name. **NOTE: Enabled As**: Indicates whether the filter is enabled as a role or attribute type. This can also be blank.
Add More Filters	Brings up the filter creation popup. Refer to "Add More Filters" on page 166.

Add More Filters

The **Configure Filter** popup defines a filter query and the related attributes to be fetched from the SQL DB store.

Figure 119: *Generic SQL DB Filter Configure Popup*



Filter Name: Authentication

Filter Query:

```
SELECT user_credential(password) AS User_Password,
       CASE WHEN enabled = FALSE THEN 225
            WHEN ((start_time > now()) OR ((expire_time is not null) AND
(expire_time <= now()))) THEN 226
```

	Name	Alias Name	Data type	Enabled As
1.	sponsor_name	Owner	String	-
2.	Click to add...			

Table 72: *Generic SQL DB Configure Filter Popup*

Parameter	Description
Filter Name	Name of the filter.
Filter Query	A SQL query to fetch the attributes from the user or device record in DB.

Parameter	Description
Name / Alias Name / Data Type/ Enabled As	**Name**: This is the name of the attribute. **Alias Name**: A friendly 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, Boolean, etc. **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.

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, and the filter query and role mapping attributes to fetch HTTP authentication sources on the following tabs:

- "General Tab" on page 167
- "Primary Tab" on page 168
- "Attributes Tab" on page 169

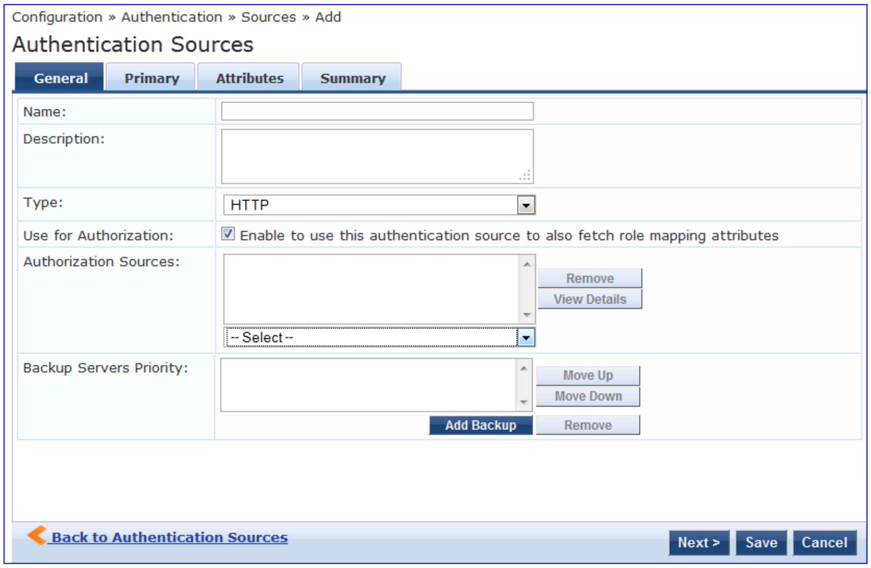
NOTE

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.

Figure 120: *HTTP (General Tab)*



Configuration » Authentication » Sources » Add

Authentication Sources

Name:	
Description:	
Type:	HTTP
Use for Authorization:	☑ Enable to use this authentication source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Backup Servers Priority:	

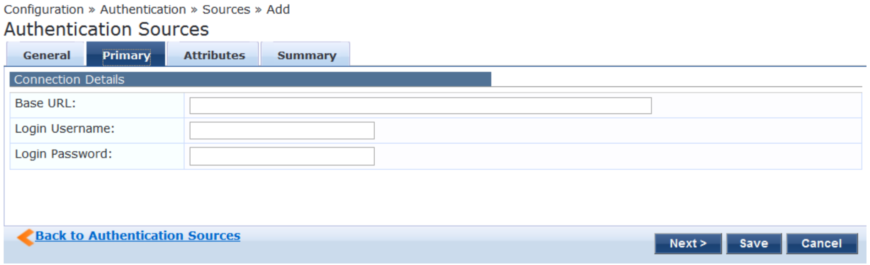
Table 73: *HTTP (General Tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, **HTTP**.
Use for Authorization	This check box instructs 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 this setting is enabled). This check box is enabled by default.
Authorization Sources	You can 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," additional authorization sources can be specified 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**. When the **Backup 1** tab appears, you can specify connection details for a backup server (same fields as 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.

Figure 121: *HTTP (Primary Tab)*



Configuration » Authentication » Sources » Add

Authentication Sources

Base URL:

Login Username:

Login Password:

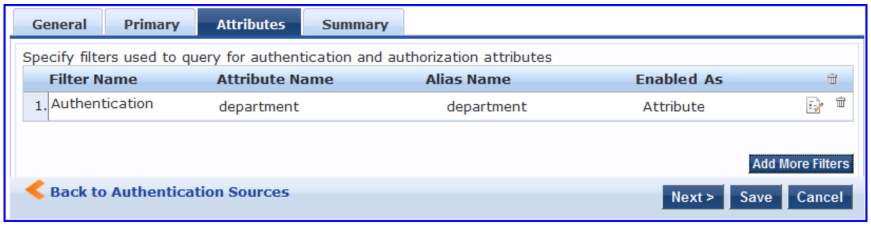
Table 74: *HTTP (Primary Tab)*

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/Password	Enter the name of the user used to log into the database. This account should have read access to all the attributes that need to be retrieved by the specified filters. Enter the password for the user account entered in the field above.

Attributes Tab

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

Figure 122: *HTTP (Attributes Tab)*



Specify filters used to query for authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	department	department	Attribute

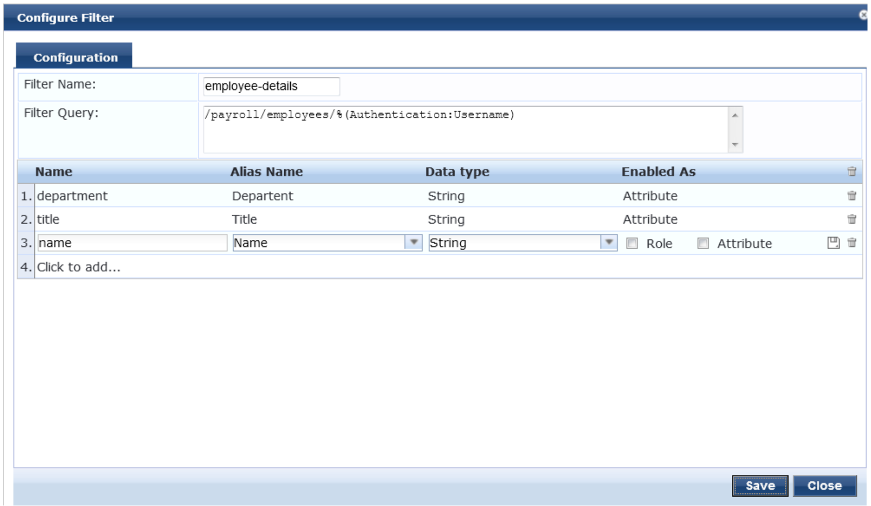
Table 75: *HTTP Attributes Tab (Filter List)*

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enabled As	Listing column descriptions: ● **Filter Name**: Name of the filter. ● **Attribute Name**: Name of the SQL DB attributes defined for this filter. ● **Alias Name**: For each attribute name selected for the filter, you can specify an alias name. ● **Enabled As**: Indicates whether an attribute has been enabled as a role.
Add More Filters	Brings up the filter creation popup. Refer to "Add More Filters" on page 169.

Add More Filters

The **Configure Filter** popup defines a filter query and the related attributes to be fetched from the SQL DB store.

Figure 123: *HTTP Filter Configure Popup*



Filter Name: employee-details

Filter Query: /payroll/employees/%(Authentication:Username)

	Name	Alias Name	Data type	Enabled As
1.	department	Departent	String	Attribute
2.	title	Title	String	Attribute
3.	name	Name	String	□ Role □ Attribute
4.	Click to add...			

Table 76: *HTTP Configure Filter Popup*

Parameter	Description
Filter Name	Name of the filter.
Filter Query	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 / Alias Name / Data Type / Enabled As	**Name**: This is the name of the attribute. **Alias Name**: A friendly 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, Boolean, etc. **Enabled As**: Specify whether 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.

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 the Microsoft Active Directory server. It is mandatory to pair this Source type with an authorization source (identity store) containing user records.

You configure Kerberos authentication sources on the following tabs:

- "General Tab" on page 170
- "Primary Tab" on page 171

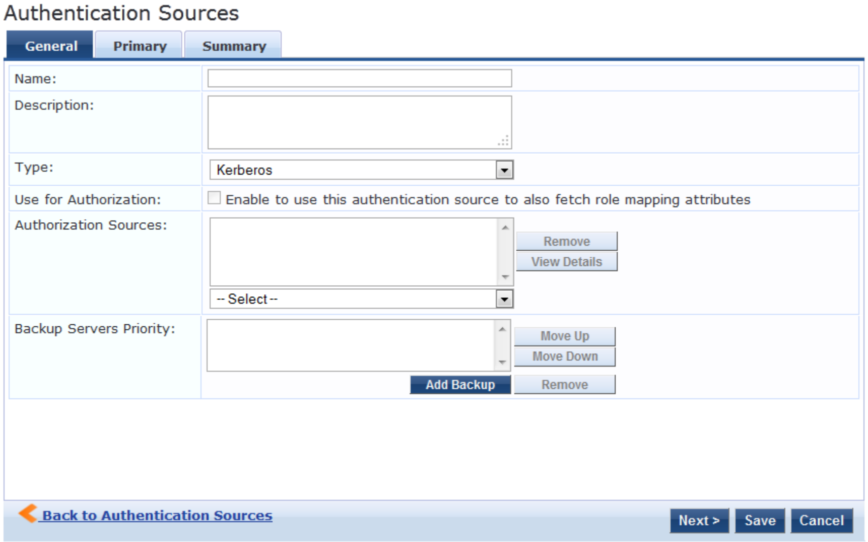
NOTE

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.

Figure 124: *Kerberos General Tab*



Authentication Sources

Name:	
Description:	
Type:	Kerberos
Use for Authorization:	□ Enable to use this authentication source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Backup Servers Priority:	

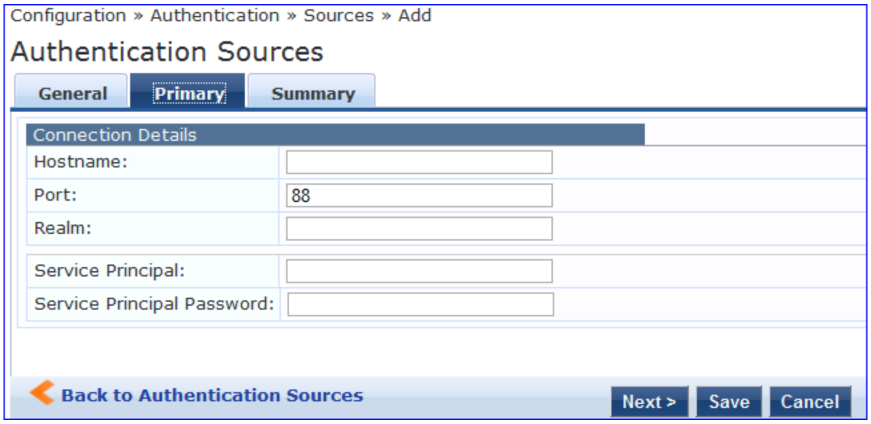
Table 77: *Kerberos (General tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, **Kerberos**.
Use for Authorization	Disabled in this context.
Authorization Sources	You must specify one or more authorization 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. **NOTE:** As described in "Services," additional authorization sources can be specified 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 kerberos server, click **Add Backup**. When the **Backup 1** tab appears, you can specify connection details for a backup server (same fields as 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.

Figure 125: *Kerberos (Primary Tab)*



Configuration » Authentication » Sources » Add

Authentication Sources

Connection Details

Hostname:	
Port:	88
Realm:	
Service Principal:	
Service Principal Password:	

Table 78: *Kerberos (Primary Tab)*

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

Okta

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

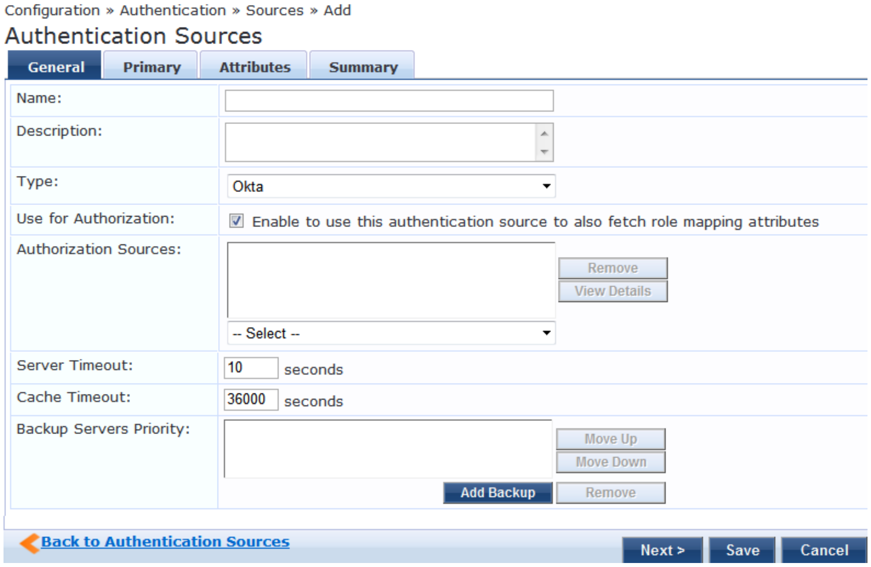
- "General Tab" on page 173
- "Primary Tab" on page 174
- "Attributes Tab" on page 174

NOTE

Click the Summary tab to view configured parameters.

General Tab

Figure 126: *Okta General Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

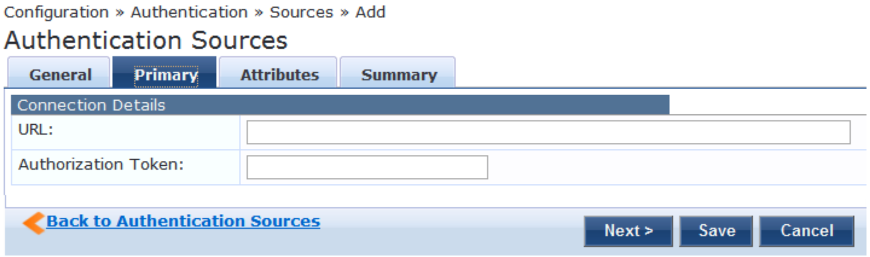
Name:	
Description:	
Type:	Okta
Use for Authorization:	☑ Enable to use this authentication source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	

Table 79: *Okta (General tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, **Okta**.
Use for Authorization	This check box instructs 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 this setting is enabled). This check box is enabled by default.
Server Timeout	The number of seconds that Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the 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 number of seconds for which the attributes are cached.
Backup Servers Priority	To add a backup server, click **Add Backup**. When the **Backup 1** tab appears, you can specify connection details for a backup server (same fields as 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

Figure 127: *Okta Primary Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Connection Details

URL:

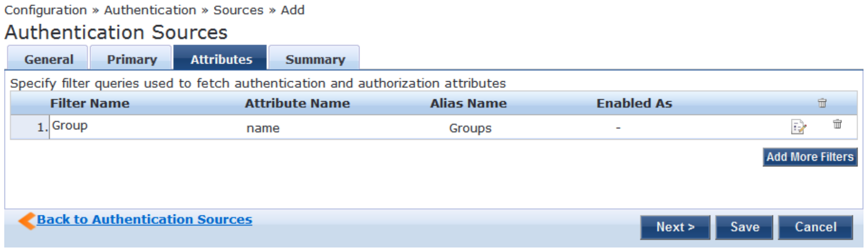
Authorization Token:

Table 80: *Okta (Primary Tab)*

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

Attributes Tab

Figure 128: *Okta Attributes Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Group	name	Groups	-

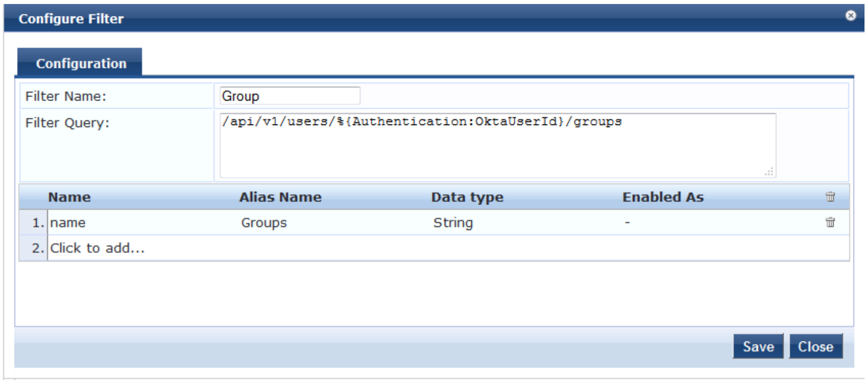
Table 81: *Okta (Attributes Tab)*

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enable as Role	Listing column descriptions: ● **Filter Name**: Name of the filter. (Only Group can be configured for Okta.) ● **Attribute Name**: Name of the LDAP/AD attributes defined for this filter. ● **Alias Name**: For each attribute name selected for the filter, you can specify an alias name. ● **Enabled As**: Specify whether 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.
Add More Filters	Brings up the filter creation popup. Refer to " Add More Filters" on page 174.

Add More Filters

The **Configure Filter** popup defines a filter query and the related attributes to be fetched from the SQL DB store.

Figure 129: *Okta Filter Configure Popup*



Filter Name: Group

Filter Query: /api/v1/users/%{Authentication:OktaUserId}/groups

	Name	Alias Name	Data type	Enabled As
1.	name	Groups	String	-
2.	Click to add...			

Table 82: *Okta Configure Filter Popup*

Parameter	Description
Filter Name	Name of the filter.
Filter Query	A SQL query to fetch the attributes from the user or device record in DB.
Name / Alias Name / Data Type/ Enabled As	**Name**: This is the name of the attribute. **Alias Name**: A friendly 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, Boolean, etc. **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.

Static Host List

An internal relational database stores Policy Manager configuration data and locally configured user and device accounts. Three pre-defined authentication sources, [Local User Repository] , [Guest User Repository], and [Guest Device Repository], represent the three databases used to store local users, guest users and registered devices, respectively.

While regular users typically reside in an authentication source such as Active Directory (or in other LDAP-compliant stores), temporary users, including guest users can be configured in the Policy Manager local repositories. For a user account created in the local database, the role is statically assigned to that account, which means a role mapping policy need not be specified 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 tab:

- "General Tab" on page 176
- "Static Host Lists Tab" on page 176

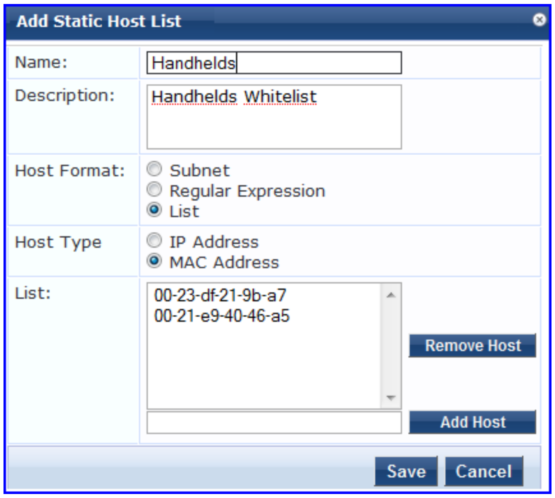
NOTE

Click the Summary tab to view configured parameters.

General Tab

The **General** Tab labels the authentication source.

Figure 130: *Static Host List (General Tab)*



Add Static Host List

Name: Handhelds

Description: Handhelds Whitelist

Host Format: ○ Subnet ○ Regular Expression ● List

Host Type ○ IP Address ● MAC Address

List:
00-23-df-21-9b-a7
00-21-e9-40-46-a5

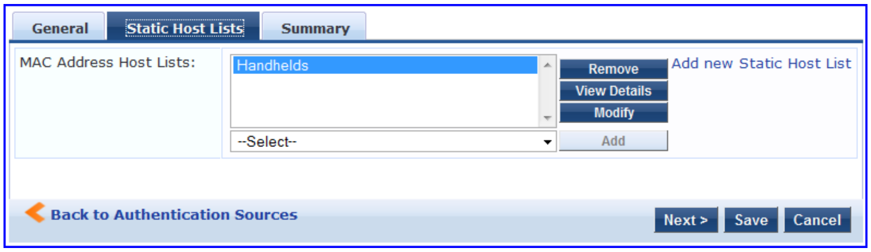
Table 83: *Static Host List (General Tab)*

Parameter	Description
Name/ Description	Freeform label.
Type	**Static Host List**, in this context.
Use for Authorization/Authorization Sources	These options are 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.

Figure 131: *Static Host List (Static Host Lists Tab)*



MAC Address Host Lists: Handhelds

--Select--

Table 84: *Static Hosts List (Static Host Lists Tab)*

Parameter	Description
Host List	Select a Static Host List from the drop-down list and **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.

NOTE

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 187 for more information.

Token Server

Policy Manager can perform GTC authentication against any token server than can authenticate users by acting as a RADIUS server (e.g., 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. See "Namespaces" on page 445.

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 177
- "Primary Tab" on page 178
- "Attributes Tab" on page 179

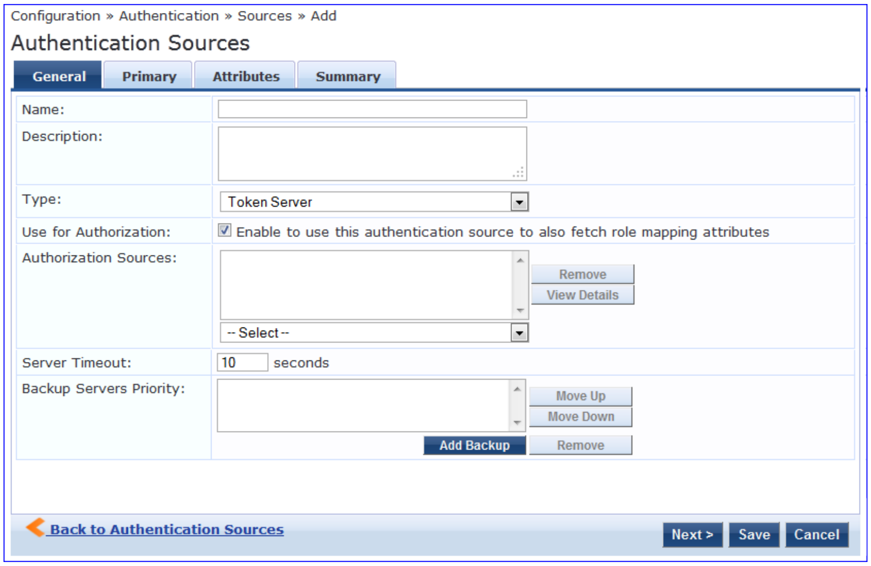
NOTE

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.

Figure 132: *Token Server General tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Name:	
Description:	
Type:	Token Server
Use for Authorization:	☑ Enable to use this authentication source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Backup Servers Priority:	

Table 85: *Token Server General tab Parameters*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, **Token Server**.

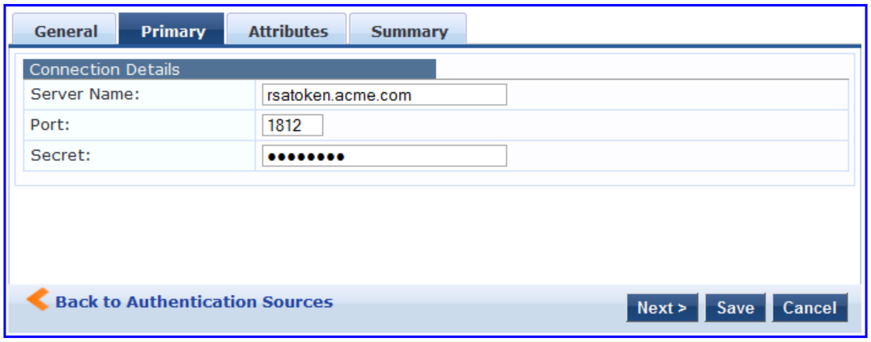
Table 85: *Token Server General tab Parameters (Continued)*

Parameter	Description
Use for Authorization	This check box instructs 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 this setting is enabled). This check box is enabled by default
Authorization Sources	You can 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," additional authorization sources can be specified at the Service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.
Server Timeout	This is the time 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**. When the **Backup 1** tab appears, you can specify connection details for a backup server (same fields as 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.

Figure 133: *Token Server (Primary Tab)*



Connection Details

Server Name:	rsatoken.acme.com
Port:	1812
Secret:	••••••••

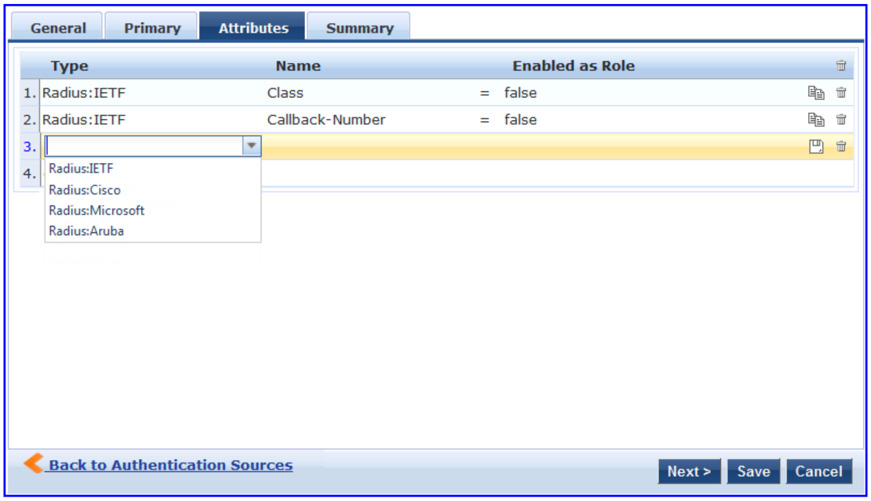
Table 86: *Token Server (Primary Tab)*

Parameter	Description
Server Name/Port	Host name or IP address of the token server, and the UDP port at which the token server listens for RADIUS connections. The default port is 1812.
Secret	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. (See "Configuring a Role Mapping Policy" on page 189 for more information.) Policy Manager loads all RADIUS vendor dictionaries in the type drop-down list to help select the attributes.

Figure 134: *Token Server (Attributes Tab)*



	Type	Name		Enabled as Role
1.	Radius:IETF	Class	=	false
2.	Radius:IETF	Callback-Number	=	false
3.				
4.				

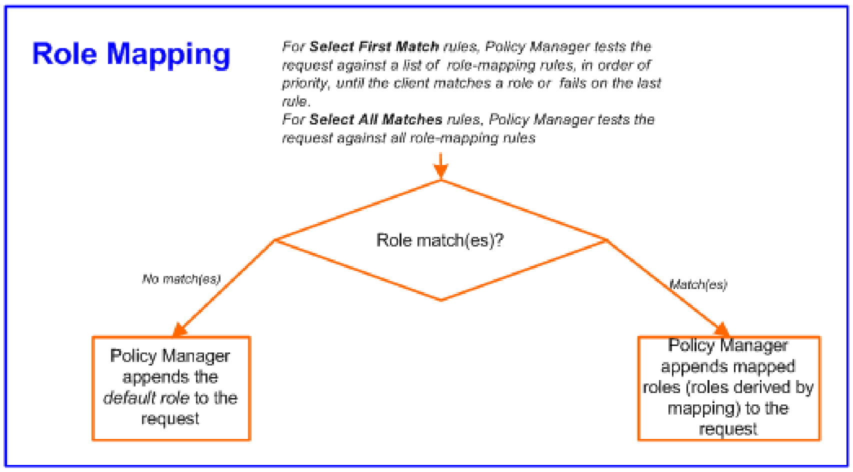
Roles can range in complexity from a simple user group (e.g., Finance, Engineering, or Human Resources) to a combination of a user group with some dynamic constraints (e.g., “San Jose Night Shift Worker”- - An employee in the Engineering department who logs in through the San Jose network device between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

For more information, see:

- "Configuring Single Sign-On, Local Users, Endpoints, and Static Host Lists" on page 181
- "Configuring a Role Mapping Policy" on page 189

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 135: *Role Mapping Process*


Role Mapping
For **Select First Match** rules, Policy Manager tests the request against a list of role-mapping rules, in order of priority, until the client matches a role or fails on the last rule.
For **Select All Matches** rules, Policy Manager tests the request against all role-mapping rules
Role match(es)?
No match(es)
Match(es)
Policy Manager appends the *default role* to the request
Policy Manager appends mapped roles (roles derived by mapping) to the request

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.

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.

NOTE

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 authentications, and Web authentications 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 182
- "Adding and Modifying Local Users" on page 183
- "Adding and Modifying Endpoints" on page 185
- "Adding and Modifying Static Host Lists" on page 187

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 (SAMP). ClearPass allows you to create trusted relationships between SPs Service Providers (SPs) and IdPs (Identity Providers).

Perform the following steps to configure and enable SSO.

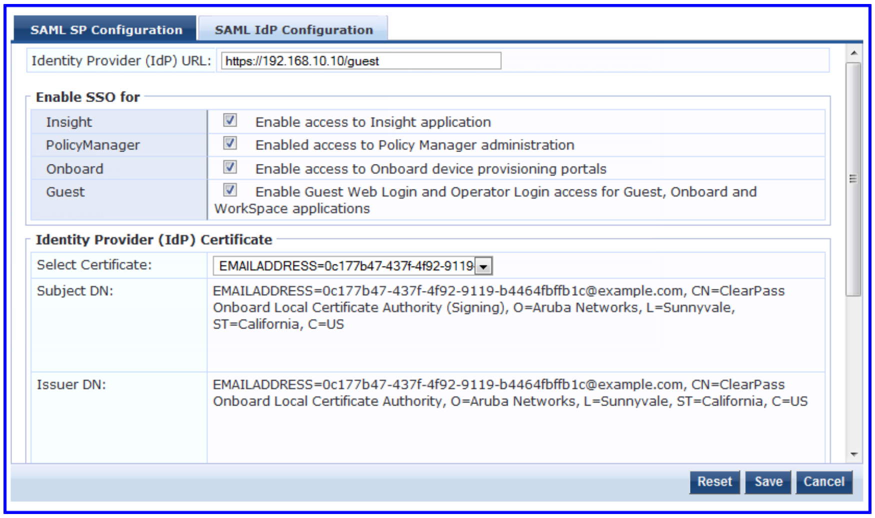
1. Go to **Configuration > Identity > Single Sign-On**.
2. The Service **SAML SP Configuration** tab, enter the IdP (Identity Provider) Single sign-on URL.
3. In the Enable SSO for section, select the checkbox for the application(s) you want users to access with single sign-on.
4. If you want to do a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

NOTE

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 396 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, and then browse to locate the metadata file.
9. Click **Save**.

Figure 136: *Single Sign-On - SAML SP Configuration tab*



Identity Provider (IdP) URL: https://192.168.10.10/guest

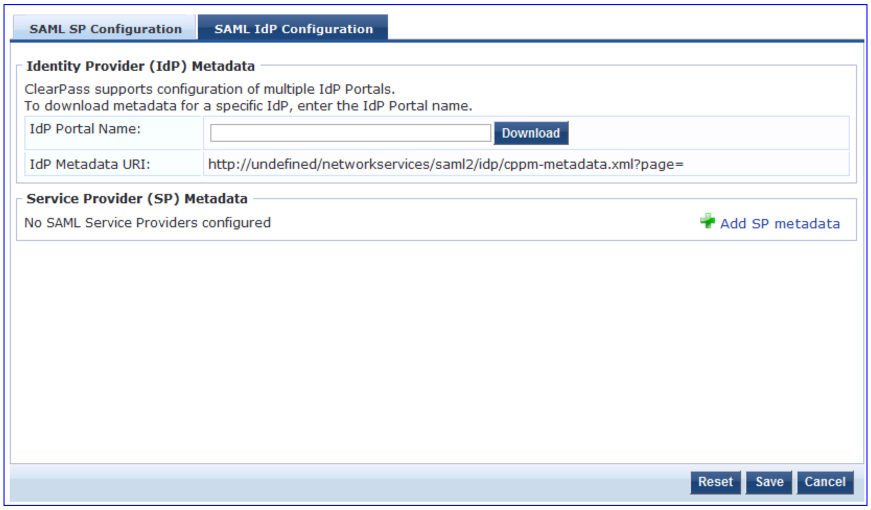
Enable SSO for

Insight	☑ Enable access to Insight application
PolicyManager	☑ Enabled access to Policy Manager administration
Onboard	☑ Enable access to Onboard device provisioning portals
Guest	☑ Enable Guest Web Login and Operator Login access for Guest, Onboard and WorkSpace applications

Identity Provider (IdP) Certificate

Select Certificate:	EMAILADDRESS=0c177b47-437f-4f92-9119
Subject DN:	EMAILADDRESS=0c177b47-437f-4f92-9119-b4464fbffb1c@example.com, CN=ClearPass Onboard Local Certificate Authority (Signing), O=Aruba Networks, L=Sunnyvale, ST=California, C=US
Issuer DN:	EMAILADDRESS=0c177b47-437f-4f92-9119-b4464fbffb1c@example.com, CN=ClearPass Onboard Local Certificate Authority, O=Aruba Networks, L=Sunnyvale, ST=California, C=US

Figure 137: *Single Sign-On SAML IdP Configuration tab*



Identity Provider (IdP) Metadata

ClearPass supports configuration of multiple IdP Portals.
To download metadata for a specific IdP, enter the IdP Portal name.

IdP Portal Name:	Download
IdP Metadata URI:	http://undefined/networkservices/saml2/idp/cppm-metadata.xml?page=

Service Provider (SP) Metadata

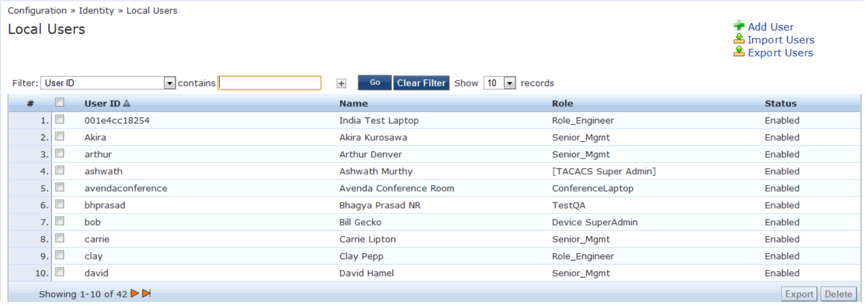
No SAML Service Providers configured

Adding and Modifying Local Users

Policy Manager lists all local users in the **Local Users** page. To add a local user, click **Add User** 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 Users**.
- To import local users, in the Local Users listing page, click **Import Users**.

Figure 138: *Local Users Listing*



Configuration » Identity » Local Users

Local Users

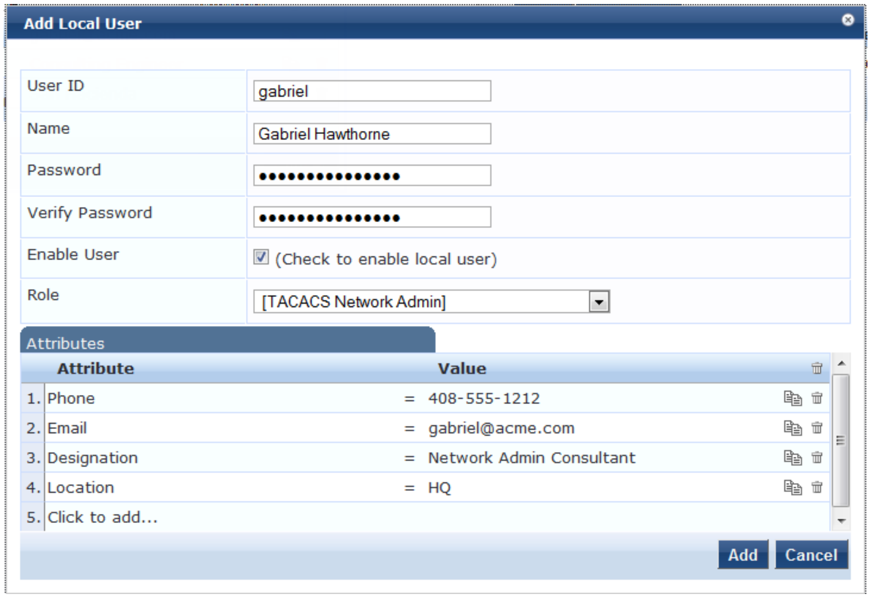
Filter: User ID contains

Show 10 records

#	□	User ID	Name	Role	Status
1.	□	001e4cc18254	India Test Laptop	Role_Engineer	Enabled
2.	□	Akira	Akira Kurosawa	Senior_Mgmt	Enabled
3.	□	arthur	Arthur Denver	Senior_Mgmt	Enabled
4.	□	ashwath	Ashwath Murthy	[TACACS Super Admin]	Enabled
5.	□	avendaconference	Avenda Conference Room	ConferenceLaptop	Enabled
6.	□	bhprasad	Bhagya Prasad NR	TestQA	Enabled
7.	□	bob	Bill Gecko	Device SuperAdmin	Enabled
8.	□	carrie	Carrie Lipton	Senior_Mgmt	Enabled
9.	□	clay	Clay Pepp	Role_Engineer	Enabled
10.	□	david	David Hamel	Senior_Mgmt	Enabled

Showing 1-10 of 42

Figure 139: *Add Local User page*



Add Local User

User ID	gabriel
Name	Gabriel Hawthorne
Password	•••••••••••••••
Verify Password	•••••••••••••••
Enable User	☑ (Check to enable local user)
Role	[TACACS Network Admin]

Attributes

	Attribute		Value
1.	Phone	=	408-555-1212
2.	Email	=	gabriel@acme.com
3.	Designation	=	Network Admin Consultant
4.	Location	=	HQ
5.	Click to add...		

Table 87: *Add Local User Page Parameters*

Parameter	Description
User ID/ Name /Password/ Verify Password:	Freeform labels and password.
Enable User:	Uncheck to disable this user account.
Role:	Select a static role for this local user.

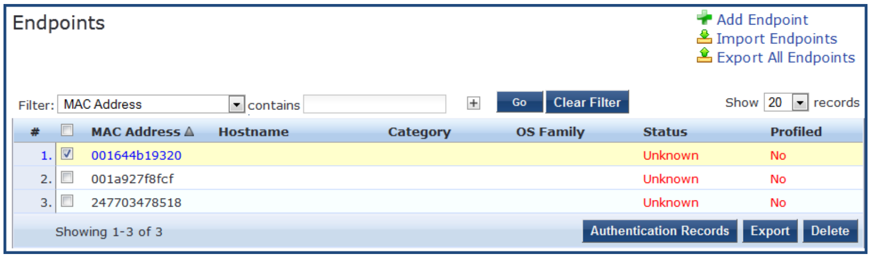
Table 87: *Add Local User Page Parameters (Continued)*

Parameter	Description
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 have authenticated) in the **Endpoints** page (**Configuration > Identity > Endpoints**):

Figure 140: *Endpoints Listing*

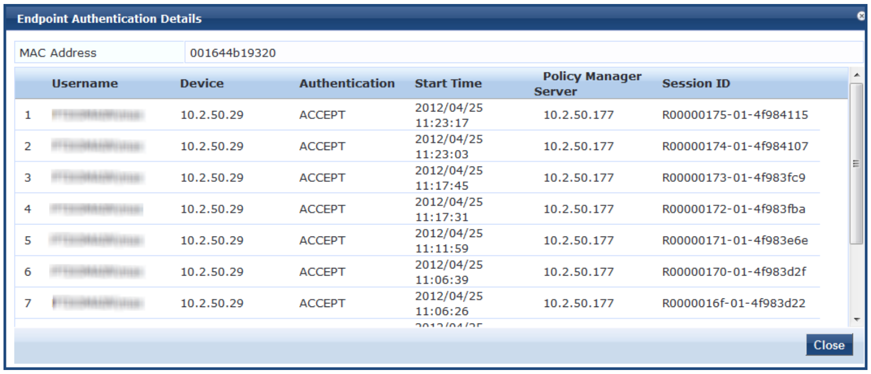


#	☐	MAC Address	Hostname	Category	OS Family	Status	Profiled
1.	☑	001644b19320				Unknown	No
2.	☐	001a927f8fcf				Unknown	No
3.	☐	247703478518				Unknown	No

Showing 1-3 of 3

To view the authentication details of an endpoint, select an endpoint by clicking on its check box, and then click the **Authentication Records** button. This opens the **Endpoint Authentication Details** popup.

Figure 141: *Endpoint Authentication Details*

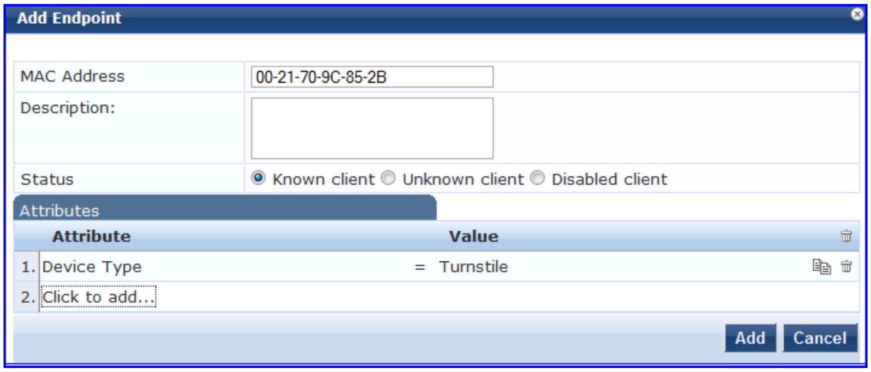


MAC Address 001644b19320

	Username	Device	Authentication	Start Time	Policy Manager Server	Session ID
1	[redacted]	10.2.50.29	ACCEPT	2012/04/25 11:23:17	10.2.50.177	R00000175-01-4f984115
2	[redacted]	10.2.50.29	ACCEPT	2012/04/25 11:23:03	10.2.50.177	R00000174-01-4f984107
3	[redacted]	10.2.50.29	ACCEPT	2012/04/25 11:17:45	10.2.50.177	R00000173-01-4f983fc9
4	[redacted]	10.2.50.29	ACCEPT	2012/04/25 11:17:31	10.2.50.177	R00000172-01-4f983fba
5	[redacted]	10.2.50.29	ACCEPT	2012/04/25 11:11:59	10.2.50.177	R00000171-01-4f983e6e
6	[redacted]	10.2.50.29	ACCEPT	2012/04/25 11:06:39	10.2.50.177	R00000170-01-4f983d2f
7	[redacted]	10.2.50.29	ACCEPT	2012/04/25 11:06:26	10.2.50.177	R0000016f-01-4f983d22

To manually add an endpoint, click **Add Endpoint** to display the **Add Endpoint** popup.

Figure 142: *Add Endpoint Page*



MAC Address	00-21-70-9C-85-2B
Description:	
Status	● Known client ○ Unknown client ○ Disabled client

Attributes

	Attribute		Value
1.	Device Type	=	Turnstile
2.	Click to add...		

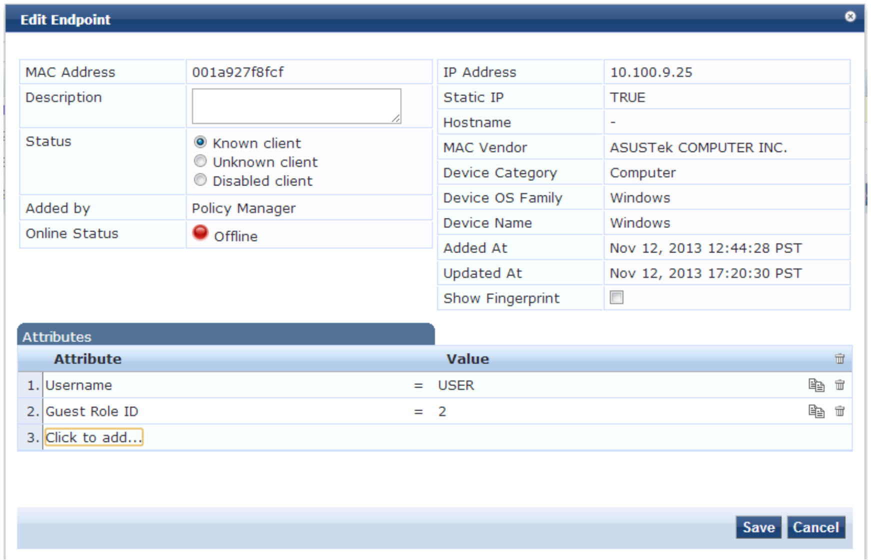
Table 88: *Add Endpoint Page Parameters*

Parameter	Description
MAC Address	MAC address of the endpoint.
Status	Mark as Known, Unknown or Disabled client. The Known and Unknown status can be used in role mapping rules via the Authentication:MacAuth attribute. The Disabled status can be used 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 listing page, click on the name to display the **Edit Endpoint** popup.

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 143: *Endpoint Popup*



Edit Endpoint

MAC Address	001a927f8fcf	IP Address	10.100.9.25
Description		Static IP	TRUE
Status	● Known client ○ Unknown client ○ Disabled client	Hostname	-
		MAC Vendor	ASUSTek COMPUTER INC.
		Device Category	Computer
Added by	Policy Manager	Device OS Family	Windows
Online Status	● Offline	Device Name	Windows
		Added At	Nov 12, 2013 12:44:28 PST
		Updated At	Nov 12, 2013 17:20:30 PST
		Show Fingerprint	□

Attributes

	Attribute		Value
1.	Username	=	USER
2.	Guest Role ID	=	2
3.	Click to add...		

Additional Available Tasks

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

Adding and Modifying Static Host Lists

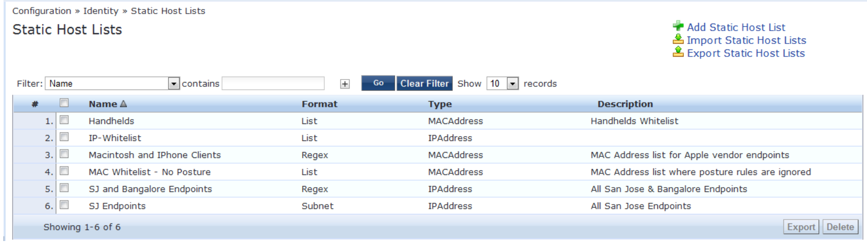
A static host list comprises a named list of MAC or IP addresses, which can be invoked the following ways:

- 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.

NOTE

> 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 white list or a black list. Therefore, they are configured independently at the global level.

Figure 144: *Static Host Lists Page*



Configuration » Identity » Static Host Lists

Static Host Lists

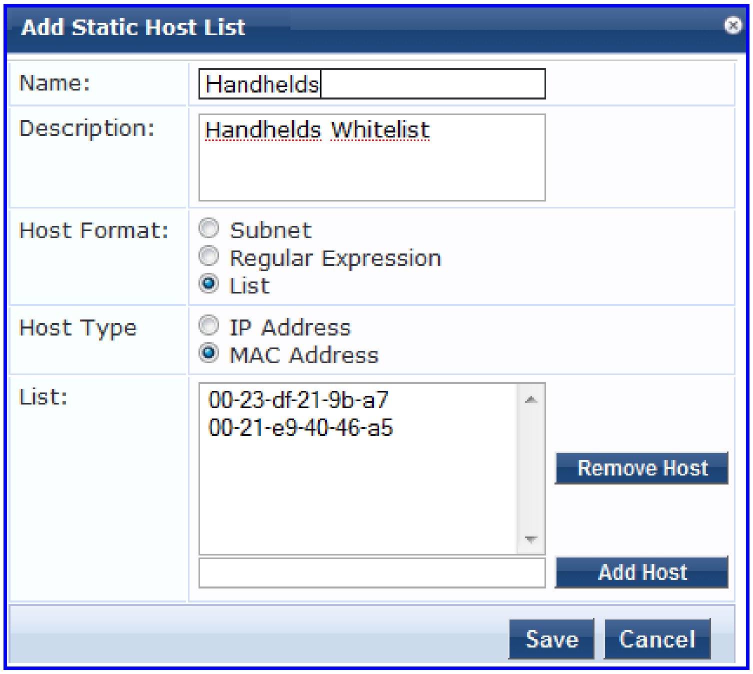
Filter: Name contains Show 10 records

#	□	Name	Format	Type	Description
1.	□	Handhelds	List	MACAddress	Handhelds Whitelist
2.	□	IP-Whitelist	List	IPAddress	
3.	□	Macintosh and IPhone Clients	Regex	MACAddress	MAC Address list for Apple vendor endpoints
4.	□	MAC Whitelist - No Posture	List	MACAddress	MAC Address list where posture rules are ignored
5.	□	SJ and Bangalore Endpoints	Regex	IPAddress	All San Jose & Bangalore Endpoints
6.	□	SJ Endpoints	Subnet	IPAddress	All San Jose Endpoints

Showing 1-6 of 6

To add a Static Host List, click the **Add Static Host List** link. This opens the **Add Static Host List** popup.

Figure 145: *Add Static Host List Page*



Add Static Host List

Name: Handhelds

Description: Handhelds Whitelist

Host Format:
○ Subnet
○ Regular Expression
● List

Host Type
○ IP Address
● MAC Address

List:
00-23-df-21-9b-a7
00-21-e9-40-46-a5

Table 89: *Add Static Host List Page Parameters*

Parameter	Description
Name/ Description:	Freeform labels and descriptions.
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 it (via check box) and click the **Delete** button.
- To export a Static Host List, in the Static Host Lists listing page, select it (via check box) and click the **Export** button.
- To export ALL Static Host Lists, in the Static Host Lists listing page, click the **Export Static Host Lists** link.
- To import Static Host Lists, in the Static Host Lists listing page, click the **Import Static Host Lists** link

Configuring a 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.

> NOTE
>
> 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

> NOTE
>
> Additional roles are available with AirGroup and Onboard licenses.

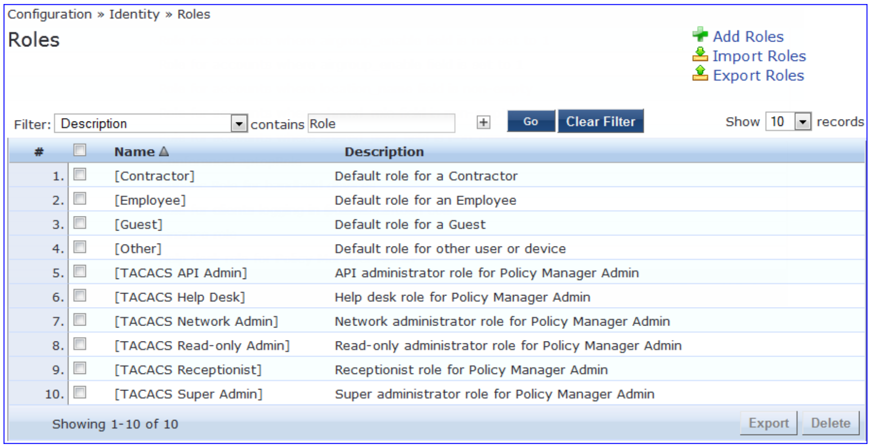
For more information, see:

- "Adding and Modifying Roles" on page 189
- "Adding and Modifying Role Mapping Policies" on page 190

Adding and Modifying Roles

Policy Manager lists all available roles in the Roles page.

Figure 146: *Roles Page*



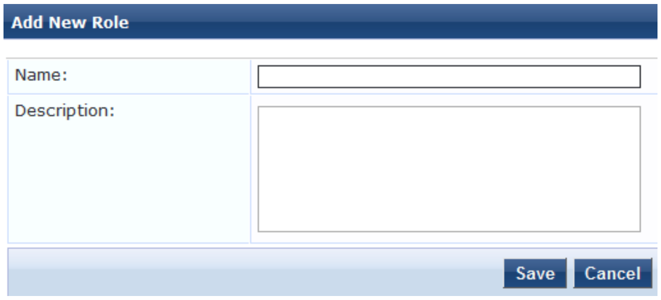
#	□	Name ▲	Description
1.	□	[Contractor]	Default role for a Contractor
2.	□	[Employee]	Default role for an Employee
3.	□	[Guest]	Default role for a Guest
4.	□	[Other]	Default role for other user or device
5.	□	[TACACS API Admin]	API administrator role for Policy Manager Admin
6.	□	[TACACS Help Desk]	Help desk role for Policy Manager Admin
7.	□	[TACACS Network Admin]	Network administrator role for Policy Manager Admin
8.	□	[TACACS Read-only Admin]	Read-only administrator role for Policy Manager Admin
9.	□	[TACACS Receptionist]	Receptionist role for Policy Manager Admin
10.	□	[TACACS Super Admin]	Super administrator role for Policy Manager Admin

Showing 1-10 of 10

You can configure a role from within a Role Mapping Policy (**Add New Role**), or independently from the menu (**Configuration** > **Identity** > **Roles** > **Add Roles**). 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.

Figure 147: *Add New Role Page*



Add New Role

Name:	
Description:	

Save Cancel

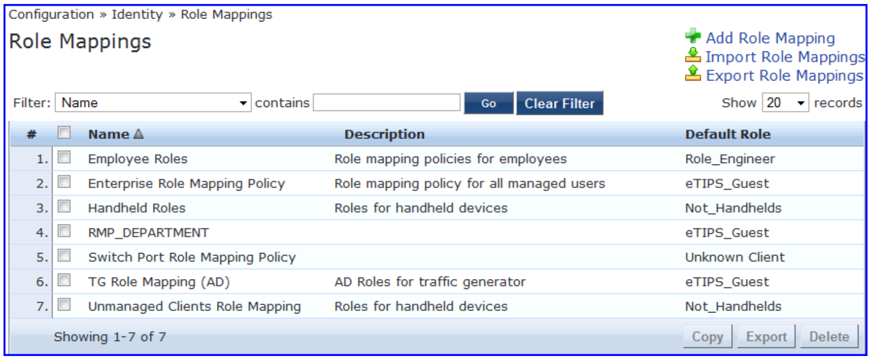
Table 90: *Add New Role Page Parameters*

Parameter	Description
Role Name /Description	Freeform label and description.

Adding and Modifying Role Mapping Policies

From the **Services** page (**Configuration** > **Service**), 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 148: *Role Mappings Page*



Configuration » Identity » Role Mappings

Role Mappings

#	□	Name	Description	Default Role
1.	□	Employee Roles	Role mapping policies for employees	Role_Engineer
2.	□	Enterprise Role Mapping Policy	Role mapping policy for all managed users	eTIPS_Guest
3.	□	Handheld Roles	Roles for handheld devices	Not_Handhelds
4.	□	RMP_DEPARTMENT		eTIPS_Guest
5.	□	Switch Port Role Mapping Policy		Unknown Client
6.	□	TG Role Mapping (AD)	AD Roles for traffic generator	eTIPS_Guest
7.	□	Unmanaged Clients Role Mapping	Roles for handheld devices	Not_Handhelds

Showing 1-7 of 7

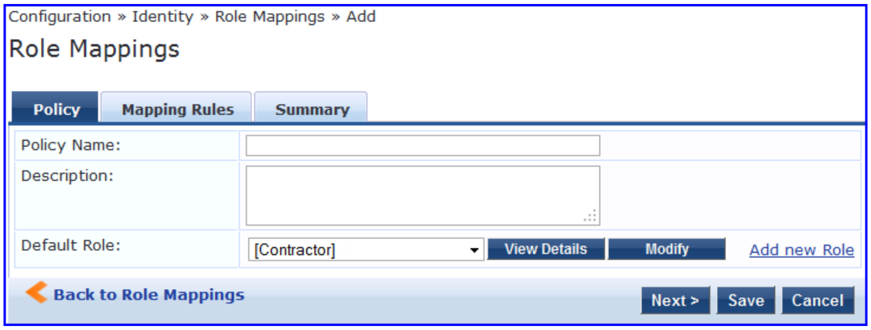
When you click **Add Role Mapping** from any of these locations, Policy Manager displays the **Add Role Mapping** popup, which contains the following three tabs:

- 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 149: *Role Mappings (Policy Tab)*



Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Name:	
Description:	
Default Role:	[Contractor]

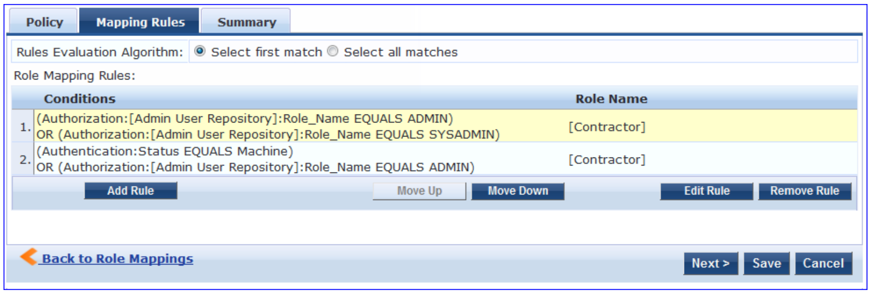
Table 91: *Role Mappings (Policy tab) Parameters*

Parameter	Description
Policy Name /Description	Freeform label and description.
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. Click on **Modify** to modify the default role. Click on **Add new Role** to add a new role.

Mapping Rules Tab

The **Mapping Rules** tab selects the evaluation algorithm, adds/edits/removes 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 150: *Role Mapping (Mapping Rules Tab)*



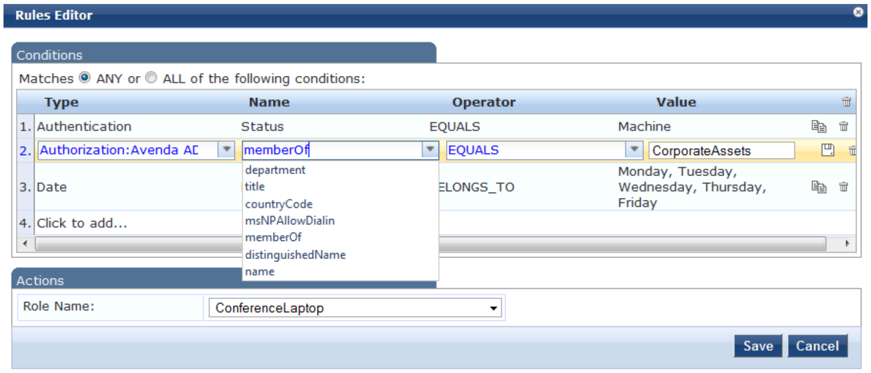
Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Role Mapping Rules:

	Conditions	Role Name
1.	(Authorization:[Admin User Repository]:Role_Name EQUALS ADMIN) OR (Authorization:[Admin User Repository]:Role_Name EQUALS SYSADMIN)	[Contractor]
2.	(Authentication:Status EQUALS Machine) OR (Authorization:[Admin User Repository]:Role_Name EQUALS ADMIN)	[Contractor]

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

Figure 151: *Rules Editor Page*



Matches ◉ ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Status	EQUALS	Machine
2.	Authorization:Avenda AD	memberOf	EQUALS	CorporateAssets
3.	Date		ELONGS_TO	Monday, Tuesday, Wednesday, Thursday, Friday
4.	Click to add...			

Role Name: ConferenceLaptop

Table 92: *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 445.) 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 149). 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 (of attribute)	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. Operators have their obvious meaning; for stated definitions of operator meaning, refer to "Operators" on page 456.
Value of attribute	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.

NOTE

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 195
- "Configuring Posture " on page 197
- "Adding a Posture Policy" on page 198
- "Adding and Modifying Posture Servers" on page 230

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.

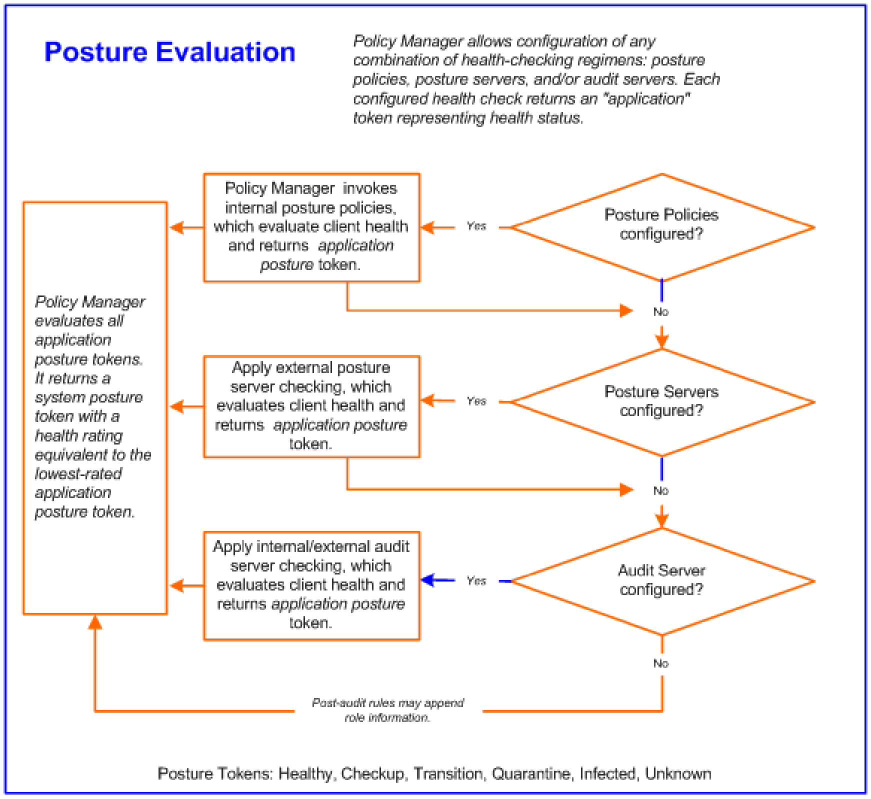
Posture Server

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 152: *Posture Evaluation Process*


Posture Evaluation
Policy Manager allows configuration of any combination of health-checking regimens: posture policies, posture servers, and/or audit servers. Each configured health check returns an "application" token representing health status.
Posture Policies configured?
Yes
Policy Manager invokes internal posture policies, which evaluate client health and returns application posture token.
No
Posture Servers configured?
Yes
Apply external posture server checking, which evaluates client health and returns application posture token.
No
Audit Server configured?
Yes
Apply internal/external audit server checking, which evaluates client health and returns application posture token.
No
Post-audit rules may append role information.
Policy Manager evaluates all application posture tokens. It returns a system posture token with a health rating equivalent to the lowest-rated application posture token.
Posture Tokens: Healthy, Checkup, Transition, Quarantine, Infected, Unknown

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.

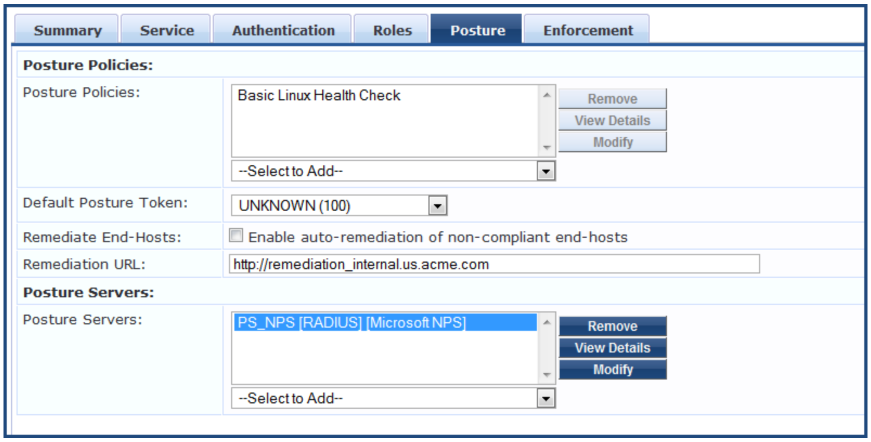
Configuring Posture

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.

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

Figure 153: *Posture Features at the Service Level*



Posture Policies:

Posture Policies: Basic Linux Health Check

--Select to Add--

Default Posture Token: UNKNOWN (100)

Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts

Remediation URL: http://remediation_internal.us.acme.com

Posture Servers:

Posture Servers: PS_NPS [RADIUS] [Microsoft NPS]

--Select to Add--

You can configure the following features of posture:

Table 93: *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 198. ● To edit the selected posture policy, click **Modify** and refer to "Adding a Posture Policy" on page 198.
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.

Table 93: *Posture Features at the Service Level (Continued)*

Configurable Component	How to Configure
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 230. - To edit the selected posture server, click **Modify** and refer to "Adding and Modifying Posture Servers" on page 230.
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 94: *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

Table 94: *NAP Agent Posture Plugins for Windows Operating Systems (Continued)*

		Operating System Versions					
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 95: *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 96: *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
ClearPass Windows 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 determine the service pack level.	yes	yes	yes	yes	yes	yes	yes
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 97: *OnGuard Agent (Persistent or Dissolvable) Posture Plugins for Mac OS X*

Plugin Name	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 - NTP Agent

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

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

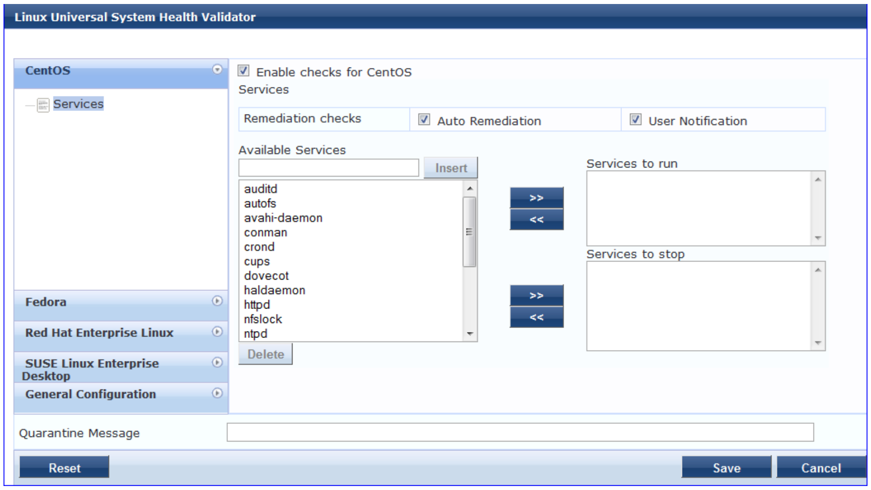
The configuration options and steps described under the "ClearPass Windows Universal System Health Validator - OnGuard Agent" on page 212 section also apply to the NTP Agent.

Even though the UI allows auto remediation configuration, the dissolvable OnGuard Agent does not support this feature.

ClearPass Linux Universal System Health Validator - NAP Agent

The **ClearPass Linux Universal System Health Validator** page popup appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration.

Figure 154: *ClearPass Linux Universal system Health Validator - NAP Agent*



Linux Universal System Health Validator

☑ Enable checks for CentOS

Services

Remediation checks ☑ Auto Remediation ☑ User Notification

Available Services

auditd
autofs
avahi-daemon
conman
crond
cups
dovecot
haldaemon
httpd
nfslock
ntpd

Quarantine Message

Select a Linux version and click the **Enable checks** check box for that version.

The **Services** view appears automatically and provides a set of widgets for specifying specific services to be explicitly running or stopped for the different Linux versions.

Table 98: *Services View*

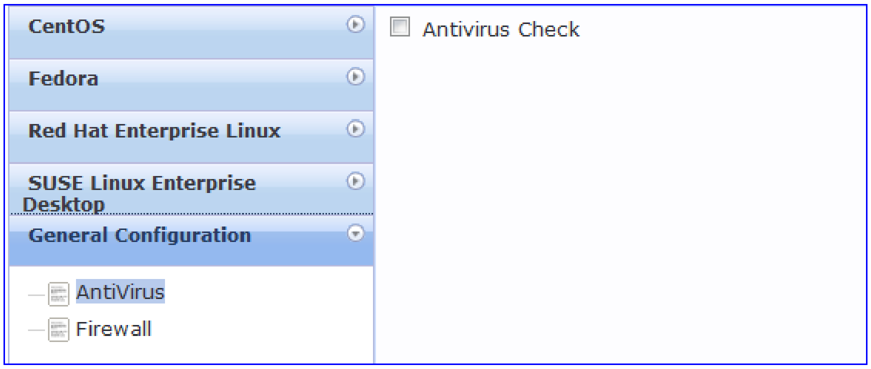
Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically start or stop services based on the entries in **Service to run** and **Service to stop** configuration).
User Notification	Enable to allow user notifications for service status policy violations.
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).
Insert	To add a service to the list of selectable services, enter its name in the text box adjacent to this button, then click **Insert**.
Delete	To remove a service from the list of selectable services, select it and click **Delete**.

The last option, located on the bottom of the list of Linux versions, is the **General Configuration** section. This section contains two pages: **Firewall Check** and **Antivirus Check**. Enable the check box in either page display its respective configuration view:

NOTE

The configurations done in the General Configuration section apply to all operating systems whose checks have been turned on.

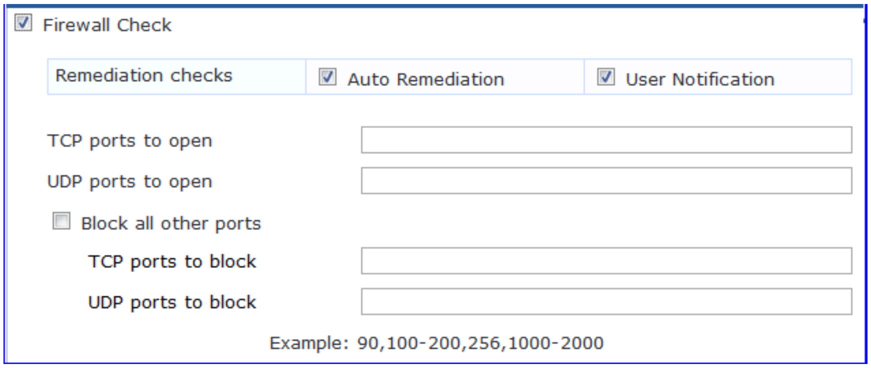
Figure 155: *General Configuration Section*



☐ Antivirus Check

Select **Firewall Check** to display a view where you can specify Firewall parameters, specifically with respect to which ports may be open or blocked.

Figure 156: *Firewall view*



☑ Firewall Check

Remediation checks	☑ Auto Remediation	☑ User Notification

TCP ports to open

UDP ports to open

☐ Block all other ports

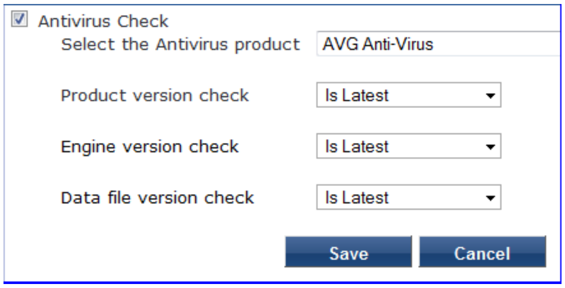
TCP ports to block

UDP ports to block

Example: 90,100-200,256,1000-2000

Select **Antivirus Check**, then click **Add** in the view that appears to specify Antivirus details.

Figure 157: *Antivirus Check view*

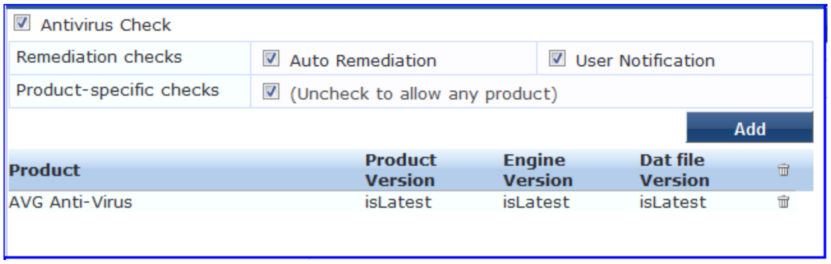


☑ Antivirus Check

Select the Antivirus product	AVG Anti-Virus
Product version check	Is Latest
Engine version check	Is Latest
Data file version check	Is Latest

When you save your Antivirus configuration, it appears in the Antivirus page list.

Figure 158: *Antivirus Check*



☑ Antivirus Check

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☑ (Uncheck to allow any product)	

Product	Product Version	Engine Version	Dat file Version	🗑
AVG Anti-Virus	isLatest	isLatest	isLatest	🗑

Table 99: *Antivirus Check*

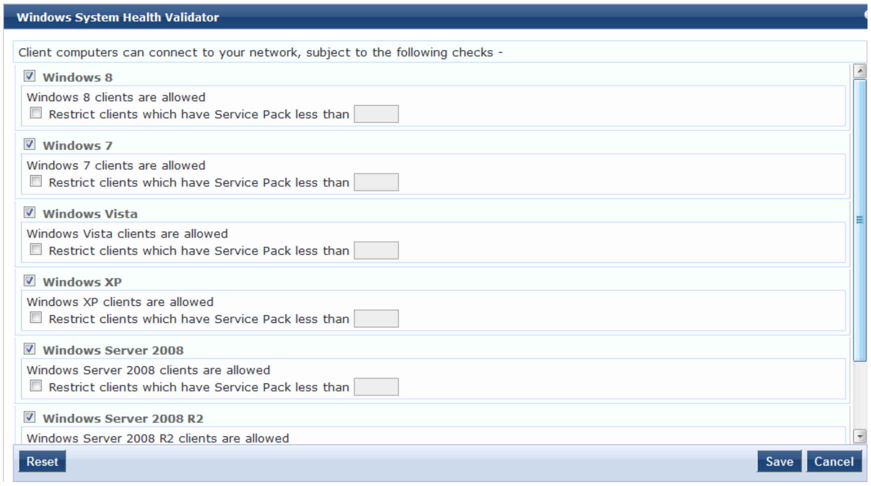
Interface	Parameter	Description
Antivirus Main view	Add	To configure Antivirus application attributes for testing against health data, click **Add.**
	Trashcan icon	To remove configured Antivirus application attributes from the list, click the **trashcan icon** in that row.
Antivirus Detail view	Product/Version/Last Check	Configure the specific settings for which to test against health data. These fields all have their obvious meaning (described in the ClearPass Windows Universal System Health Validator section).

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 159: *Windows System Health Validator (Overview)*



Windows System Health Validator

Client computers can connect to your network, subject to the following checks -

☑ Windows 8

Windows 8 clients are allowed

☐ Restrict clients which have Service Pack less than

☑ Windows 7

Windows 7 clients are allowed

☐ Restrict clients which have Service Pack less than

☑ Windows Vista

Windows Vista clients are allowed

☐ Restrict clients which have Service Pack less than

☑ Windows XP

Windows XP clients are allowed

☐ Restrict clients which have Service Pack less than

☑ Windows Server 2008

Windows Server 2008 clients are allowed

☐ Restrict clients which have Service Pack less than

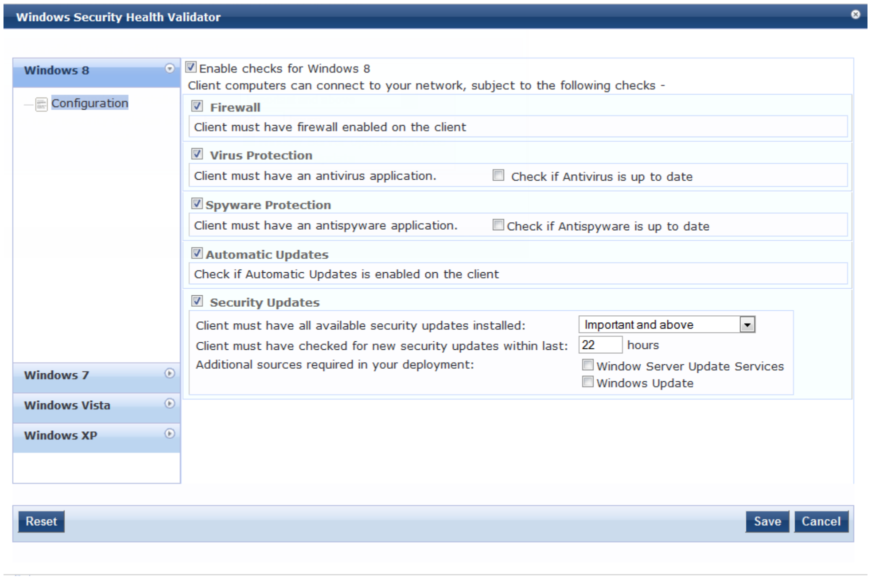
☑ Windows Server 2008 R2

Windows Server 2008 R2 clients are allowed

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 160: *Windows Security Health Validator*



☑ Enable checks for Windows 8

Client computers can connect to your network, subject to the following checks -

☑ **Firewall**

Client must have firewall enabled on the client

☑ **Virus Protection**

Client must have an antivirus application. □ Check if Antivirus is up to date

☑ **Spyware Protection**

Client must have an antispyware application. □ Check if Antispyware is up to date

☑ **Automatic Updates**

Check if Automatic Updates is enabled on the client

☑ **Security Updates**

Client must have all available security updates installed: Important and above

Client must have checked for new security updates within last: 22 hours

Additional sources required in your deployment: □ Window Server Update Services □ Windows Update

ClearPass Linux Universal System Health Validator - OnGuard Agent

The **ClearPass Linux Universal System Health Validator - OnGuard Agent** page popup appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration (When you select **Linux** and **OnGuard Agent** from the posture policy page).

The dissolvable agent version of the ClearPass Linux Universal System Health Validator supports all the features supported by the "ClearPass Linux Universal System Health Validator - NAP Agent" on page 201 except for the following:

- Auto-remediation
- Firewall status check and control

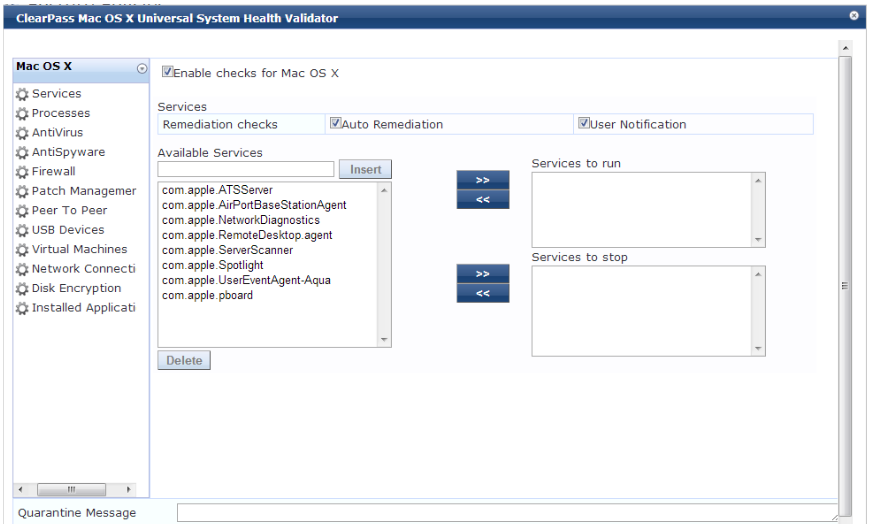
ClearPass Mac OS X Universal System Health Validator - OnGuard Agent

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 206
- "Processes" on page 206
- "Antivirus" on page 207
- "AntiSpyware" on page 207
- "Firewall " on page 208
- "Patch Management" on page 209
- "USB Devices" on page 209
- "Virtual Machine" on page 210
- "Network Connections" on page 210
- "Disk Encryption" on page 210
- "Installed Applications" on page 211

Figure 161: *ClearPass Mac OS X Universal System Health Validator - OnGuard Agent*



☑ Enable checks for Mac OS X

Services

Remediation checks ☑ Auto Remediation ☑ User Notification

Available Services

com.apple.ATSServer
com.apple.AirPortBaseStationAgent
com.apple.NetworkDiagnostics
com.apple.RemoteDesktop.agent
com.apple.ServerScanner
com.apple.Spotlight
com.apple.UserEventAgent-Aqua
com.apple.pboard

Services to run

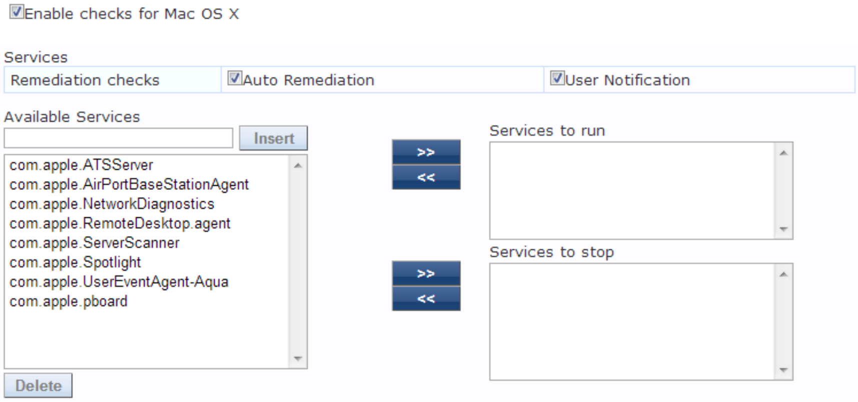
Services to stop

Quarantine Message

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 212 for a description of the fields on this page.

Figure 162: *Services Configuration Page*



☑ Enable checks for Mac OS X

Services

Remediation checks ☑ Auto Remediation ☑ User Notification

Available Services

com.apple.ATSServer
com.apple.AirPortBaseStationAgent
com.apple.NetworkDiagnostics
com.apple.RemoteDesktop.agent
com.apple.ServerScanner
com.apple.Spotlight
com.apple.UserEventAgent-Aqua
com.apple.pboard

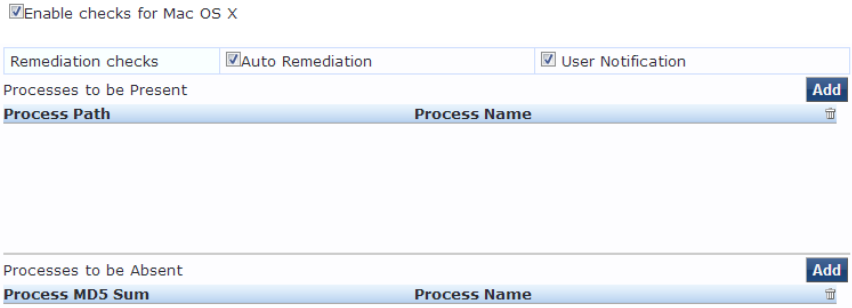
Services to run

Services to stop

Processes

The **Processes** page provides a set of components for specifying specific processes to be explicitly present or absent on the system.

Figure 163: *Processes Page*



☑ Enable checks for Mac OS X

Remediation checks ☑ Auto Remediation ☑ User Notification

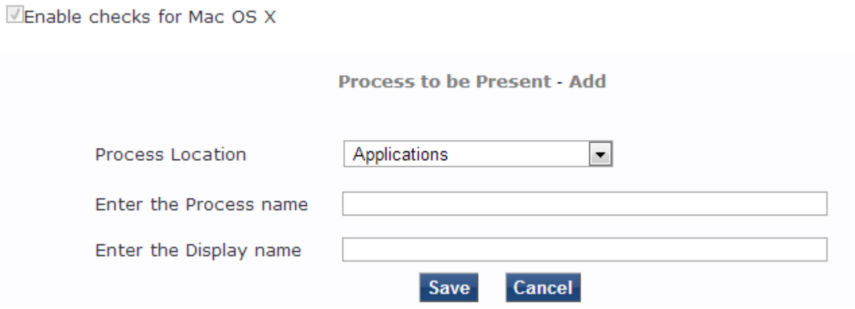
Processes to be Present

Process Path	Process Name

Processes to be Absent

Process MD5 Sum	Process Name

Figure 164: *Processes Add Page*



☑ Enable checks for Mac OS X

Process to be Present - Add

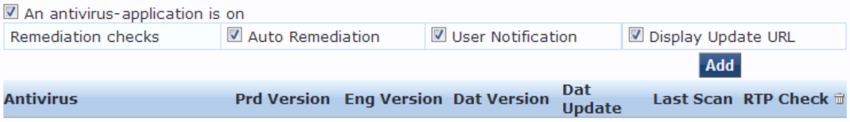
Process Location	Applications
Enter the Process name	
Enter the Display name	

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 165: *Antivirus Page (Detail 1)*



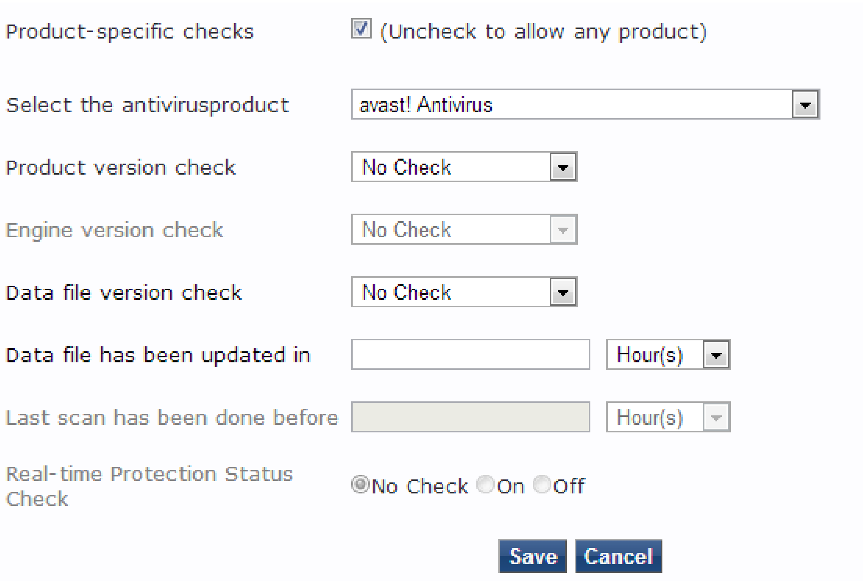
☑ An antivirus-application is on

Remediation checks	☑ Auto Remediation	☑ User Notification	☑ Display Update URL

Antivirus	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	RTP Check

Click **Add** to specify product and version check information.

Figure 166: *Antivirus Page (Detail 2)*



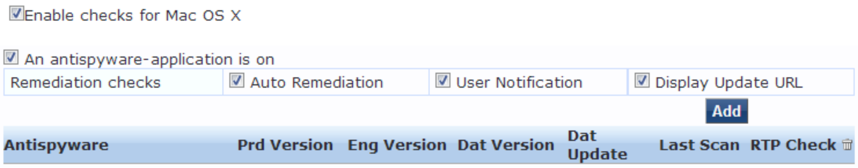
Product-specific checks	☑ (Uncheck to allow any product)
Select the antivirusproduct	avast! Antivirus
Product version check	No Check
Engine version check	No Check
Data file version check	No Check
Data file has been updated in	Hour(s)
Last scan has been done before	Hour(s)
Real-time Protection Status Check	● No Check ○ On ○ Off

When you save your Antivirus configuration, it appears in the **Antivirus** page list. See "ClearPass Windows Universal System Health Validator - OnGuard Agent" on page 212 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 167: *AntiSpyware Page*



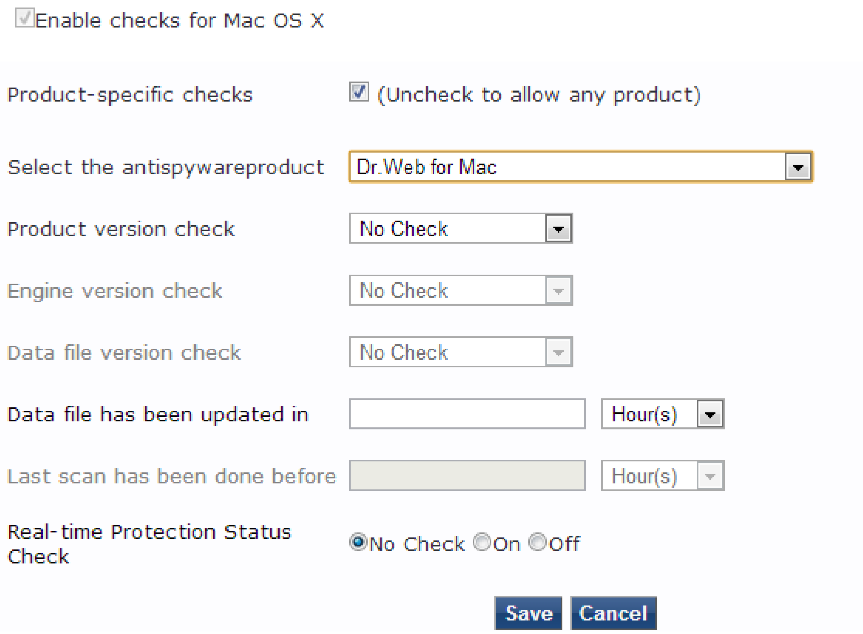
☑Enable checks for Mac OS X

☑ An antispyware-application is on

Remediation checks	☑ Auto Remediation	☑ User Notification	☑ Display Update URL

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	RTP Check

Figure 168: *AntiSpyware Add Page*



☑Enable checks for Mac OS X

Product-specific checks	☑ (Uncheck to allow any product)
Select the antispywareproduct	Dr.Web for Mac
Product version check	No Check
Engine version check	No Check
Data file version check	No Check
Data file has been updated in	Hour(s)
Last scan has been done before	Hour(s)
Real-time Protection Status Check	● No Check ○ On ○ Off

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.

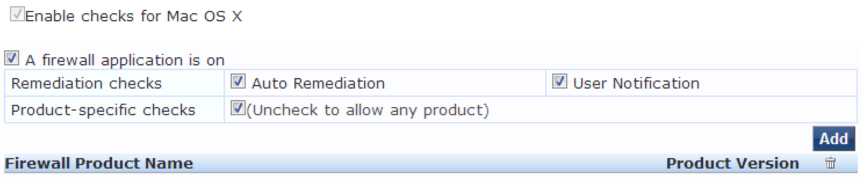
The configuration elements are the same for anti-virus and antispyware products. Refer to the anti-virus configuration instructions above.

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 169: *Firewall Page*



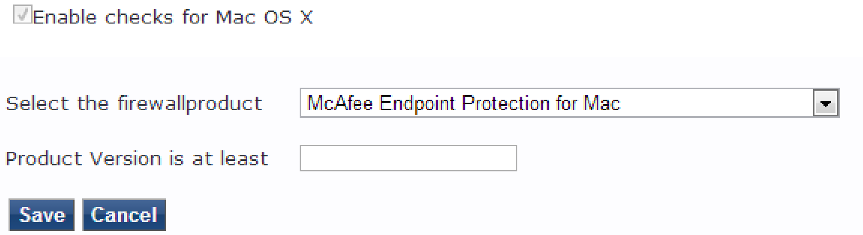
☑Enable checks for Mac OS X

☑ A firewall application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☑(Uncheck to allow any product)	

Firewall Product Name	Product Version

Figure 170: *Firewall Add Page*



☑ Enable checks for Mac OS X

Select the firewallproduct: McAfee Endpoint Protection for Mac

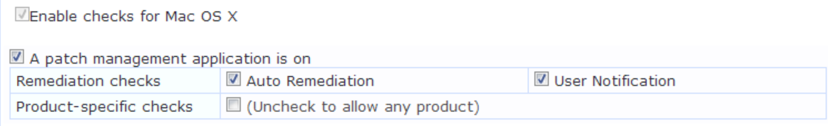
Product Version is at least:

When enabled, the **Firewall** detail page appears. See "ClearPass Windows Universal System Health Validator - OnGuard Agent" on page 212 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 171: *Patch Management Overview*

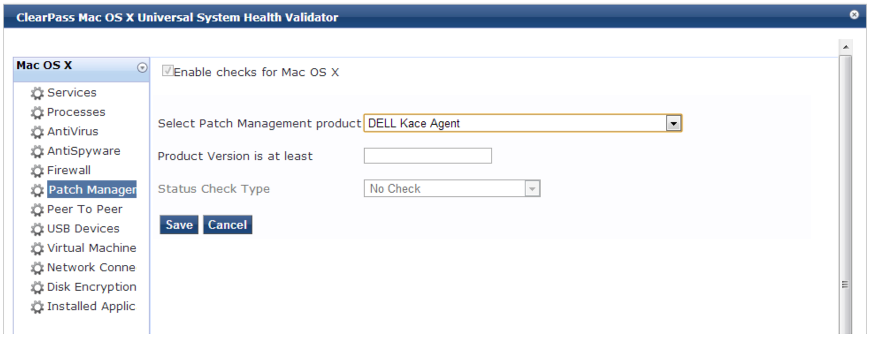


☑ Enable checks for Mac OS X

☑ A patch management application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	□ (Uncheck to allow any product)	

Figure 172: *Patch Management Add Page*



☑ Enable checks for Mac OS X

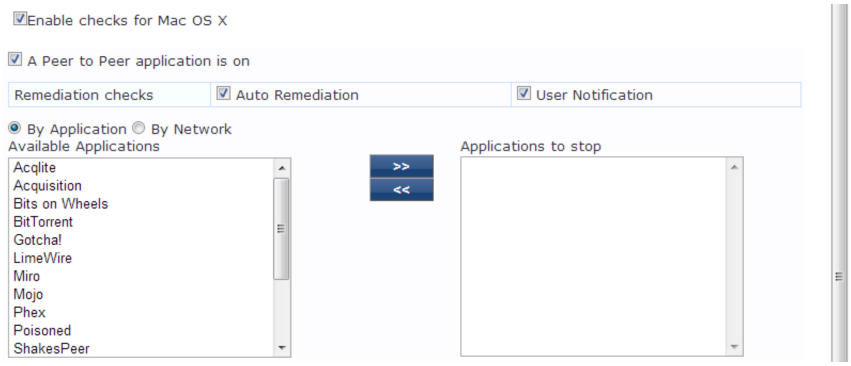
Select Patch Management product: DELL Kace Agent

Product Version is at least:

Status Check Type: No Check

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.



☑ Enable checks for Mac OS X

☑ A Peer to Peer application is on

Remediation checks	☑ Auto Remediation	☑ User Notification

● By Application ○ By Network

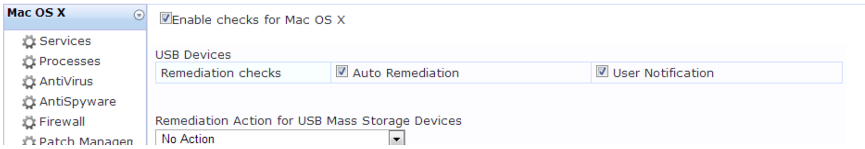
Available Applications: Acqlite, Acquisition, Bits on Wheels, BitTorrent, Gotcha!, LimeWire, Miro, Mojo, Phex, Poisoned, ShakesPeer

Applications to stop:

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 173: *USB Devices Page*



☑Enable checks for Mac OS X

USB Devices

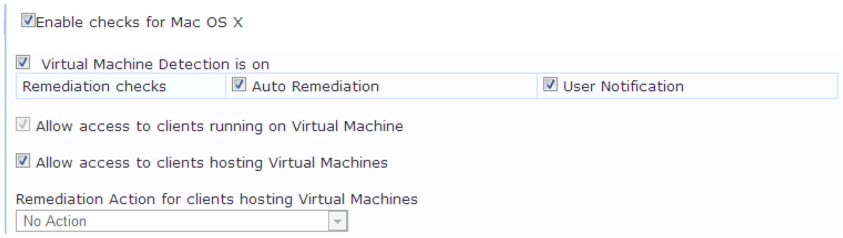
Remediation checks	☑ Auto Remediation	☑ User Notification

Remediation Action for USB Mass Storage Devices: No Action

Virtual Machine

The **Virtual Machines** page provides configuration to Virtual Machines utilized by your network.

Figure 174: *Virtual Machine Page*



☑Enable checks for Mac OS X

☑ Virtual Machine Detection is on

Remediation checks	☑ Auto Remediation	☑ User Notification

☑ Allow access to clients running on Virtual Machine

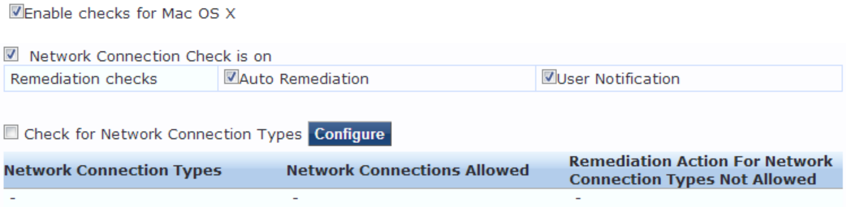
☑ Allow access to clients hosting Virtual Machines

Remediation Action for clients hosting Virtual Machines: No Action

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 175: *Network Connections Overview Page*



☑Enable checks for Mac OS X

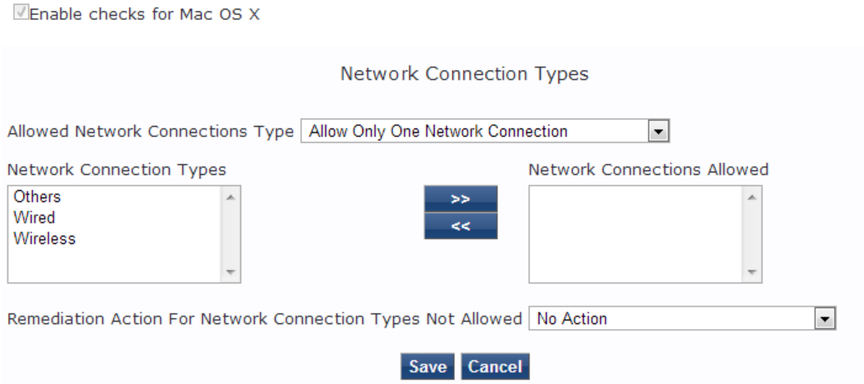
☑ Network Connection Check is on

Remediation checks	☑Auto Remediation	☑User Notification

□ Check for Network Connection Types

Network Connection Types	Network Connections Allowed	Remediation Action For Network Connection Types Not Allowed
-	-	-

Figure 176: *Network Connections Configuration Page*



☑Enable checks for Mac OS X

Network Connection Types

Allowed Network Connections Type: Allow Only One Network Connection

Network Connection Types: Others, Wired, Wireless

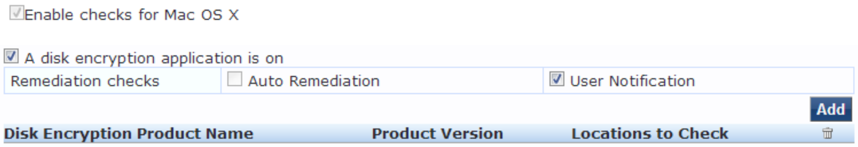
Network Connections Allowed:

Remediation Action For Network Connection Types Not Allowed: No Action

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 177: *Disk Encryption Page*



☑ Enable checks for Mac OS X

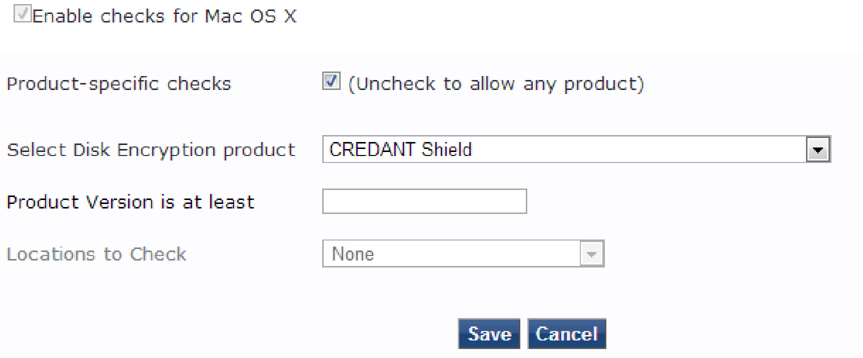
☑ A disk encryption application is on

Remediation checks	□ Auto Remediation	☑ User Notification

Add

Disk Encryption Product Name	Product Version	Locations to Check

Figure 178: *Disk Encryption Add Page*



☑ Enable checks for Mac OS X

Product-specific checks	☑ (Uncheck to allow any product)
Select Disk Encryption product	CREDANT Shield
Product Version is at least	
Locations to Check	None

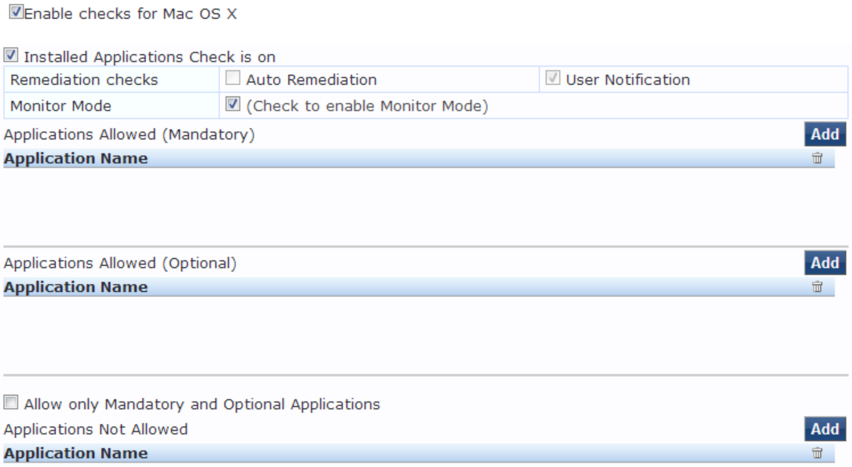
Save Cancel

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 179: *Installed Applications Page*



☑ Enable checks for Mac OS X

☑ Installed Applications Check is on

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	☑ (Check to enable Monitor Mode)	

Applications Allowed (Mandatory) Add

Application Name

Applications Allowed (Optional) Add

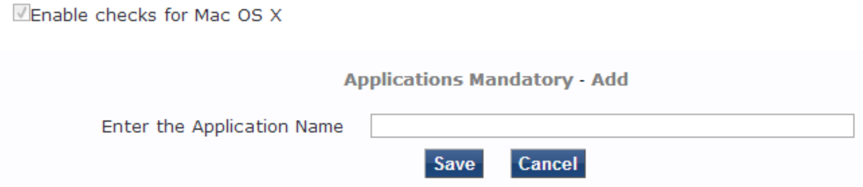
Application Name

□ Allow only Mandatory and Optional Applications

Applications Not Allowed Add

Application Name

Figure 180: *Installed Applications Add Page*



☑ Enable checks for Mac OS X

Applications Mandatory - Add

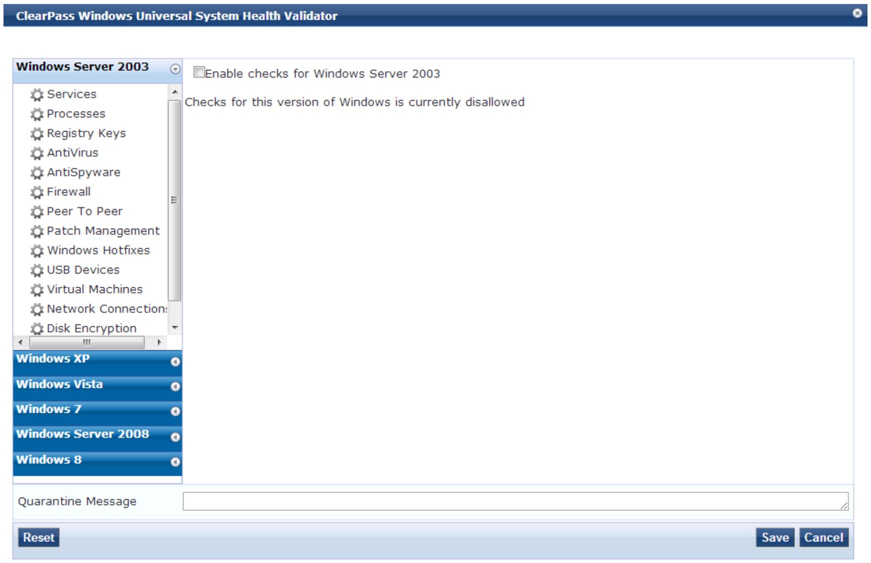
Enter the Application Name

Save Cancel

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 181: *ClearPass Windows Universal System Health Validator*



□ Enable checks for Windows Server 2003

Checks for this version of Windows is currently disallowed

Quarantine Message

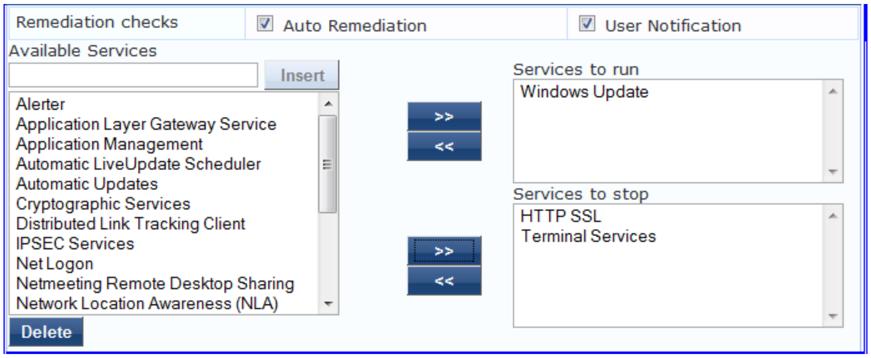
Select a version of Windows and click the check box to enable checks for that version. Enabling checks for a specific version displays the following set of configuration pages. These pages are explained in the following sections.

- "Services" on page 212
- "Processes" on page 213
- "Registry Keys" on page 216
- "AntiVirus" on page 217
- "AntiSpyware" on page 219
- "Firewall" on page 220
- "Peer To Peer" on page 221
- "Patch Management" on page 222
- "Windows Hotfixes" on page 224
- "USB Devices" on page 224
- "Virtual Machines" on page 225
- "Network Connections" on page 225
- "Disk Encryption" on page 227
- "Installed Applications" on page 228

Services

The **Services** page provides a set of widgets for specifying services to run or stop.

Figure 182: *Services Page*



Remediation checks ☑ Auto Remediation ☑ User Notification

Available Services

Alerter
Application Layer Gateway Service
Application Management
Automatic LiveUpdate Scheduler
Automatic Updates
Cryptographic Services
Distributed Link Tracking Client
IPSEC Services
Net Logon
Netmeeting Remote Desktop Sharing
Network Location Awareness (NLA)

Services to run

Windows Update

Services to stop

HTTP SSL
Terminal Services

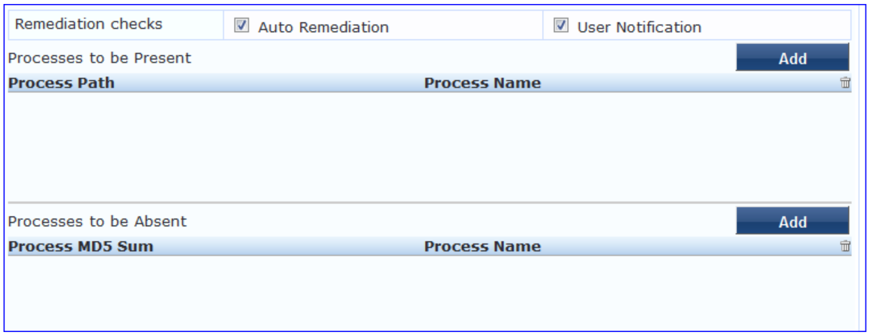
Table 100: *Services Page*

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 183: *Processes Page (Overview)*



Remediation checks ☑ Auto Remediation ☑ User Notification

Processes to be Present

Process Path	Process Name

Processes to be Absent

Process MD5 Sum	Process Name

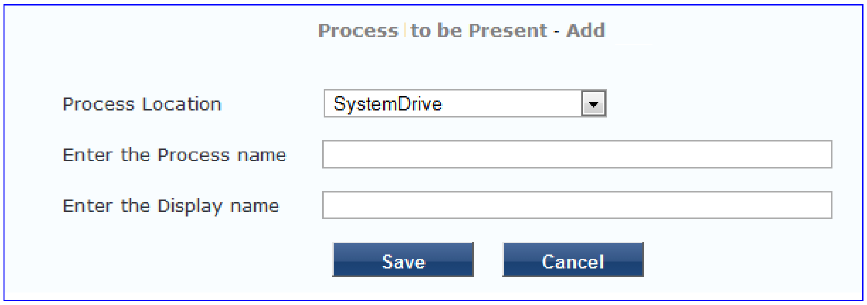
Table 101: *Process Page (Overview - Pre-Add)*

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 184: *Process to be Present Page (Detail)*



Process to be Present - Add

Process Location: SystemDrive

Enter the Process name:

Enter the Display name:

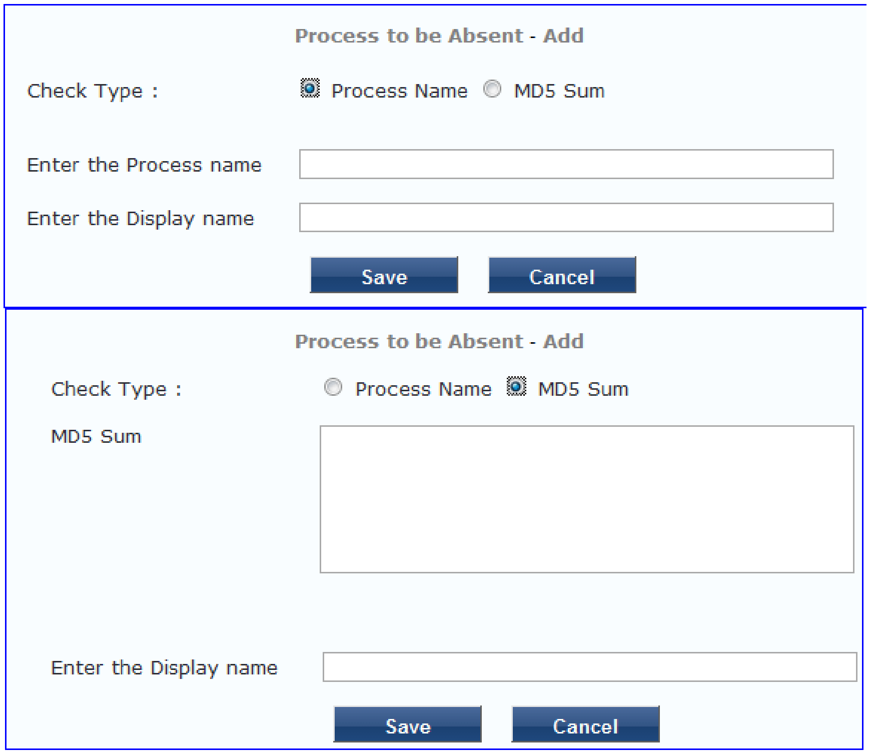
Table 102: *Process to be Present Page (Detail)*

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 185: *Process to be Absent Page (Detail)*



Process to be Absent - Add

Check Type : ● Process Name ○ MD5 Sum

Enter the Process name

Enter the Display name

Process to be Absent - Add

Check Type : ○ Process Name ● MD5 Sum

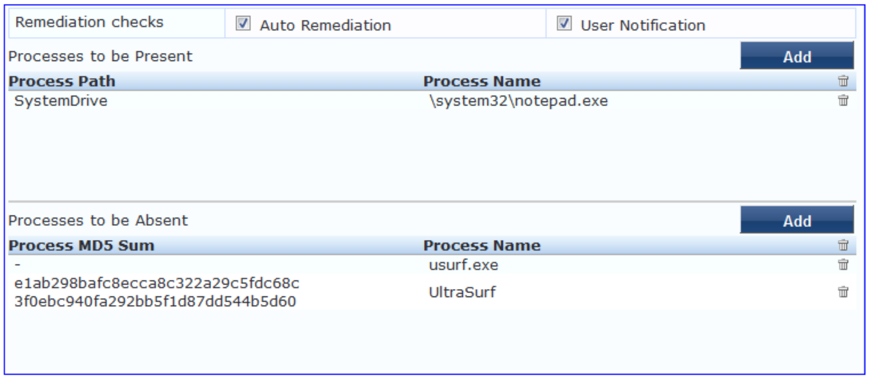
MD5 Sum

Enter the Display name

Table 103: *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 186: *Process Page (Overview - Post Add)*



Remediation checks ☑ Auto Remediation ☑ User Notification

Processes to be Present

Process Path	Process Name
SystemDrive	\system32\notepad.exe

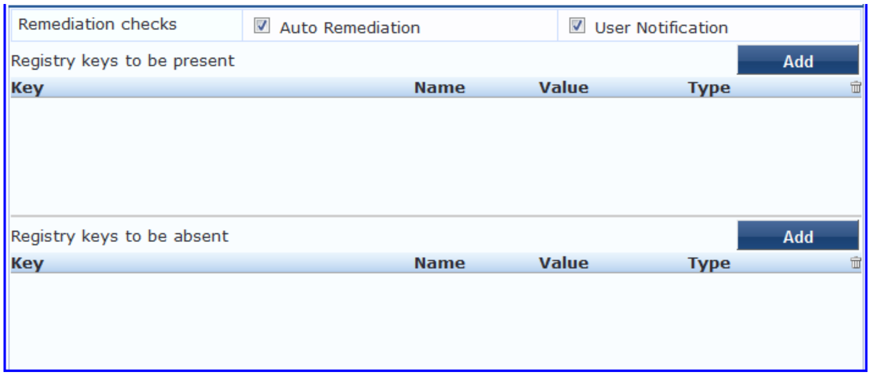
Processes to be Absent

Process MD5 Sum	Process Name
-	usurf.exe
e1ab298bafc8ecca8c322a29c5fdc68c 3f0ebc940fa292bb5f1d87dd544b5d60	UltraSurf

Registry Keys

The **Registry Keys** page provides a set of parameters that are used to specify which registry keys are to be explicitly present or absent.

Figure 187: *Registry Keys Page (Overview)*



Remediation checks ☑ Auto Remediation ☑ User Notification

Registry keys to be present

Key	Name	Value	Type

Registry keys to be absent

Key	Name	Value	Type

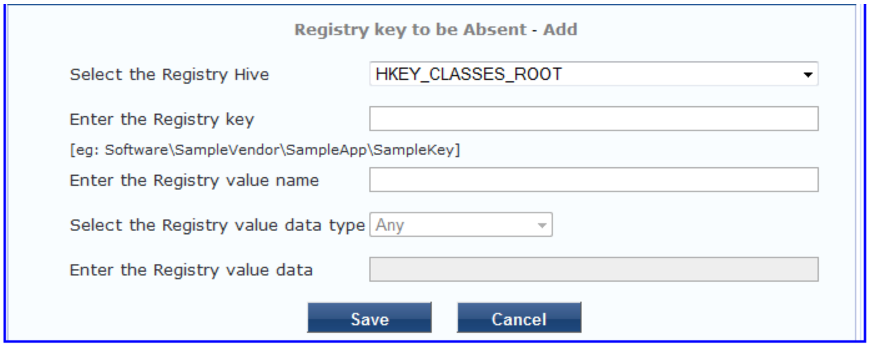
Table 104: *Registry Keys Page (Overview - Pre-Add)*

Parameter	Description
Auto Remediation	Enable to allow 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** configuration.
User Notification	Enable to allow user notifications for registry check policy violations.
Registry keys to be present/absent	Click **Add** to specify a registry key to be added, either to the **Registry keys to be present** or **Registry keys to be absent** lists.

Click **Add** for either condition to display the **Registry** page detail.

Registry Keys to be Absent

Figure 188: *Registry Keys Page (Detail)*



Registry key to be Absent - Add

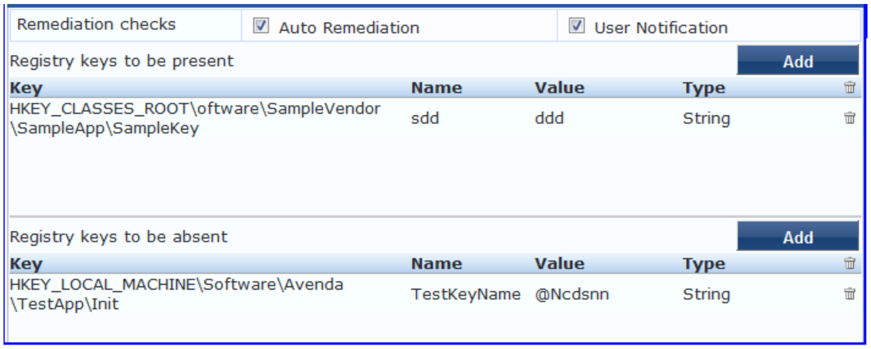
Select the Registry Hive	HKEY_CLASSES_ROOT
Enter the Registry key [eg: Software\SampleVendor\SampleApp\SampleKey]	
Enter the Registry value name	
Select the Registry value data type	Any
Enter the Registry value data	

Table 105: *Registry Keys Page (Detail)*

Parameter	Description
Hive/Key/value (name, type, data)	Identifying information for a specific setting for a specific registry key.

After you save the Registry details, the information appears in the **Registry** page list.

Figure 189: *Registry Keys Page (Overview - Post Add)*



Remediation checks ☑ Auto Remediation ☑ User Notification

Registry keys to be present

Key	Name	Value	Type
HKEY_CLASSES_ROOT\oftware\SampleVendor\SampleApp\SampleKey	sdd	ddd	String

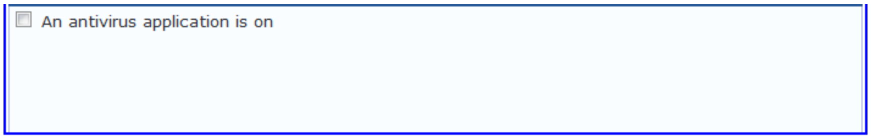
Registry keys to be absent

Key	Name	Value	Type
HKEY_LOCAL_MACHINE\Software\Avenda\TestApp\Init	TestKeyName	@Ncdsnn	String

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.

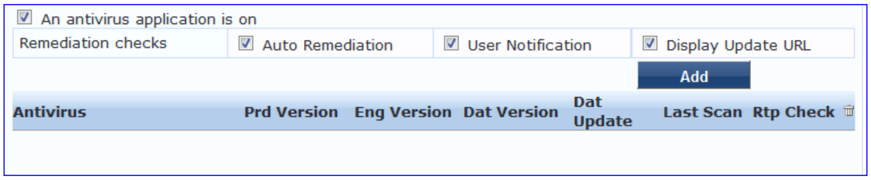
Figure 190: *Antivirus Page (Overview - Before)*



☐ An antivirus application is on

When enabled, the **Antivirus** detail page appears.

Figure 191: *Antivirus Page (Detail 1)*



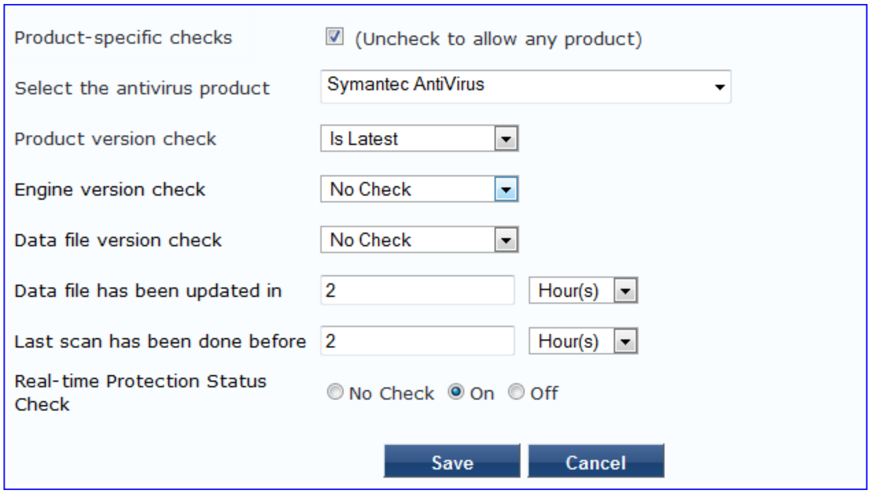
☑ An antivirus application is on

Remediation checks ☑ Auto Remediation ☑ User Notification ☑ Display Update URL

Antivirus	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check

Click **Add** to specify product, and version check information.

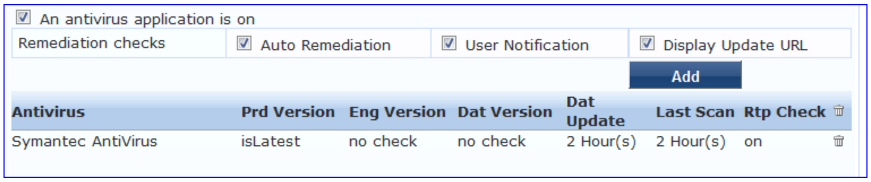
Figure 192: *Antivirus Page (Detail 2)*



Product-specific checks	☑ (Uncheck to allow any product)
Select the antivirus product	Symantec AntiVirus
Product version check	Is Latest
Engine version check	No Check
Data file version check	No Check
Data file has been updated in	2 Hour(s)
Last scan has been done before	2 Hour(s)
Real-time Protection Status Check	○ No Check ● On ○ Off

After you save your Antivirus configuration, it appears in the **Antivirus** page list.

Figure 193: *Antivirus Page (Overview - After)*



☑ An antivirus application is on

Remediation checks ☑ Auto Remediation ☑ User Notification ☑ Display Update URL

Antivirus	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check
Symantec AntiVirus	isLatest	no check	no check	2 Hour(s)	2 Hour(s)	on

Table 106: *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**.

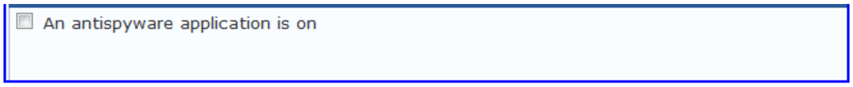
Table 106: *Antivirus Page (Continued)*

Interface	Parameter	Description
Antivirus Page (Detail 2)	- Product-specific checks - Select the antivirus product - Product version check - Engine version check - Engine version check - Datafile version check - Data file has been updated in - Last scan has been done before - Real-time Protection Status 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 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, On, or 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.

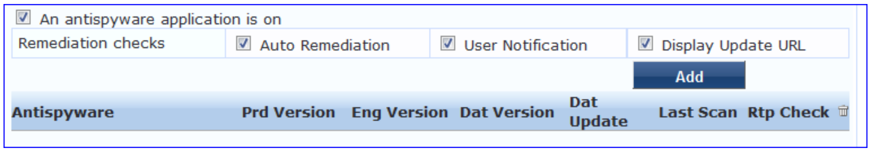
Figure 194: *AntiSpyware Page (Overview Before)*



□ An antispyware application is on

When enabled, the **AntiSpyware** detail page appears.

Figure 195: *AntiSpyware Page (Detail 1)*



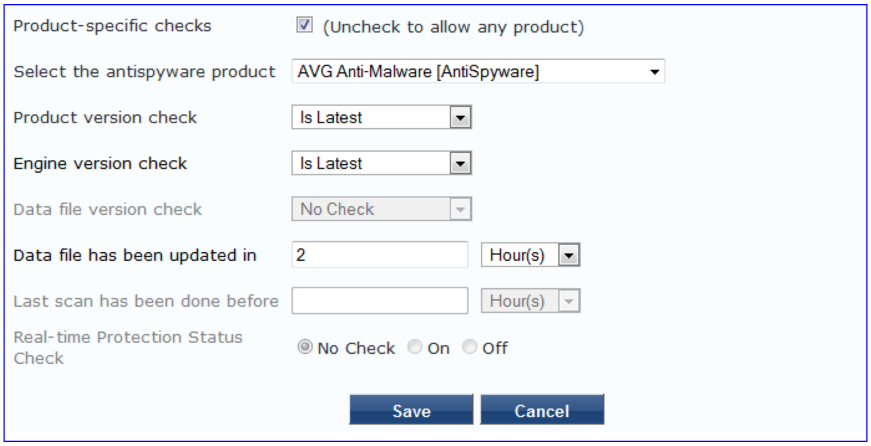
☑ An antispyware application is on

Remediation checks	☑ Auto Remediation	☑ User Notification	☑ Display Update URL

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check

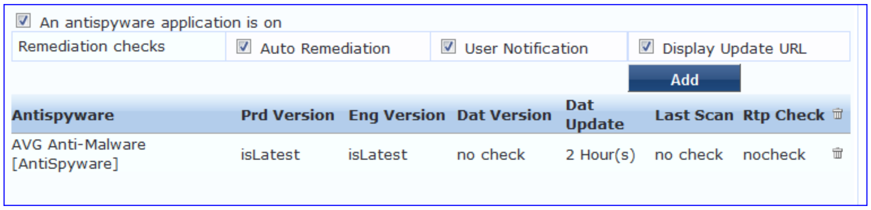
Click **Add** to specify product, and version check information.

Figure 196: *AntiSpyware Page (Detail 2)*



Product-specific checks	☑ (Uncheck to allow any product)
Select the antispyware product	AVG Anti-Malware [AntiSpyware]
Product version check	Is Latest
Engine version check	Is Latest
Data file version check	No Check
Data file has been updated in	2 Hour(s)
Last scan has been done before	Hour(s)
Real-time Protection Status Check	● No Check ○ On ○ Off

Figure 197: *AntiSpyware Page (Overview After)*



☑ An antispyware application is on

Remediation checks ☑ Auto Remediation ☑ User Notification ☑ Display Update URL

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check
AVG Anti-Malware [AntiSpyware]	isLatest	isLatest	no check	2 Hour(s)	no check	nocheck

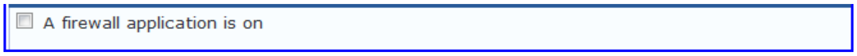
When you save your AntiSpyware configuration, it appears in the **AntiSpyware** page list.

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.

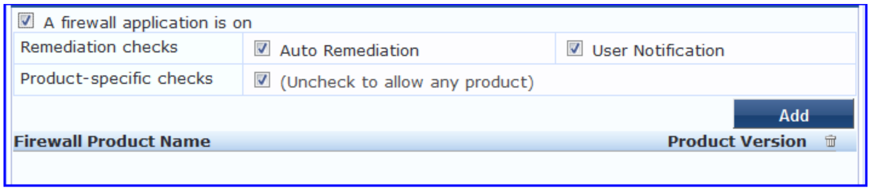
Figure 198: *Firewall Page (Overview Before)*



□ A firewall application is on

In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

Figure 199: *Firewall Page (Detail 1)*



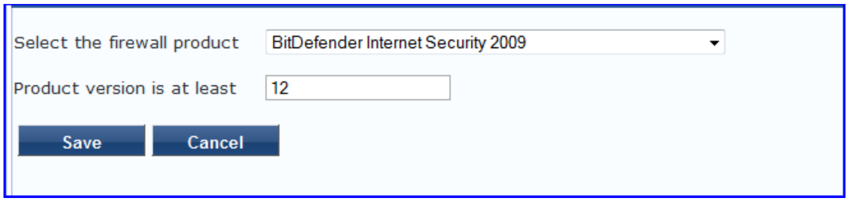
☑ A firewall application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☑ (Uncheck to allow any product)	

Firewall Product Name	Product Version

When enabled, the **Firewall** detail page appears.

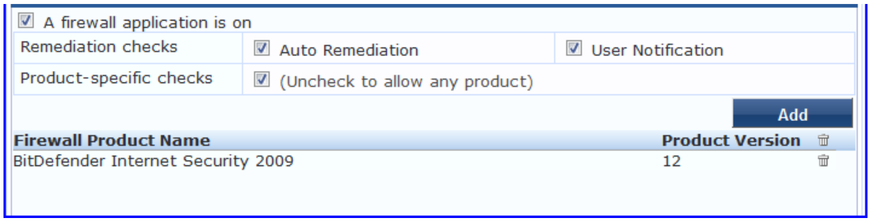
Figure 200: *Firewall Page (Detail 2)*



Select the firewall product	BitDefender Internet Security 2009
Product version is at least	12

When you save your Firewall configuration, it appears in the **Firewall** page list.

Figure 201: *Firewall Page (Overview After)*



☑ A firewall application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☑ (Uncheck to allow any product)	

Firewall Product Name	Product Version
BitDefender Internet Security 2009	12

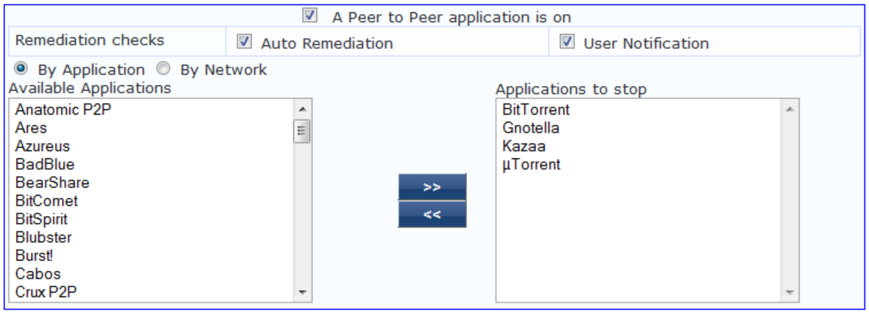
Table 107: *Firewall Page*

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 202: *Peer to Peer Page*



☑ A Peer to Peer application is on

Remediation checks	☑ Auto Remediation	☑ User Notification

● By Application ○ By Network

Available Applications

Anatomic P2P
Ares
Azureus
BadBlue
BearShare
BitComet
BitSpirit
Blubster
Burst!
Cabos
Crux P2P

Applications to stop

BitTorrent
Gnotella
Kazaa
µTorrent

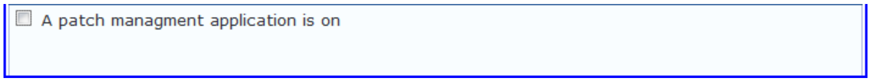
Table 108: *Peer to Peer Page*

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.

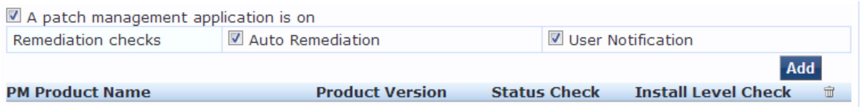
Figure 203: *Patch Management Page (Overview - Before)*



☐ A patch managment application is on

When enabled, the **Patch Management** detail page appears.

Figure 204: *Patch Management Page (Detail 1)*



☑ A patch management application is on

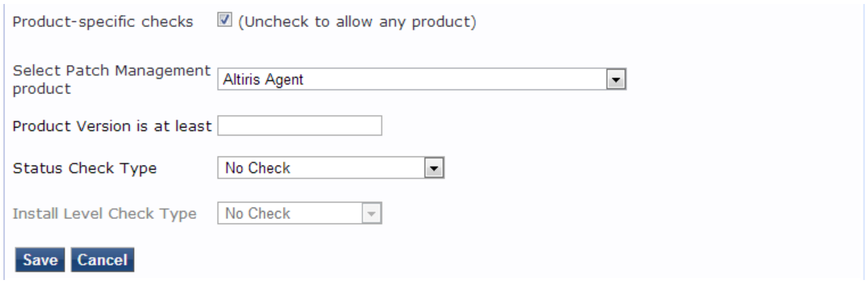
Remediation checks ☑ Auto Remediation ☑ User Notification

Add

PM Product Name	Product Version	Status Check	Install Level Check	

Click **Add** to specify PM Product Name, Product Version, Status Check and Install Level Check information.

Figure 205: *Patch Management Page (Detail 2)*



Product-specific checks ☑ (Uncheck to allow any product)

Select Patch Management product: Altiris Agent

Product Version is at least:

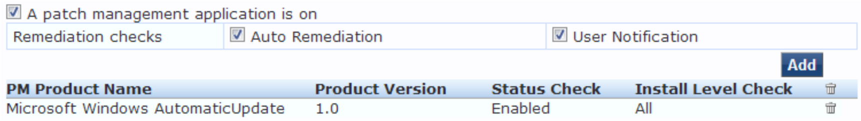
Status Check Type: No Check

Install Level Check Type: No Check

Save Cancel

When you save your patches configuration, it appears in the **Patch Management** page list.

Figure 206: *Patch Management Page (Overview - After)*



☑ A patch management application is on

Remediation checks ☑ Auto Remediation ☑ User Notification

Add

PM Product Name	Product Version	Status Check	Install Level Check
Microsoft Windows AutomaticUpdate	1.0	Enabled	All

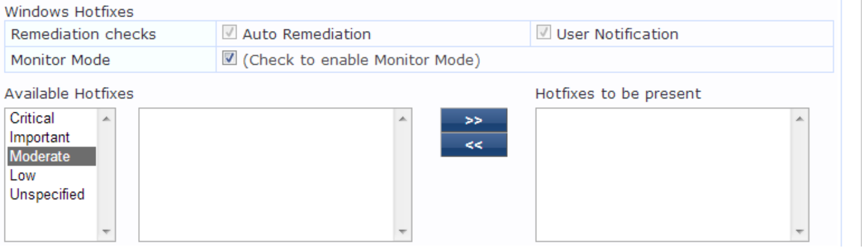
Table 109: *Patch Management Page*

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 checkbox is checked. - **Product version is at least:** Enter version number. This option is *only* enabled if the Product-specific checks check box is checked. - **Status Check Type:** Select No check, Enabled, or Disabled. This option is always available. - **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 207: *Windows Hotfixes Page*



Windows Hotfixes

Remediation checks ☑ Auto Remediation ☑ User Notification

Monitor Mode ☑ (Check to enable Monitor Mode)

Available Hotfixes

Hotfixes to be present

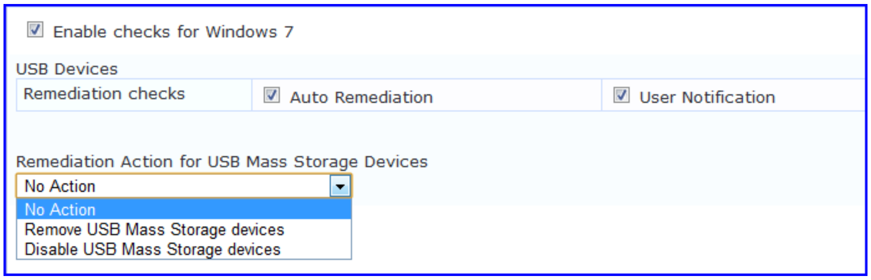
Table 110: *Windows Hotfixes*

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 208: *USB Devices*



☑ Enable checks for Windows 7

USB Devices

Remediation checks ☑ Auto Remediation ☑ User Notification

Remediation Action for USB Mass Storage Devices

No Action

No Action
Remove USB Mass Storage devices
Disable USB Mass Storage devices

Table 111: *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).

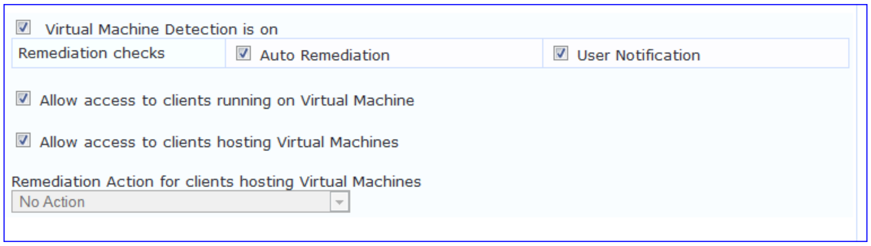
Table 111: *USB Devices (Continued)*

Parameter	Description
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 209: *Virtual Machines*



☑ Virtual Machine Detection is on

Remediation checks ☑ Auto Remediation ☑ User Notification

☑ Allow access to clients running on Virtual Machine

☑ Allow access to clients hosting Virtual Machines

Remediation Action for clients hosting Virtual Machines: No Action

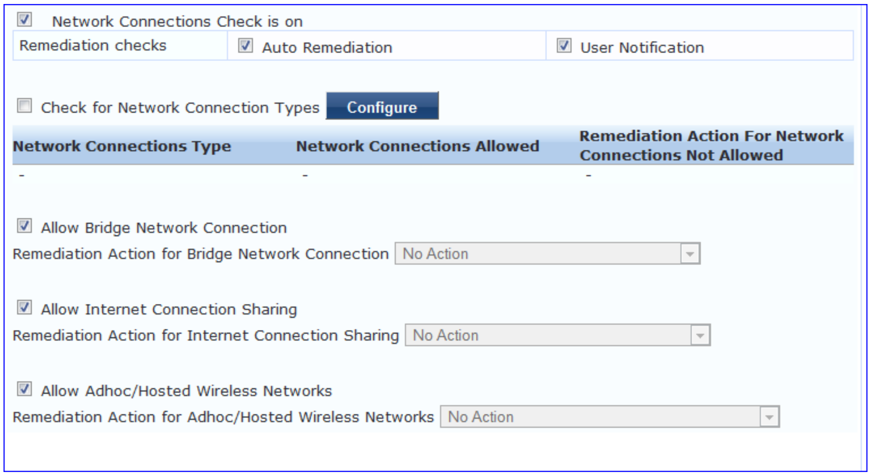
Table 112: *Virtual Machines*

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 210: *Network Connections*



☑ Network Connections Check is on

Remediation checks	☑ Auto Remediation	☑ User Notification

□ Check for Network Connection Types

Network Connections Type	Network Connections Allowed	Remediation Action For Network Connections Not Allowed
-	-	-

☑ Allow Bridge Network Connection

Remediation Action for Bridge Network Connection: No Action

☑ Allow Internet Connection Sharing

Remediation Action for Internet Connection Sharing: No Action

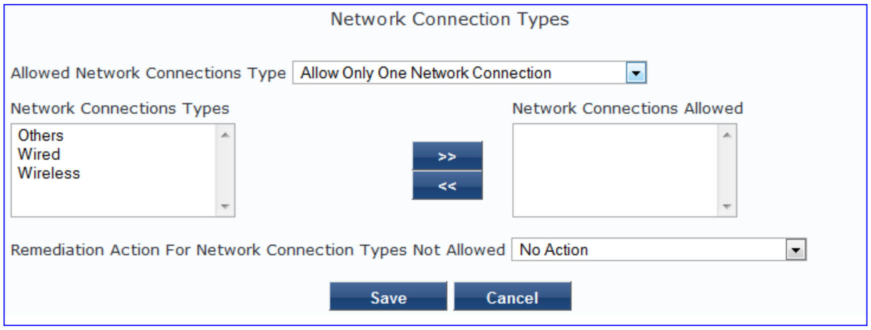
☑ Allow Adhoc/Hosted Wireless Networks

Remediation Action for Adhoc/Hosted Wireless Networks: No Action

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 211: *Network Connection Type Configuration*



Network Connection Types

Allowed Network Connections Type: Allow Only One Network Connection

Network Connections Types: Others, Wired, Wireless

Network Connections Allowed:

Remediation Action For Network Connection Types Not Allowed: No Action

Table 113: *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.

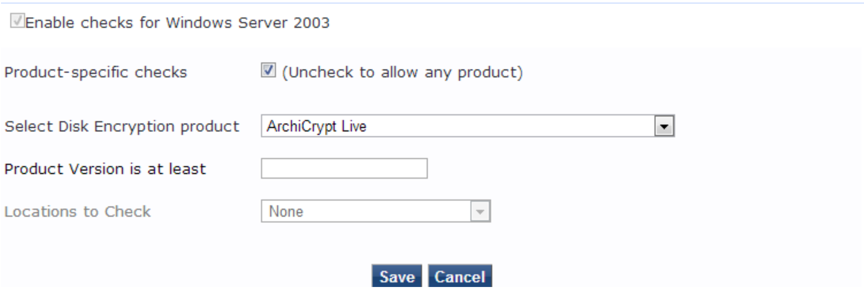
Table 114: *Network Connections Configuration*

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 212: *Disk Encryption Configuration Page*



☑Enable checks for Windows Server 2003

Product-specific checks ☑ (Uncheck to allow any product)

Select Disk Encryption product: ArchiCrypt Live

Product Version is at least:

Locations to Check: None

Table 115: *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.

Table 115: *Disk Encryption Parameters (Continued)*

Parameter	Description
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.

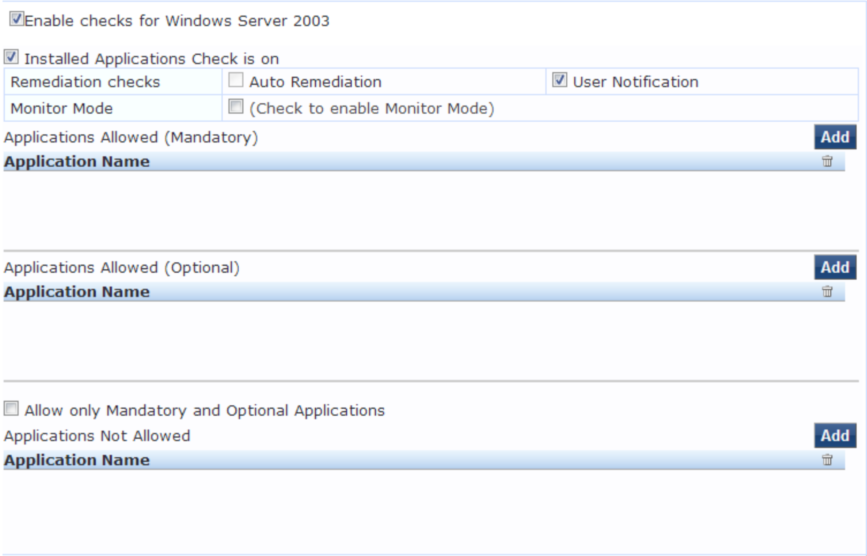
Installed Applications

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, registration actions, and so on. 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, registration actions, and so on.

There will be a check box - "Allow only Mandatory and Optional Applications"

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.



☑ Enable checks for Windows Server 2003

☑ Installed Applications Check is on

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

Applications Allowed (Mandatory)

Application Name

Applications Allowed (Optional)

Application Name

□ Allow only Mandatory and Optional Applications

Applications Not Allowed

Application Name

Table 116: *Installed Applications Configuration Page*

Parameter	Description
Remediation checks	Auto-remediation for Installed Applications health class is not supported.

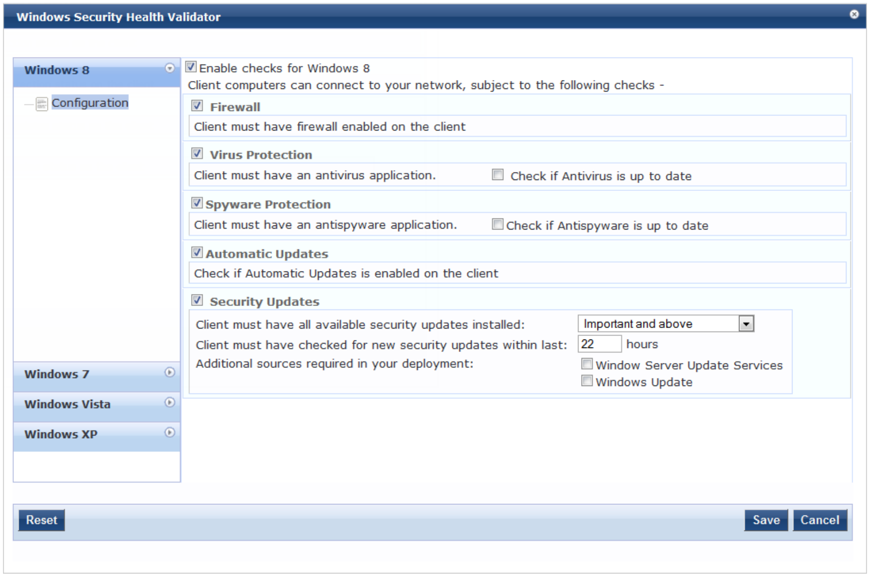
Table 116: *Installed Applications Configuration Page (Continued)*

Parameter	Description
User Notification	A Remediation message having a list of applications to install/uninstall will be displayed to end user.
Monitor Mode	In the Network Monitor (NetMon) operation mode, the 802.11 station operates as a wireless LAN (WLAN) device that is used to monitor packets that are sent over the WLAN media by other devices.
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' should 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 213: *Windows Security Health Validator*



Windows Security Health Validator

Windows 8

Configuration

☑ Enable checks for Windows 8

Client computers can connect to your network, subject to the following checks -

☑ Firewall

Client must have firewall enabled on the client

☑ Virus Protection

Client must have an antivirus application. □ Check if Antivirus is up to date

☑ Spyware Protection

Client must have an antispyware application. □ Check if Antispyware is up to date

☑ Automatic Updates

Check if Automatic Updates is enabled on the client

☑ Security Updates

Client must have all available security updates installed: Important and above

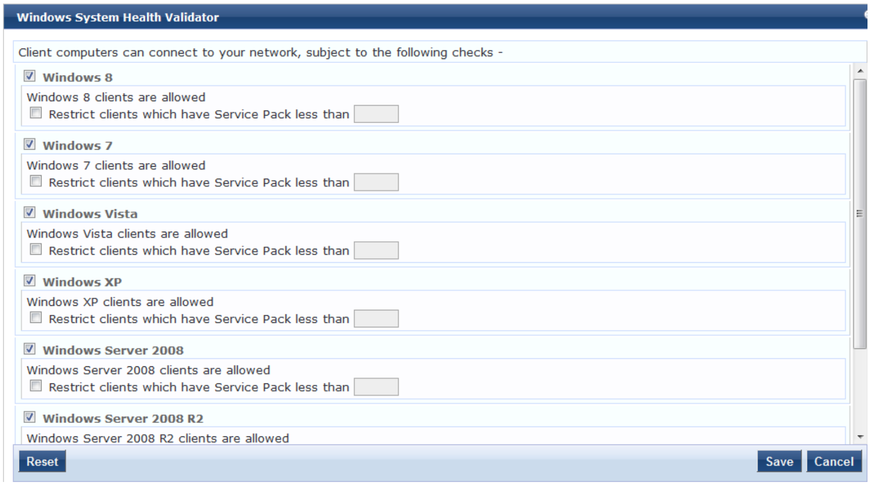
Client must have checked for new security updates within last: 22 hours

Additional sources required in your deployment: □ Window Server Update Services □ Windows Update

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 214: *Windows System Health Validator - OnGuard Agent (Overview)*


Windows System Health Validator

Client computers can connect to your network, subject to the following checks -

☑ Windows 8

Windows 8 clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows 7

Windows 7 clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows Vista

Windows Vista clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows XP

Windows XP clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows Server 2008

Windows Server 2008 clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows Server 2008 R2

Windows Server 2008 R2 clients are allowed

Adding and Modifying Posture Servers

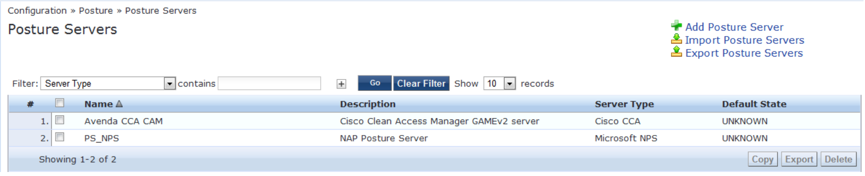
Policy Manager can forward all or part of the posture data received from the client to Posture Servers. The Posture Server evaluates the posture data and returns Application Posture Tokens.

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 231.

Figure 215: *Posture Servers Listing Page*


Configuration » Posture » Posture Servers

Posture Servers

Filter: Server Type contains

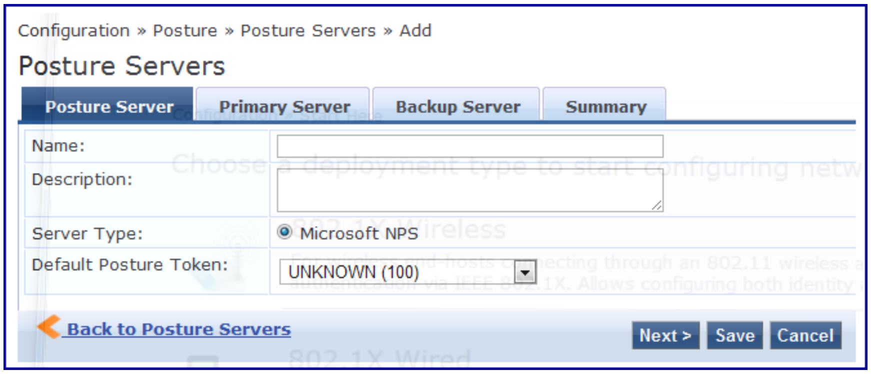
Show 10 records

#	□	Name ▲	Description	Server Type	Default State
1.	□	Avenda CCA CAM	Cisco Clean Access Manager GAMEv2 server	Cisco CCA	UNKNOWN
2.	□	PS_NPS	NAP Posture Server	Microsoft NPS	UNKNOWN

Showing 1-2 of 2

When you click **Add Posture Server** from any of these locations, Policy Manager displays the **Posture Servers** configuration page.

Figure 216: *Add Posture Server Page*


Configuration » Posture » Posture Servers » Add

Posture Servers

Name:	
Description:	
Server Type:	● Microsoft NPS
Default Posture Token:	UNKNOWN (100)

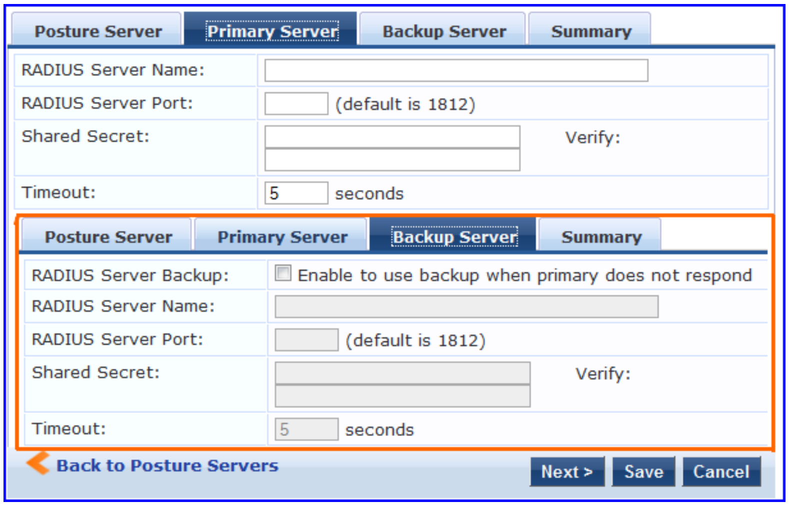
Microsoft NPS

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 117: *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 217: *Microsoft NPS Settings (Primary and Backup Server tabs)*



RADIUS Server Name:

RADIUS Server Port: (default is 1812)

Shared Secret: Verify:

Timeout: 5 seconds

RADIUS Server Backup: □ Enable to use backup when primary does not respond

RADIUS Server Name:

RADIUS Server Port: (default is 1812)

Shared Secret: Verify:

Timeout: 5 seconds

Table 118: *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.

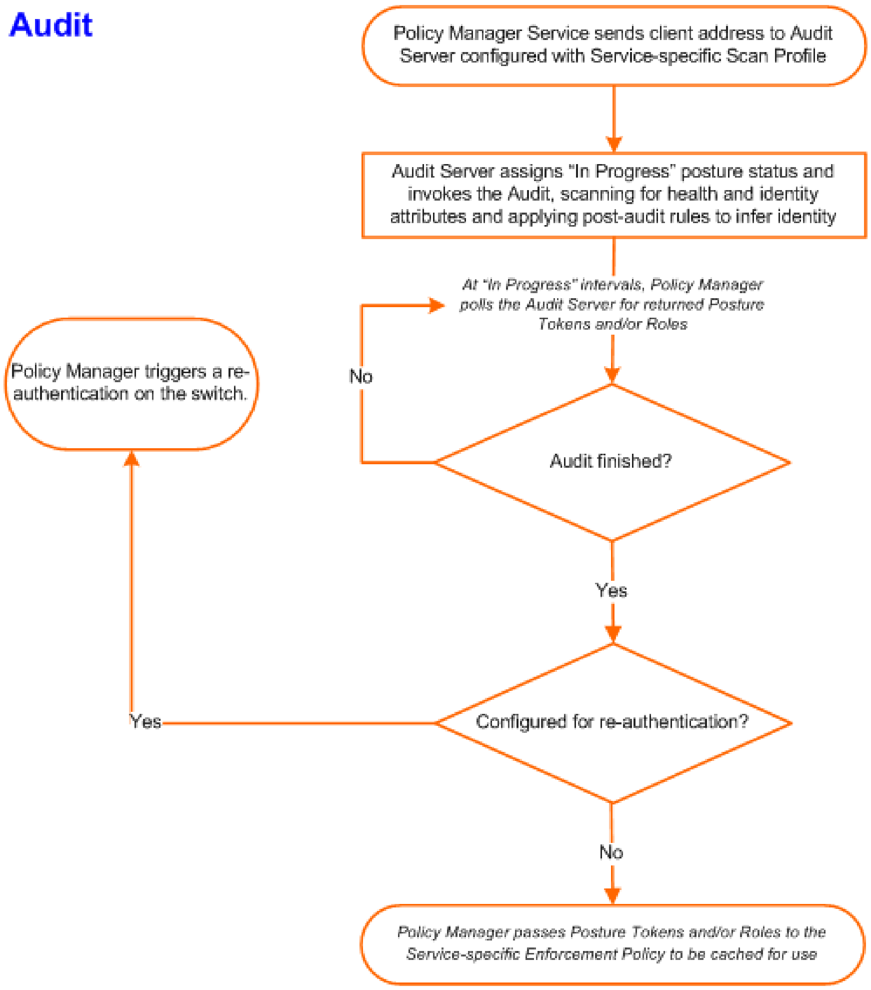
Audit Servers

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 233.

Figure 218: *Flow of Control of Policy Manager Auditing*


Audit
Policy Manager Service sends client address to Audit Server configured with Service-specific Scan Profile
Audit Server assigns "In Progress" posture status and invokes the Audit, scanning for health and identity attributes and applying post-audit rules to infer identity
At "In Progress" intervals, Policy Manager polls the Audit Server for returned Posture Tokens and/or Roles
No
Policy Manager triggers a re-authentication on the switch.
Audit finished?
Yes
Yes
Configured for re-authentication?
No
Policy Manager passes Posture Tokens and/or Roles to the Service-specific Enforcement Policy to be cached for use

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 234
- "Custom Audit Servers" on page 236
- "Post-Audit Rules" on page 242

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

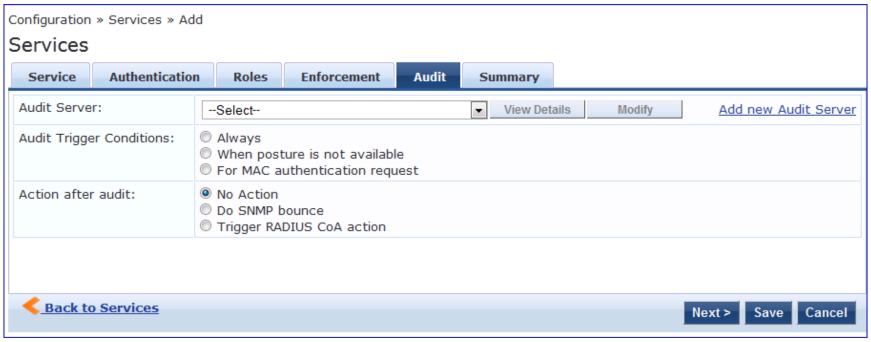
1. Navigate to the **Audit** tab from one of the following locations:
   - To configure an audit server for a new service (as part of the flow of the Add Service wizard), navigate to **Configuration** > **Services**. Select the **Add Services** link. In the **Add Services** form, select the **Audit** tab.

NOTE

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 219: *Audit Tab*



Audit Server:	--Select--
Audit Trigger Conditions:	○ Always ○ When posture is not available ○ For MAC authentication request
Action after audit:	● No Action ○ Do SNMP bounce ○ Trigger RADIUS CoA action

Table 119: *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.

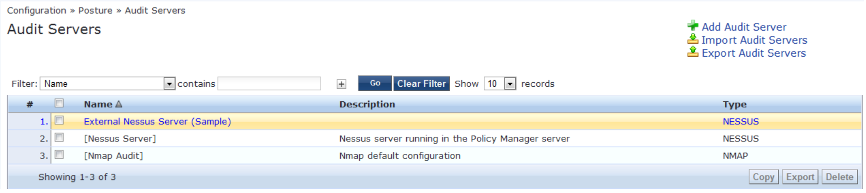
Modifying Built-In Audit Servers

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 220: *Audit Servers Listing*



Configuration » Posture » Audit Servers

Audit Servers

#	□	Name ▲	Description	Type
1.	□	External Nessus Server (Sample)		NESSUS
2.	□	[Nessus Server]	Nessus server running in the Policy Manager server	NESSUS
3.	□	[Nmap Audit]	Nmap default configuration	NMAP

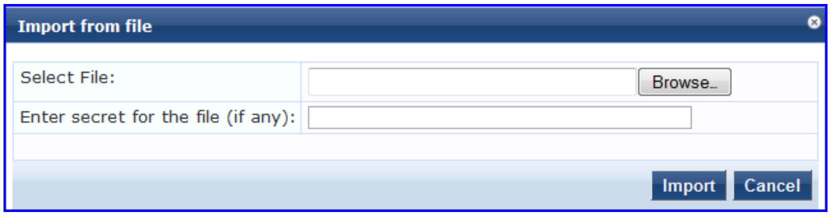
Showing 1-3 of 3

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 238 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 221: *Upload Nessus Plugins Popup*



Import from file

Select File:

Enter secret for the file (if any):

   - 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 242.

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:

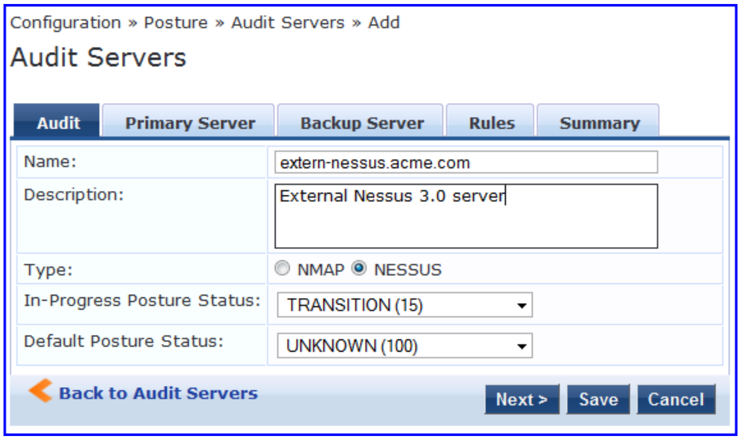
   - "Nessus Audit Server" on page 236
   - "NMAP Audit Server" on page 240

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 222: *Nessus Audit Server (Audit Tab)*



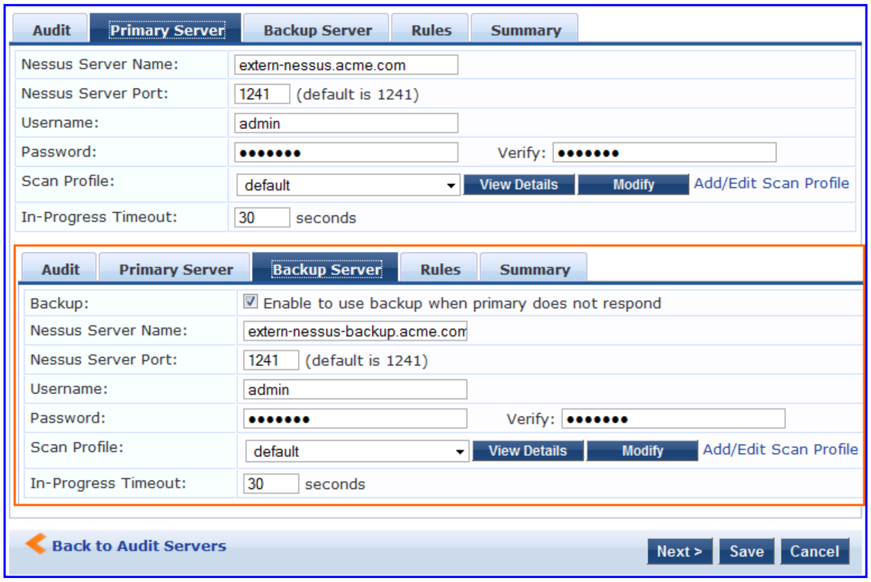
Name:	extern-nessus.acme.com
Description:	External Nessus 3.0 server
Type:	○ NMAP ● NESSUS
In-Progress Posture Status:	TRANSITION (15)
Default Posture Status:	UNKNOWN (100)

Table 120: *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 223: *Nessus Audit Server (Primary & Backup Tabs)*



Nessus Server Name:	extern-nessus.acme.com
Nessus Server Port:	1241 (default is 1241)
Username:	admin
Password:	••••••• Verify: •••••••
Scan Profile:	default
In-Progress Timeout:	30 seconds

Backup:	☑ Enable to use backup when primary does not respond
Nessus Server Name:	extern-nessus-backup.acme.com
Nessus Server Port:	1241 (default is 1241)
Username:	admin
Password:	••••••• Verify: •••••••
Scan Profile:	default
In-Progress Timeout:	30 seconds

Table 121: *Nessus Audit Server - Primary and Backup Server tabs*

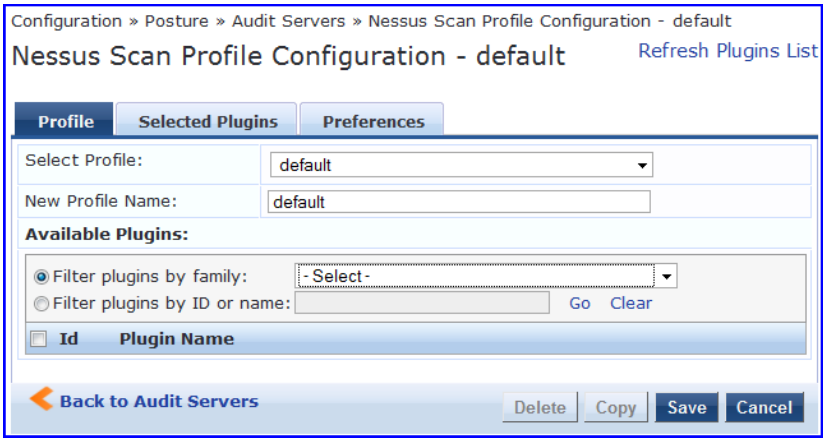
Parameter	Description
Server Name and Port/ Username/ Password	Standard NESSUS server configuration fields. **NOTE:** For the backup server to be invoked on primary server failover, check the **Enable to use backup when primary does not respond** check box.
Scan Profile	You can accept the default Scan 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 238.

The **Rules** tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to "Post-Audit Rules" on page 242.

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 224: *Nessus Scan Profile Configuration Page*



Configuration » Posture » Audit Servers » Nessus Scan Profile Configuration - default

Nessus Scan Profile Configuration - default

Select Profile: default

New Profile Name: default

Available Plugins:

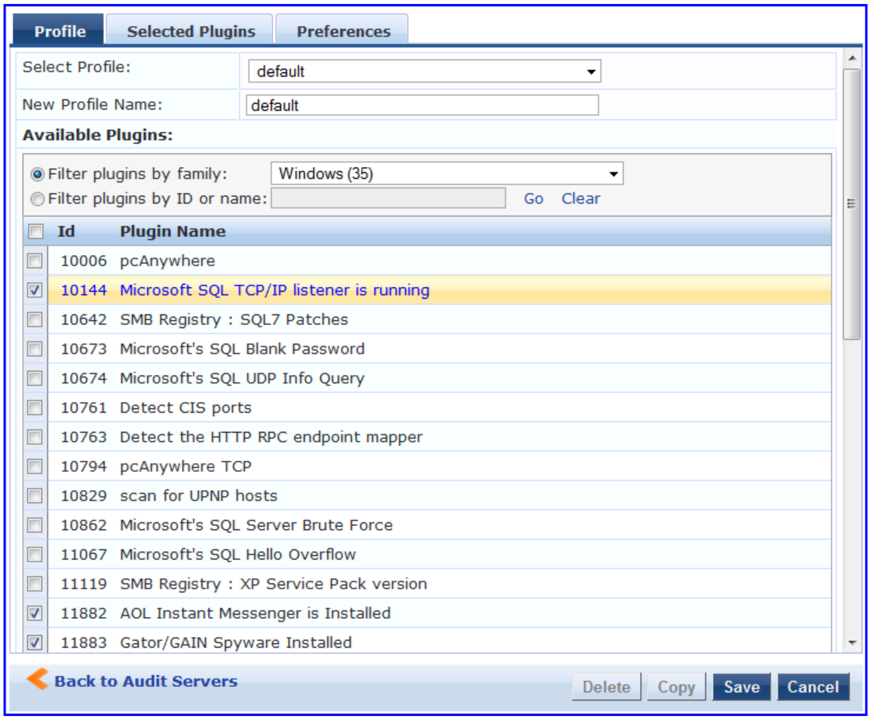
● Filter plugins by family: - Select -

○ Filter plugins by ID or name:

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 225: *Nessus Scan Profile Configuration (Profile Tab)*



Select Profile: default

New Profile Name: default

Available Plugins:

● Filter plugins by family: Windows (35)

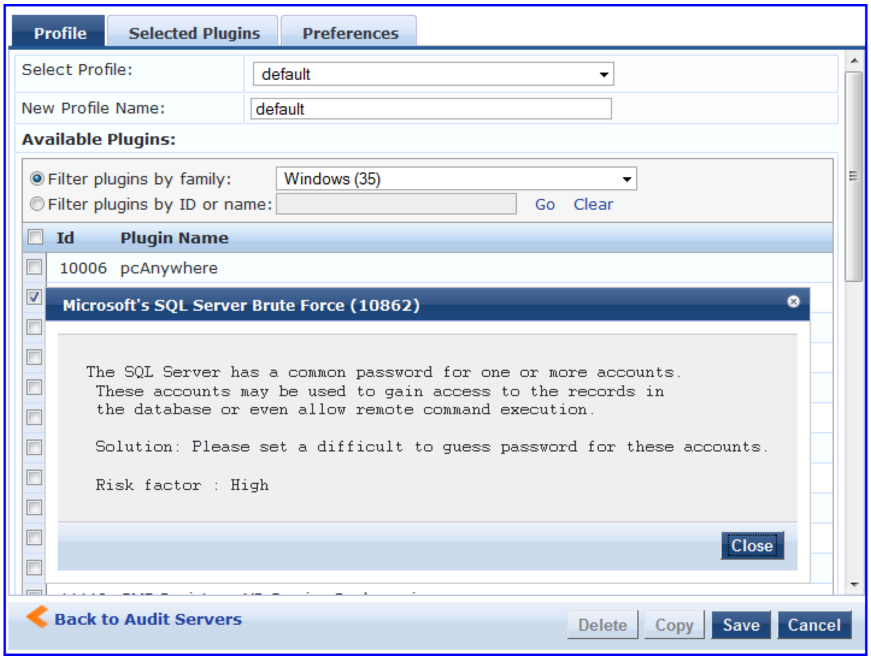
○ Filter plugins by ID or name:

☐	Id	Plugin Name
☐	10006	pcAnywhere
☑	10144	Microsoft SQL TCP/IP listener is running
☐	10642	SMB Registry : SQL7 Patches
☐	10673	Microsoft's SQL Blank Password
☐	10674	Microsoft's SQL UDP Info Query
☐	10761	Detect CIS ports
☐	10763	Detect the HTTP RPC endpoint mapper
☐	10794	pcAnywhere TCP
☐	10829	scan for UPNP hosts
☐	10862	Microsoft's SQL Server Brute Force
☐	11067	Microsoft's SQL Hello Overflow
☐	11119	SMB Registry : XP Service Pack version
☑	11882	AOL Instant Messenger is Installed
☑	11883	Gator/GAIN Spyware Installed

- The **Selected Plugins** tab displays all selected plugins, plus any dependencies.

  To display a synopsis of any listed plugin, click on its row.

Figure 226: *Nessus Scan Profile Configuration (Profile Tab) - Plugin Synopsis*



Select Profile: default

New Profile Name: default

Available Plugins:

● Filter plugins by family: Windows (35)

○ Filter plugins by ID or name:

☐	Id	Plugin Name
☐	10006	pcAnywhere

Microsoft's SQL Server Brute Force (10862)

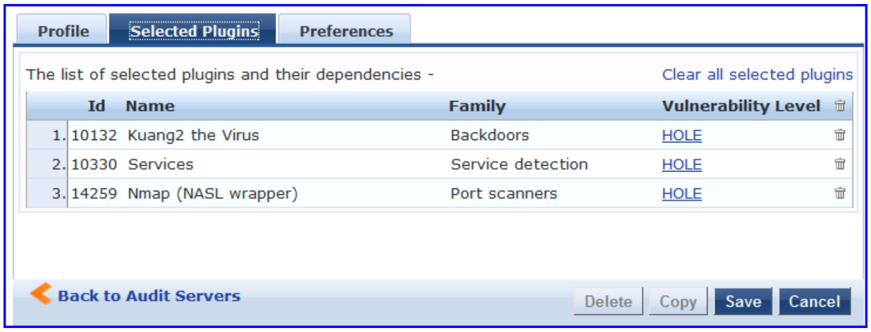
```
The SQL Server has a common password for one or more accounts.
 These accounts may be used to gain access to the records in
 the database or even allow remote command execution.

 Solution: Please set a difficult to guess password for these accounts.

 Risk factor : High
```

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.

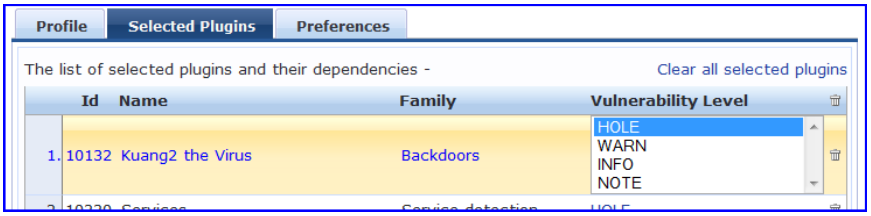
Figure 227: *Nessus Scan Profile Configuration (Selected Plugins Tab)*



The list of selected plugins and their dependencies -

	Id	Name	Family	Vulnerability Level
1.	10132	Kuang2 the Virus	Backdoors	HOLE
2.	10330	Services	Service detection	HOLE
3.	14259	Nmap (NASL wrapper)	Port scanners	HOLE

Figure 228: *Nessus Scan Profile Configuration (Selected Plugins Tab) - Vulnerability Level*



The list of selected plugins and their dependencies -

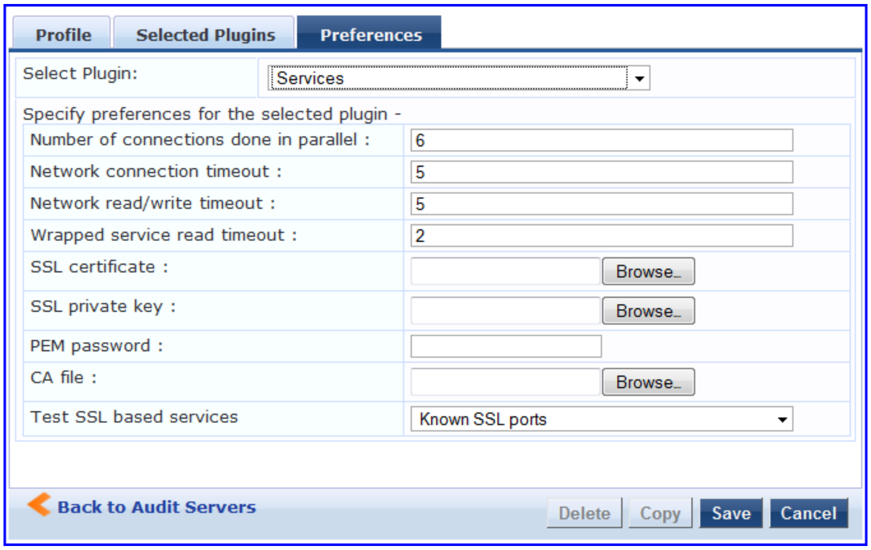
	Id	Name	Family	Vulnerability Level
1.	10132	Kuang2 the Virus	Backdoors	HOLE WARN INFO NOTE
2.	10330	Services	Service detection	HOLE

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 229: *Nessus Scan Profile Configuration (Preferences Tab)*



Select Plugin: Services

Specify preferences for the selected plugin -

Number of connections done in parallel :	6
Network connection timeout :	5
Network read/write timeout :	5
Wrapped service read timeout :	2
SSL certificate :	Browse...
SSL private key :	Browse...
PEM password :	
CA file :	Browse...
Test SSL based services	Known SSL ports

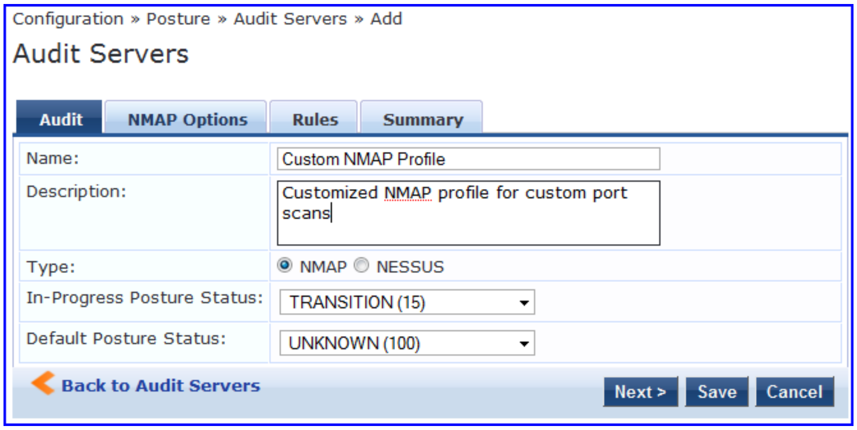
After saving the profile, plugin, and preference information for your new (or modified) plugin, you can go to the **Primary/Backup Servers** tabs and select it from the **Scan Profile** drop-down list.

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 230: *Audit Tab (NMAP)*



Configuration » Posture » Audit Servers » Add

Audit Servers

Name: Custom NMAP Profile

Description: Customized NMAP profile for custom port scans

Type: ● NMAP ○ NESSUS

In-Progress Posture Status: TRANSITION (15)

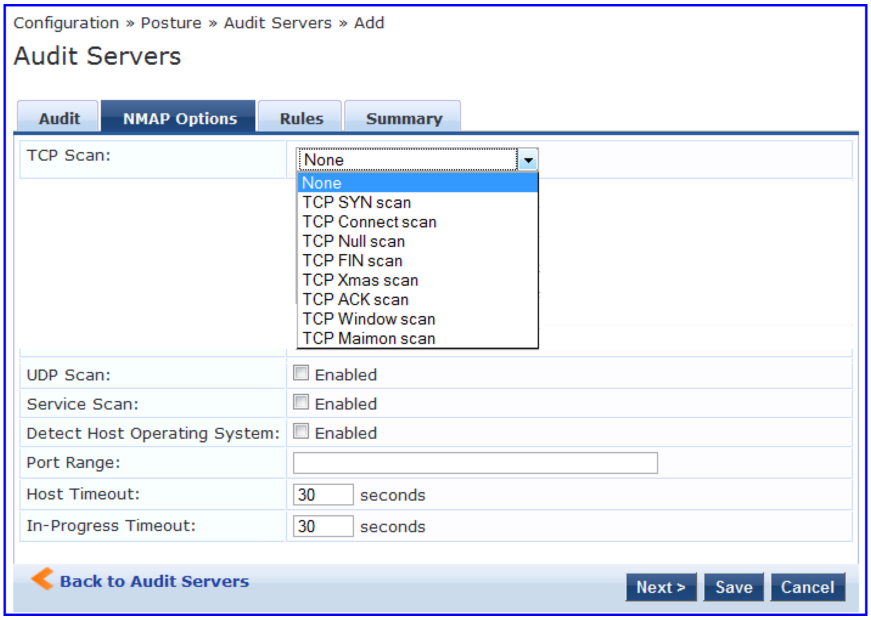
Default Posture Status: UNKNOWN (100)

Table 122: *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 231: *Options Tab (NMAP)*



Configuration » Posture » Audit Servers » Add

Audit Servers

TCP Scan: None

UDP Scan: □ Enabled

Service Scan: □ Enabled

Detect Host Operating System: □ Enabled

Port Range:

Host Timeout: 30 seconds

In-Progress Timeout: 30 seconds

Table 123: *Options Tab (NMAP)*

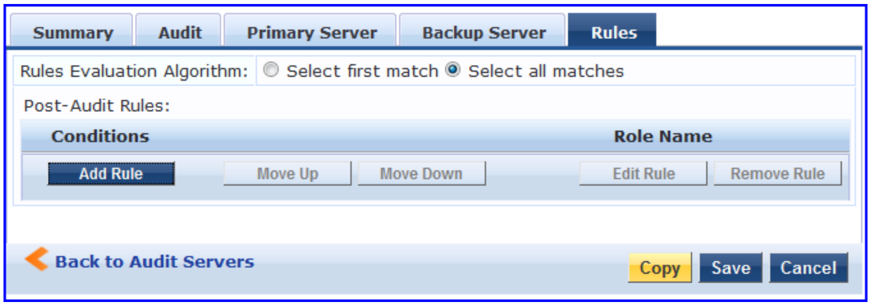
Parameter	Description
TCP Scan	To specify a TCP scan, select from the **TCP Scan** drop-down list. Refer to NMAP documentation for more information on these options. NMAP option --scanflags.
UDP Scan	To enable, check the **UDP Scan** check box. NMAP option -sU.
Service Scan	To enable, check the **Service Scan** check box. NMAP option -sV.
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 242.

Post-Audit Rules

The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role.

Figure 232: *All Audit Server Configurations (Rules Tab)*



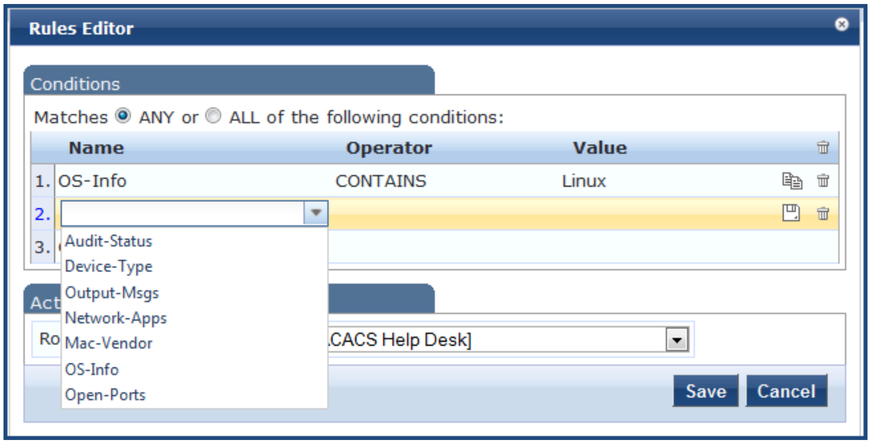
Rules Evaluation Algorithm: ○ Select first match ● Select all matches

Post-Audit Rules:

Table 124: *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 233: *All Audit Server Configurations (Rules Editor)*



Rules Editor

Conditions

Matches ● ANY or ○ ALL of the following conditions:

	Name	Operator	Value
1.	OS-Info	CONTAINS	Linux
2.			
3.			

Table 125: *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 "Rules Editing and Namespaces" on page 445.
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 245
- "Configuring Enforcement Profiles " on page 246
- "Configuring Enforcement Policies" on page 277

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.

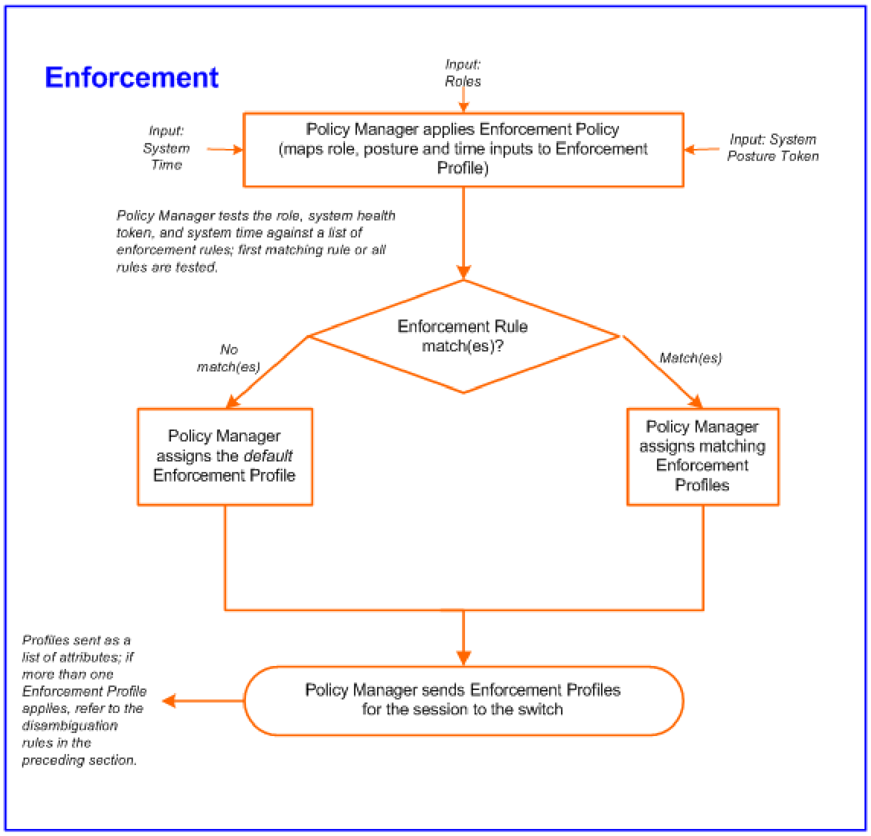
Each Enforcement Policy contains a rule or set of rules for matching Conditions (role, posture and time) to Actions (Enforcement Profiles). For each request, it yields one or more matches, in the form of Enforcement Profiles, from which Policy Manager assembles access-control attributes for return to 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.

NOTE

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 234: *Flow of Control of Policy Manager Enforcement*


Enforcement
Input: Roles
Input: System Time
Policy Manager applies Enforcement Policy (maps role, posture and time inputs to Enforcement Profile)
Input: System Posture Token
Policy Manager tests the role, system health token, and system time against a list of enforcement rules; first matching rule or all rules are tested.
Enforcement Rule match(es)?
No match(es)
Match(es)
Policy Manager assigns the *default* Enforcement Profile
Policy Manager assigns matching Enforcement Profiles
Profiles sent as a list of attributes; if more than one Enforcement Profile applies, refer to the disambiguation rules in the preceding section.
Policy Manager sends Enforcement Profiles for the session to the switch

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.

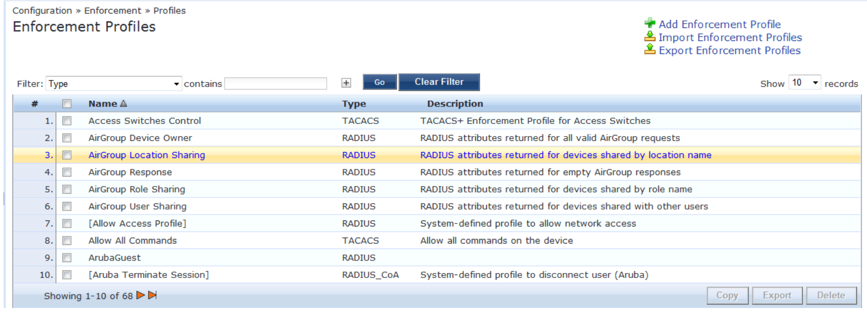
From the **Enforcement Policies** page (**Configuration** > **Enforcement** > **Policies**), you can configure an Enforcement Profile for a new enforcement policy (as part of the flow of the **Add Enforcement Policy** wizard), or modify an existing Enforcement Profile directly (**Configuration** > **Enforcement** > **Profiles**, then click on its name in the **Enforcement Profile** listing).

For information about configuring individual Enforcement Profiles, see:

- "Agent Enforcement" on page 248
- "Aruba Downloadable Role Enforcement" on page 250
- "Aruba RADIUS Enforcement" on page 256
- "Cisco Downloadable ACL Enforcement" on page 257
- "Cisco Web Authentication Enforcement" on page 259
- "ClearPass Entity Update Enforcement" on page 260
- "CLI Based Enforcement" on page 262
- "Filter ID Based Enforcement" on page 263
- "Generic Application Enforcement" on page 265
- "HTTP Based Enforcement" on page 266
- "RADIUS Based Enforcement" on page 267

- "RADIUS Change of Authorization (CoA)" on page 269
- "Session Restrictions Enforcement" on page 271
- "SNMP Based Enforcement" on page 272
- "TACACS+ Based Enforcement" on page 274
- "VLAN Enforcement" on page 276

Figure 235: *Enforcement Profiles Page*



Configuration » Enforcement » Profiles

Enforcement Profiles

Add Enforcement Profile
Import Enforcement Profiles
Export Enforcement Profiles

Filter: Type contains

Show 10 records

#	☐	Name △	Type	Description
1.	☐	Access Switches Control	TACACS	TACACS+ Enforcement Profile for Access Switches
2.	☐	AirGroup Device Owner	RADIUS	RADIUS attributes returned for all valid AirGroup requests
3.	☐	AirGroup Location Sharing	RADIUS	RADIUS attributes returned for devices shared by location name
4.	☐	AirGroup Response	RADIUS	RADIUS attributes returned for empty AirGroup responses
5.	☐	AirGroup Role Sharing	RADIUS	RADIUS attributes returned for devices shared by role name
6.	☐	AirGroup User Sharing	RADIUS	RADIUS attributes returned for devices shared with other users
7.	☐	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
8.	☐	Allow All Commands	TACACS	Allow all commands on the device
9.	☐	ArubaGuest	RADIUS	
10.	☐	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)

Showing 1-10 of 68

Policy Manager comes pre-packaged with the default profiles described in :

Table 126: *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
[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

Table 126: *Default Enforcement Profiles (Continued)*

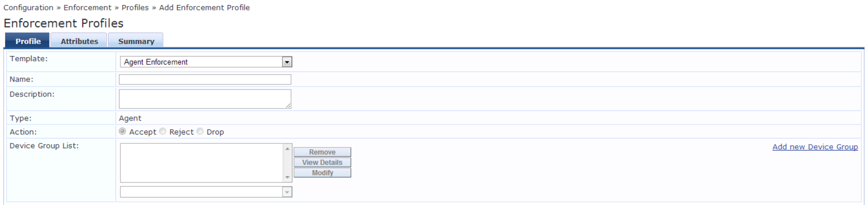
Profile	Available for the following Enforcement Types
[Drop Access Profile]	RADIUS
[Handle AirGroup Time Sharing]	HTTP
[HP - Terminate Session]	RADIUS_CoA
[Juniper Terminate Session]	RADIUS_CoA
[Motorola - Terminate Session]	RADIUS_CoA
[Operator Login - Admin Users]	Application
[Operator Login - Local 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 236: *Agent Enforcement Profile tab*



Template: Agent Enforcement

Name:

Description:

Type: Agent

Action: ● Accept ○ Reject ○ Drop

Device Group List:

Table 127: *Add Agent Enforcement Profile tab Parameters*

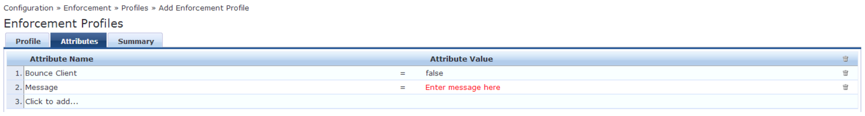
Parameter	Description
Template	Agent Enforcement

Table 127: *Add Agent Enforcement Profile tab Parameters (Continued)*

Parameter	Description
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 285.

Attributes tab

Figure 237: *Agent Enforcement Attributes tab*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Attribute Name		Attribute Value
1.	Bounce Client	=	false
2.	Message	=	Enter message here
3.	Click to add...		

Table 128: *Agent Enforcement Attributes tab Parameters*

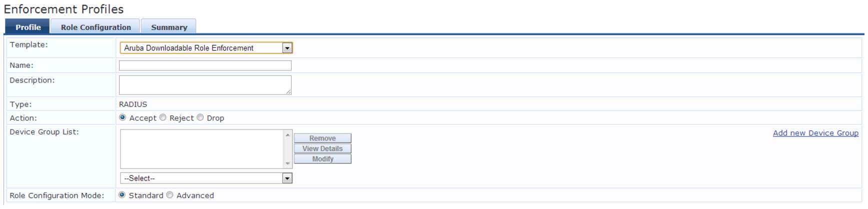
Attribute	Parameter
Attribute Name	Select one of the following attribute names: ● Bounce Client ● Message ● Session Timeout (in seconds)
Attribute Value	The Attribute Value settings depend on the selected Attribute Name.

Aruba Downloadable Role Enforcement

Use this page to configure profile and role configuration attributes for the Aruba Downloadable Role Enforcement Profile.

Profile tab

Figure 238: *Aruba Downloadable Role Enforcement Profile tab*



Template: Aruba Downloadable Role Enforcement

Name:

Description:

Type: RADIUS

Action: ● Accept ○ Reject ○ Drop

Device Group List: --Select--

Role Configuration Mode: ● Standard ○ Advanced

Table 129: *Aruba Downloadable Role Enforcement Profile tab Parameters*

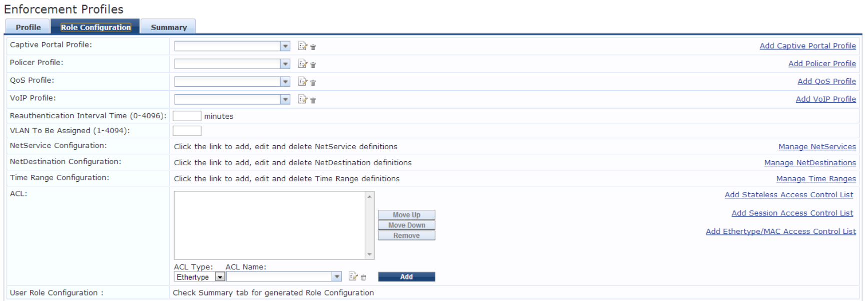
Parameter	Description
Template:	Aruba Downloadable Role Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	RADIUS. This 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 285.

Role Configuration tab

Ten fields on the role configuration tab require that you select a link to launch a new page where you set role configuration attributes, such as adding a Captive Portal profile.

Details about working with the fields that require links and new pages follow the first table in this section.

Figure 239: *Aruba Downloadable Role Enforcement Role Configuration tab*



Enforcement Profiles

Captive Portal Profile:		Add Captive Portal Profile
Policer Profile:		Add Policer Profile
QoS Profile:		Add QoS Profile
VoIP Profile:		Add VoIP Profile
Reauthentication Interval Time (0-4096):	minutes	
VLAN To Be Assigned (1-4094):		
NetService Configuration:	Click the link to add, edit and delete NetService definitions	Manage NetServices
NetDestination Configuration:	Click the link to add, edit and delete NetDestination definitions	Manage NetDestinations
Time Range Configuration:	Click the link to add, edit and delete Time Range definitions	Manage Time Ranges
ACL:	ACL Type: Ethertype ACL Name:	Add Stateless Access Control List Add Session Access Control List Add Ethertype/MAC Access Control List
User Role Configuration :	Check Summary tab for generated Role Configuration	

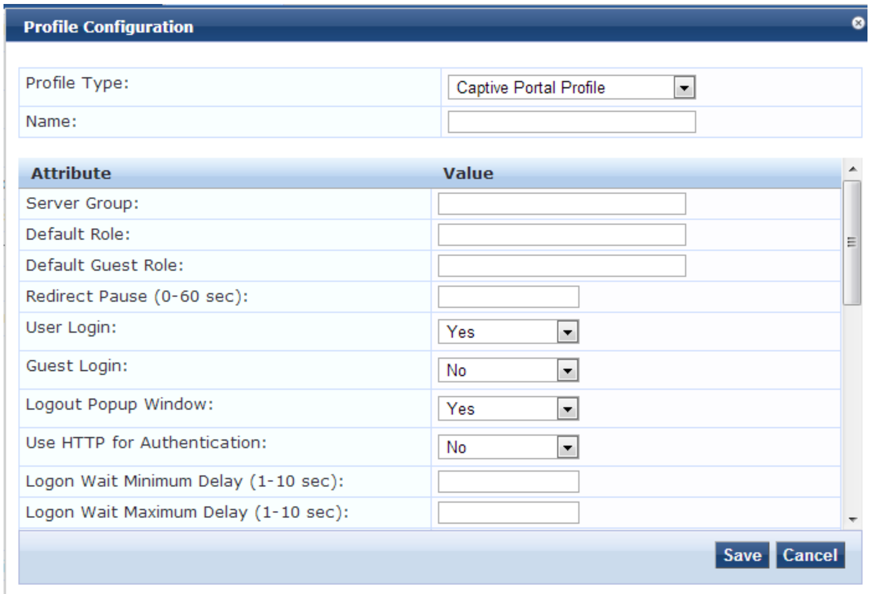
Table 130: *Role Configuration Attributes page*

Role Configuration	Parameter
Reauthentication Interval Time (0-4096)	Enter the number of minutes between reauthentication intervals.
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: - Ethertype - MAC - Session - Stateless
ACL Name:	Click the name of the selected 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 240: *Add Captive Portal Profile Attributes Page*



Profile Configuration

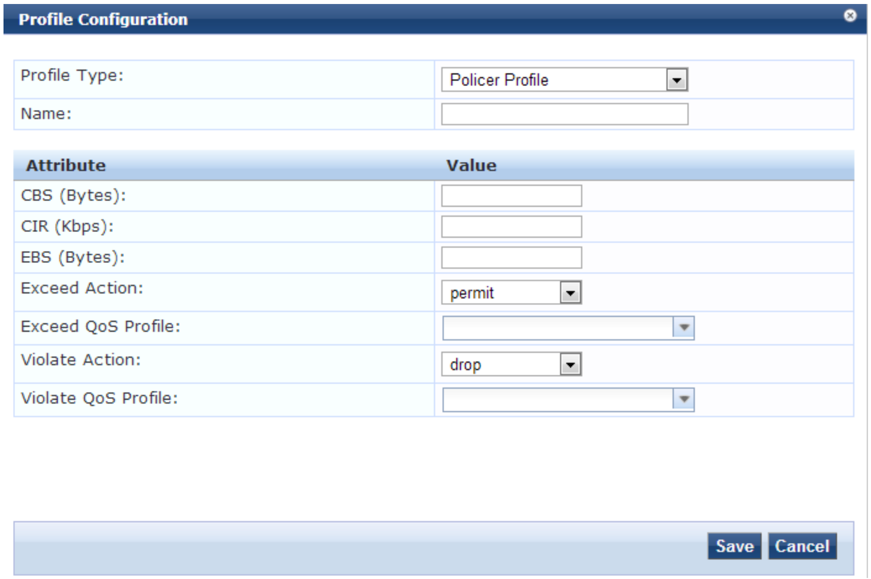
Profile Type:	Captive Portal Profile
Name:	

Attribute	Value
Server Group:	
Default Role:	
Default Guest Role:	
Redirect Pause (0-60 sec):	
User Login:	Yes
Guest Login:	No
Logout Popup Window:	Yes
Use HTTP for Authentication:	No
Logon Wait Minimum Delay (1-10 sec):	
Logon Wait Maximum Delay (1-10 sec):	

Policer Profile:

Click the **Add Policer Profile** link. Enter a name for the profile. Configure the required attributes and click **Save** or **Cancel**.

Figure 241: *Add Policer Profile Attributes Page*



Profile Configuration

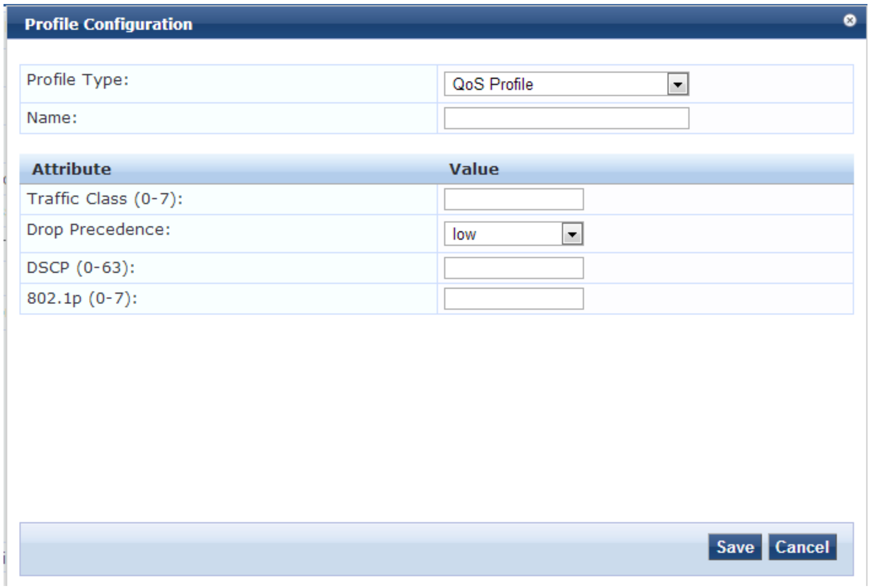
Profile Type:	Policer Profile
Name:	

Attribute	Value
CBS (Bytes):	
CIR (Kbps):	
EBS (Bytes):	
Exceed Action:	permit
Exceed QoS Profile:	
Violate Action:	drop
Violate QoS Profile:	

QOs Profile

Click the **Add QoS Profile** link. Enter a name for the profile. Configure the required attributes and click **Save** or **Cancel**.

Figure 242: *Add QosProfle Attributes Page*



Profile Configuration

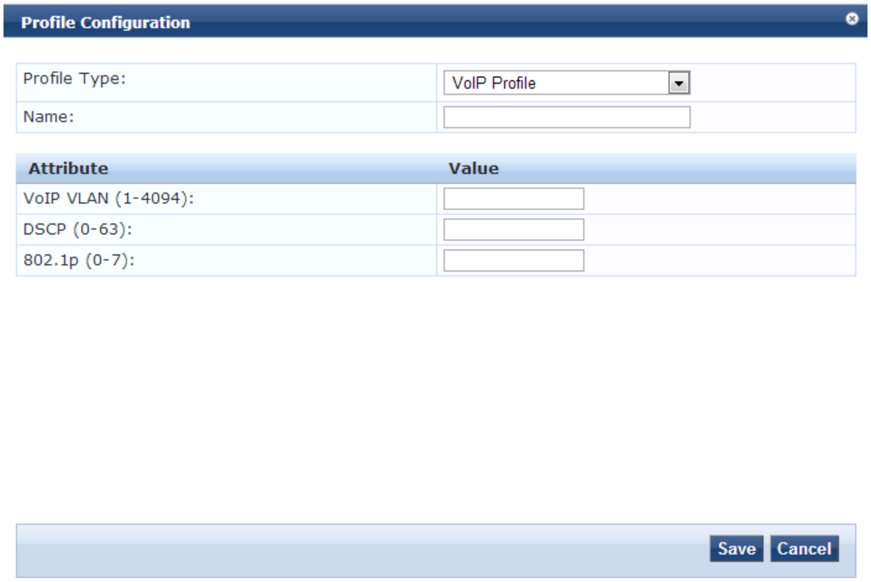
Profile Type:	QoS Profile
Name:	

Attribute	Value
Traffic Class (0-7):	
Drop Precedence:	low
DSCP (0-63):	
802.1p (0-7):	

VoIP Profile

Click the **Add VoIP Profile** link. Enter a name for the profile. Configure the required attributes and click **Save** or **Cancel**.

Figure 243: *Add VoIP Profile Attributes page*



Profile Configuration

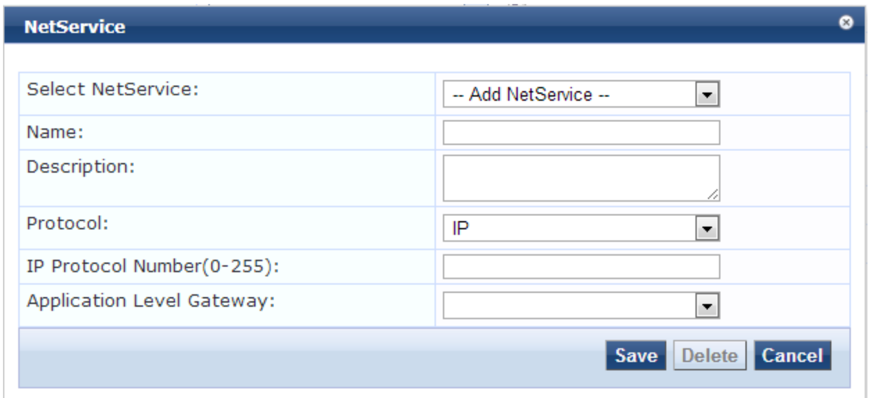
Profile Type:	VoIP Profile
Name:	

Attribute	Value
VoIP VLAN (1-4094):	
DSCP (0-63):	
802.1p (0-7):	

NetService Configuration

Click the **Manage NetServices** link. Configure the required attributes and click **Save, Delete** or **Cancel**.

Figure 244: *Manage NetServices Attributes Page*



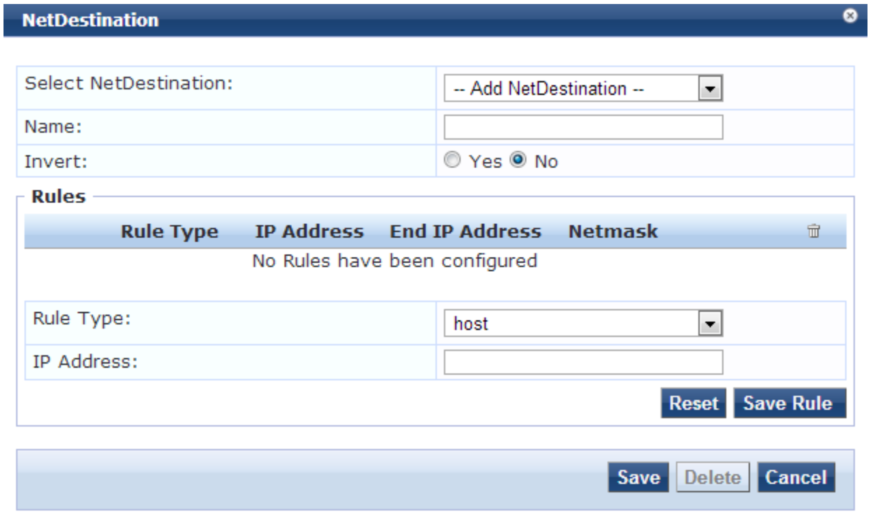
NetService

Select NetService:	-- Add NetService --
Name:	
Description:	
Protocol:	IP
IP Protocol Number(0-255):	
Application Level Gateway:	

NetDestination Configuration

Click the **Manage NetDestinations** link. Configure the required attributes. Click **Reset** or **Save Rule**. Then click **Save**, **Delete**, **Reset**, or **Cancel**.

Figure 245: *Manage NetDestinations Attributes page*



NetDestination

Select NetDestination:	-- Add NetDestination --
Name:	
Invert:	○ Yes ● No

Rules

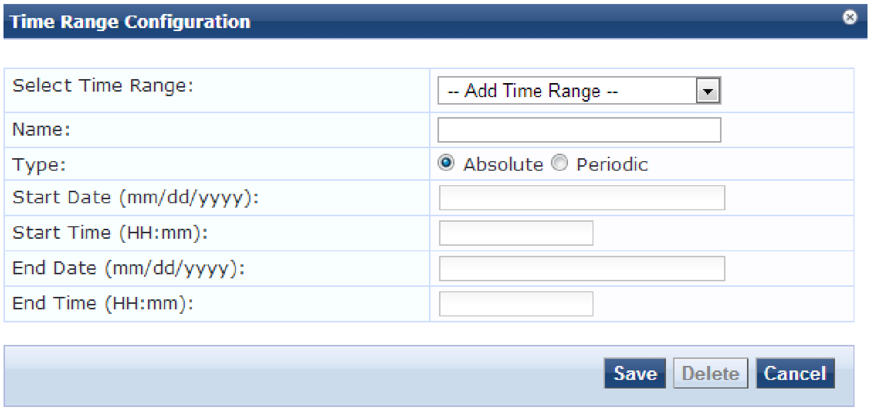
Rule Type	IP Address	End IP Address	Netmask
No Rules have been configured			

Rule Type:	host
IP Address:	

Time Range Configuration

Click the **Manage Time Ranges** link. Configure the required attributes and click **Save**, **Delete** or **Cancel**.

Figure 246: *Time Range Configuration Attributes page*



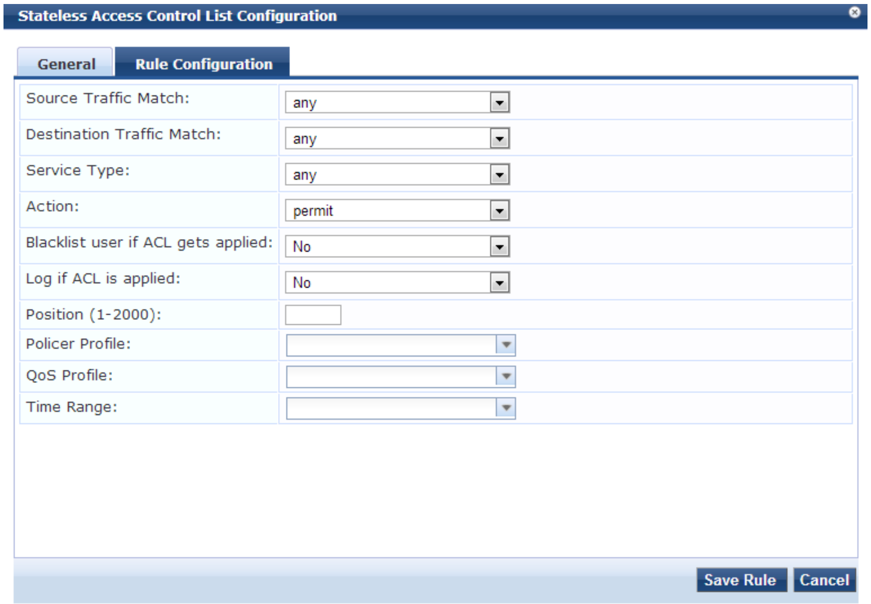
Time Range Configuration

Select Time Range:	-- Add Time Range --
Name:	
Type:	● Absolute ○ Periodic
Start Date (mm/dd/yyyy):	
Start Time (HH:mm):	
End Date (mm/dd/yyyy):	
End Time (HH:mm):	

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**.

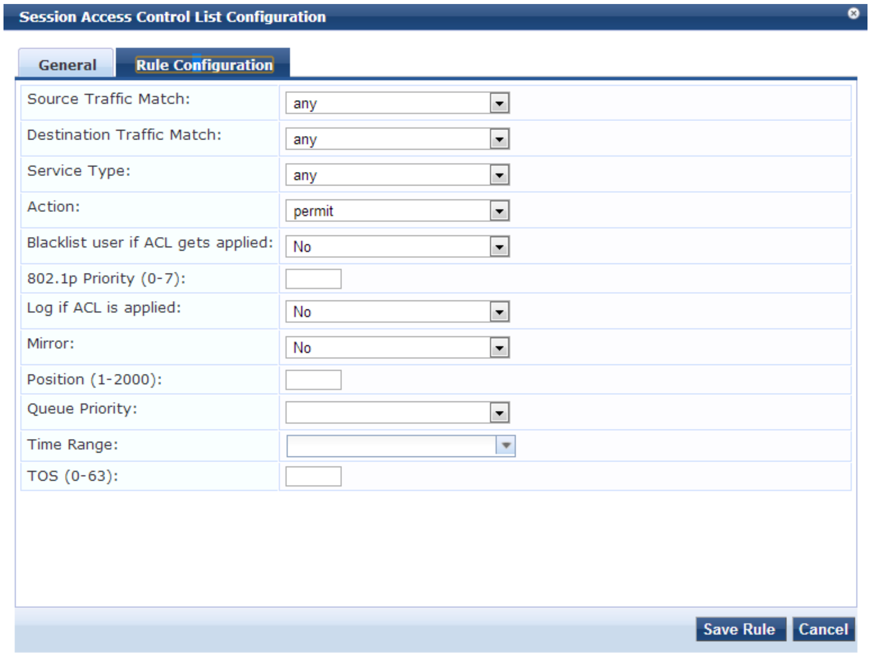
Figure 247: *Stateless Access Control List Configuration Attributes Page*



Source Traffic Match:	any
Destination Traffic Match:	any
Service Type:	any
Action:	permit
Blacklist user if ACL gets applied:	No
Log if ACL is applied:	No
Position (1-2000):	
Policer Profile:	
QoS Profile:	
Time Range:	

Click the **Add Session Access Control List** link. Enter a name for the Session 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**.

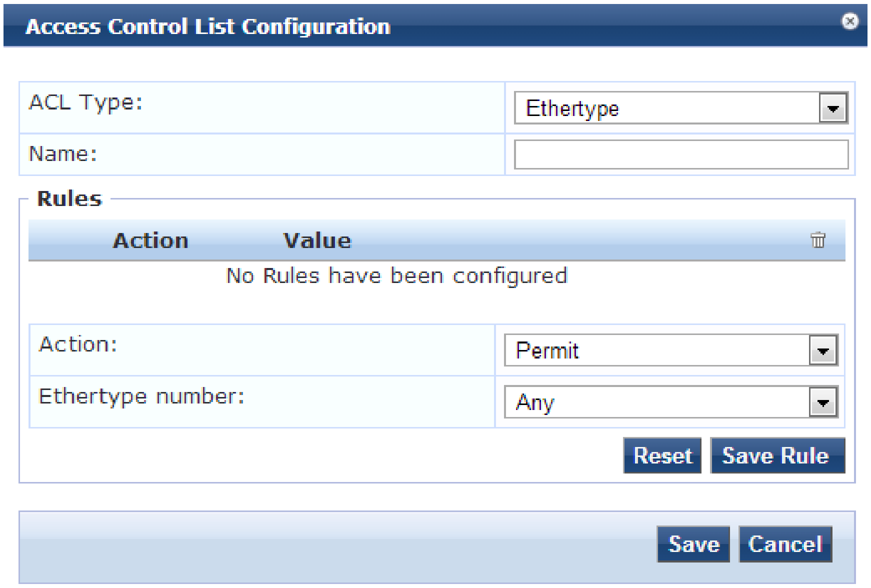
Figure 248: *Session Access Control List Attributes Page*



Source Traffic Match:	any
Destination Traffic Match:	any
Service Type:	any
Action:	permit
Blacklist user if ACL gets applied:	No
802.1p Priority (0-7):	
Log if ACL is applied:	No
Mirror:	No
Position (1-2000):	
Queue Priority:	
Time Range:	
TOS (0-63):	

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 249: *Ethernet/MAC Access Control List Attributes Page*



Access Control List Configuration

ACL Type:	Ethertype
Name:	

Rules

Action	Value
No Rules have been configured	

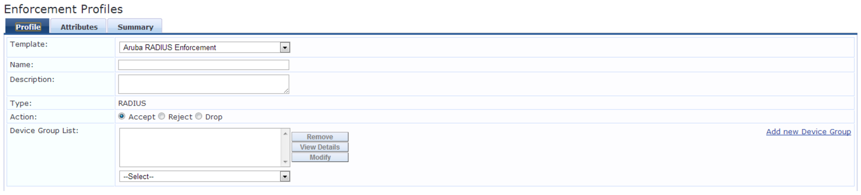
Action:	Permit
Ethertype number:	Any

Aruba RADIUS Enforcement

Use this page to configure profile and attribute parameters for the Aruba RADIUS Enforcement Profile.

Profile tab

Figure 250: *Aruba RADIUS Enforcement Profile tab*



Enforcement Profiles

Template:	Aruba RADIUS Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Table 131: *Aruba RADIUS Enforcement Profile tab Parameters*

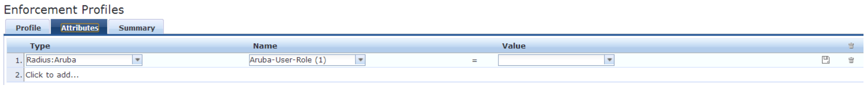
Parameter	Description
Template	Aruba RADIUS Enforcement
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > 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.

Table 131: *Aruba RADIUS Enforcement Profile tab Parameters (Continued)*

Parameter	Description
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 285.

Attributes tab

Figure 251: *Aruba RADIUS Enforcement Attributes tab*



	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role (1)	=	
2.	Click to add...			

Table 132: *Aruba RADIUS Enforcement Attributes tab Parameters*

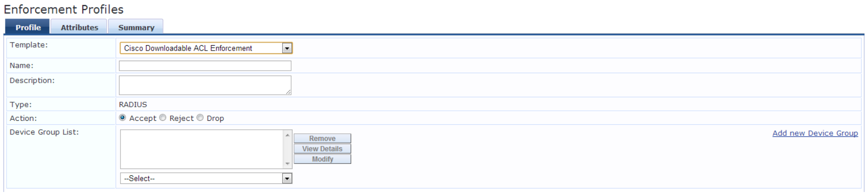
Attribute	Description
Type:	Select one of the following attribute types: ● Radius:Aruba ● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda For more information, see "RADIUS Namespaces" on page 454
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
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 252: *Cisco Downloadable ACL Enforcement Profile tab*



Enforcement Profiles

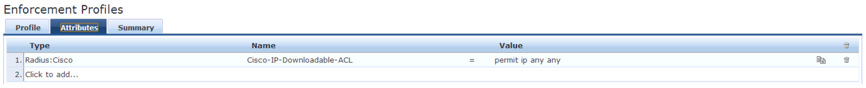
Template:	Cisco Downloadable ACL Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Table 133: *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 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 285.

Attributes tab

Figure 253: *Cisco Downloadable ACL Enforcement Attributes tab*



Enforcement Profiles

	Type	Name		Value
1.	Radius:Cisco	Cisco-IP-Downloadable-ACL	=	permit ip any any
2.	Click to add...			

Table 134: *Cisco Downloadable ACL Enforcement Attributes tab Parameters*

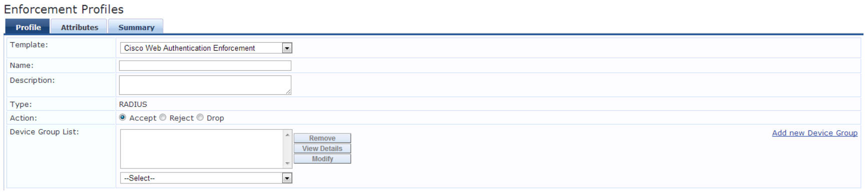
Parameter	Description
Type:	Select one of the following attribute types: - Radius:Aruba - Radius:IETF - Radius:Cisco - Radius:Microsoft - Radius:Avenda For more information, see "RADIUS Namespaces" on page 454
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
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 254: *Cisco Web Authentication Enforcement Profile tab*



Enforcement Profiles

Template:	Cisco Web Authentication Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Table 135: *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.

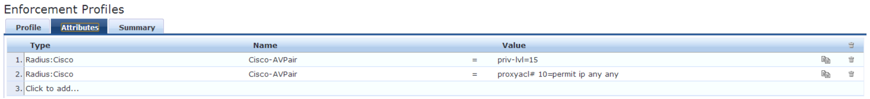
Table 135: *Cisco Web Authentication Enforcement Parameters (Continued)*

Parameter	Description
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 285.

Attributes tab

After you complete setting the attributes, click **Save**. Click **Next** to open the Summary tab.

Figure 255: *Cisco Web Authentication Enforcement Attributes tab*



Enforcement Profiles

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	priv-lvl=15
2.	Radius:Cisco	Cisco-AVPair	=	proxyacl# 10=permit ip any any
3.	Click to add...			

Table 136: *Cisco Web Authentication Enforcement Parameters*

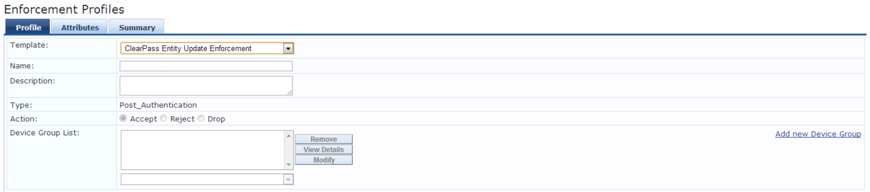
Parameter	Description
Type	Select one of the following attribute types: ● Radius:Aruba ● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda For more information, see "RADIUS Namespaces" on page 454
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
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 256: *ClearPass Entity Update Enforcement Profile tab*



Enforcement Profiles

Template: ClearPass Entity Update Enforcement

Name:

Description:

Type: Post_Authentication

Action: ◉ Accept ○ Reject ○ Drop

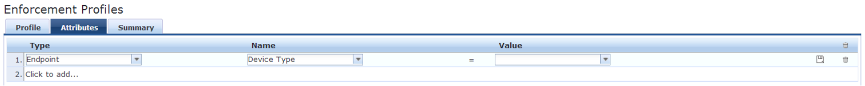
Device Group List:

Table 137: *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.
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 285.

Attributes tab

Figure 257: *ClearPass Entity Update Enforcement Attributes tab*



Enforcement Profiles

	Type	Name		Value
1.	Endpoint	Device Type	=	
2.	Click to add...			

Table 138: *ClearPass Entity Update Enforcement Attributes tab Parameters*

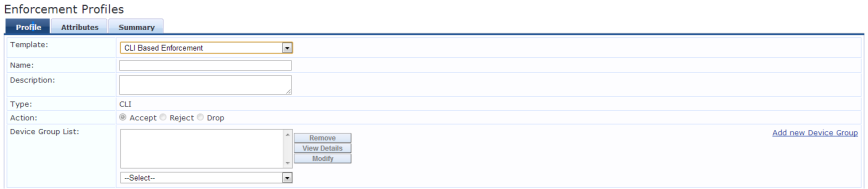
Attribute	Description
Type:	● Endpoint ● Expire-Time-Update ● GuestUser ● Status-Update
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

CLI Based Enforcement

Use this page to configure profile and attribute parameters for the CLI Based Enforcement Profile.

Profile tab

Figure 258: *CLI Based Enforcement Profile tab*



Template: CLI Based Enforcement

Name:

Description:

Type: CLI

Action: ● Accept ○ Reject ○ Drop

Device Group List: --Select--

Table 139: *CLI Based Enforcement Profile tab Parameters*

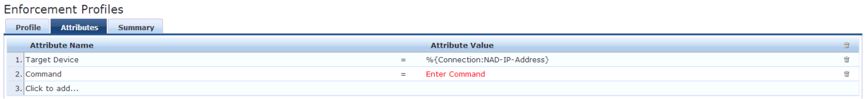
Parameter	Description
Template:	CLI Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	CLI
Action:	Disabled.

Table 139: *CLI Based Enforcement Profile tab Parameters (Continued)*

Parameter	Description
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 285.

Attributes tab

Figure 259: *CLI Based Enforcement Attributes tab*



Enforcement Profiles

	Attribute Name		Attribute Value
1.	Target Device	=	%{Connection:NAD-IP-Address}
2.	Command	=	Enter Command
3.	Click to add...		

Table 140: *CLI Based Enforcement Attributes tab Parameters*

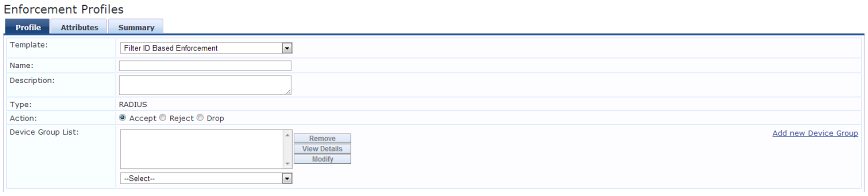
Attribute	Parameter
Attribute Name	Select Command or Target Device.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

Filter ID Based Enforcement

Use this page to configure profile and attribute parameters for the Filter ID Based Enforcement Profile.

Profile tab

Figure 260: *Filter ID Based Enforcement Profile tab*



Enforcement Profiles

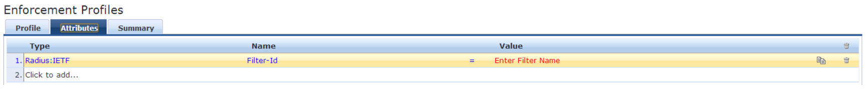
Template:	Filter ID Based Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Table 141: *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.
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 285.

Attributes tab

Figure 261: *Filter ID Based Enforcement Profile Attributes tab*



	Type	Name		Value
1.	Radius:IETF	Filter-Id	=	Enter Filter Name
2.	Click to add...			

Table 142: *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 454

Table 142: *Filter ID Based Enforcement Profile Attributes tab Parameters (Continued)*

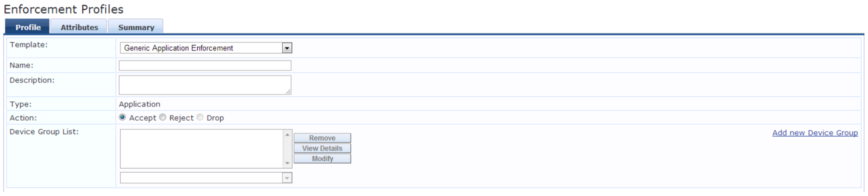
Parameter	Description
Name:	The options displayed for the Name Attribute depend on the attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Generic Application Enforcement

Use this page to configure profile and attribute parameters for the Generic Application Enforcement Profile.

Profile tab

Figure 262: *Generic Application Enforcement Profile tab*



Enforcement Profiles

Template:	Generic Application Enforcement
Name:	
Description:	
Type:	Application
Action:	● Accept ○ Reject ○ Drop
Device Group List:	

Table 143: *Generic Application Enforcement Profile tab Parameters*

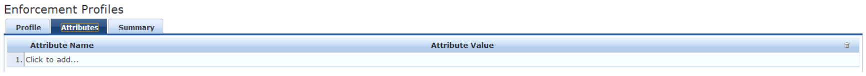
Parameter	Description
Template:	Generic Application Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column 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.

Table 143: *Generic Application Enforcement Profile tab Parameters (Continued)*

Parameter	Description
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 285.

Attributes tab

Figure 263: *Generic Application Enforcement Attributes tab*



Enforcement Profiles

	Attribute Name	Attribute Value
1.	Click to add...	

Table 144: *Generic Application Enforcement Attributes tab Parameters*

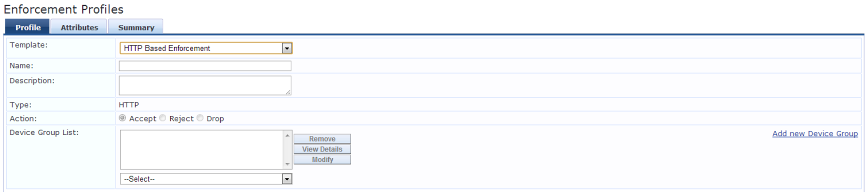
Parameter	Description
Attribute Name	Select an attribute name from the list. The list has multiple pages.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

HTTP Based Enforcement

Use this page to configure profile and attribute parameters for the HTTP Based Enforcement Profile.

Profile tab

Figure 264: *HTTP Based Enforcement Profile tab*



Enforcement Profiles

Template:	HTTP Based Enforcement
Name:	
Description:	
Type:	HTTP
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Table 145: *HTTP Based Enforcement Profile tab Parameters*

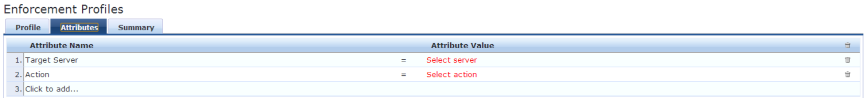
Parameter	Description
Template:	HTTP Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	HTTP. The field is populated automatically.
Action:	Disabled.

Table 145: *HTTP Based Enforcement Profile tab Parameters (Continued)*

Parameter	Description
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 285.

Attributes tab

Figure 265: *HTTP Based Enforcement Attributes tab*



	Attribute Name		Attribute Value
1.	Target Server	=	Select server
2.	Action	=	Select action
3.	Click to add...		

Table 146: *HTTP Based Enforcement Attributes tab Parameters*

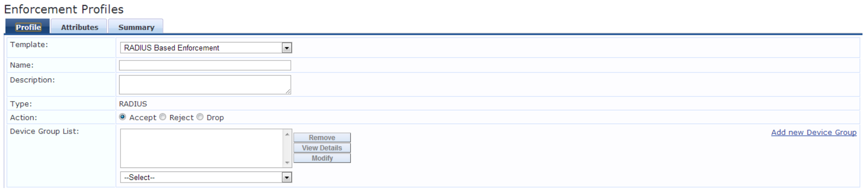
Parameter	Description
Attribute Name	Select Target Server or Action.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

RADIUS Based Enforcement

Use this page to configure profile and attribute parameters for the RADIUS Based Enforcement Profiles.

Profile tab

Figure 266: *RADIUS Based Enforcement Profile tab*



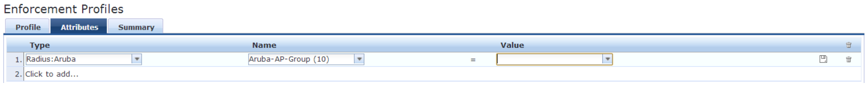
Template:	RADIUS Based Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Table 147: *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.
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 285.

Attributes tab

Figure 267: *RADIUS Based Enforcement Attributes tab*



	Type	Name		Value
1.	Radius:Aruba	Aruba-AP-Group (10)	=	
2.	Click to add...			

Table 148: *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 454

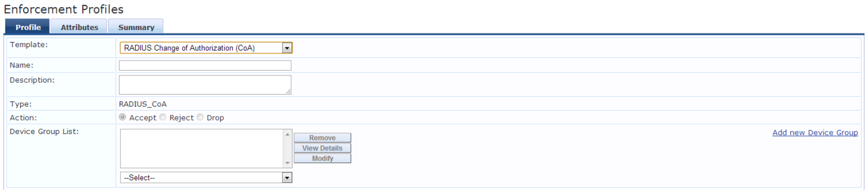
Parameter	Description
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

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 268: *Radius Change of Authorization (CoA) Profile tab*



Enforcement Profiles

Template: RADIUS Change of Authorization (CoA)

Name:

Description:

Type: RADIUS_CoA

Action: ● Accept ○ Reject ○ Drop

Device Group List: --Select--

Table 149: *Radius Change of Authorization (CoA) Profile tab Parameters*

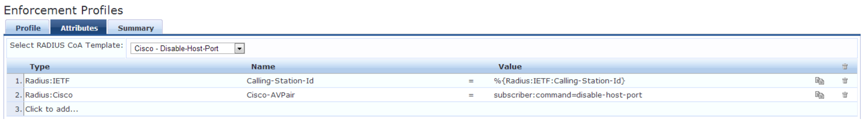
Parameter	Description
Template:	Select from: - Cisco-Disable-Host-Port - Cisco - Bounce-Host-Port - Cisco - Reauthenticate-Session - HP - Change-VLAN - HP - Generic-CoA - Aruba - Change-User-Role - IETF - Terminate-Session-IETF - Aruba - Change-VPN-User-Role - IETF- Generic-CoA-IETF
Type:	Select one of the following attribute types: - Radius:Aruba - Radius:IETF - Radius:Cisco - Radius:Microsoft - Radius:Avenda For more information, see "RADIUS Namespaces" on page 454
Name:	The options displayed for the Name Attribute depend on the RADIUS CoA Template selected and the Type Attribute that were selected.

Table 149: *Radius Change of Authorization (CoA) Profile tab Parameters (Continued)*

Parameter	Description
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.
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 285.

Attributes tab

Figure 269: *Radius Change of Authorization (CoA) Attributes tab*



Select RADIUS CoA Template: Cisco - Disable-Host-Port

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:Cisco	Cisco-AVPair	=	subscriber:command=disable-host-port
3.	Click to add...			

Table 150: *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

Table 150: *Radius Change of Authorization (CoA) Attributes tab Parameters (Continued)*

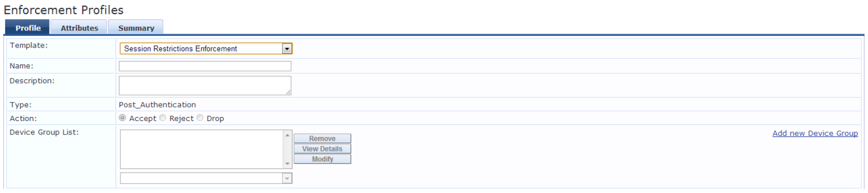
Parameter	Description
Type:	Select one of the following attribute types: - Radius:Aruba - Radius:IETF - Radius:Cisco - Radius:Microsoft - Radius:Avenda For more information, see "RADIUS Namespaces" on page 454
Name:	The options displayed for the Name Attribute depend on the Template and Type Attribute 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 270: *Session Restrictions Enforcement Profile tab*



Enforcement Profiles

Template:	Session Restrictions Enforcement
Name:	
Description:	
Type:	Post_Authentication
Action:	● Accept ○ Reject ○ Drop
Device Group List:	

Table 151: *Session Restrictions Enforcement Profile tab Parameters*

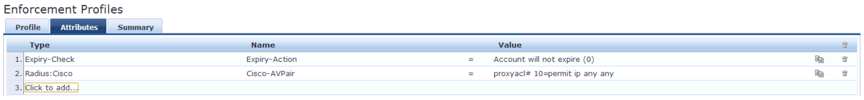
Parameter	Description
Template:	Session Restrictions Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	Post_Authentication. The field is populated automatically.
Action:	Disabled.

Table 151: *Session Restrictions Enforcement Profile tab Parameters (Continued)*

Parameter	Description
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 285.

Attributes tab

Figure 271: *Session Restrictions Enforcement Attributes tab*



	Type	Name		Value
1.	Expiry-Check	Expiry-Action	=	Account will not expire (0)
2.	Radius:Cisco	Cisco-AVPair	=	proxyacl# 10=permit ip any any
3.	Click to add...			

Table 152: *Session Restrictions Enforcement Attributes tab*

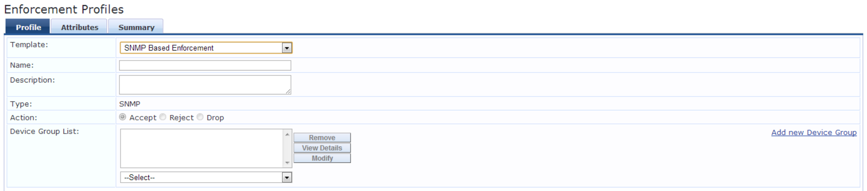
Parameter	Description
Type	Select from: - Bandwidth-Check - Expire-Check - Post-Auth-Check - Session-Check
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value:	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

SNMP Based Enforcement

Use this page to configure profile and attribute parameters for the SNMP Based Enforcement Profile.

Profile tab

Figure 272: *SNMP Based Enforcement Profile tab*



Template: SNMP Based Enforcement

Name:

Description:

Type: SNMP

Action: ● Accept ○ Reject ○ Drop

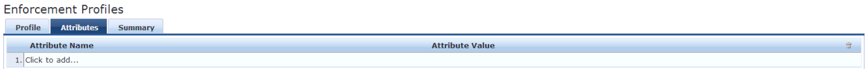
Device Group List: --Select--

Table 153: *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.
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 285.

Attributes tab

Figure 273: *SNMP Based Enforcement Attributes tab*



	Attribute Name	Attribute Value
1.	Click to add...	

Table 154: *SNMP Based Enforcement Attributes tab Parameters*

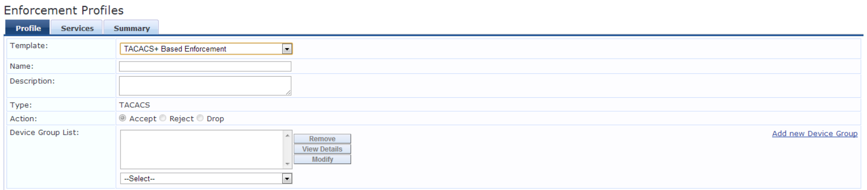
Parameter	Description
Attribute Name:	Select from: ● VLAN ID ● Session Timeout (in seconds) ● Reset Connection (after the settings are applied)
Attribute Value:	The options displayed for the Attribute Value depend on Attribute Name that was selected.

TACACS+ Based Enforcement

Use this page to configure profile, service, and attribute parameters for the TACACS+ Based Enforcement Profile.

Profile tab

Figure 274: *TACACS+ Based Enforcement Profile tab*



Enforcement Profiles

Template: TACACS+ Based Enforcement

Name:

Description:

Type: TACACS

Action: ◉ Accept ○ Reject ○ Drop

Device Group List:

Table 155: *TACACS+ Based Enforcement Profile tab Parameters*

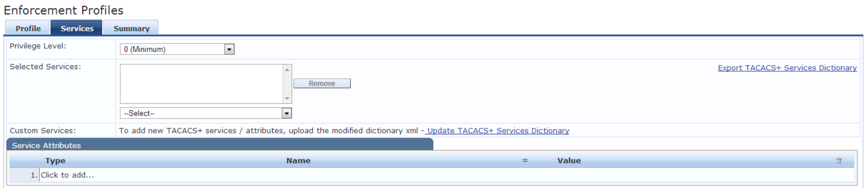
Parameter	Description
Template:	TACACS+ Based Enforcement
Name:	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description:	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type:	TACACS. The field is populated automatically.
Action:	Disabled.

Table 155: *TACACS+ Based Enforcement Profile tab Parameters (Continued)*

Parameter	Description
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 285.

Services tab

Figure 275: *TACACS+ Based Enforcement Services tab*



Privilege Level: 0 (Minimum)

Selected Services: --Select--

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary xml - Update TACACS+ Services Dictionary

Table 156: *TACACS+ Based Enforcement Services tab Parameters*

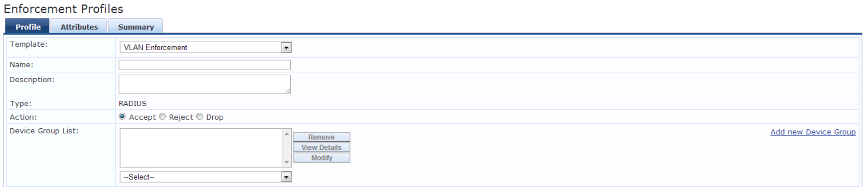
Parameter	Description
Privilege Level:	Select a level between 0 and 15.
Selected Services	Select a service from the list and add it to the Selected Services: field. Click **Remove** to remove a service from the field.
Export TACACS+ Services Dictionary link	Click this link to download the TACACS+ Services 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 ta

Figure 276: *VLAN Enforcement Profile tab*



Enforcement Profiles

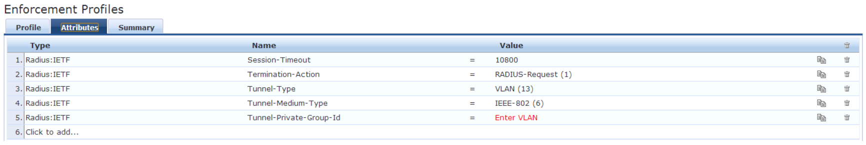
Template:	VLAN Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Table 157: *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.
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 285.

Attributes tab

Figure 277: *VLAN Enforcement Attributes tab*



Enforcement Profiles

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	10800
2.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
5.	Radius:IETF	Tunnel-Private-Group-Id	=	Enter VLAN
6.	Click to add...			

Table 158: *VLAN Enforcement Attributes tab Parameters*

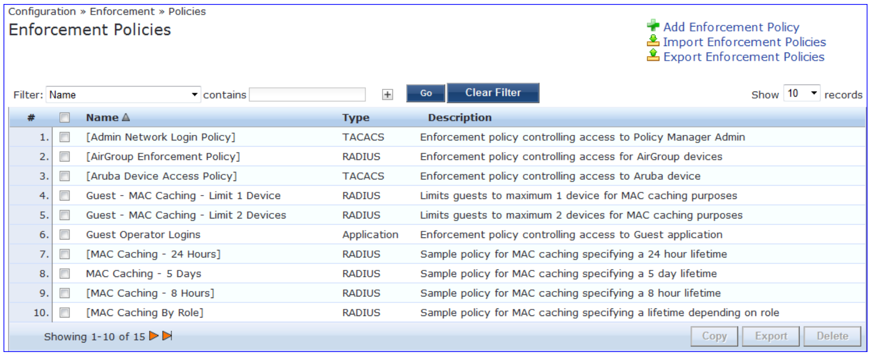
Parameter	Description
Type:	Select one of the following attribute types: - Radius:Aruba - Radius:IETF - Radius:Cisco - Radius:Microsoft - Radius:Avenda For more information, see "RADIUS Namespaces" on page 454
Name:	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
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 278: *Enforcement Policies Listing Page*



Configuration » Enforcement » Policies

Enforcement Policies

Add Enforcement Policy
Import Enforcement Policies
Export Enforcement Policies

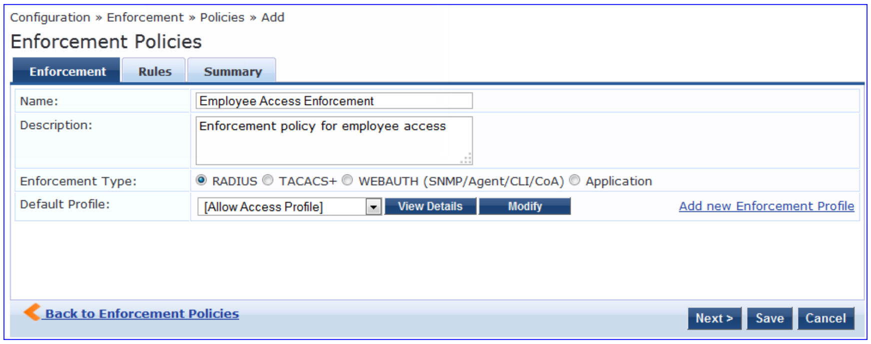
Filter: Name contains [+] Go Clear Filter Show 10 records

#	□	Name ▲	Type	Description
1.	□	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin
2.	□	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	□	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device
4.	□	Guest - MAC Caching - Limit 1 Device	RADIUS	Limits guests to maximum 1 device for MAC caching purposes
5.	□	Guest - MAC Caching - Limit 2 Devices	RADIUS	Limits guests to maximum 2 devices for MAC caching purposes
6.	□	Guest Operator Logins	Application	Enforcement policy controlling access to Guest application
7.	□	[MAC Caching - 24 Hours]	RADIUS	Sample policy for MAC caching specifying a 24 hour lifetime
8.	□	MAC Caching - 5 Days	RADIUS	Sample policy for MAC caching specifying a 5 day lifetime
9.	□	[MAC Caching - 8 Hours]	RADIUS	Sample policy for MAC caching specifying a 8 hour lifetime
10.	□	[MAC Caching By Role]	RADIUS	Sample policy for MAC caching specifying a lifetime depending on role

Showing 1-10 of 15 ▶ ▶|

Click **Add Enforcement Policy** to open the **Add Enforcement Policy** wizard:

Figure 279: *Add Enforcement Policy (Enforcement tab)*



Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement | Rules | Summary

Name:	Employee Access Enforcement
Description:	Enforcement policy for employee access
Enforcement Type:	● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application
Default Profile:	[Allow Access Profile] View Details Modify Add new Enforcement Profile

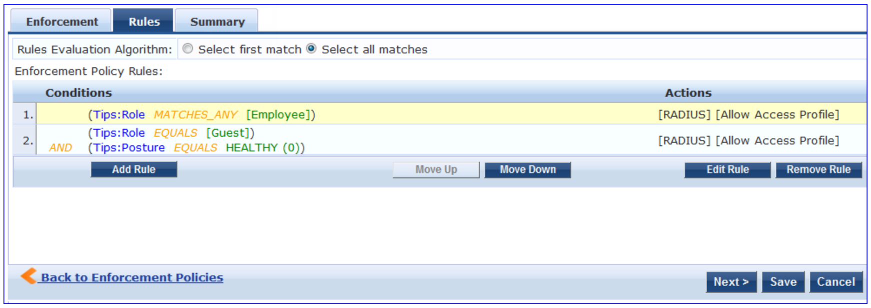
Back to Enforcement Policies — Next > | Save | Cancel

Table 159: *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 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 280: *Add Enforcement Policy (Rules Tab)*



Enforcement | Rules | Summary

Rules Evaluation Algorithm: ○ Select first match ● Select all matches

Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role MATCHES_ANY [Employee])	[RADIUS] [Allow Access Profile]
2.	(Tips:Role EQUALS [Guest]) AND (Tips:Posture EQUALS HEALTHY (0))	[RADIUS] [Allow Access Profile]

Add Rule | Move Up | Move Down | Edit Rule | Remove Rule

Back to Enforcement Policies — Next > | Save | Cancel

Table 160: *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 161: *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 block access to WorkSpace and Workspace apps if the device is not MDM managed, choose **Application:ClearPass** in the Type field and select **Device-MDM-Managed** and set value to **False**. 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 246 for a list of the default profiles.

Network Access Devices

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:

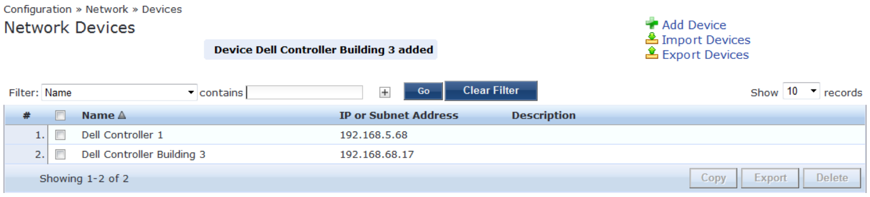
- "Adding and Modifying Devices" on page 281
- "Adding and Modifying Device Groups" on page 285
- "Adding and Modifying Proxy Targets" on page 287

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 281: *Network Devices page*



Configuration » Network » Devices

Network Devices

Device Dell Controller Building 3 added

Filter: Name contains

Show 10 records

#	□	Name	IP or Subnet Address	Description
1.	□	Dell Controller 1	192.168.5.68	
2.	□	Dell Controller Building 3	192.168.68.17	

Showing 1-2 of 2

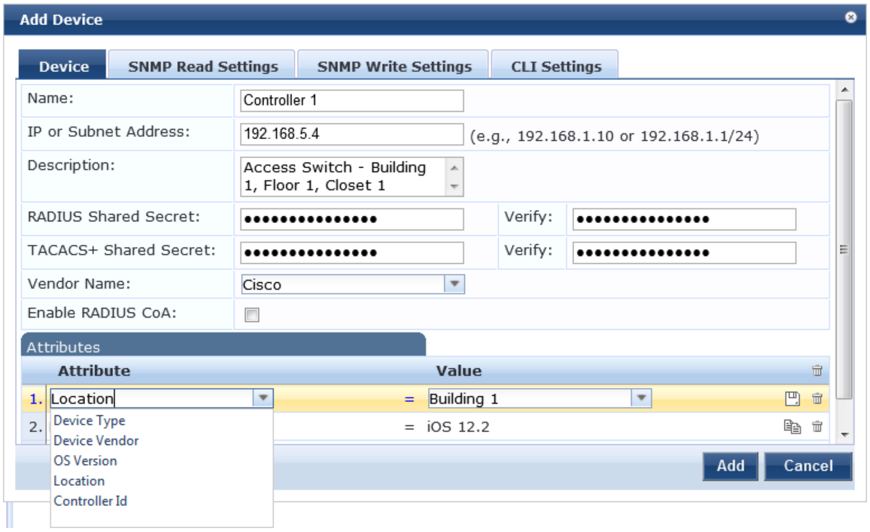
For more information, see:

- "Adding a Device" on page 281
- "Additional Available Tasks" on page 285

Adding a Device

To add a device, click the **Add Device** link, and then complete the fields in the **Add Device** popup. The tabs and fields are described in the images that follow.

Figure 282: *Device tab*



Name: Controller 1

IP or Subnet Address: 192.168.5.4 (e.g., 192.168.1.10 or 192.168.1.1/24)

Description: Access Switch - Building 1, Floor 1, Closet 1

RADIUS Shared Secret: ••••••••••••••• Verify: •••••••••••••••

TACACS+ Shared Secret: ••••••••••••••• Verify: •••••••••••••••

Vendor Name: Cisco

Enable RADIUS CoA: □

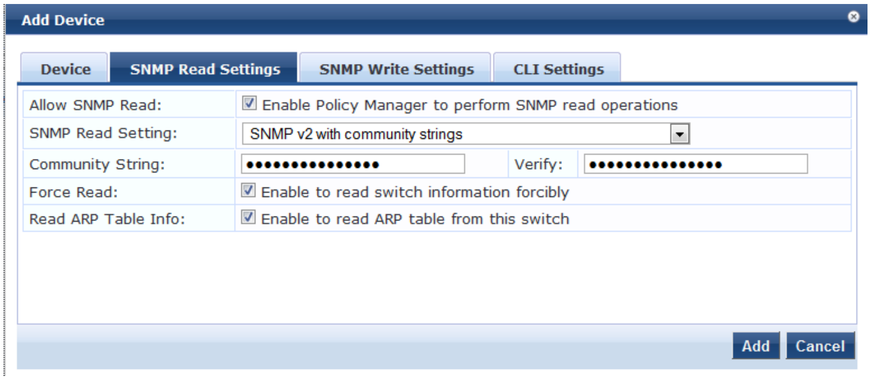
	Attribute		Value
1.	Location	=	Building 1
2.		=	iOS 12.2

Device Type
Device Vendor
OS Version
Location
Controller Id

Table 162: *Device tab Parameters*

Parameter	Description
Name/ Description	Specify identity of the device.
IP Address or Subnet	Specify the IP address or the subnet (E.g., 192.168.5.0/24) of the device.
RADIUS/TACACS+ Shared Secret	Enter and confirm a Shared Secret for each of the two supported request protocols.
Vendor	Optionally, specify the dictionary to be loaded for this device. **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 Change of Authorization (RFC 3576/5176) for this device. Set the UDP port on the device to send CoA actions. 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 dropdown: 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 Attribute dropdown for all devices. **NOTE:** All attributes entered for a device are available in the role mapping rules editor under the Device namespace.
Add/Cancel	Click **Add** to commit or **Cancel** to dismiss the popup.

Figure 283: *SNMP Read/Write Settings tabs*



Allow SNMP Read: ☑ Enable Policy Manager to perform SNMP read operations

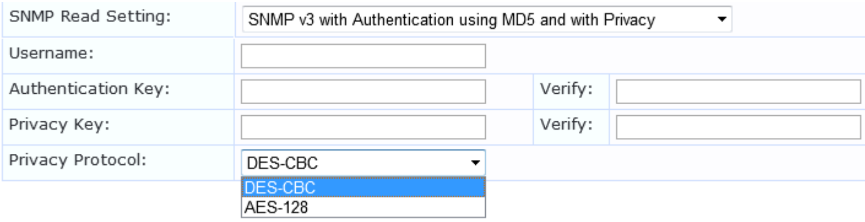
SNMP Read Setting: SNMP v2 with community strings

Community String: ••••••••••••••• Verify: •••••••••••••••

Force Read: ☑ Enable to read switch information forcibly

Read ARP Table Info: ☑ Enable to read ARP table from this switch

Figure 284: *SNMP Read/Write Settings tabs - SNMP v3 Details*



SNMP Read Setting: SNMP v3 with Authentication using MD5 and with Privacy

Username:

Authentication Key: Verify:

Privacy Key: Verify:

Privacy Protocol: DES-CBC

Table 163: *SNMP Read/Write Settings tabs*

Parameter	Description
Allow SNMP Read/Write	Toggle to enable/disable SNMP Read/Write.
Default VLAN (SNMP Write only)	VLAN port setting after SNMP-enforced session expires.
SNMP Read/Write Setting	SNMP settings for the device.
Community String (SNMP v2 only)	
Force Read (SNMP v1 and v2 only)	Enable this setting to ensure that all CPPM nodes in the cluster read SNMP information from this device regardless of the 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.
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 as a way to discover endpoints in the network. Static IP endpoints discovered this way are further probed via SNMP to profile the device.

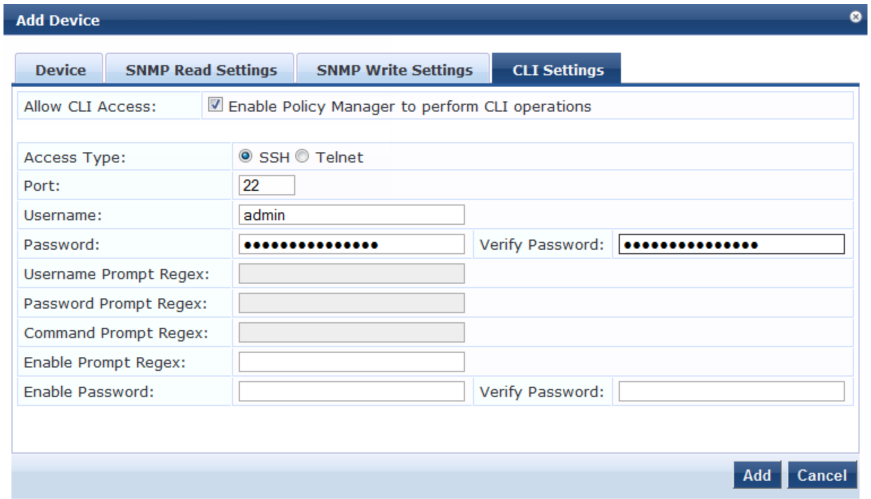
Table 163: *SNMP Read/Write Settings tabs (Continued)*

Parameter	Description
Username (SNMP v3 only)	Admin user name to use for SNMP read/write operations
Authentication Key (SNMP v3 only)	SNMP v3 with authentication option (SHA & MD5)
Privacy Key (SNMP v3 only)	SNMP v3 with privacy option
Privacy Protocol (SNMP v3 w/ privacy only)	Choose one of the available privacy protocols: - DES-CBC - AES-128
Add/Cancel	Click **Add** to commit or **Cancel** to dismiss the popup.

NOTE

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.

Figure 285: *CLI Settings tab*



Allow CLI Access: ☑ Enable Policy Manager to perform CLI operations

Access Type: ● SSH ○ Telnet

Port: 22

Username: admin

Password: ••••••••••••••• Verify Password: •••••••••••••••

Username Prompt Regex:

Password Prompt Regex:

Command Prompt Regex:

Enable Prompt Regex:

Enable Password: Verify Password:

Table 164: *CLI Settings tab*

Parameter	Description
Allow CLI Access	Toggle to enable/disable CLI access.

Table 164: *CLI Settings tab (Continued)*

Parameter	Description
Access Type	Select SSH or Telnet. Policy Manager uses this access method to log into the device CLI.
Port	SSH or Telnet TCP port number.
Username/Password	Credentials to log into the CLI.
Username Prompt Regex	Regular expression for the username prompt. Policy Manager looks for this pattern to recognize the telnet username prompt.
Password Prompt Regex	Regular expression for the password prompt. Policy Manager looks for this pattern to recognize the telnet password prompt.
Command Prompt Regex	Regular expression for the command line prompt. Policy Manager looks for this pattern to recognize the telnet command line prompt.
Enable Prompt Regex	Regular expression for the command line "enable" prompt. Policy Manager looks for this pattern to recognize the telnet command line prompt.
Enable Password	Credentials for "Enable" in the CLI.
Add/Cancel	Click **Add** to commit or **Cancel** to dismiss the popup.

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.**

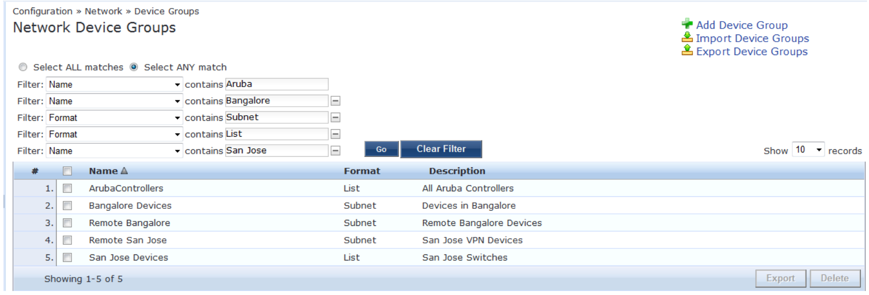
Adding and Modifying Device Groups

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 286: *Device Groups Page*



Configuration » Network » Device Groups

Network Device Groups

○ Select ALL matches ● Select ANY match

Filter: Name contains Aruba

Filter: Name contains Bangalore

Filter: Format contains Subnet

Filter: Format contains List

Filter: Name contains San Jose

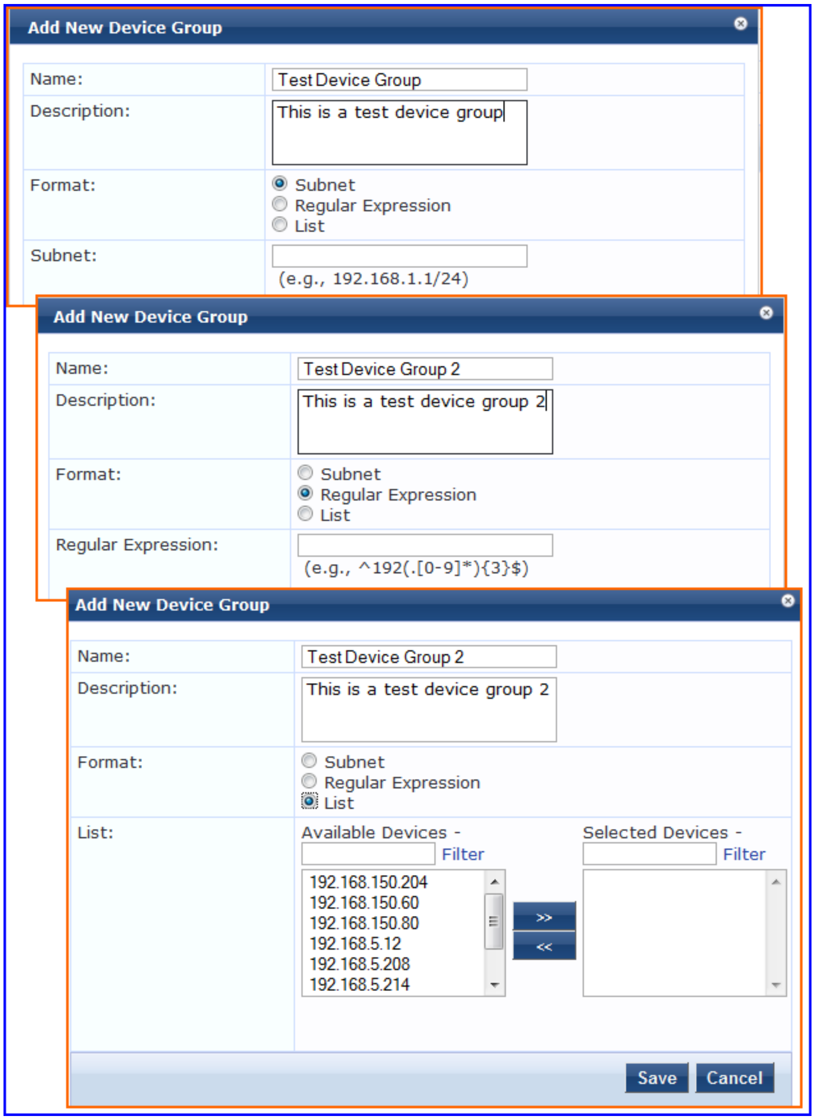
Show 10 records

#	□	Name ▲	Format	Description
1.	□	ArubaControllers	List	All Aruba Controllers
2.	□	Bangalore Devices	Subnet	Devices in Bangalore
3.	□	Remote Bangalore	Subnet	Remote Bangalore Devices
4.	□	Remote San Jose	Subnet	San Jose VPN Devices
5.	□	San Jose Devices	List	San Jose Switches

Showing 1-5 of 5

To add a Device Group, click **Add Device Group**. Complete the fields in the **Add New Device Group** popup:

Figure 287: *Add New Device Group Popup*



Add New Device Group

Name: Test Device Group

Description: This is a test device group

Format: ● Subnet ○ Regular Expression ○ List

Subnet:

(e.g., 192.168.1.1/24)

Add New Device Group

Name: Test Device Group 2

Description: This is a test device group 2

Format: ○ Subnet ● Regular Expression ○ List

Regular Expression:

(e.g., ^192(.[0-9]*){3}$)

Add New Device Group

Name: Test Device Group 2

Description: This is a test device group 2

Format: ○ Subnet ○ Regular Expression ● List

List: Available Devices - Filter

192.168.150.204
192.168.150.60
192.168.150.80
192.168.5.12
192.168.5.208
192.168.5.214

Selected Devices - Filter

Table 165: *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}$
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.

NOTE

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 Device Groups**; in the **Import from File** popup, browse to select a file, then click **Import**.
- To export all Device Groups from the configuration, click **Export Devices**; 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**.

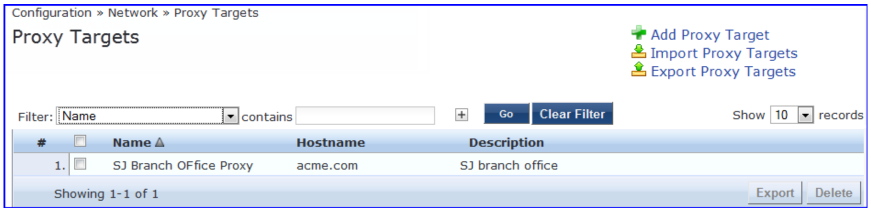
Adding and Modifying Proxy Targets

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 99.)

Policy Manager lists all configured proxy servers in the **Proxy Servers** page: **Configuration** > **Network** > **Proxy Servers**.

Figure 288: *Proxy Targets Page*



Configuration » Network » Proxy Targets

Proxy Targets

Filter: Name contains

Show 10 records

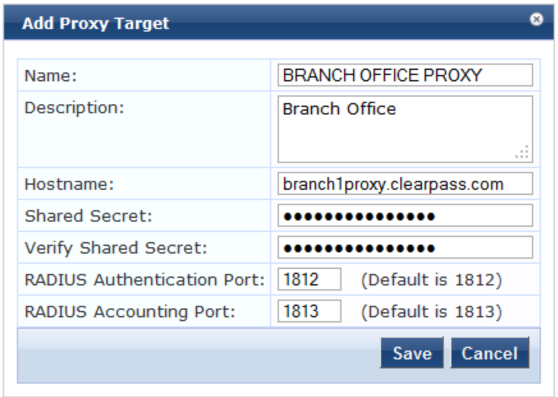
#	□	Name	Hostname	Description
1.	□	SJ Branch OFfice Proxy	acme.com	SJ branch office

Showing 1-1 of 1

Add a Proxy Target

To add a Proxy Target, click **Add Proxy Target**, 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 289: *Add Proxy Target Popup*



Add Proxy Target

Name:	BRANCH OFFICE PROXY
Description:	Branch Office
Hostname:	branch1proxy.clearpass.com
Shared Secret:	•••••••••••••••
Verify Shared Secret:	•••••••••••••••
RADIUS Authentication Port:	1812 (Default is 1812)
RADIUS Accounting Port:	1813 (Default is 1813)

Table 166: *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 Proxy Targets**. In the **Import from File** popup, browse to select a file and click **Import**.

Export all Proxy Targets

Click **Export Proxy Targets**. 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**.

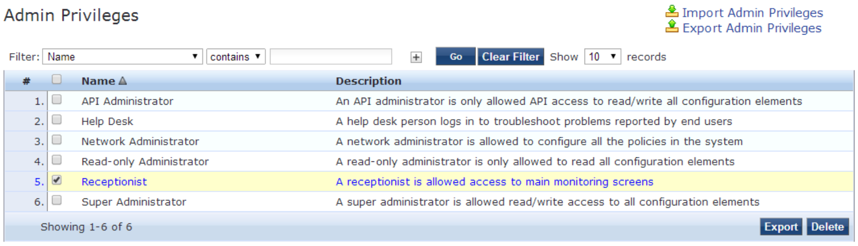
Custom Admin Privileges

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 321
- "Administrator Privileges and IDs" on page 322
- "Creating Custom Administrator Privileges" on page 323
- "Sample Administrator Privilege XML File" on page 324
- "Data Filters" on page 65

Figure 290: *Admin Privileges Page*



Admin Privileges

#	□	Name △	Description
1.	□	API Administrator	An API administrator is only allowed API access to read/write all configuration elements
2.	□	Help Desk	A help desk person logs in to troubleshoot problems reported by end users
3.	□	Network Administrator	A network administrator is allowed to configure all the policies in the system
4.	□	Read-only Administrator	A read-only administrator is only allowed to read all configuration elements
5.	☑	Receptionist	A receptionist is allowed access to main monitoring screens
6.	□	Super Administrator	A super administrator is allowed read/write access to all configuration elements

Showing 1-6 of 6

Table 167: *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 Admin Privileges	Click to navigate to and import a new or changed custom administrator privileges XML file.
Export Admin Privileges	Select a file and click this button to export an administrator privileges XML file to a local drive.

Chapter 13
Policy Simulation

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 292
- "Application Authentication" on page 292
- "Audit" on page 294
- "Chained Simulation" on page 295
- "Enforcement Policy" on page 298
- "RADIUS Authentication" on page 301
- "Role Mapping" on page 306
- "Service Categorization" on page 309

Figure 291: *Policy Simulation page*

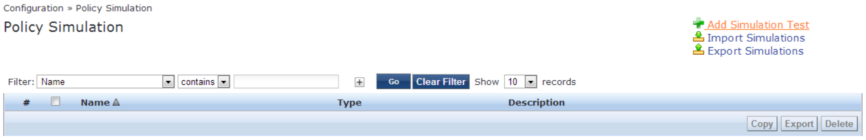


Table 168: *Policy Simulation Page Parameters*

Parameter	Description
Add Simulation Test:	Opens the Configuration >> Policy Simulation>>Add page.
Import Simulations:	Opens the **Import from file** popup.
Export Simulations:	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

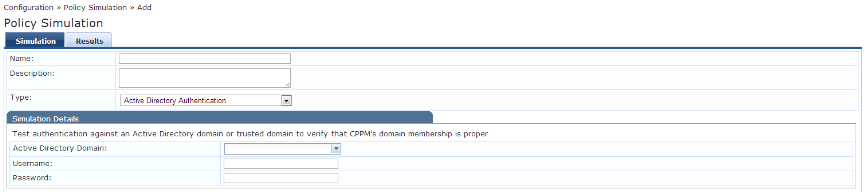
This simulation tests authentication against an Active Directory domain or trusted domain to verify that the CPPM domain membership is valid.

NOTE

The Attributes tab is not available for this simulation type.

Simulation tab

Figure 292: *Active Directory Authentication Simulation tab*



Configuration » Policy Simulation » Add

Policy Simulation

Name:

Description:

Type: Active Directory Authentication

Simulation Details

Test authentication against an Active Directory domain or trusted domain to verify that CPPM's domain membership is proper

Active Directory Domain:

Username:

Password:

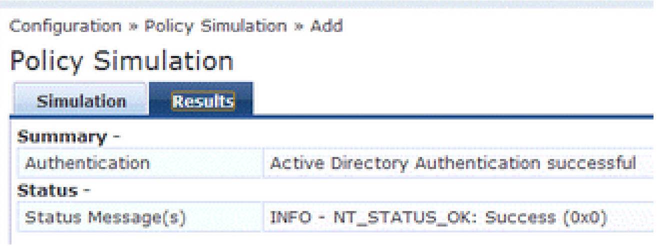
Table 169: *Active Directory Authentication Simulation tab Parameters*

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 293: *Active Directory Authentication Results tab*



Configuration » Policy Simulation » Add

Policy Simulation

Summary -

Authentication: Active Directory Authentication successful

Status -

Status Message(s): INFO - NT_STATUS_OK: Success (0x0)

Table 170: *Active Directory Authentication Results tab Parameters*

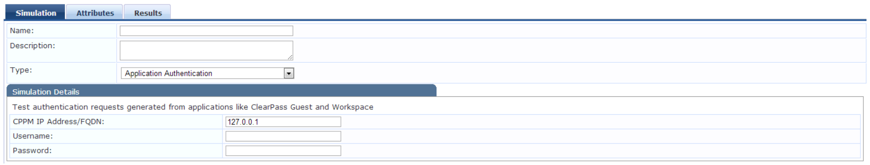
Parameter	Description
Summary -	Displays the results of the Active Directory Authentication simulation.
Status -	Displays the status message.

Application Authentication

This simulation tests authentication requests generated from applications such as ClearPass Guest and Workspace.

Simulation tab

Figure 294: *Application Authentication Simulation tab*



Name:

Description:

Type: Application Authentication

Test authentication requests generated from applications like ClearPass Guest and Workspace

CPPM IP Address/FQDN: 127.0.0.1

Username:

Password:

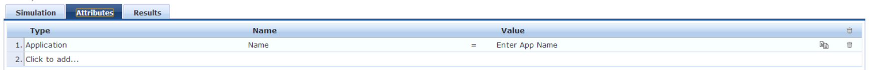
Table 171: *Application Authentication Simulation tab Parameters*

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 295: *Application Authentication Attributes tab*



	Type	Name		Value
1.	Application	Name	=	Enter App Name
2.	Click to add...			

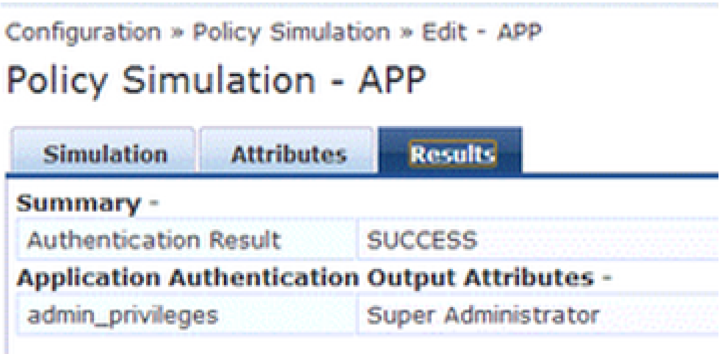
Table 172: *Application Authentication Attributes tab Parameters*

Attribute	Parameter
Type:	Select Application or select Application:ClearPass. See "Application Namespace" on page 446
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 296: *Application Authentication Results tab*


Configuration » Policy Simulation » Edit - APP

Policy Simulation - APP

Summary -

Authentication Result	SUCCESS

Application Authentication Output Attributes -

admin_privileges	Super Administrator

Table 173: *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.

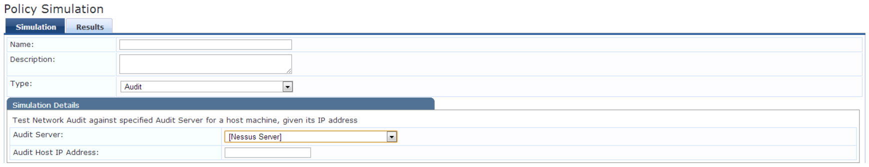
NOTE

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 297: *Audit Simulation tab*


Policy Simulation

Name:

Description:

Type: Audit

Simulation Details

Test Network Audit against specified Audit Server for a host machine, given its IP address

Audit Server: [Nessus Server]

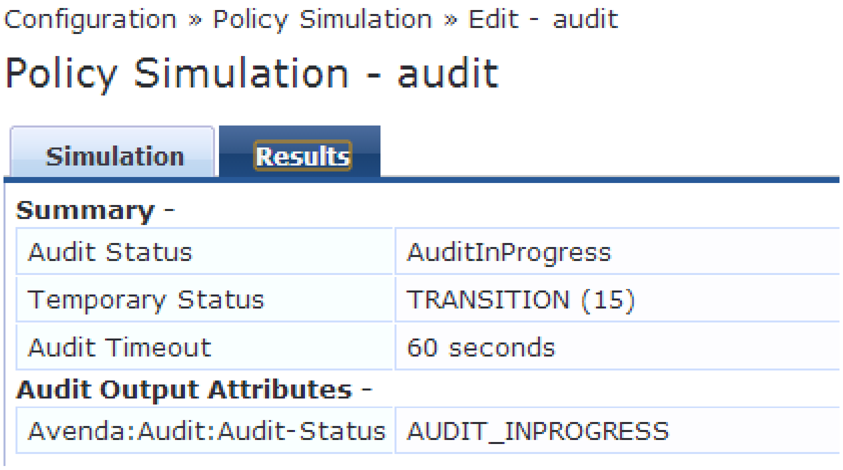
Audit Host IP Address:

Table 174: *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 298: *Audit Simulation Results tab*



Configuration » Policy Simulation » Edit - audit
Policy Simulation - audit
Simulation
Results

Summary -

Audit Status	AuditInProgress
Temporary Status	TRANSITION (15)
Audit Timeout	60 seconds

Audit Output Attributes -

Avenda:Audit:Audit-Status	AUDIT_INPROGRESS

Table 175: *Audit Results tab Parameters*

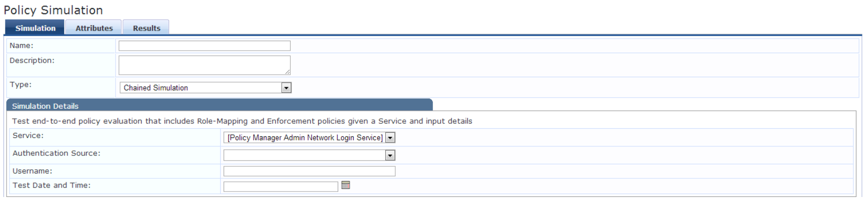
Parameter	Description
Summary -	Displays information about the Audit Status, Temporary Status, and Audit Timeout.
Audit Output Attributes -	Displays the Audit-Status, such as AUDIT_INPROGRESS.

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 299: *Chained Simulation tab*



Name:

Description:

Type: Chained Simulation

Test end-to-end policy evaluation that includes Role-Mapping and Enforcement policies given a Service and input details

Service: [Policy Manager Admin Network Login Service]

Authentication Source:

Username:

Test Date and Time:

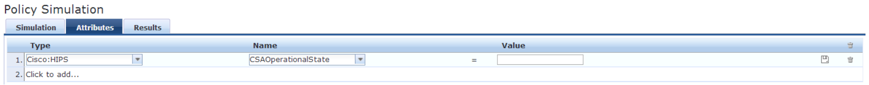
Table 176: *Chained Simulation tab Parameters*

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 452

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 300: *Chained Simulation Attributes tab*



	Type	Name		Value
1.	Cisco:HIPS	CSAOperationalState	=	
2.	Click to add...			

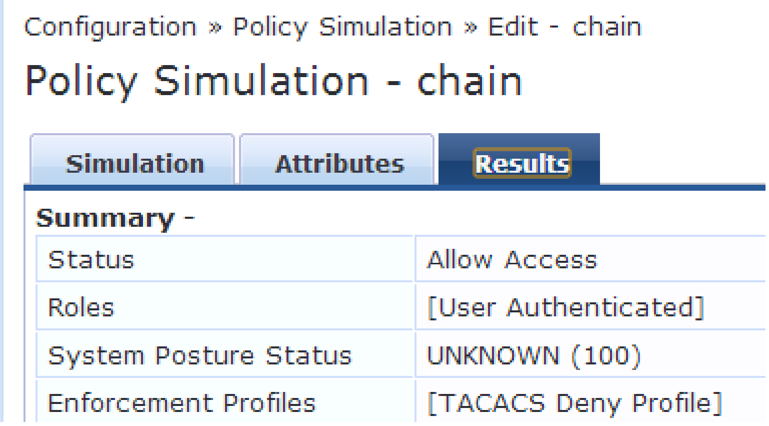
Table 177: *Chained Simulation Attributes tab Parameters*

Attribute	Parameter
Type:	
Host	See "Host Namespaces" on page 453
Authentication	See "Authentication Namespaces" on page 447
Connection	See "Connection Namespaces" on page 451

Attribute	Parameter
Application	See "Application Namespace" on page 446
Certificate	See "Certificate Namespaces" on page 450
• 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 454
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 301: *Chained Simulation Results tab*



Configuration » Policy Simulation » Edit - chain

Policy Simulation - chain

Summary -

Status	Allow Access
Roles	[User Authenticated]
System Posture Status	UNKNOWN (100)
Enforcement Profiles	[TACACS Deny Profile]

Table 178: *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

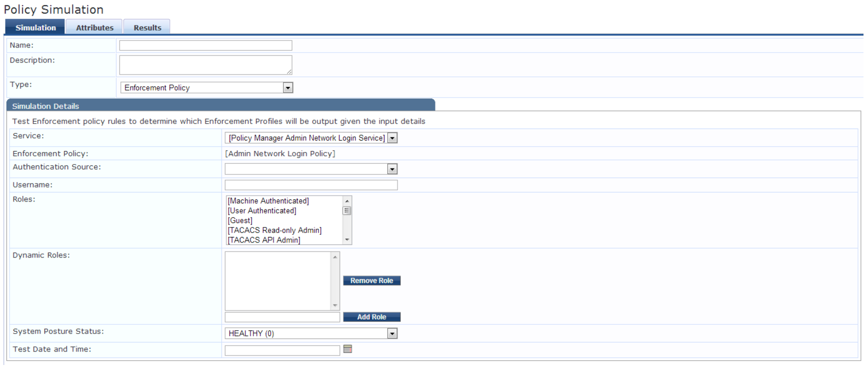
Given the service name (and the associated enforcement policy), a role or a set of roles, the system posture status, and an optional date and time, the enforcement policy simulation evaluates the rules in the enforcement policy and displays the resulting enforcement profiles and their contents.

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 "Adding and Modifying Authentication Sources" on page 149.

Simulation tab

Figure 302: *Enforcement Policy Simulation tab*



Name:

Description:

Type: Enforcement Policy

Test Enforcement policy rules to determine which Enforcement Profiles will be output given the input details

Service: [Policy Manager Admin Network Login Service]

Enforcement Policy: [Admin Network Login Policy]

Authentication Source:

Username:

Roles: [Machine Authenticated]
[User Authenticated]
[Guest]
[TACACS Read-only Admin]
[TACACS API Admin]

Dynamic Roles:

System Posture Status: HEALTHY (0)

Test Date and Time:

Table 179: *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

Table 179: *Enforcement Policy Simulation tab Parameters (Continued)*

Parameter	Description
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] - [Onboard Mac OS X] - Onboard iOS] - [Aruba TACACS root Admin] - [Aruba TACACS read-only Admin] - [Device Registration] - [BYOD Operator] - [AirGroup V1] - [AirGroup v2]

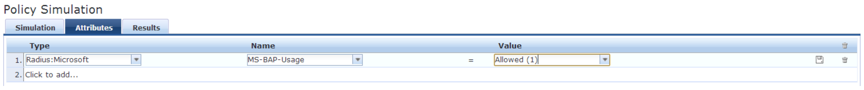
Table 179: *Enforcement Policy Simulation tab Parameters (Continued)*

Parameter	Description
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 454
Test Date and Time:	Click calendar icon to select start date and time for simulation test. See "Date Namespaces" on page 452

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 303: *Enforcement Policy Attributes tab*



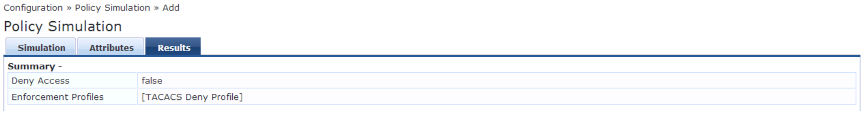
	Type	Name		Value
1.	Radius:Microsoft	MS-BAP-Usage	=	Allowed (1)
2.	Click to add...			

Table 180: *Enforcement Policy Attributes tab Parameters*

Attribute	Description
Type:	
Host:	See "Host Namespaces" on page 453
Authentication:	See "Authentication Namespaces" on page 447
Connection:	See "Connection Namespaces" on page 451
Application:	See "Application Namespace" on page 446
● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda ● Radius:Aruba	See "RADIUS Namespaces" on page 454
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 304: *Policy Simulation Results tab*



Configuration » Policy Simulation » Add

Policy Simulation

Summary -

Deny Access	false
Enforcement Profiles	[TACACS Deny Profile]

Table 181: *Enforcement Policy Results tab Parameters*

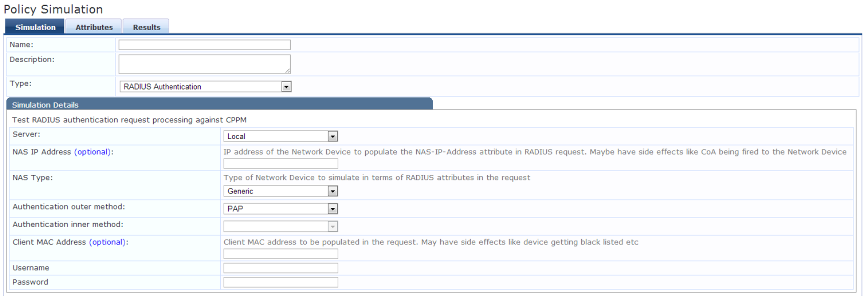
Parameter	Description
Deny Access-	Displays the output of the Deny Access test.
Enforcement Profile	Displays the name of the Enforcement Profile.

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 398 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 305: *RADIUS Authentication Simulation tab (Local Server selected)*



Policy Simulation

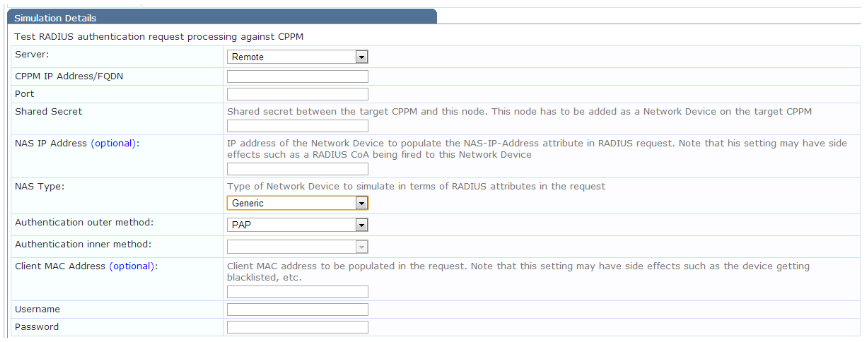
Name:	
Description:	
Type:	RADIUS Authentication

Simulation Details

Test RADIUS authentication request processing against CPPM

Server:	Local
NAS IP Address (optional):	IP address of the Network Device to populate the NAS-IP-Address attribute in RADIUS request. Maybe have side effects like CoA being fired to the Network Device
NAS Type:	Type of Network Device to simulate in terms of RADIUS attributes in the request Generic
Authentication outer method:	PAP
Authentication inner method:	
Client MAC Address (optional):	Client MAC address to be populated in the request. May have side effects like device getting black listed etc
Username	
Password	

Figure 306: *RADIUS Authentication Simulation tab (Remote Server selected)*



Simulation Details

Test RADIUS authentication request processing against CPPM

Server:	Remote
CPPM IP Address/FQDN	
Port	
Shared Secret	Shared secret between the target CPPM and this node. This node has to be added as a Network Device on the target CPPM
NAS IP Address (optional):	IP address of the Network Device to populate the NAS-IP-Address attribute in RADIUS request. Note that his setting may have side effects such as a RADIUS CoA being fired to this Network Device
NAS Type:	Type of Network Device to simulate in terms of RADIUS attributes in the request Generic
Authentication outer method:	PAP
Authentication inner method:	
Client MAC Address (optional):	Client MAC address to be populated in the request. Note that this setting may have side effects such as the device getting blacklisted, etc.
Username	
Password	

Table 182: *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.
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

Table 182: *RADIUS Simulation tab Parameters (Continued)*

Parameter	Description
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 447
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**.
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.	

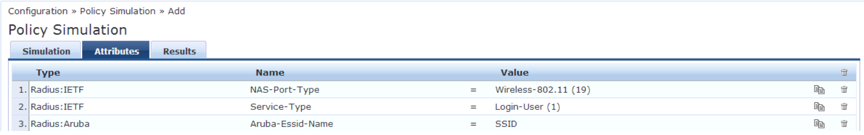
Attributes tab

Enter the attributes of the policy component to be tested.

The attributes that you set depend on the NAS Type selected on the Simulation page.

NAS Type: Aruba Wireless Controller

Figure 307: *Aruba Wireless Controller Type Attributes tab*



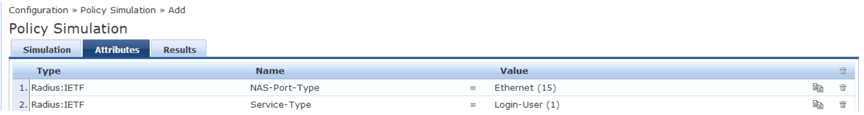
	Type	Name		Value
1.	Radius:IETF	NAS-Port-Type	=	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	=	Login-User (1)
3.	Radius:Aruba	Aruba-Essid-Name	=	SSID

Table 183: *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 308: *NAS Type: Aruba Wired Switch Controller Attributes tab*



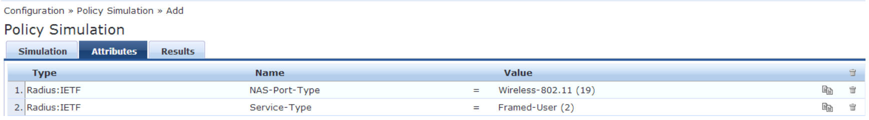
	Type	Name		Value
1.	Radius:IETF	NAS-Port-Type	=	Ethernet (15)
2.	Radius:IETF	Service-Type	=	Login-User (1)

Table 184: *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 309: *NAS Type: Cisco Wireless Switch Attributes tab*



Configuration » Policy Simulation » Add

Policy Simulation

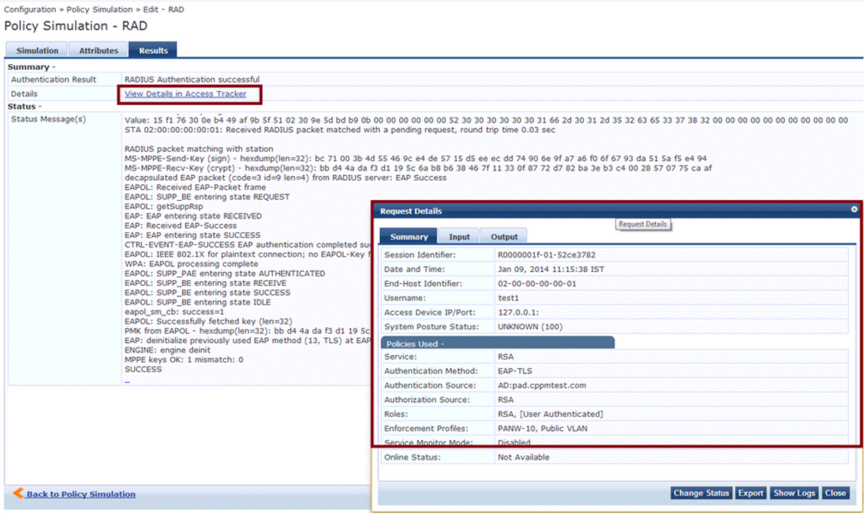
	Type	Name		Value
1.	Radius:IETF	NAS-Port-Type	=	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	=	Framed-User (2)

Table 185: *[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 310: *Results tab*



Configuration » Policy Simulation » Edit - RAD

Policy Simulation - RAD

Summary -

Authentication Result	RADIUS Authentication successful
Details	View Details in Access Tracker

Status -

Status Message(s)

```
Value: 15 f1 76 30 0e b4 49 af 9b 5f 51 02 30 9e 5d bd b9 0b 00 00 00 00 00 00 52 30 30 30 30 30 30 31 66 2d 30 31 2d 35 32 63 65 33 37 38 32 00 00 00 00 00 00 00 00 00 00
STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.03 sec

RADIUS packet matching with station
MS-MPPE-Send-Key (sign) - hexdump(len=32): bc 71 00 3b 4d 55 46 9c e4 de 57 15 d5 ee ec dd 74 90 6e 9f a7 a6 f0 6f 67 93 da 51 5a f5 e4 94
MS-MPPE-Recv-Key (crypt) - hexdump(len=32): bb d4 4a da f3 d1 19 5c 6a b8 b6 38 46 7f 11 33 0f 87 72 d7 82 ba 3e b3 c4 00 28 57 07 75 ca af
decapsulated EAP packet (code=3 id=9 len=4) from RADIUS server: EAP Success
EAPOL: Received EAP-Packet frame
EAPOL: SUPP_BE entering state REQUEST
EAPOL: getSuppRsp
EAP: EAP entering state RECEIVED
EAP: Received EAP-Success
EAP: EAP entering state SUCCESS
CTRL-EVENT-EAP-SUCCESS EAP authentication completed su
EAPOL: IEEE 802.1X for plaintext connection; no EAPOL-Key f
WPA: EAPOL processing complete
EAPOL: SUPP_PAE entering state AUTHENTICATED
EAPOL: SUPP_BE entering state RECEIVE
EAPOL: SUPP_BE entering state SUCCESS
EAPOL: SUPP_BE entering state IDLE
eapol_sm_cb: success=1
EAPOL: Successfully fetched key (len=32)
PMK from EAPOL - hexdump(len=32): bb d4 4a da f3 d1 19 5c
EAP: deinitialize previously used EAP method (13, TLS) at EAP
ENGINE: engine deinit
MPPE keys OK: 1 mismatch: 0
SUCCESS
```

Back to Policy Simulation

Request Details

Session Identifier:	R0000001f-01-52ce3782
Date and Time:	Jan 09, 2014 11:15:38 IST
End-Host Identifier:	02-00-00-00-00-01
Username:	test1
Access Device IP/Port:	127.0.0.1:
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	RSA
Authentication Method:	EAP-TLS
Authentication Source:	AD:pad.cppmtest.com
Authorization Source:	RSA
Roles:	RSA, [User Authenticated]
Enforcement Profiles:	PANW-10, Public VLAN
Service Monitor Mode:	Disabled
Online Status:	Not Available

Table 186: *RADIUS Authentication Results tab Parameters*

Parameter	Description
Summary -	Displays a summary of the simulation.
Authentication Result	Displays the outcome of the Authentication test.

Table 186: *RADIUS Authentication Results tab Parameters (Continued)*

Parameter	Description
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.

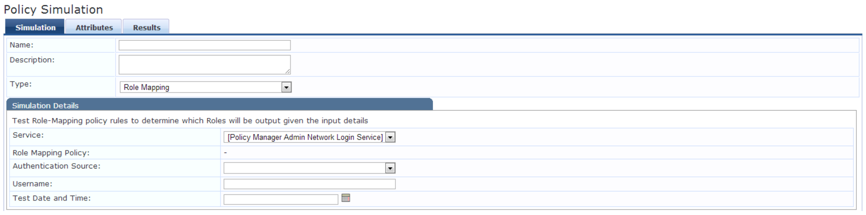
Role Mapping

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 311: *Role Mapping Simulation tab*



Name:	
Description:	
Type:	Role Mapping

Simulation Details

Test Role-Mapping policy rules to determine which Roles will be output given the input details

Service:	[Policy Manager Admin Network Login Service]
Role Mapping Policy:	-
Authentication Source:	
Username:	
Test Date and Time:	

Table 187: *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

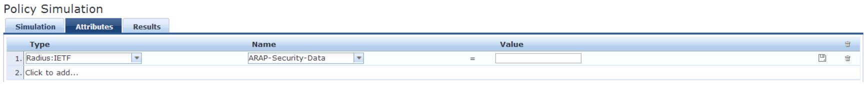
Table 187: *Role Mapping Simulation tab Parameters (Continued)*

Parameter	Description
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 ● 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 452

Attributes tab

Enter the attributes of the policy component to be tested.

Figure 312: *Role Mapping Simulation Attributes tab*


Policy Simulation

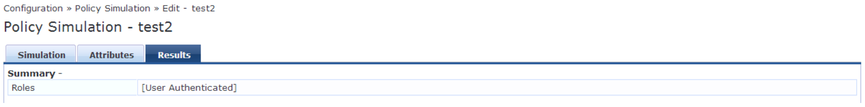
	Type	Name		Value
1.	Radius:IETF	ARAP-Security-Data	=	
2.	Click to add...			

Table 188: *Role Mapping Simulation Attributes tab Parameters*

Attribute	Parameter
Type:	
Host	See "Host Namespaces" on page 453
Authentication	See "Authentication Namespaces" on page 447
Connection	See "Connection Namespaces" on page 451
Application	See "Application Namespace" on page 446
Certificate	See "Certificate Namespaces" on page 450
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba	See "RADIUS Namespaces" on page 454
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 313: *Results tab*



Configuration » Policy Simulation » Edit - test2

Policy Simulation - test2

Summary -

Roles	[User Authenticated]

Table 189: *Role Mapping Results tab Parameters*

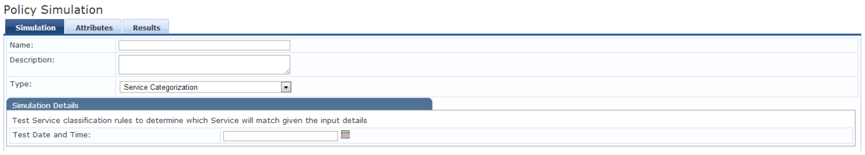
Parameter	Description
Summary -	Displays the results of the simulation.

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 314: *Service Categorization Simulation tab*



Name:

Description:

Type: Service Categorization

Simulation Details

Test Service classification rules to determine which Service will match given the input details

Test Date and Time:

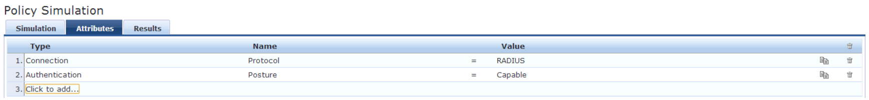
Table 190: *Service Categorization Simulation tab Parameter Description*

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 315: *Service Categorization Attributes tab*



	Type	Name		Value
1.	Connection	Protocol	=	RADIUS
2.	Authentication	Posture	=	Capable
3.	Click to add...			

Table 191: *Service Categorization Simulation Attributes tab Parameters*

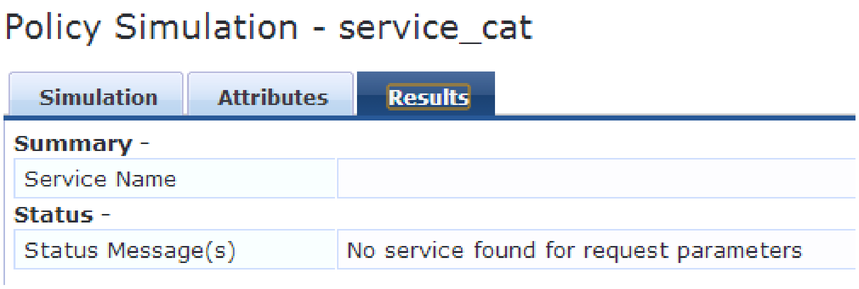
Attribute	Parameter
Type:	
Host	See "Host Namespaces" on page 453
Authentication	See "Authentication Namespaces" on page 447
Connection	See "Connection Namespaces" on page 451
Application	See "Application Namespace" on page 446
● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Aruba	See "RADIUS Namespaces" on page 454

Table 191: *Service Categorization Simulation Attributes tab Parameters (Continued)*

Attribute	Parameter
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 316: *Results tab*



Policy Simulation - service_cat

Summary -

Service Name	

Status -

Status Message(s)	No service found for request parameters

Table 192: *Service Configuration Results tab Parameters*

Parameter	Description
Summary -	Gives the name of the service.

Chapter 14
ClearPass Policy Manager Profile

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 311
- "Collectors" on page 311
- "Fingerprint Dictionaries" on page 316
- "Profiling" on page 314

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 312
- "ClearPass Onboard" on page 312
- "HTTP User-Agent" on page 312

- "MAC OUI" on page 312*
- "ActiveSync Plugin" on page 313
- "CPPM OnGuard" on page 313
- "SNMP" on page 313
- "Subnet Scan" on page 314

* 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.

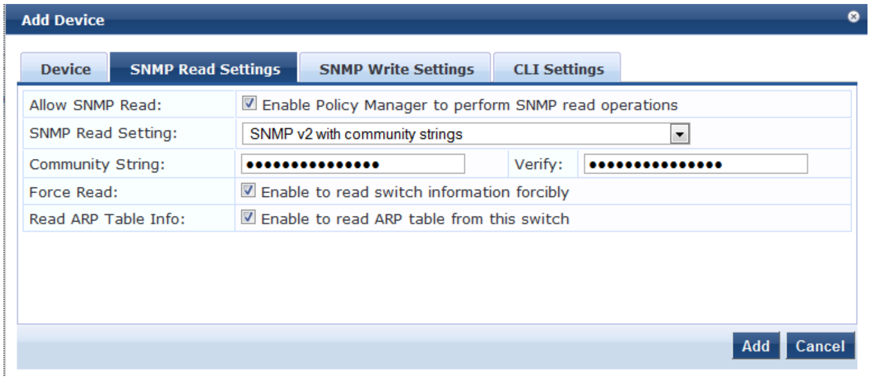
Note that the SNMP based mechanism is only capable of profiling devices if they respond to SNMP, or if the device advertises its capability via LLDP. When performing SNMP reads for a device, CPPM uses SNMP Read credentials configured in Network Devices, or defaults to using SNMP v2c with "public" community 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 317: *SNMP Read/Write Settings Tabs*



Allow SNMP Read:	☑ Enable Policy Manager to perform SNMP read operations
SNMP Read Setting:	SNMP v2 with community strings
Community String:	••••••••••••••• Verify: •••••••••••••••
Force Read:	☑ Enable to read switch information forcibly
Read ARP Table Info:	☑ Enable to read ARP table from this switch

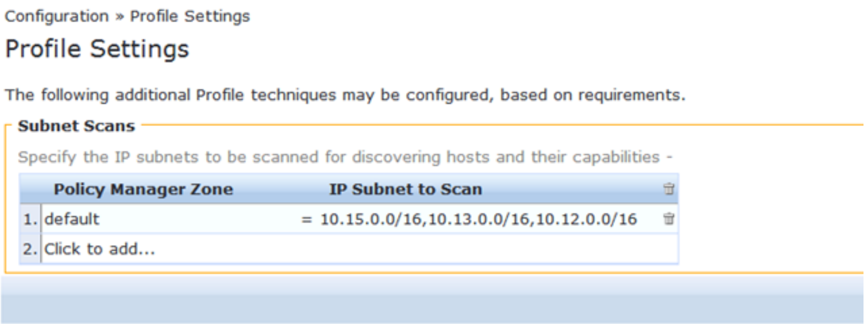
In large or geographically spread cluster deployments, you do not want all CPPM nodes to probe all SNMP configured devices. The default behavior is for a CPPM node in the cluster to read network device information only for devices configured to send traps to that CPPM node.

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 350.

Figure 318: *Subnet Scans page*



Configuration » Profile Settings

Profile Settings

The following additional Profile techniques may be configured, based on requirements.

Subnet Scans

Specify the IP subnets to be scanned for discovering hosts and their capabilities -

	Policy Manager Zone	IP Subnet to Scan
1.	default	= 10.15.0.0/16,10.13.0.0/16,10.12.0.0/16
2.	Click to add...	

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 315

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.

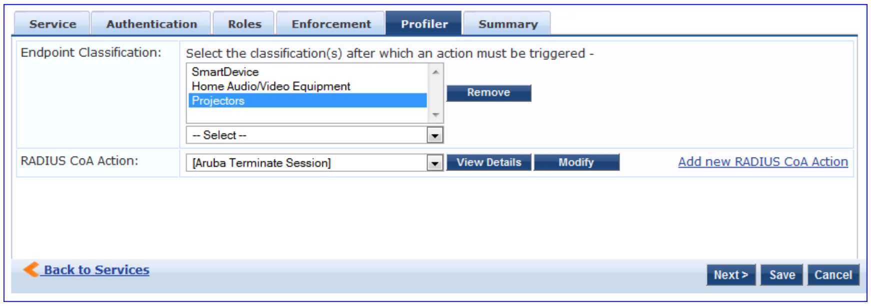
For more information, see:

- "Endpoint Profiler" on page 51
- "Policy Manager Dashboard" on page 29

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 319: *Profiler tab*



Endpoint Classification: Select the classification(s) after which an action must be triggered -

SmartDevice
Home Audio/Video Equipment
Projectors

RADIUS CoA Action: [Aruba Terminate Session]

Table 193: *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.

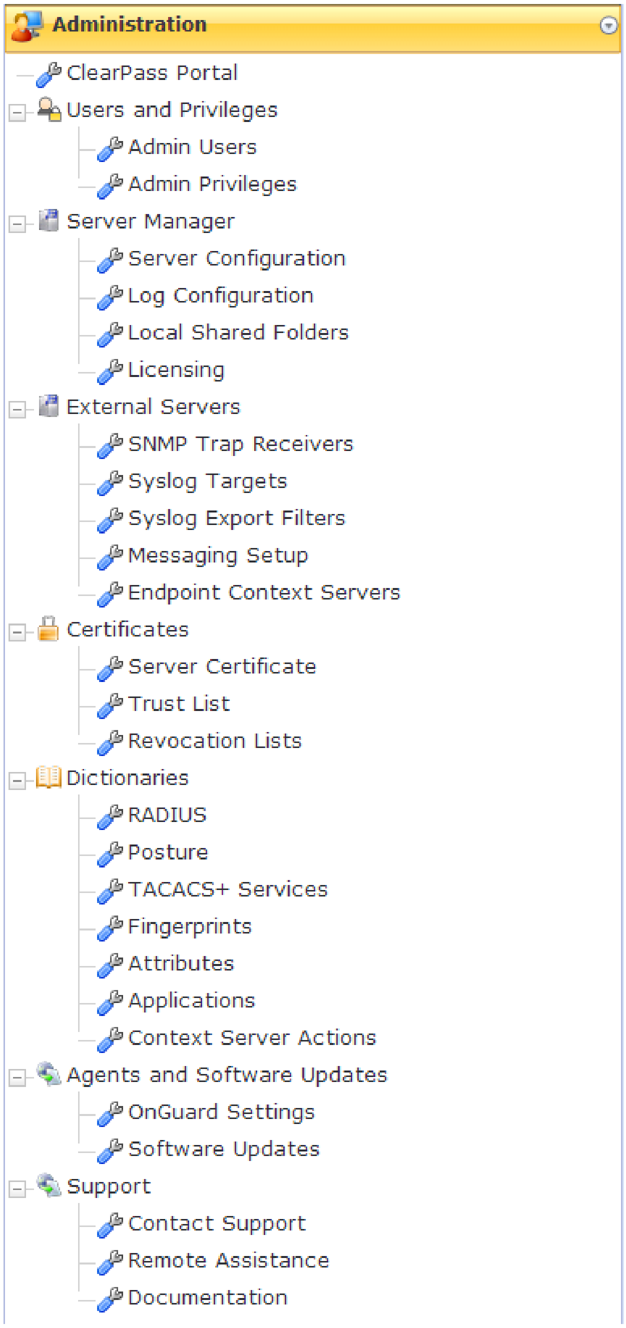
For more information, see "Fingerprints Dictionary" on page 402.

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 411.

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:



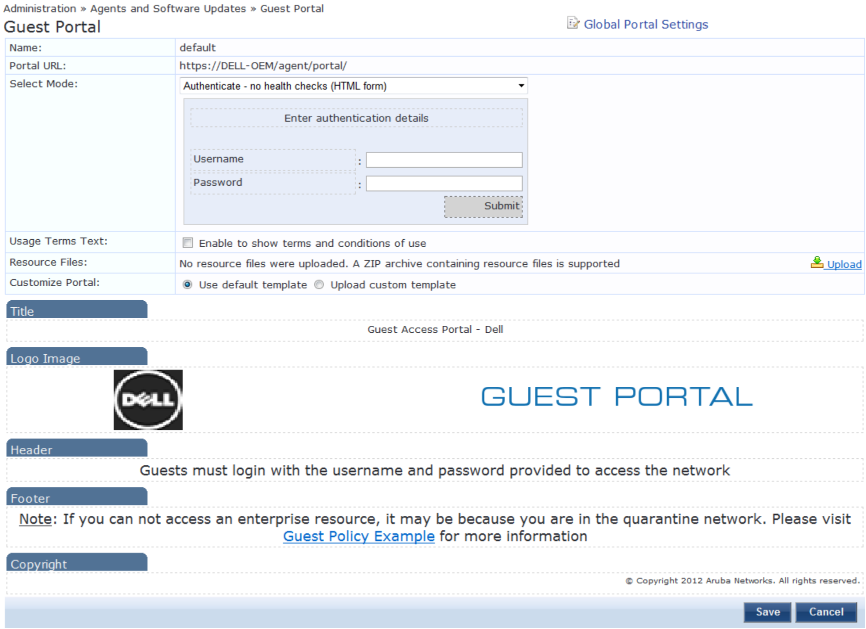
- "ClearPass Portal" on page 318
- "Admin Users" on page 319
- "Admin Privileges" on page 321
- "Server Configuration" on page 327
- "Log Configuration" on page 325
- "Local Shared Folders" on page 361
- "Licensing" on page 361
- "SNMP Trap Receivers" on page 364
- "Syslog Targets" on page 366
- "Syslog Export Filters" on page 368
- "Messaging Setup" on page 373
- "Endpoint Context Servers" on page 375
- "Server Certificate" on page 388
- "Certificate Trust List" on page 396
- "Revocation Lists" on page 397
- "RADIUS Dictionary" on page 398
- "Posture Dictionary" on page 400
- "TACACS+ Services Dictionary" on page 401
- "Fingerprints Dictionary" on page 402
- "Attributes Dictionary" on page 403
- "Applications Dictionary" on page 406
- "Endpoint Context Server Actions" on page 406
- "OnGuard Settings" on page 409
- "Software Updates" on page 411
- "Contact Support" on page 416
- "Remote Assistance" on page 416
- "Documentation" on page 418

ClearPass Portal

Navigate to the **Administration** > **Agents and Software Updates** > **ClearPass Portal** page.

Click on any of the editable sections of this page to customize the content for your enterprise:

Figure 320: *ClearPass Portal*



Administration » Agents and Software Updates » Guest Portal

Guest Portal

Name:	default
Portal URL:	https://DELL-OEM/agent/portal/
Select Mode:	Authenticate - no health checks (HTML form)
Usage Terms Text:	□ Enable to show terms and conditions of use
Resource Files:	No resource files were uploaded. A ZIP archive containing resource files is supported
Customize Portal:	● Use default template ○ Upload custom template

Guest Access Portal - Dell

Guests must login with the username and password provided to access the network

Note: If you can not access an enterprise resource, it may be because you are in the quarantine network. Please visit Guest Policy Example for more information

© Copyright 2012 Aruba Networks. All rights reserved.

Table 194: *ClearPass Portal parameters*

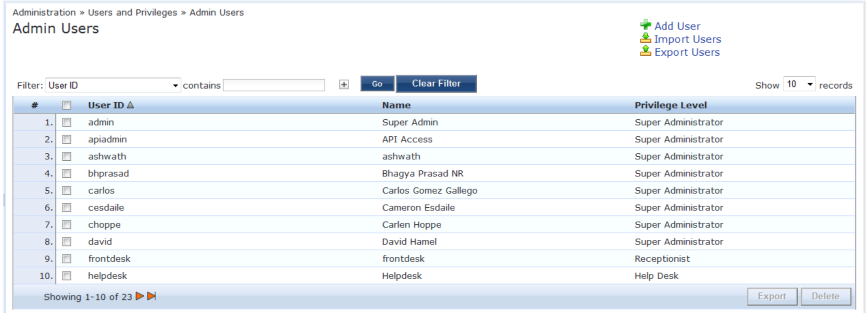
Parameter	Description
Select Option	Select the page that the user sees when first logging in to ClearPass: ● Default Landing Page ● Application Login Page: ■ ClearPass Policy Manager ■ ClearPass Guest ■ ClearPass Insight ■ ClearPass Onboard ● Guest Portal
Page Title	Click on the current title text to change the way the title appears.
Logo Image	Click on the logo image to browse and select an image for the banner.
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.

Admin Users

The Policy Manager Admin Users menu **Administration > Users and Privileges > Admin Users** provides the following interfaces for configuration:

- "Add User" on page 319
- "Import Users" on page 320
- "Export Users" on page 320
- "Export" on page 321

Figure 321: *Admin Users*



Administration » Users and Privileges » Admin Users

Admin Users

Add User
Import Users
Export Users

Filter: User ID contains Go Clear Filter Show 10 records

#	□	User ID	Name	Privilege Level
1.	□	admin	Super Admin	Super Administrator
2.	□	apiadmin	API Access	Super Administrator
3.	□	ashwath	ashwath	Super Administrator
4.	□	bhprasad	Bhagya Prasad NR	Super Administrator
5.	□	carlos	Carlos Gomez Gallego	Super Administrator
6.	□	cesdaile	Cameron Esdaile	Super Administrator
7.	□	choppe	Carlen Hoppe	Super Administrator
8.	□	david	David Hamel	Super Administrator
9.	□	frontdesk	frontdesk	Receptionist
10.	□	helpdesk	Helpdesk	Help Desk

Showing 1-10 of 23

Export Delete

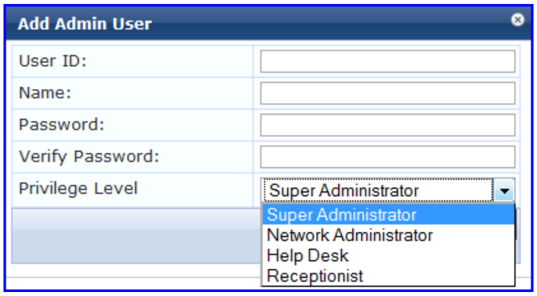
Table 195: *Admin Users*

Container	Description
Add User	Opens the **Add User** popup form.
Import Users	Opens the **Import Users** popup form.
Export Users	Exports all users to an XML file.
Export	Exports a selected to an XML file.
Delete	Deletes a selected User.

Add User

Select the **Add User** link in the upper right portion of the page.

Figure 322: *Add Admin User*



Add Admin User

User ID:	
Name:	
Password:	
Verify Password:	
Privilege Level	Super Administrator

Table 196: *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 Users** link in the upper right portion of the page.

Figure 323: *Import (Admin) Users*

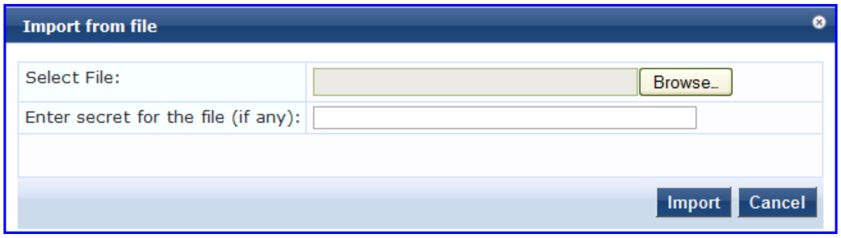


Table 197: *Import (Admin) Users*

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 Users** 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

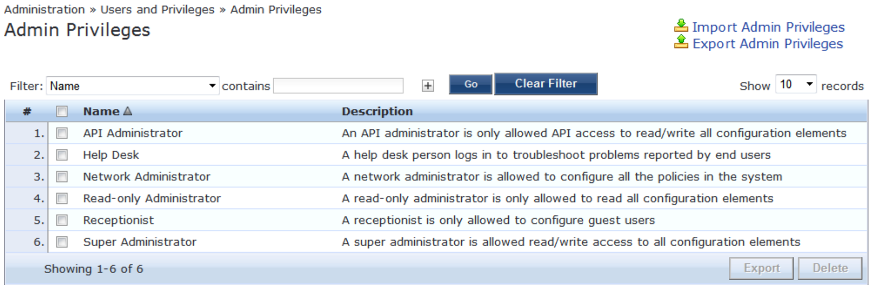
Select the **Export** button on the lower right portion of the page.

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 324: *Admin Privileges*



Administration » Users and Privileges » Admin Privileges

Admin Privileges

#	□	Name ▲	Description
1.	□	API Administrator	An API administrator is only allowed API access to read/write all configuration elements
2.	□	Help Desk	A help desk person logs in to troubleshoot problems reported by end users
3.	□	Network Administrator	A network administrator is allowed to configure all the policies in the system
4.	□	Read-only Administrator	A read-only administrator is only allowed to read all configuration elements
5.	□	Receptionist	A receptionist is only allowed to configure guest users
6.	□	Super Administrator	A super administrator is allowed read/write access to all configuration elements

Showing 1-6 of 6

See "Custom Admin Privileges" on page 289 to create additional administrator privileges and "Exporting" on page 22 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 list provides the areas and sub-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.

- Dashboard: `taskId="dnd"`
- Monitoring: `taskId="mon"`
  - Live Monitoring: `taskId="mon.li"`
    - Access Tracker: `taskId="mon.li.ad"`
    - Accounting: `taskId="mon.li.ac"`
    - Onguard Activity: `taskId="mon.li.ag"`
    - Analysis and Trending `taskId="mon.li.sp"`
    - Endpoint Profiles: `taskId="mon.li.ep"`
    - System Monitor: `taskId="mon.li.sy"`
  - Audit Viewer: `taskId="mon.av"`
  - Event Viewer: `taskId="mon.ev"`
  - Data Filters: `taskId="mon.df"`
- Configuration: `taskId="con"`
  - Start Here (Services Wizard): taskId="con.sh"
  - Services: `taskId="con.se"`
  - Service Templates: `taskId=”con.st”`
  - Authentication: `taskId="con.au"`
    - Methods: `taskId="con.au.am"`
    - Sources: `taskId="con.au.as"`
  - Identity: `taskId="con.id"`
    - Single Sign-On: `taskId=”con.id.sso”`
    - Local Users: `taskId="con.id.lu"`
    - Guest Users: `taskId="con.id.gu"`
    - Onboard Devices: `taskId="con.id.od"`
    - Endpoints: `taskId="con.id.ep"`
    - Static Host Lists: `taskId="con.id.sh"`
    - Roles: `taskId="con.id.rs"`
    - Role Mappings: `taskId="con.id.rm"`
  - Posture: `taskId="con.pv"`
    - Posture Policies: `taskId="con.pv.in`
    - Posture Servers: `taskId="con.pv.ex"`
    - Audit Servers: `taskId="con.pv.au"`
  - Enforcements: `taskId="con.en"`
    - Policies: `taskId="con.en.epo"`
    - Profiles: `taskId="con.en.epr"`
  - Network: `taskID="con.nw"`
    - Devices: `taskId="con.nw.nd"`

        - Device Groups: `taskId="con.nw.ng"`
        - Proxy Targets: `taskId="con.nw.pr"`
    - Policy Simulation: `taskId="con.ps"`
    - Profile Settings: `taskId="con.prs"`
- Administration: `taskId="adm"`
    - User and Privileges: `taskId="adm.us"`
        - Admin Users: `taskId="adm.us.au"`
        - Admin Privileges: `taskId="adm.us.ap"`
    - Server Manager: `taskId="adm.mg"`
        - Server Configuration: `taskId="adm.mg.sc"`
        - Log Configuration: `taskId="adm.mg.ls"`
        - Local Shared Folders: `taskId="adm.mg.sf"`
        - Licensing: `taskId="adm.mg.sf"`
    - External Servers: `taskId="adm.xs"`
        - SNMP Trap Receivers: `taskId="adm.xs.st"`
        - Syslog Targets: `taskId="adm.xs.es"`
        - Syslog Export Filters: `taskId="adm.xs.sx"`
        - Messaging Setup: `taskId="adm.xs.me"`
    - Certificates: `taskId="adm.cm"`
        - Server Certificate: `taskId="adm.cm.mc"`
        - Trust List: `taskId="adm.cm.ctl"`
        - Revocation List: `taskId="adm.cm.crl"`
    - Dictionaries: `taskId="adm.di"`
        - RADIUS: `taskId="adm.di.rd"`
        - Posture: `taskId="adm.di.pd"`
        - TACACS+ Services: `taskId="adm.di.td"`
        - Fingerprints: `taskId="adm.di.df"`
        - Attributes: `taskId="adm.di.at"`
        - Applications: `taskid=”adm.di.ad”`
    - Agents and Software Updates: `taskId="adm.po"`
        - Onguard Settings: `taskId="adm.po.aas"`
        - Guest Portal: `taskId="adm.po.gp"`
        - Software Updates: `taskId="adm.po.es"`

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 321
- "Administrator Privileges and IDs" on page 322
- "Sample Administrator Privilege XML File" on page 324

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 o
nly 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" descripti
on="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">
```

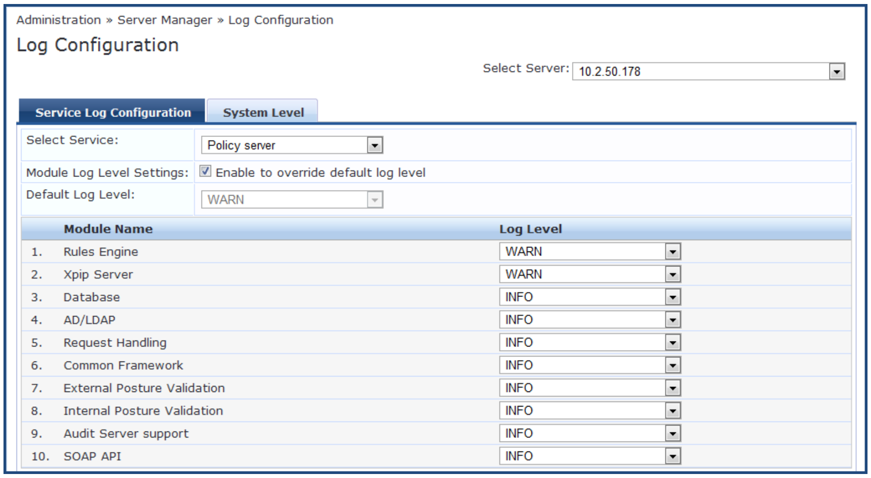
```
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Limited access permission" description="A read-only administrator is
only allowed to read all configuration elements">
      <AdminTask taskid="dnd"> //Refers to DashBoard
        <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 325: *Log Configuration (Service Log Configuration tab)*



Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 10.2.50.178

Select Service: Policy server

Module Log Level Settings: ☑ Enable to override default log level

Default Log Level: WARN

	Module Name	Log Level
1.	Rules Engine	WARN
2.	Xpip Server	WARN
3.	Database	INFO
4.	AD/LDAP	INFO
5.	Request Handling	INFO
6.	Common Framework	INFO
7.	External Posture Validation	INFO
8.	Internal Posture Validation	INFO
9.	Audit Server support	INFO
10.	SOAP API	INFO

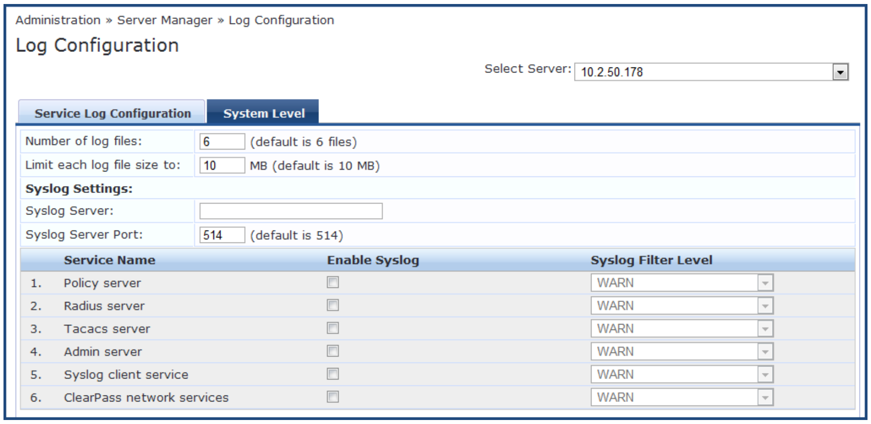
Table 198: *Log Configuration Service Log Configuration tab Parameters*

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.

Table 198: *Log Configuration Service Log Configuration tab Parameters (Continued)*

Parameter	Description
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 326: *Log Configuration System Level tab*



Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 10.2.50.178

Number of log files: 6 (default is 6 files)

Limit each log file size to: 10 MB (default is 10 MB)

Syslog Settings:

Syslog Server:

Syslog Server Port: 514 (default is 514)

	Service Name	Enable Syslog	Syslog Filter Level
1.	Policy server	□	WARN
2.	Radius server	□	WARN
3.	Tacacs server	□	WARN
4.	Admin server	□	WARN
5.	Syslog client service	□	WARN
6.	ClearPass network services	□	WARN

Table 199: *Log Configuration System Level tab Parameters*

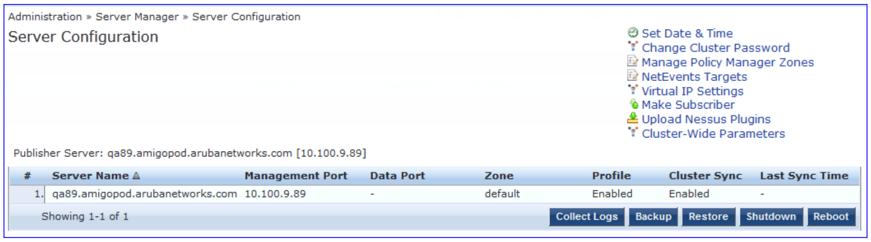
Parameter	Description
Select Server	Specify the server for which to configure logs.
Number of log files	Specify the number of log files of a specific module to keep at any given time. When a log file reaches the specified size (see below), Policy Manager rolls the log over to another file until the specified 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 328
- "Set Date & Time" on page 347
- "Change Cluster Password" on page 349
- "Manage Policy Manager Zones" on page 350
- "NetEvents Targets" on page 351
- "Virtual IP Settings" on page 351
- "Make Subscriber" on page 352
- "Upload Nessus Plugins" on page 353
- "Cluster-Wide Parameters" on page 353
- "Collect Logs" on page 357
- "Backup" on page 358
- "Restore" on page 359
- "Shutdown/Reboot" on page 361
- "Drop Subscriber" on page 361

Figure 327: *Server Configuration Page*



Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: qa89.amigopod.arubanetworks.com [10.100.9.89]

#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	qa89.amigopod.arubanetworks.com	10.100.9.89	-	default	Enabled	Enabled	-

Showing 1-1 of 1

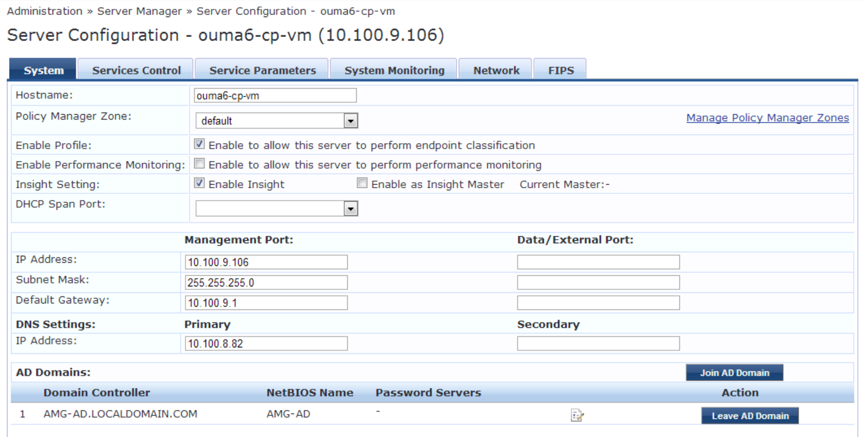
Editing Server Configuration Settings

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 328
- "Services Control Tab" on page 332
- "Service Parameters Tab" on page 333
- "System Monitoring Tab " on page 343
- "Network Tab" on page 345

Figure 328: *Editing Server Configuration*



Administration » Server Manager » Server Configuration - ouma6-cp-vm

Server Configuration - ouma6-cp-vm (10.100.9.106)

Hostname:	ouma6-cp-vm	
Policy Manager Zone:	default	Manage Policy Manager Zones
Enable Profile:	☑ Enable to allow this server to perform endpoint classification	
Enable Performance Monitoring:	☐ Enable to allow this server to perform performance monitoring	
Insight Setting:	☑ Enable Insight	☐ Enable as Insight Master Current Master:-
DHCP Span Port:		

	Management Port:	Data/External Port:
IP Address:	10.100.9.106	
Subnet Mask:	255.255.255.0	
Default Gateway:	10.100.9.1	
DNS Settings:	**Primary**	**Secondary**
IP Address:	10.100.8.82	

AD Domains:

	Domain Controller	NetBIOS Name	Password Servers		Action
1	AMG-AD.LOCALDOMAIN.COM	AMG-AD	-		Leave AD Domain

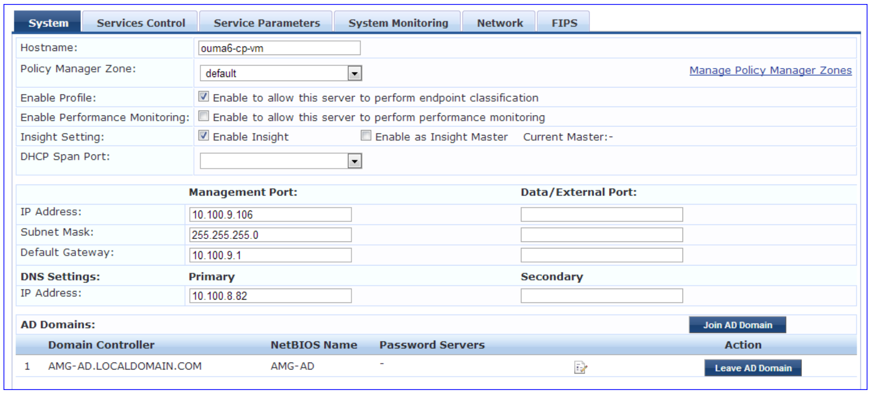
System Tab

The Server Configuration form 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 350
- "Join AD Domain" on page 330
- "Add Password Server" on page 332 (for joined AD domains)

Figure 329: *System Tab*



Hostname: ouma6-cp-vm

Policy Manager Zone: default

Enable Profile: ☑ Enable to allow this server to perform endpoint classification

Enable Performance Monitoring: □ Enable to allow this server to perform performance monitoring

Insight Setting: ☑ Enable Insight □ Enable as Insight Master Current Master:-

DHCP Span Port:

	Management Port:	Data/External Port:
IP Address:	10.100.9.106	
Subnet Mask:	255.255.255.0	
Default Gateway:	10.100.9.1	
DNS Settings:	**Primary**	**Secondary**
IP Address:	10.100.8.82	

AD Domains:

	Domain Controller	NetBIOS Name	Password Servers	Action
1	AMG-AD.LOCALDOMAIN.COM	AMG-AD	-	Leave AD Domain

Table 200: *Server Configuration System tab*

Parameter	Description
Hostname	Hostname of Policy Manager appliance. It is not necessary to enter the fully qualified domain name here.
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 from within this page.
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 admin enables the checkbox for Insight on a node in cluster, Admin will automatically update the [Insight Repository] configuration to point to the management IP of that server. ● When enabling the checkbox for other servers in the cluster, they will be added as backups for the same auth source. ● The order of the primary and backup servers in the [Insight Repository] is the 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 is also the Insight Master. **NOTE:** This option is only available if **Enable Insight** is selected.
DHCP Span Port	If desired, specify the port number for DHCP spanning.
Management Port: IP Address	Management interface IP address. You access the Policy Manager UI via the management interface.
Management Port: Subnet Mask	Management interface Subnet Mask

Table 200: *Server Configuration System tab (Continued)*

Parameter	Description
Management Port: Default Gateway	Default gateway for management interface
Data/External Port: IP Address	Data interface IP address. All authentication and authorization requests arrive on the data interface.
Data/External Port: Subnet Mask	Data interface Subnet Mask
Data/External Port: Default Gateway	Default gateway for data interface
DNS: Primary DNS	Primary DNS for name lookup
DNS: Secondary DNS	Secondary DNS for name lookup
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 330 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 332 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.

NOTE

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.

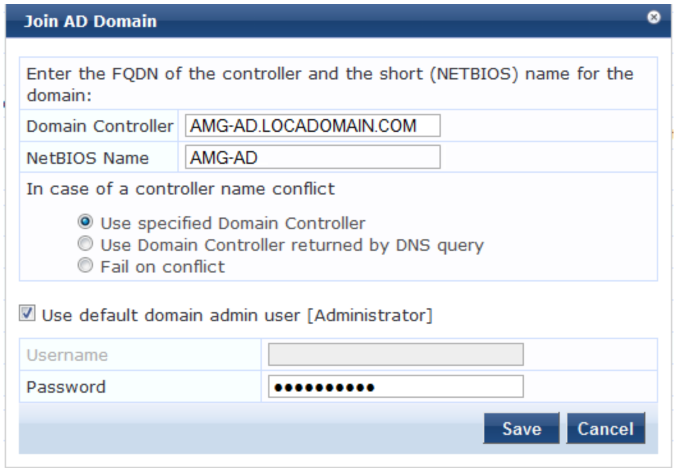
Join Domain - Click on this button to join this Policy Manager appliance to an Active Directory domain. Password servers can be configured after Policy Manager is successfully joined. Refer to "Add Password Server" on page 332 for more information.

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.

NOTE

For most use cases, if you have multiple nodes in the cluster, you must join each node to the same Active Directory domain.

Figure 330: *Join AD Domain*



Join AD Domain

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller	AMG-AD.LOCADOMAIN.COM
NetBIOS Name	AMG-AD

In case of a controller name conflict

● Use specified Domain Controller
○ Use Domain Controller returned by DNS query
○ Fail on conflict

☑ Use default domain admin user [Administrator]

Username	
Password	●●●●●●●●●●●

Table 201: *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.

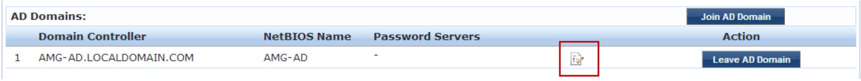
Add Password Server

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 331.)

Figure 331: *Add Password Server icon*



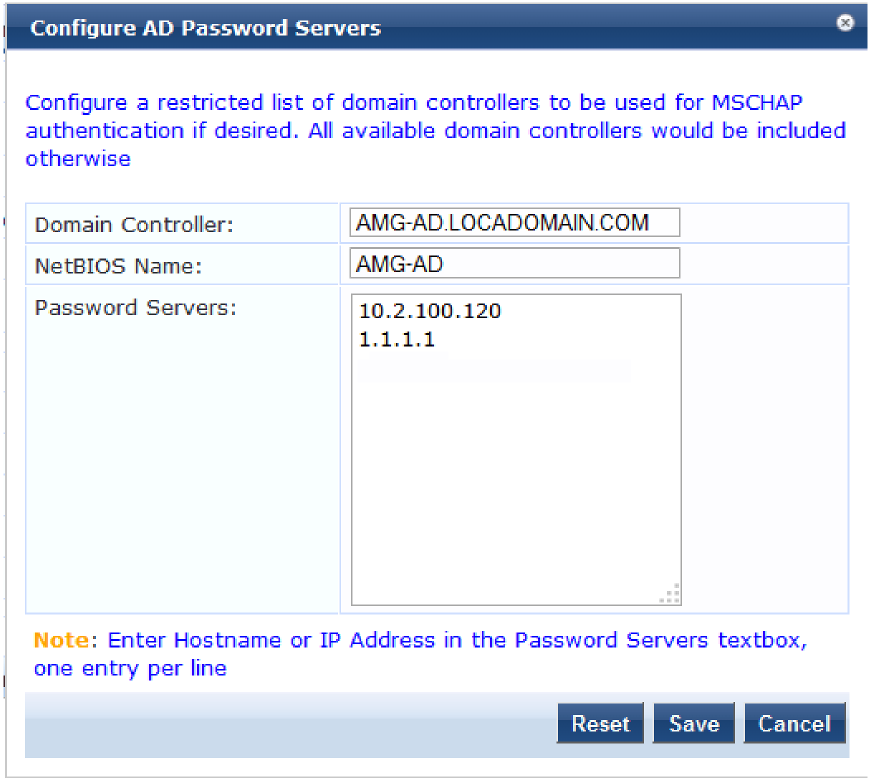
AD Domains:

Join AD Domain

	Domain Controller	NetBIOS Name	Password Servers		Action
1	AMG-AD.LOCALDOMAIN.COM	AMG-AD	-		Leave AD Domain

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 332: *Configure AD Password Servers*



Configure AD Password Servers

Configure a restricted list of domain controllers to be used for MSCHAP authentication if desired. All available domain controllers would be included otherwise

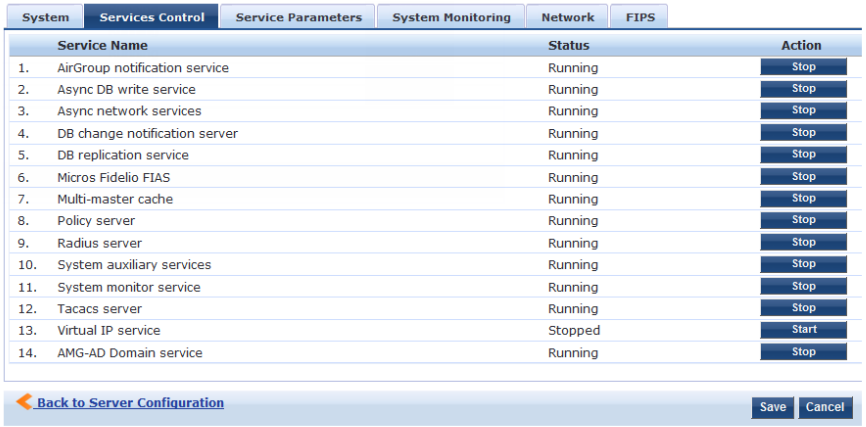
Domain Controller:	AMG-AD.LOCADOMAIN.COM
NetBIOS Name:	AMG-AD
Password Servers:	10.2.100.120 1.1.1.1

Note: Enter Hostname or IP Address in the Password Servers textbox, one entry per line

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 333: *Services Control Tab*



	Service Name	Status	Action
1.	AirGroup notification service	Running	Stop
2.	Async DB write service	Running	Stop
3.	Async network services	Running	Stop
4.	DB change notification server	Running	Stop
5.	DB replication service	Running	Stop
6.	Micros Fidelio FIAS	Running	Stop
7.	Multi-master cache	Running	Stop
8.	Policy server	Running	Stop
9.	Radius server	Running	Stop
10.	System auxiliary services	Running	Stop
11.	System monitor service	Running	Stop
12.	Tacacs server	Running	Stop
13.	Virtual IP service	Stopped	Start
14.	AMG-AD Domain service	Running	Stop

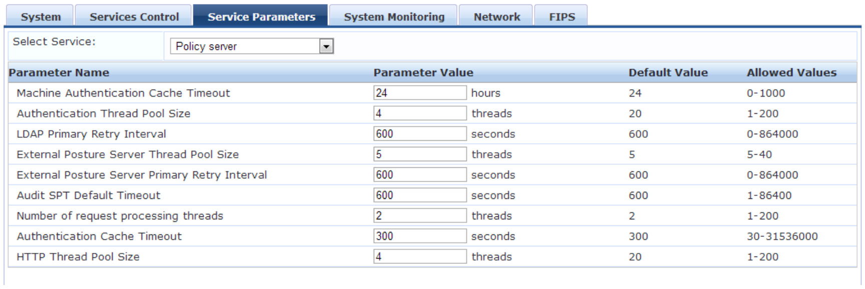
Service Parameters Tab

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 333
- "ClearPass Network Services Options" on page 334
- "ClearPass System Services Options" on page 336
- "Policy Server Options" on page 338
- "Radius Server Options" on page 339
- "Stats Collection Service Options" on page 342
- "System Monitor Service Options" on page 342
- "Tacacs Server Options" on page 343

Figure 334: *Service Parameters tab - Policy server example*



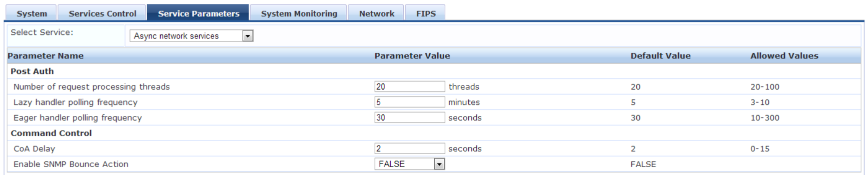
Select Service: Policy server

Parameter Name	Parameter Value		Default Value	Allowed Values
Machine Authentication Cache Timeout	24	hours	24	0-1000
Authentication Thread Pool Size	4	threads	20	1-200
LDAP Primary Retry Interval	600	seconds	600	0-864000
External Posture Server Thread Pool Size	5	threads	5	5-40
External Posture Server Primary Retry Interval	600	seconds	600	0-864000
Audit SPT Default Timeout	600	seconds	600	1-86400
Number of request processing threads	2	threads	2	1-200
Authentication Cache Timeout	300	seconds	300	30-31536000
HTTP Thread Pool Size	4	threads	20	1-200

Async Network Services Options

Configure the Post-Auth and Command Control parameters for the Async network service on this page.

Figure 335: *Async Network Services*



Select Service: Async network services

Parameter Name	Parameter Value		Default Value	Allowed Values
Post Auth				
Number of request processing threads	20	threads	20	20-100
Lazy handler polling frequency	5	minutes	5	3-10
Eager handler polling frequency	30	seconds	30	10-300
Command Control				
CoA Delay	2	seconds	2	0-15
Enable SNMP Bounce Action	FALSE		FALSE	

Table 202: *Service Parameters tab - Async Network Services*

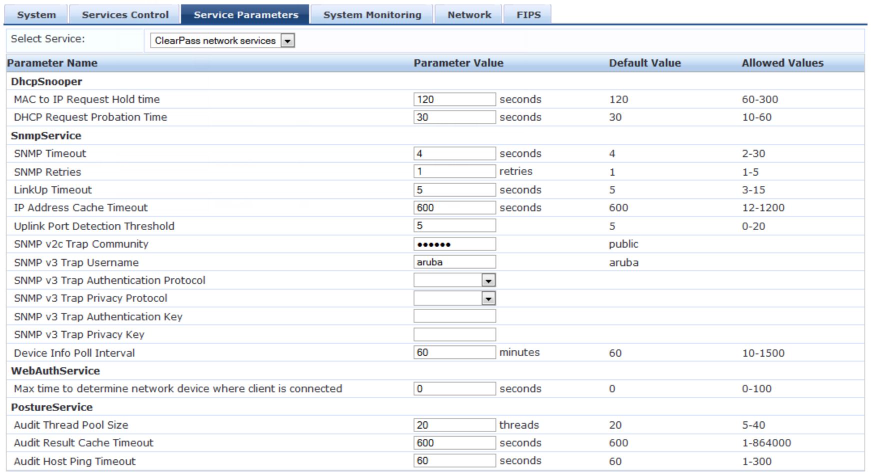
Parameter	Description
Post Auth	
Number of request processing threads	Set the number of request processing threads. The default value is 20 threads, and the allowed values are between 20 and 100.
Lazy handler polling frequency	Set the Lazy handler polling frequency. The frequency is configured in minutes. 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

Figure 336: *ClearPass Network Services Parameters*



Select Service: ClearPass network services

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

Table 203: *Service Parameters - ClearPass network services*

Service Parameters	Description
DhcpSnooper	
MAC to IP Request Hold time	Number of seconds to wait before responding to a query to get IP address corresponding to a MAC address. Any DHCP message received in this time period will refresh the MAC to IP binding. Typically, audit service will request 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	Number of seconds to wait before considering the MAC to IP binding received in a DHCPREQUEST message as final. This wait would handle 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	Seconds to wait for an SNMP response from the network device.
SNMP Retries	Number of retries for SNMP requests.
LinkUp Timeout	Seconds to wait before processing link-up traps. If a MAC notification trap arrives in this time, SNMP service will not try to poll the switch for MAC addresses behind a port for link-up processing.
IP Address Cache Timeout	Duration in seconds for which MAC to IP lookup response is cached.
Uplink Port Detection Threshold	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	Community string that must be checked in all incoming SNMP v2 traps.
SNMP v3 Trap Username	SNMP v3 Username to be used for all incoming traps.
SNMP v3 Trap Authentication Protocol	SNMP v3 Authentication protocol for traps. Must be one of MD5, SHA or empty (to disable authentication).
SNMP v3 Trap Privacy Protocol	SNMP v3 Privacy protocol for traps. Must be one of DES_CBC, AES_128 or empty (to disable privacy).

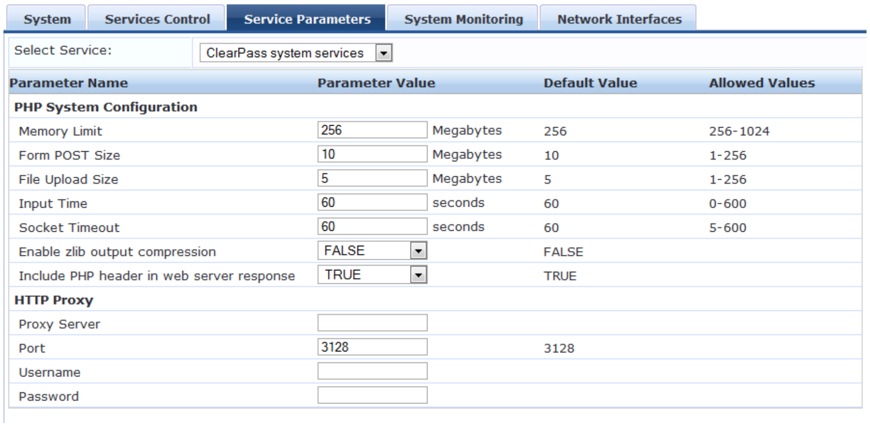
Table 203: *Service Parameters - ClearPass network services (Continued)*

Service Parameters	Description
SNMP v3 Trap Authentication Key	SNMP v3 authentication key and privacy key for incoming traps.
SNMP v3 Trap Privacy Key	
Device Info Poll Interval	This specifics the time (in minutes) between polling for device information.
WebAuthService	**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	This specifies the number of threads to use for connections to audit servers.
Audit Result Cache Timeout	This specifies the time (in seconds) for which audit result entries are cached by Policy Manager.
Audit Host Ping Timeout	This 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 337: *ClearPass System Services Parameters (partial view)*



Select Service: ClearPass system services

Parameter Name	Parameter Value		Default Value	Allowed Values
PHP System Configuration				
Memory Limit	256	Megabytes	256	256-1024
Form POST Size	10	Megabytes	10	1-256
File Upload Size	5	Megabytes	5	1-256
Input Time	60	seconds	60	0-600
Socket Timeout	60	seconds	60	5-600
Enable zlib output compression	FALSE		FALSE	
Include PHP header in web server response	TRUE		TRUE	
HTTP Proxy				
Proxy Server				
Port	3128		3128	
Username				
Password				

Table 204: *Service Parameters - ClearPass system services*

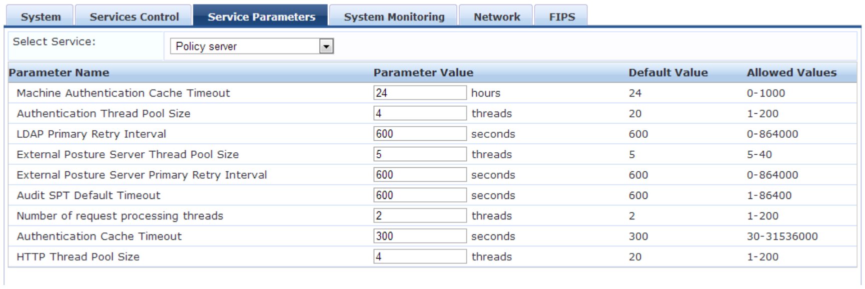
Service Parameter	Description
PHP System Configuration	
Memory Limit	Maximum memory that can be used by the PHP applications.
Form POST Size	Maximum HTTP POST content size that can be sent to the PHP application.
File Upload Size	Maximum file size that can be uploaded into the PHP application.
Input 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	
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	

Table 204: *Service Parameters - ClearPass system services (Continued)*

Service Parameter	Description
Maximum connections	Specify a number between 300 and 1500 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.

Policy Server Options

Figure 338: *Policy Server Service Parameters*



Select Service: Policy server

Parameter Name	Parameter Value		Default Value	Allowed Values
Machine Authentication Cache Timeout	24	hours	24	0-1000
Authentication Thread Pool Size	4	threads	20	1-200
LDAP Primary Retry Interval	600	seconds	600	0-864000
External Posture Server Thread Pool Size	5	threads	5	5-40
External Posture Server Primary Retry Interval	600	seconds	600	0-864000
Audit SPT Default Timeout	600	seconds	600	1-86400
Number of request processing threads	2	threads	2	1-200
Authentication Cache Timeout	300	seconds	300	30-31536000
HTTP Thread Pool Size	4	threads	20	1-200

Table 205: *Service Parameters tab - Policy Server service*

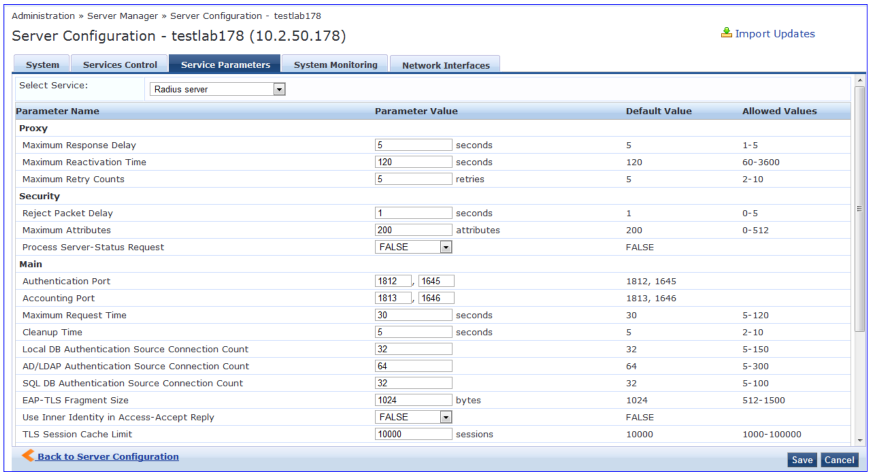
Service Parameter	Description
Machine Authentication Cache Timeout	This specifies the time (in hours) for which machine authentication entries are cached by Policy Manager.
Authentication Thread Pool Size	This specifies the number of threads to use for LDAP/AD and SQL connections.
LDAP Primary Retry 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 205: *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 339: *RADIUS Server Service Parameters*



Administration » Server Manager » Server Configuration - testlab178

Server Configuration - testlab178 (10.2.50.178)

Select Service: Radius server

Parameter Name	Parameter Value		Default Value	Allowed Values
Proxy				
Maximum Response Delay	5	seconds	5	1-5
Maximum Reactivation Time	120	seconds	120	60-3600
Maximum Retry Counts	5	retries	5	2-10
Security				
Reject Packet Delay	1	seconds	1	0-5
Maximum Attributes	200	attributes	200	0-512
Process Server-Status Request	FALSE		FALSE	
Main				
Authentication Port	1812, 1645		1812, 1645	
Accounting Port	1813, 1646		1813, 1646	
Maximum Request Time	30	seconds	30	5-120
Cleanup Time	5	seconds	5	2-10
Local DB Authentication Source Connection Count	32		32	5-150
AD/LDAP Authentication Source Connection Count	64		64	5-300
SQL DB Authentication Source Connection Count	32		32	5-100
EAP-TLS Fragment Size	1024	bytes	1024	512-1500
Use Inner Identity in Access-Accept Reply	FALSE		FALSE	
TLS Session Cache Limit	10000	sessions	10000	1000-100000

Table 206: *Service Parameters tab - Radius Server Service*

Service Parameter	Description
Proxy	

Table 206: *Service Parameters tab - Radius Server Service (Continued)*

Service Parameter	Description
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 Counts	Maximum number of times to retry a proxy request if the target server doesn't respond.
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.

Table 206: *Service Parameters tab - Radius Server Service (Continued)*

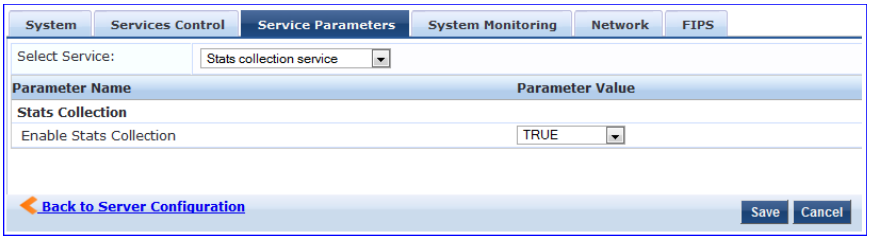
Service Parameter	Description
AD/LDAP Authentication Source Connection Count	Maximum number of AD/LDAP connections opened.
SQL DB Authentication Source Connection Count	Maximum number of SQL DB.
EAP - TLS Fragment Size	Maximum size of the EAP-TLS fragment size.
Use Inner Identity in Access-Accept Reply	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	

Table 206: *Service Parameters tab - Radius Server Service (Continued)*

Service Parameter	Description
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.
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 340: *Stats Collection Service Parameters*



Select Service: Stats collection service

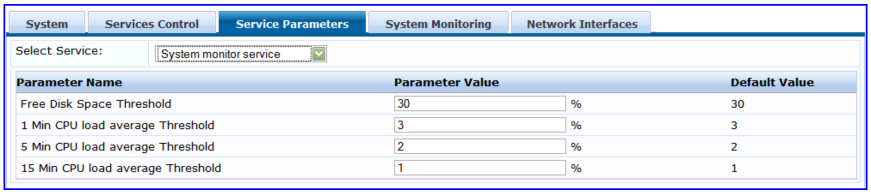
Parameter Name	Parameter Value
Stats Collection	
Enable Stats Collection	TRUE

Table 207: *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 341: *System Monitor Service Parameters*



Select Service: System monitor service

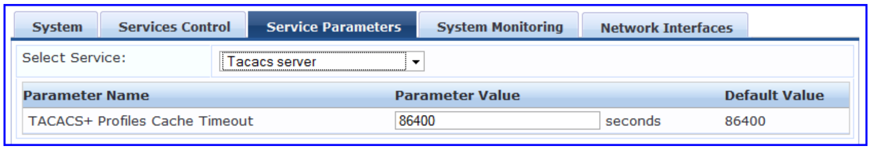
Parameter Name	Parameter Value		Default Value
Free Disk Space Threshold	30	%	30
1 Min CPU load average Threshold	3	%	3
5 Min CPU load average Threshold	2	%	2
15 Min CPU load average Threshold	1	%	1

Table 208: *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 342: *TACACS+ Service Parameters*



Select Service: Tacacs server

Parameter Name	Parameter Value		Default Value
TACACS+ Profiles Cache Timeout	86400	seconds	86400

Table 209: *Service Parameters tab - TACACS server*

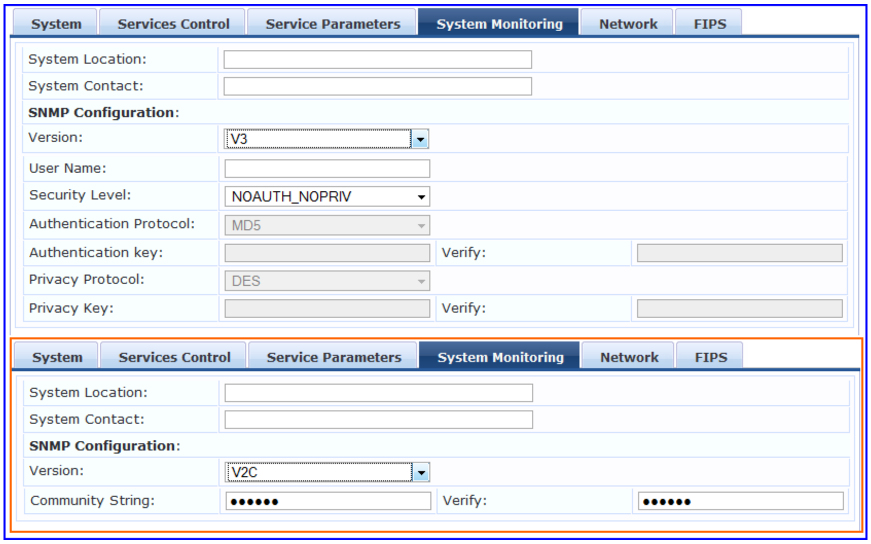
Service Parameter	Description
TACACS+ Profiles Cache Timeout	This specifies the time (in seconds) for which TACACS+ profile result entries are cached by Policy Manager

System Monitoring Tab

Navigate to the **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 on this page vary based on the SNMP version that you select.

Figure 343: *System Monitoring Tab*



System Location:			
System Contact:			
SNMP Configuration:			
Version:	V3		
User Name:			
Security Level:	NOAUTH_NOPRIV		
Authentication Protocol:	MD5		
Authentication key:		Verify:	
Privacy Protocol:	DES		
Privacy Key:		Verify:	

System Location:			
System Contact:			
SNMP Configuration:			
Version:	V2C		
Community String:	••••••	Verify:	••••••

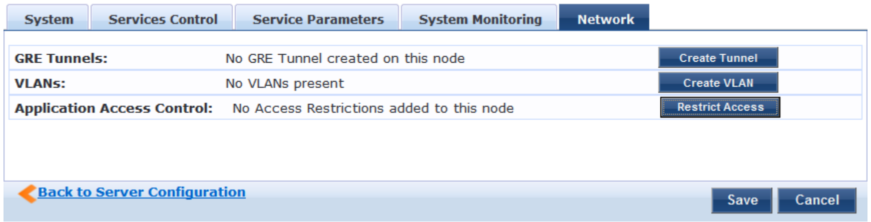
Table 210: *System Monitoring tab details*

Parameter	Description
System Location/System Contact:	Policy Manager appliance location and contact information.
SNMP Configuration: Version:	V1, V2C or V3.
SNMP Configuration: Community String:	Read community string.
SNMP Configuration: SNMP v3: Username:	Username to use for SNMP v3 communication.
SNMP Configuration: SNMP v3: Security Level:	One of NOAUTH_NOPRIV (no authentication or privacy), AUTH_NOPRIV (authenticate, but no privacy), or AUTH _PRIV (authenticate and keep the communication private).
SNMP Configuration: SNMP v3: Authentication Protocol:	Authentication protocol (MD5 or SHA) and key.
SNMP Configuration: SNMP v3: Authentication key:	
SNMP Configuration: SNMP v3: Privacy Protocol:	Privacy protocol (DES or AES) and key.
SNMP Configuration: SNMP v3: Privacy Key:	

Network Tab

Navigate to the **Network** tab to create GRE tunnels and VLANs related to guest users and to control what applications have access to the node.

Figure 344: *Network Interfaces Tab*



GRE Tunnels:	No GRE Tunnel created on this node	Create Tunnel
VLANs:	No VLANs present	Create VLAN
Application Access Control:	No Access Restrictions added to this node	Restrict Access

Creating GRE tunnels

The administrator can create a generic routing encapsulation (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 345: *Create Tunnel page*

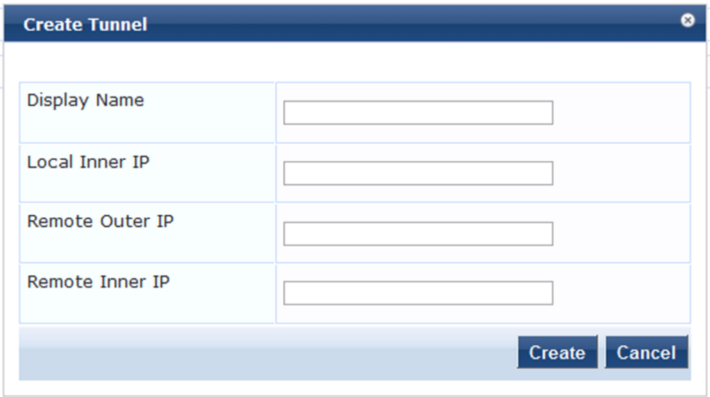


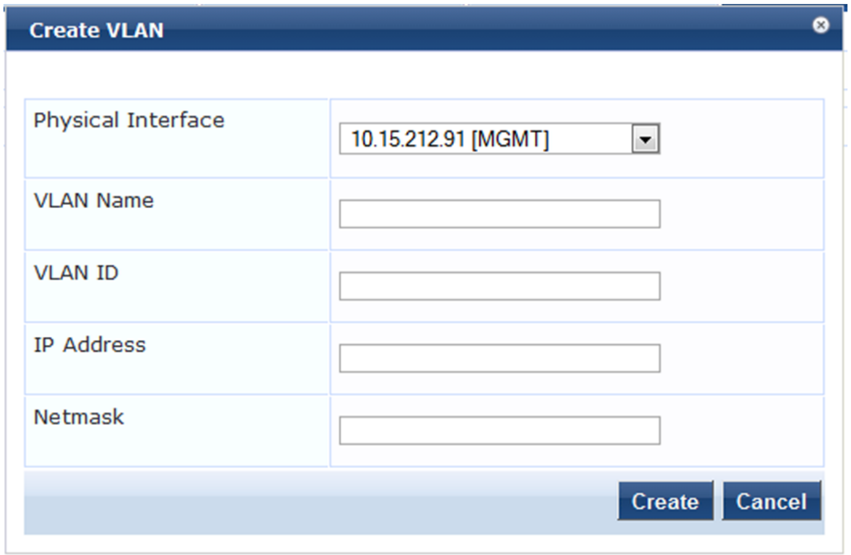
Table 211: *Create Tunnel Page Parameters*

Parameter	Description
Display Name	Optional 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 346: *Creating VLAN Page*



Create VLAN

Physical Interface	10.15.212.91 [MGMT]
VLAN Name	
VLAN ID	
IP Address	
Netmask	

Table 212: *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 347: *Restrict Access dialog box*

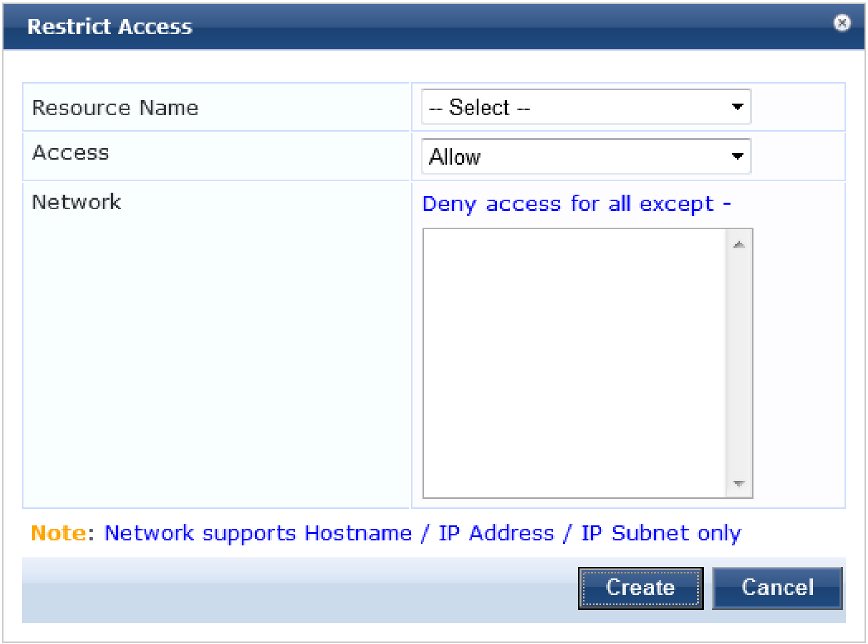

Restrict Access
Resource Name
-- Select --
Access
Allow
Network
Deny access for all except -
Note: Network supports Hostname / IP Address / IP Subnet only
Create
Cancel

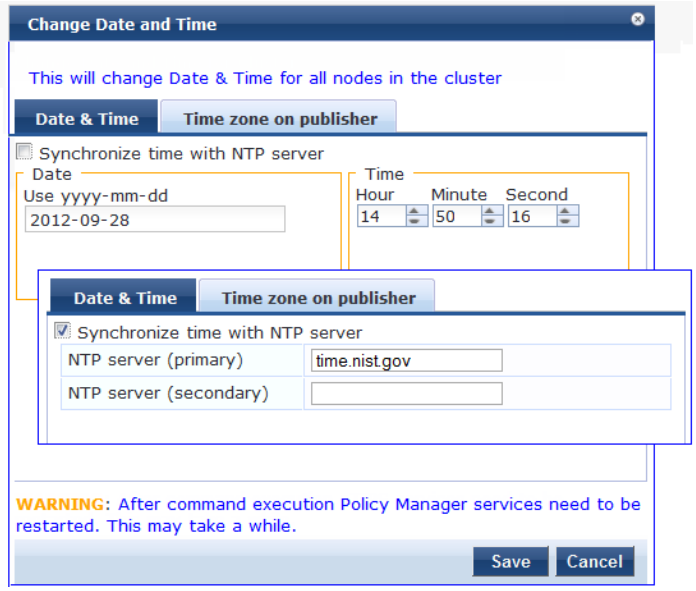
Table 213: *Restrict Access Parameters*

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 UP subnets, separated by commas. The devices defined by what you enter here will be either specifically allowed or specifically denied access to the application you select.

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 348: *Change Date and Time - Date & Time tab*



Change Date and Time

This will change Date & Time for all nodes in the cluster

□ Synchronize time with NTP server

Date

Use yyyy-mm-dd

2012-09-28

Time

Hour	Minute	Second
14	50	16

☑ Synchronize time with NTP server

NTP server (primary)	time.nist.gov
NTP server (secondary)	

WARNING: After command execution Policy Manager services need to be restarted. This may take a while.

Table 214: *Change Date and Time - Date & Time tab Parameters*

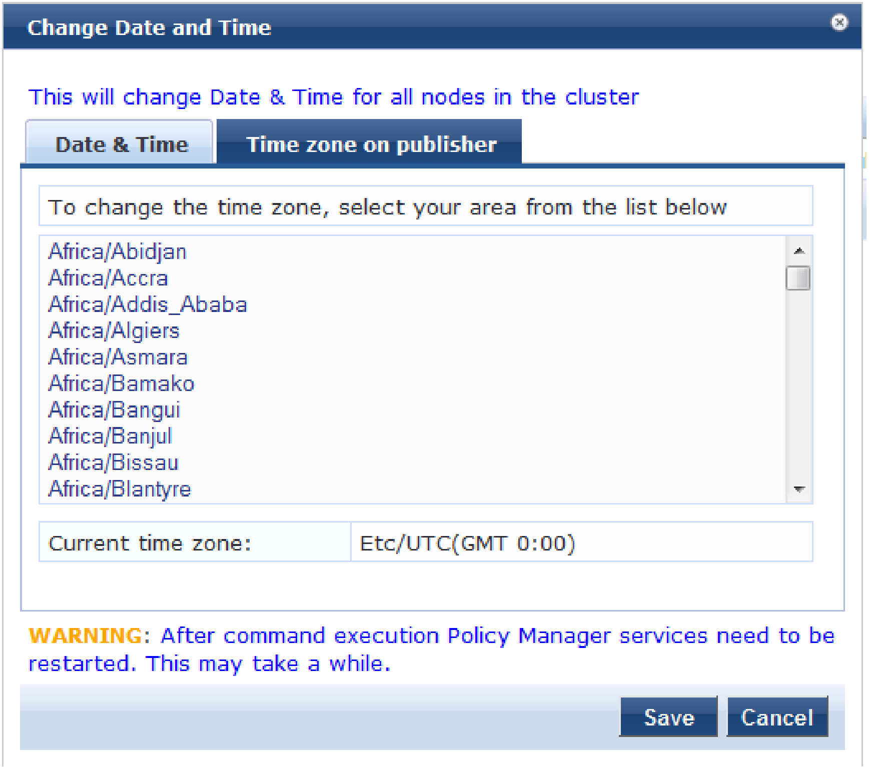
Parameter	Description
Date in yyyy-mm-dd format	To specify date and time, use the indicated syntax. This is available only when Synchronize time with NTP server is unchecked.
Time in hh:mm:ss format	
Synchronize Time With NTP Server	To synchronize with a Network Time Protocol Server, enable this check 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**.

NOTE

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 349: *Time zone on publisher tab*



Change Date and Time

This will change Date & Time for all nodes in the cluster

To change the time zone, select your area from the list below

Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre

Current time zone:	Etc/UTC(GMT 0:00)

WARNING: After command execution Policy Manager services need to be restarted. This may take a while.

Change Cluster Password

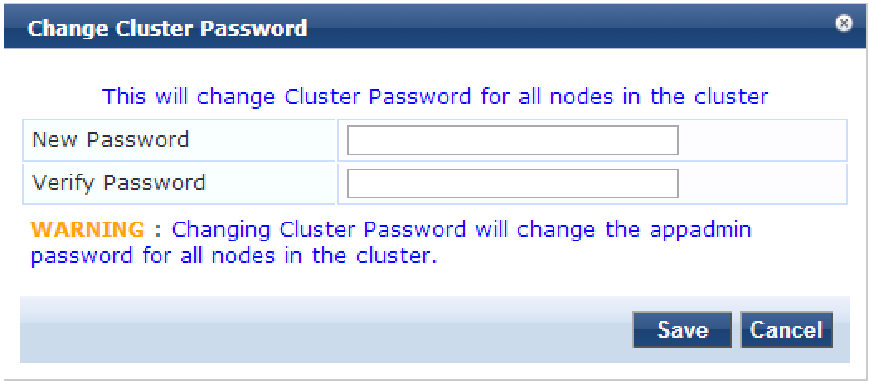
Navigate to **Administration > Server Manager > Server Configuration**, and click on the **Change Cluster Password** link.

Use this function to change the cluster-wide password.

NOTE

Changing this password also changes the password for the CLI user - 'appadmin'.

Figure 350: *Change Cluster Password*



Change Cluster Password

This will change Cluster Password for all nodes in the cluster

New Password	
Verify Password	

WARNING : Changing Cluster Password will change the appadmin password for all nodes in the cluster.

Table 215: *Change Cluster Password*

Parameter	Description
New Password	Enter and confirm the new password.
Verify Password	
Save/Cancel	Commit or dismiss changes.

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

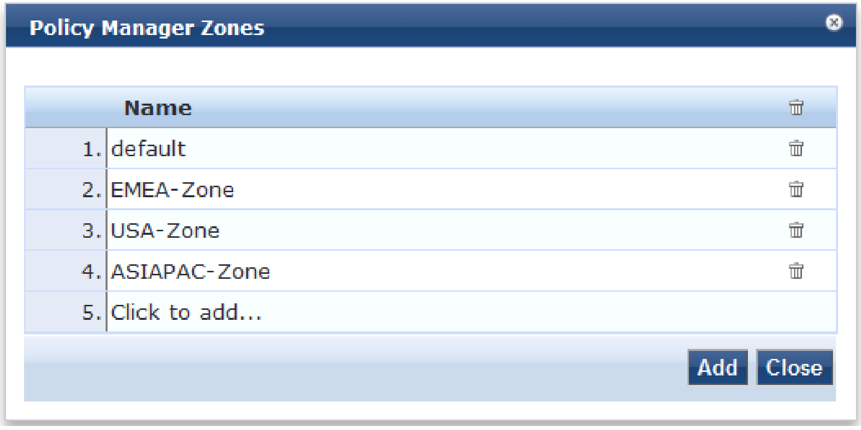
CPPM uses this runtime state information to make policy decisions across multiple transactions.

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 351: *Policy Manager Zones*



Policy Manager Zones

	Name
1.	default
2.	EMEA-Zone
3.	USA-Zone
4.	ASIAPAC-Zone
5.	Click to add...

Table 216: *Policy Manager Zones*

Parameter	Description
Name	Enter the name of the configured Policy Manager Zone.

Table 216: *Policy Manager Zones (Continued)*

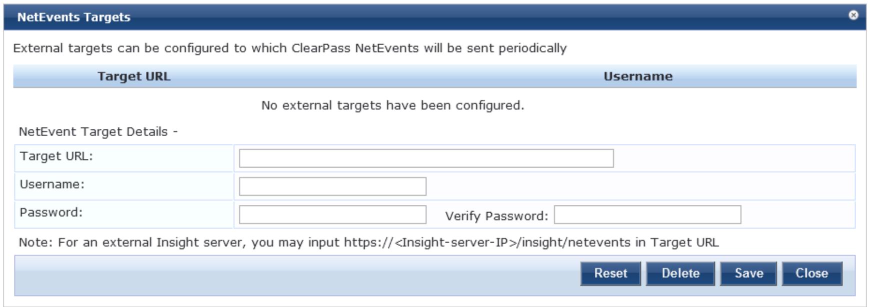
Parameter	Description
Add	
Delete	Select the delete (trashcan) icon to delete a zone.

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 352: *NetEvents Targets*



NetEvents Targets

External targets can be configured to which ClearPass NetEvents will be sent periodically

Target URL	Username
No external targets have been configured.	

NetEvent Target Details -

Target URL:	
Username:	
Password:	Verify Password:

Note: For an external Insight server, you may input https://<Insight-server-IP>/insight/netevents in Target URL

Table 217: *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.

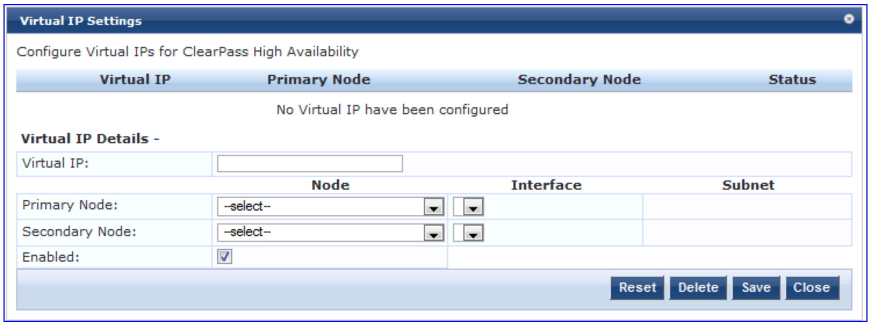
Virtual IP Settings

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.

NOTE

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 353: *Virtual IP Settings*



Virtual IP Settings

Configure Virtual IPs for ClearPass High Availability

Virtual IP	Primary Node	Secondary Node	Status
No Virtual IP have been configured			

Virtual IP Details -

	Node	Interface	Subnet
Virtual IP:			
Primary Node:	--select--		
Secondary Node:	--select--		
Enabled:	☑		

Table 218: *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.

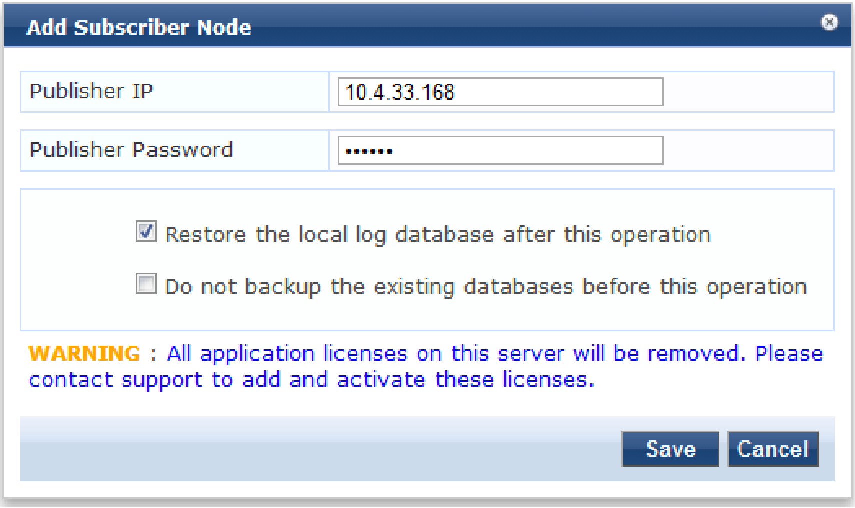
Make Subscriber

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 354: *Add Subscriber Node*



Add Subscriber Node

Publisher IP	10.4.33.168
Publisher Password	••••••

☑ Restore the local log database after this operation

☐ Do not backup the existing databases before this operation

WARNING : All application licenses on this server will be removed. Please contact support to add and activate these licenses.

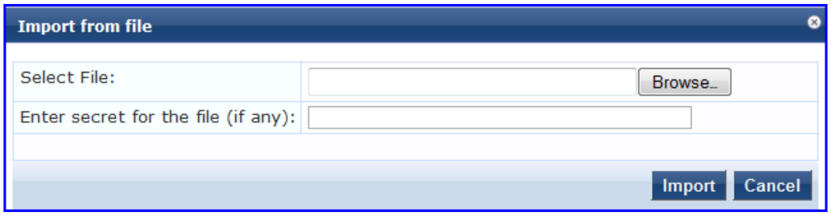
Table 219: *Add Subscriber Node*

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 355: *Upload Nessus Plugins*



Import from file

Select File:

Enter secret for the file (if any):

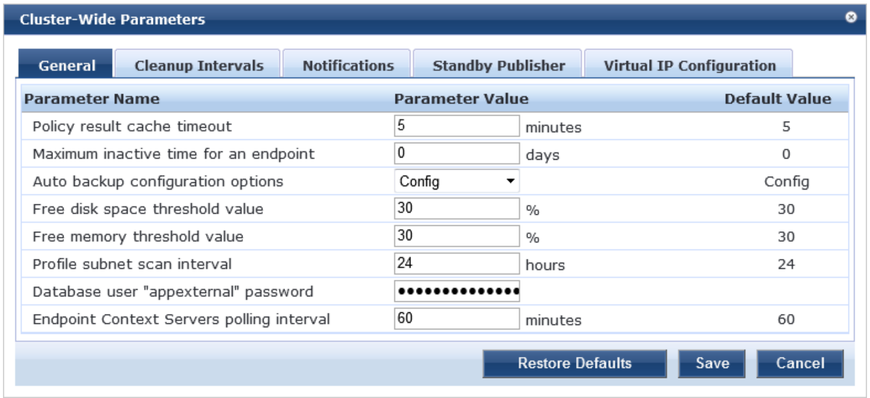
Table 220: *Upload Nessus Plugins*

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

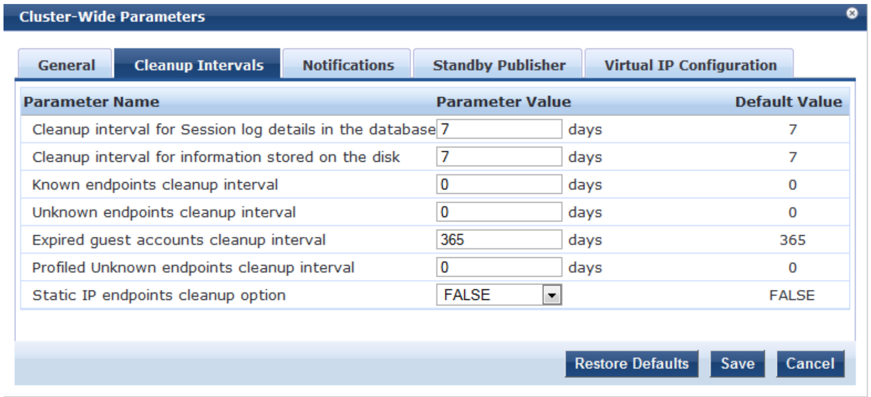
Navigate to the **Administration** > **Server Manager** > **Server Configuration** page, and click on the **Cluster-Wide Parameters** link.

Figure 356: *Cluster-Wide Parameters dialog box, General tab*



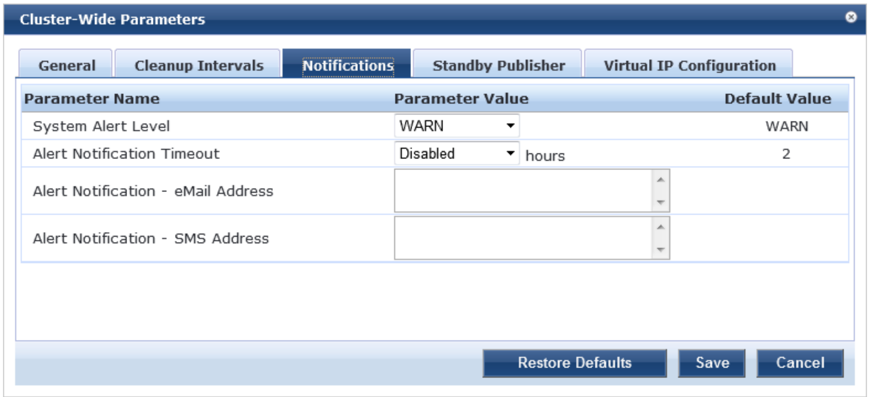
Parameter Name	Parameter Value		Default Value
Policy result cache timeout	5	minutes	5
Maximum inactive time for an endpoint	0	days	0
Auto backup configuration options	Config		Config
Free disk space threshold value	30	%	30
Free memory threshold value	30	%	30
Profile subnet scan interval	24	hours	24
Database user "appexternal" password	••••••••••••••		
Endpoint Context Servers polling interval	60	minutes	60

Figure 357: *Cluster-Wide Parameters dialog box, Cleanup Interval tab*



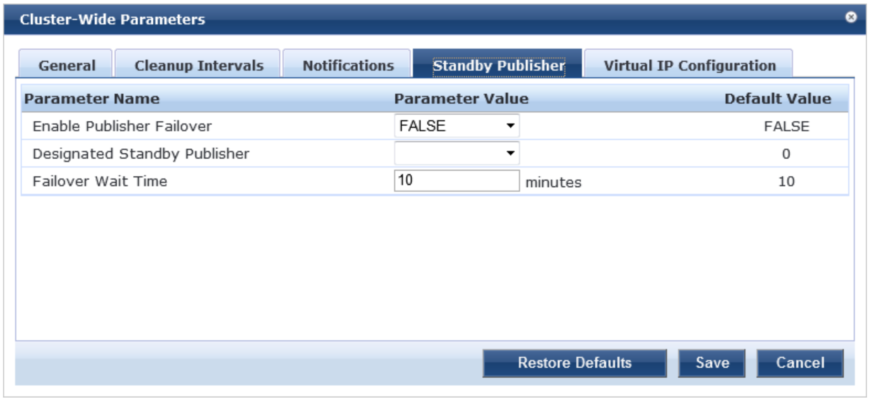
Parameter Name	Parameter Value		Default Value
Cleanup interval for Session log details in the database	7	days	7
Cleanup interval for information stored on the disk	7	days	7
Known endpoints cleanup interval	0	days	0
Unknown endpoints cleanup interval	0	days	0
Expired guest accounts cleanup interval	365	days	365
Profiled Unknown endpoints cleanup interval	0	days	0
Static IP endpoints cleanup option	FALSE		FALSE

Figure 358: *Cluster-Wide Parameters dialog box, Notifications tab*



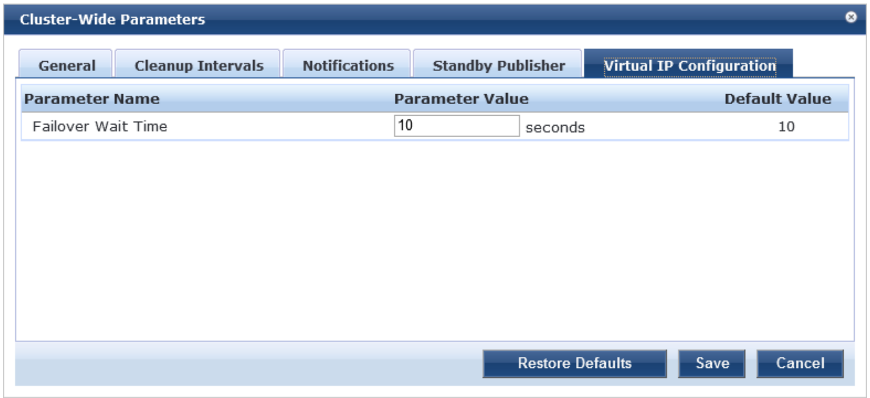
Parameter Name	Parameter Value		Default Value
System Alert Level	WARN		WARN
Alert Notification Timeout	Disabled	hours	2
Alert Notification - eMail Address			
Alert Notification - SMS Address			

Figure 359: *Cluster-Wide Parameters dialog box, Standby Publisher tab*



Parameter Name	Parameter Value		Default Value
Enable Publisher Failover	FALSE		FALSE
Designated Standby Publisher			0
Failover Wait Time	10	minutes	10

Figure 360: *Cluster-Wide Parameters dialog box, Virtual IP Configuration tab*



Parameter Name	Parameter Value	Default Value
Failover Wait Time	10 seconds	10

Table 221: *Cluster-Wide Parameters*

Parameter	Description
General	
Policy result cache cleanup timeout	The number of minutes to store the role mapping and posture results derived by the policy engine during policy evaluation. This result can then be used in subsequent evaluation of policies associated with a service, if "Use cached Roles and Posture attributes from previous sessions" is turned on for the service. A value of 0 disables caching.
Maximum inactive time for an endpoint	The number of days to keep an endpoint in the endpoints table since its last authentication. If the endpoint has not authenticated for this period, the entry is removed from the endpoint table. 0 specifies no time limit.
Auto backup configuration options	• Off - Do not perform periodic backups. • Config - Perform a periodic backup of only the configuration database. • Config|SessionInfo - Perform a backup of both the configuration database and the session log database.
Free disk space threshold value	This controls 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 below of disk space is available.
Free memory threshold value	This controls 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 below of RAM is available.
Profile subnet scan interval	Enter a value in hours.
Database user "appexternal" password	For this connection to the database, enter the password for the "appexternal" username.

Table 221: *Cluster-Wide Parameters (Continued)*

Parameter	Description
Endpoint Context Servers polling interval	Enter the number of minutes between polling of endpoint context servers. The default is 60.
Cleanup Intervals	
Cleanup interval for session log details in the database	The Number of days to keep the following data in the Policy Manager DB: session logs (found on Access Tracker), event logs (found on Event Viewer), machine authentication cache.
Cleanup interval for information stored on disk	The Number of days to keep log files, etc., written to the disk.
Known endpoints cleanup interval	A value (in days) that ClearPass uses to determine when to start deleting known or disabled entries from the Endpoint repository. Known entries are deleted based on their last "Updated At" value for each Endpoint. For example, if this value is 7, then known Endpoints that do not have an "Updated At" value within the last 7 days will be deleted.
Unknown endpoints cleanup interval	A value (in days) that ClearPass uses to determine when to start deleting unknown entries from the Endpoint repository. Unknown entries are deleted based on their last "Updated At" value for each Endpoint. For example, if this value is 7, then unknown Endpoints that do not have an "Updated At" value within the last 7 days (perhaps stale endpoints) will be deleted.
Expired guest accounts cleanup interval	This controls the cleanup interval of expired guest accounts. This is the number of days after expiry that the cleanup occurs. No cleanup is performed if the value is 0.
Profiled endpoints cleanup interval	A value (in days) that ClearPass uses to determine when to start deleting profiled entries from the Endpoint repository. Profiled entries are deleted based on their last "Updated At" value for each Endpoint. For example, if this value is 7, then profiled Endpoints that do not have an "Updated At" value within the last 7 days will be deleted.
Static IP endpoints cleanup option	Specify whether to enable the option to cleanup static IP endpoints.
Notifications	

Table 221: *Cluster-Wide Parameters (Continued)*

Parameter	Description
System Alert Level	Alert notifications 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.
Alert Notification Timeout	This indicates how often (in hours) alert messages are generated and sent out. Selecting 'Disabled" disables alert generation.
Alert Notification - eMail Address	Comma separated list of email addresses to which alert messages are sent.
Alert Notification - SMS Address	Comma-separated list of SMS addresses to which alert messages are sent. For example, 4085551212@txt.att.net.
Standby Publisher	
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.
Designated Standby Publisher	Select the server in the cluster to act as the standby publisher. **NOTE:** If the Standby Publisher is on a different subnet than the Publisher, then ensure a reliable connection between the two subnets 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 Primary node failure before it acquires the Virtual IP Address. The default is 10 minutes so the Secondary node doesn't take over unnecessarily in conditions where the Primary node's unavailability is brief, such as a restart.
Virtual IP Configuration	
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 is 10 seconds so the Secondary node will take over and respond quickly to authentication access and requests.

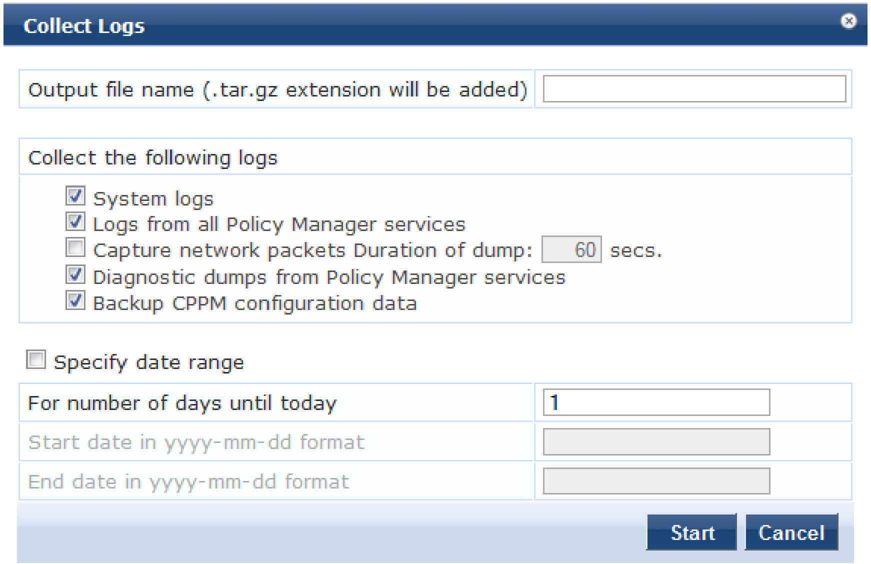
Collect Logs

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 361: *Collect Logs*



Collect Logs

Output file name (.tar.gz extension will be added)	

Collect the following logs

☑ System logs
☑ Logs from all Policy Manager services
☐ Capture network packets Duration of dump: 60 secs.
☑ Diagnostic dumps from Policy Manager services
☑ Backup CPPM configuration data

☐ Specify date range

For number of days until today	1
Start date in yyyy-mm-dd format	
End date in yyyy-mm-dd format	

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.

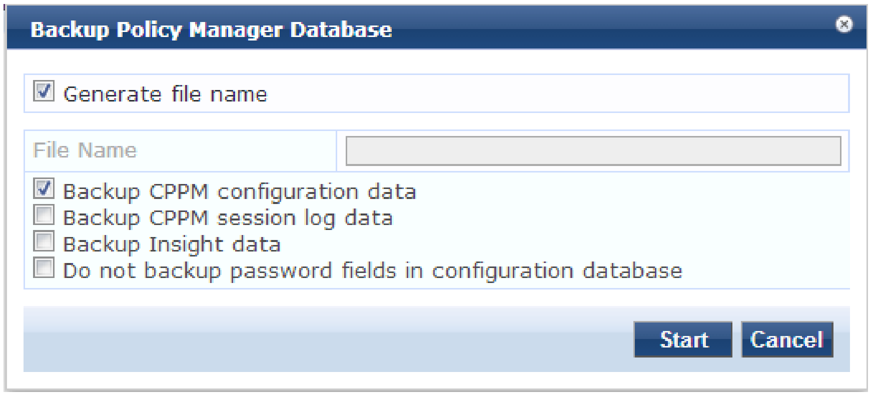
NOTE

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 362: *Backup Popup*



Backup Policy Manager Database

☑ Generate file name

File Name

☑ Backup CPPM configuration data
□ Backup CPPM session log data
□ Backup Insight data
□ Do not backup password fields in configuration database

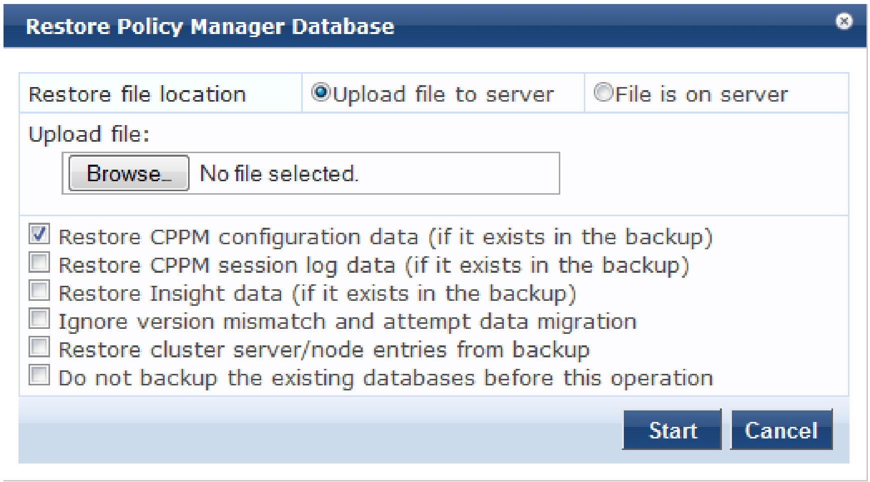
Table 222: *Backup*

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 363: *Restore*



Restore Policy Manager Database

Restore file location	● Upload file to server	○ File is on server

Upload file:

Browse... No file selected.

☑ Restore CPPM configuration data (if it exists in the backup)
☐ Restore CPPM session log data (if it exists in the backup)
☐ Restore Insight data (if it exists in the backup)
☐ Ignore version mismatch and attempt data migration
☐ Restore cluster server/node entries from backup
☐ Do not backup the existing databases before this operation

Table 223: *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.
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.

NOTE

This option is not available in a single node deployment.

Local Shared Folders

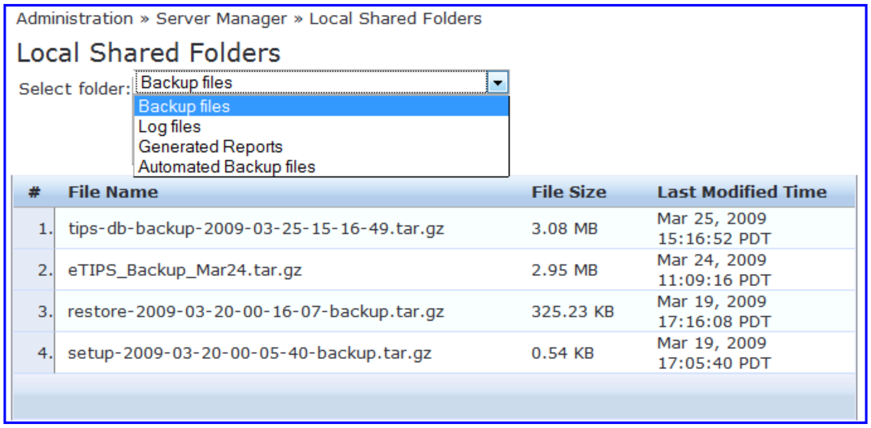
Select the specific folder from the **Select folder** drop-down list. Currently supported folder types are listed below:

- 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 357

Figure 364: *Local Shared Folders Page*



Administration » Server Manager » Local Shared Folders

Local Shared Folders

Select folder: Backup files

#	File Name	File Size	Last Modified Time
1.	tips-db-backup-2009-03-25-15-16-49.tar.gz	3.08 MB	Mar 25, 2009 15:16:52 PDT
2.	eTIPS_Backup_Mar24.tar.gz	2.95 MB	Mar 24, 2009 11:09:16 PDT
3.	restore-2009-03-20-00-16-07-backup.tar.gz	325.23 KB	Mar 19, 2009 17:16:08 PDT
4.	setup-2009-03-20-00-05-40-backup.tar.gz	0.54 KB	Mar 19, 2009 17:05:40 PDT

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 362
- "Activating a Server License" on page 362
- "Adding an Application License" on page 363
- "Updating an Application License" on page 363

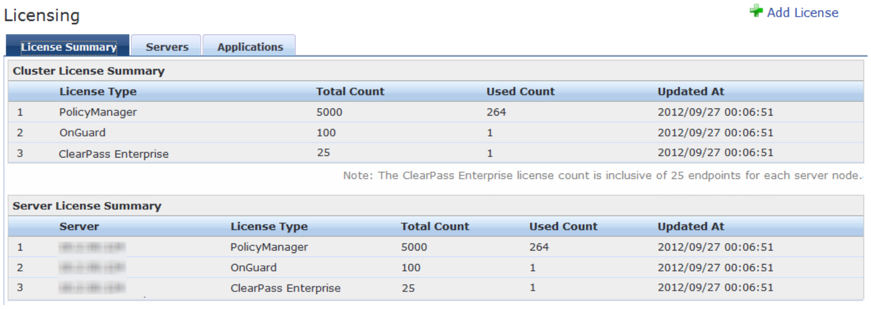
NOTE

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, Enterprise, and WorkSpace application licenses. The Summary section shows the number of purchased licenses for Policy Manager, OnGuard, Guest, Onboard, and WorkSpace.

Figure 365: *Licensing Page - License Summary tab*



Cluster License Summary

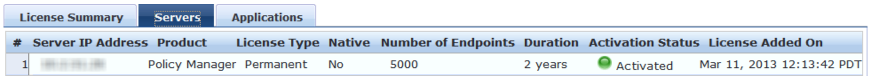
	License Type	Total Count	Used Count	Updated At
1	PolicyManager	5000	264	2012/09/27 00:06:51
2	OnGuard	100	1	2012/09/27 00:06:51
3	ClearPass Enterprise	25	1	2012/09/27 00:06:51

Note: The ClearPass Enterprise license count is inclusive of 25 endpoints for each server node..

Server License Summary

	Server	License Type	Total Count	Used Count	Updated At
1	[redacted]	PolicyManager	5000	264	2012/09/27 00:06:51
2	[redacted]	OnGuard	100	1	2012/09/27 00:06:51
3	[redacted]	ClearPass Enterprise	25	1	2012/09/27 00:06:51

Figure 366: *Licensing Page - Servers tab*



#	Server IP Address	Product	License Type	Native	Number of Endpoints	Duration	Activation Status	License Added On
1	[redacted]	Policy Manager	Permanent	No	5000	2 years	● Activated	Mar 11, 2013 12:13:42 PDT

NOTE

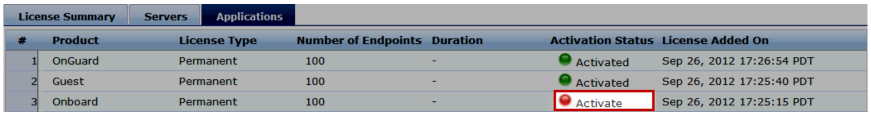
If the number of licenses used exceeds the number purchased, you will see a warning four months after the number is exceeded. The licenses used number is based on the daily moving average.

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 367: *Application License Page*



#	Product	License Type	Number of Endpoints	Duration	Activation Status	License Added On
1	OnGuard	Permanent	100	-	● Activated	Sep 26, 2012 17:26:54 PDT
2	Guest	Permanent	100	-	● Activated	Sep 26, 2012 17:25:40 PDT
3	Onboard	Permanent	100	-	● Activate	Sep 26, 2012 17:25:15 PDT

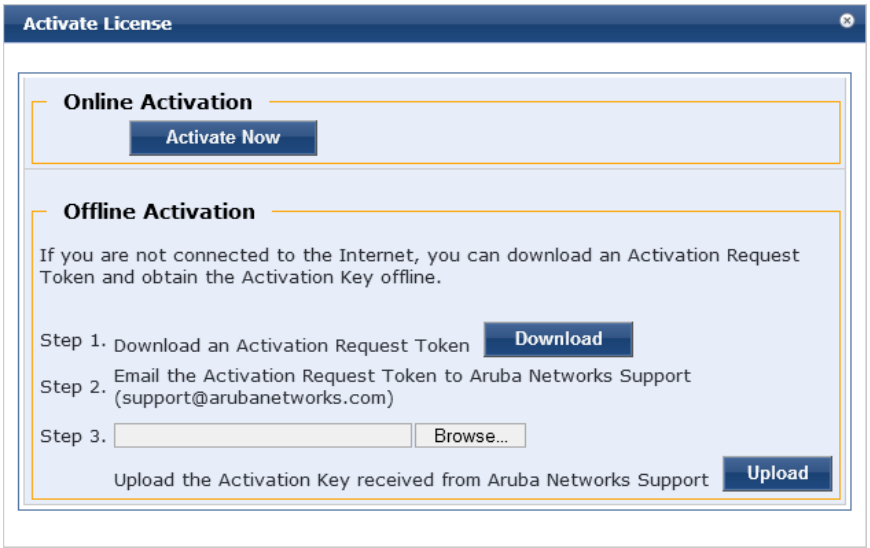
Activating a Server License

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 368: *Online Activation Page*



If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

Step 1. Download an Activation Request Token

Step 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com)

Step 3.

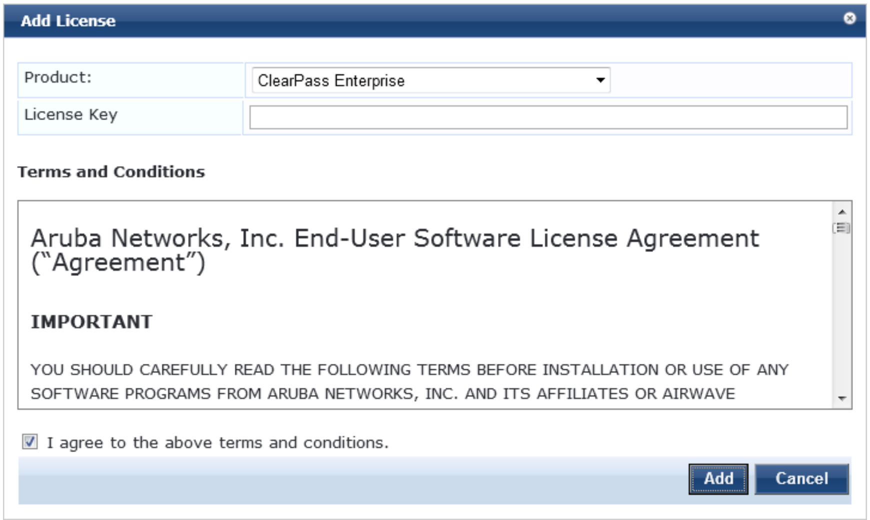
Upload the Activation Key received from Aruba Networks Support

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. WorkSpace licenses require a valid Onboard or ClearPass Enterprise license. The default 25 endpoint ClearPass Enterprise license does not qualify.
2. Enter the license key for the new license.
3. Read the Terms and Conditions before adding a license.
4. Click the I agree to the above terms and conditions check box.
5. Click the **Add** button.

Figure 369: *Add License Page*



Product:	ClearPass Enterprise
License Key	

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement (“Agreement”)

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE

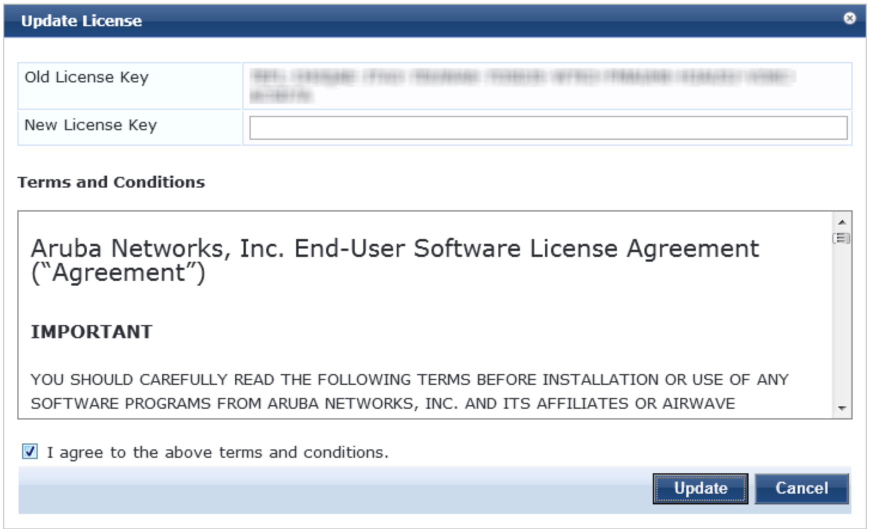
☑ I agree to the above terms and conditions.

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**.



Update License

Old License Key	[redacted]
New License Key	

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE

☑ I agree to the above terms and conditions.

SNMP Trap Receivers

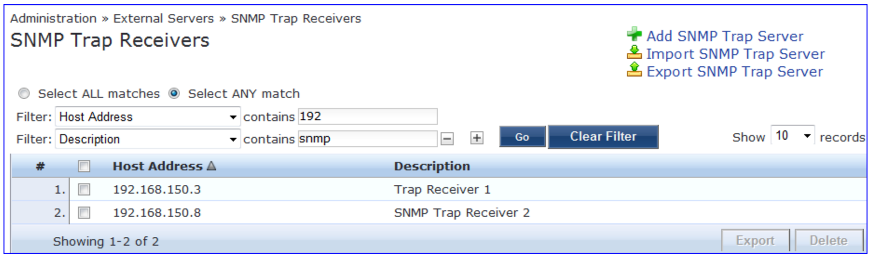
Policy Manager sends SNMP traps that expose the following server information:

- **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 365
- "Exporting all SNMP Trap Servers" on page 365
- "Exporting a Single SNMP Trap Server" on page 365
- "Importing an SNMP Trap Server" on page 365

Figure 370: *SNMP Trap Receivers Listing Page*



Administration » External Servers » SNMP Trap Receivers

SNMP Trap Receivers

○ Select ALL matches ● Select ANY match

Filter: Host Address contains 192

Filter: Description contains snmp

Show 10 records

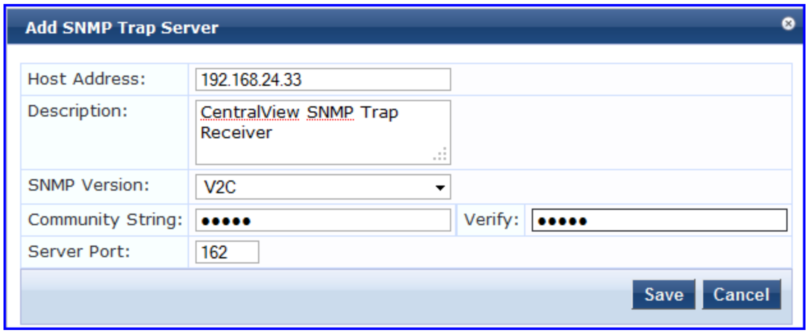
#	□	Host Address ▲	Description
1.	□	192.168.150.3	Trap Receiver 1
2.	□	192.168.150.8	SNMP Trap Receiver 2

Showing 1-2 of 2

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 371: *Add SNMP Trap Server*



Add SNMP Trap Server

Host Address:	192.168.24.33		
Description:	CentralView SNMP Trap Receiver		
SNMP Version:	V2C		
Community String:	●●●●●	Verify:	●●●●●
Server Port:	162		

Table 224: *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 372: *Import SNMP Trap Server*

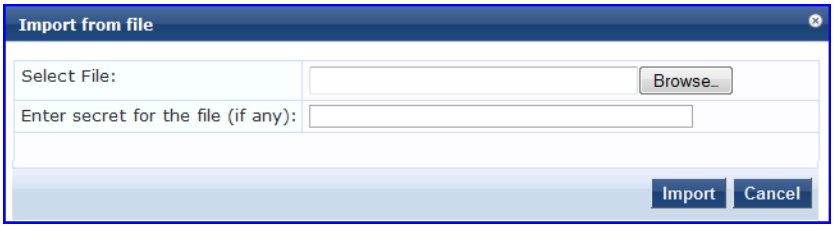


Table 225: *Import SNMP Trap Server*

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.

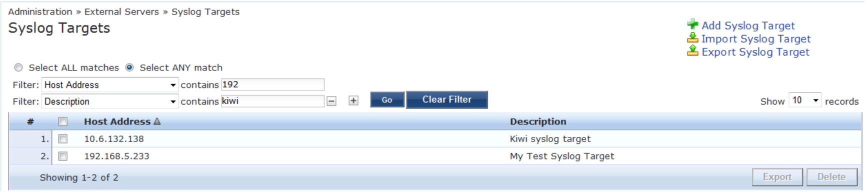
Syslog Targets

Dell Networking W-ClearPass Policy Manager can export session data (see "Access Tracker" on page 33), audit records (see "Audit Viewer" on page 58) and event records (see "Event Viewer" on page 63). 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 367
- "Import Syslog Target" on page 367
- "Export Syslog Target" on page 368
- "Export" on page 368

Figure 373: *Syslog Target Listing Page*



Administration » External Servers » Syslog Targets

Syslog Targets

○ Select ALL matches ● Select ANY match

Filter: Host Address contains 192

Filter: Description contains kiwi

Show 10 records

#	□	Host Address ▵	Description
1.	□	10.6.132.138	Kiwi syslog target
2.	□	192.168.5.233	My Test Syslog Target

Showing 1-2 of 2

Table 226: *Syslog Target Configuration*

Parameter	Description
Add Syslog Target	Opens the **Add Syslog Target** popup.
Import Syslog Target	Opens the **Import Syslog Target** popup.
Export Syslog Target	Opens the **Export Syslog Target** popup.

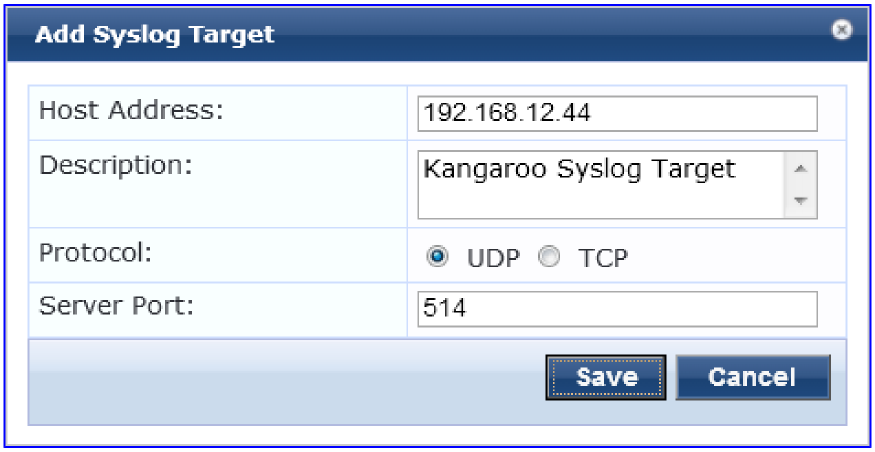
Table 226: *Syslog Target Configuration (Continued)*

Parameter	Description
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 Syslog Target**.

Figure 374: *Add Syslog Target*



Host Address: 192.168.12.44

Description: Kangaroo Syslog Target

Protocol: ● UDP ○ TCP

Server Port: 514

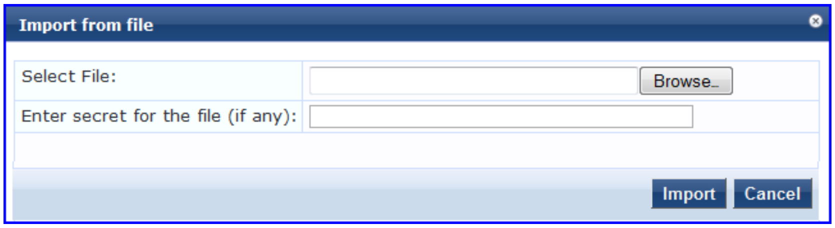
Table 227: *Add Syslog Target*

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 Syslog Target**.

Figure 375: *Import Syslog Target*



Import from file

Select File:

Enter secret for the file (if any):

Table 228: *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 Syslog Target** link.

The **Export Syslog Target** 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

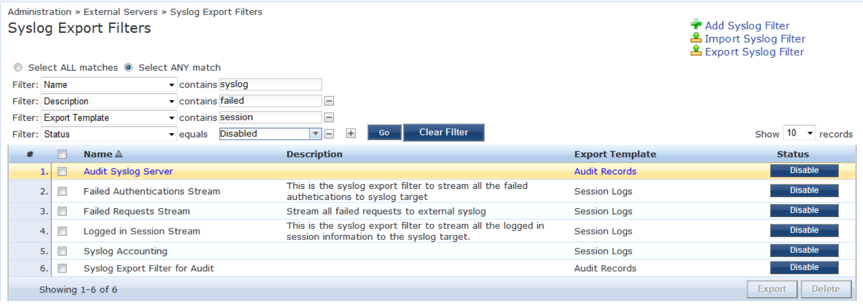
Policy Manager can export session data (see "Access Tracker" on page 33), audit records (see "Audit Viewer" on page 58) and event records (see "Event Viewer" on page 63).

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 370
- "Adding a Syslog Export Filter (General tab)" on page 371
- "Adding a Syslog Export Filter (Summary tab)" on page 372
- "Import Syslog Filter" on page 369
- "Export Syslog Filter" on page 370
- "Export" on page 370

Figure 376: *Syslog Export Filters Page*



Administration » External Servers » Syslog Export Filters

Syslog Export Filters

○ Select ALL matches ● Select ANY match

Filter: Name contains syslog

Filter: Description contains failed

Filter: Export Template contains session

Filter: Status equals Disabled

#	□	Name ▵	Description	Export Template	Status
1.	□	Audit Syslog Server		Audit Records	Disable
2.	□	Failed Authentications Stream	This is the syslog export filter to stream all the failed authetications to syslog target	Session Logs	Disable
3.	□	Failed Requests Stream	Stream all failed requests to external syslog	Session Logs	Disable
4.	□	Logged in Session Stream	This is the syslog export filter to stream all the logged in session information to the syslog target.	Session Logs	Disable
5.	□	Syslog Accounting		Session Logs	Disable
6.	□	Syslog Export Filter for Audit		Audit Records	Disable

Showing 1-6 of 6

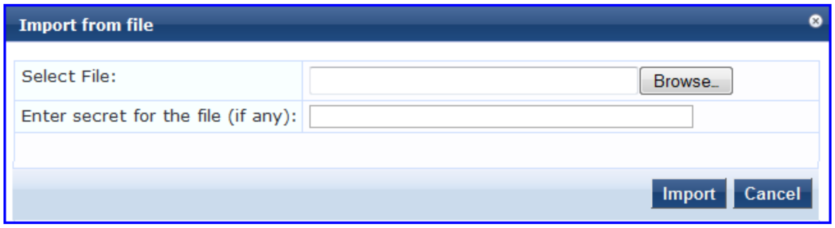
Table 229: *Syslog Export Filters Page Parameters*

Parameter	Description
Add Syslog Filter	Opens **Add Syslog Filter** page (**Administration > External Servers > Syslog Export Filters > Add**).
Import Syslog Filter	Opens **Import Syslog Filter** popup.
Export Syslog Filter	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 Syslog Filter**.

Figure 377: *Import Syslog Filter*



Import from file

Select File:

Enter secret for the file (if any):

Table 230: *Import from File*

Parameter	Description
Select File	Browse to the Syslog Filter configuration file to be imported.

Table 230: *Import from File (Continued)*

Parameter	Description
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 Syslog Filter** link.

The **Export Syslog Filter** 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 is only visible if you This tab provides two methods for configuring data filters and is only visible if you selected Session Logs as the export template in the General tab.

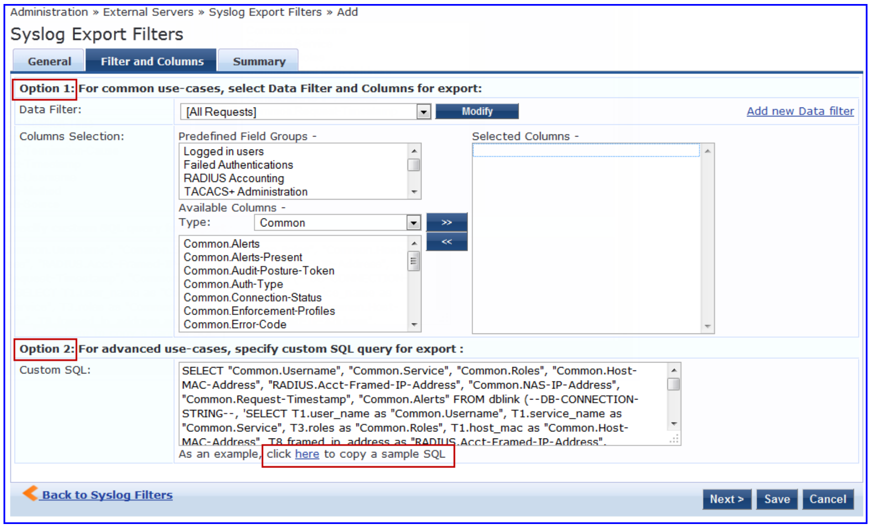
Option 1 allows you to choose from pre-defined field groups and to select columns based on the Type.

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.

NOTE

We recommend that users who choose Option 2: the Custom SQL option contact Support. Support can assist you with entering the correct information in this template.

Figure 378: *Add Syslog Filters (Filter and Columns tab)*



Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

Option 1: For common use-cases, select Data Filter and Columns for export:

Data Filter: [All Requests]

Columns Selection:

Predefined Field Groups -

- Logged in users
- Failed Authentications
- RADIUS Accounting
- TACACS+ Administration

Selected Columns -

Available Columns -

Type: Common

- Common.Alerts
- Common.Alerts-Present
- Common.Audit-Posture-Token
- Common.Auth-Type
- Common.Connection-Status
- Common.Enforcement-Profiles
- Common.Error-Code

Option 2: For advanced use-cases, specify custom SQL query for export :

Custom SQL:

```
SELECT "Common.Username", "Common.Service", "Common.Roles", "Common.Host-
MAC-Address", "RADIUS.Acct-Framed-IP-Address", "Common.NAS-IP-Address",
"Common.Request-Timestamp", "Common.Alerts" FROM dblink (--DB-CONNECTION-
STRING--, 'SELECT T1.user_name as "Common.Username", T1.service_name as
"Common.Service", T3.roles as "Common.Roles", T1.host_mac as "Common.Host-
MAC-Address", T8.framed_ip_address as "RADIUS.Acct-Framed-IP-Address",
```

As an example, click here to copy a sample SQL

Table 231: *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 provides a way 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 pre-defined 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.

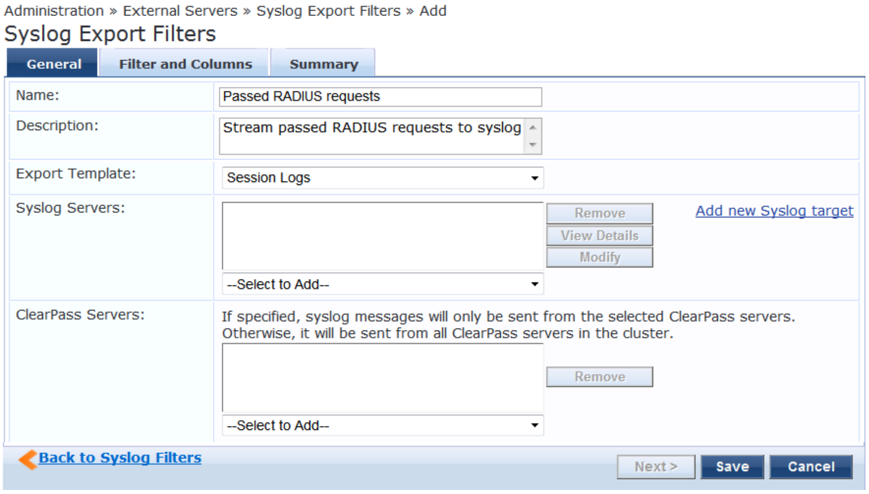
Adding a Syslog Export Filter (General tab)

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 370).

Figure 379: *Add Syslog Export Filters (General tab)*



Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

Name: Passed RADIUS requests

Description: Stream passed RADIUS requests to syslog

Export Template: Session Logs

Syslog Servers: --Select to Add--

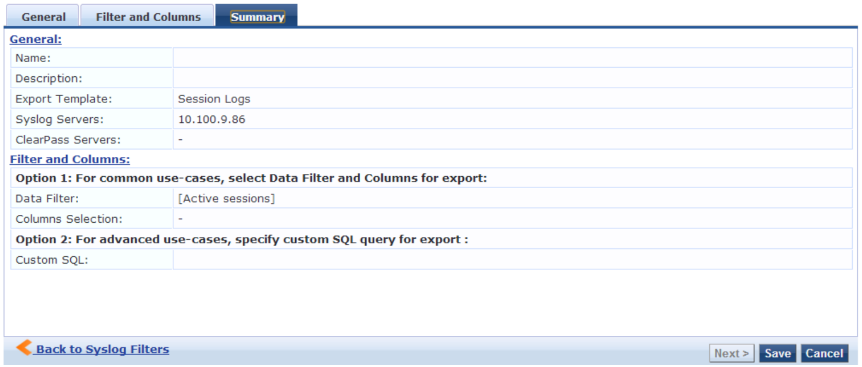
ClearPass Servers: If specified, syslog messages will only be sent from the selected ClearPass servers. Otherwise, it will be sent from all ClearPass servers in the cluster. --Select to Add--

Table 232: *Syslog Export Filters General tab Parameters*

Parameter	Description
Name/Description	Enter name and description in the respective text fields.
Export Template	Session Logs, Audit Records or 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.



General:

Name:	
Description:	
Export Template:	Session Logs
Syslog Servers:	10.100.9.86
ClearPass Servers:	-

Filter and Columns:

Option 1: For common use-cases, select Data Filter and Columns for export:	
Data Filter:	[Active sessions]
Columns Selection:	-
Option 2: For advanced use-cases, specify custom SQL query for export :	
Custom SQL:	

Table 233: *Syslog Export Filters Summary tab Parameters*

Parameter	Description
General:	
Name:	Name created for the new filter.
Description:	Description of the new syslog export filter.

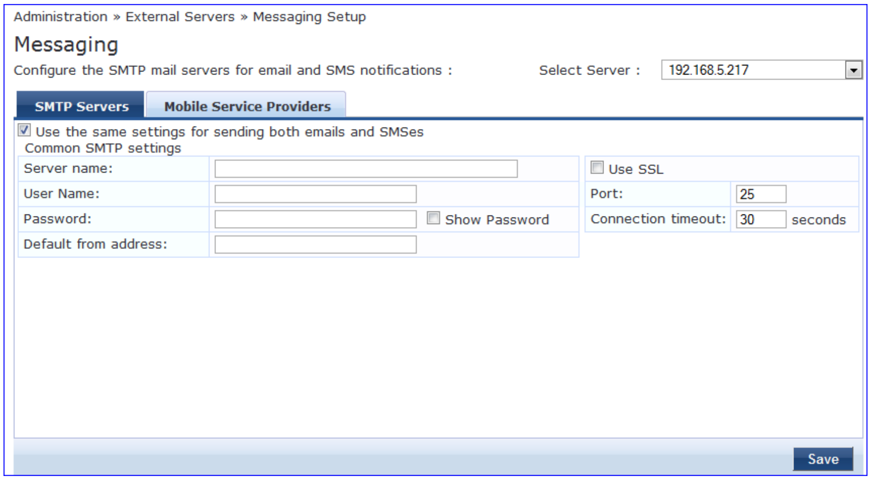
Table 233: *Syslog Export Filters Summary tab Parameters (Continued)*

Parameter	Description
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 Policy Manager Messaging Setup menu at **Administration** > **Server Manager** > **Messaging Setup** provides the following interface for configuration:

Figure 380: *Messaging Setup SMTP Servers tab*



Administration » External Servers » Messaging Setup

Messaging

Configure the SMTP mail servers for email and SMS notifications : Select Server : 192.168.5.217

☑ Use the same settings for sending both emails and SMSes

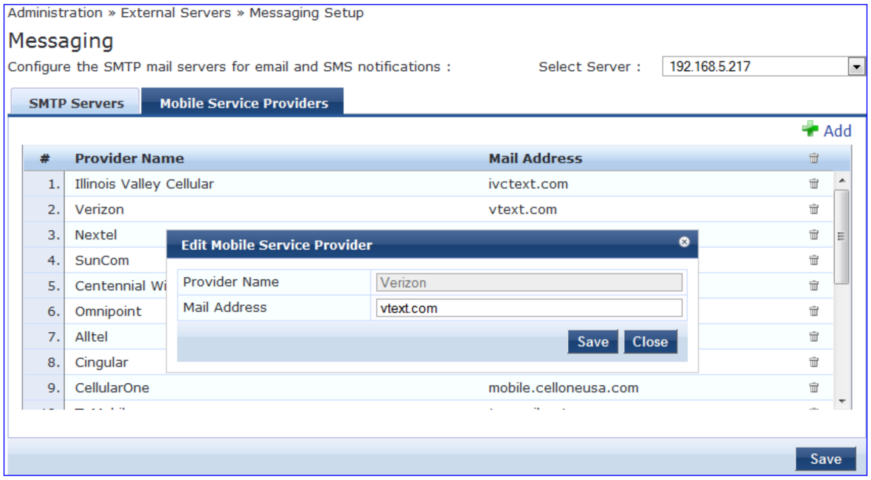
Common SMTP settings

Server name:			☐ Use SSL	
User Name:			Port:	25
Password:		☐ Show Password	Connection timeout:	30 seconds
Default from address:				

Table 234: *Messaging Setup MTP Servers tab Parameters*

Parameter	Description
Select Server:	Specify the server for which to configure messaging. All nodes in the cluster appear in the drop-down list.
Use the same settings for sending both emails and SMSes:	Check this box to configure the same settings for both your SMTP and SMS email servers. This box is checked, by default.
Server name:	Fully qualified domain name or IP address of the server.
Username/password:	If your email server requires authentication for sending email messages, enter the credentials here.
Default from address:	All emails sent out will have this from address in the message.
Use SSL:	Use secure SSL connection for communications with the server.
Port:	This is TCP the port number that the SNMP server listens on.
Connection timeout:	Timeout for connection to the server (in seconds).

Figure 381: *Messaging Setup Mobile Service Providers tab*



Administration » External Servers » Messaging Setup

Messaging

Configure the SMTP mail servers for email and SMS notifications :

Select Server : 192.168.5.217

#	Provider Name	Mail Address
1.	Illinois Valley Cellular	ivctext.com
2.	Verizon	vtext.com
3.	Nextel	
4.	SunCom	
5.	Centennial Wi	
6.	Omnipoint	
7.	Alltel	
8.	Cingular	
9.	CellularOne	mobile.celloneusa.com

Edit Mobile Service Provider

Provider Name: Verizon

Mail Address: vtext.com

Table 235: *Messaging Setup Mobile Service Providers tab Parameters*

Parameter	Description
Add:	Add a mobile service provider
Provider Name:	Name of the provider
Mail Address:	Domain name of the provider

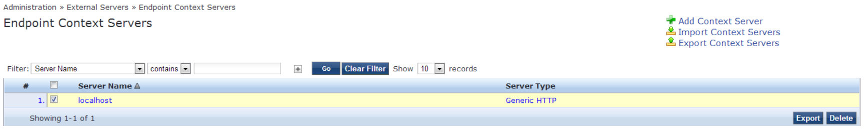
Endpoint Context Servers

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 382: *Endpoint Context Servers Page*



Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

Filter: Server Name contains | Show 10 records

#	☐	Server Name	Server Type
1.	☑	localhost	Generic HTTP

Showing 1-1 of 1

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 375 for more information.
4. Click **Save**.

Delete an endpoint context server

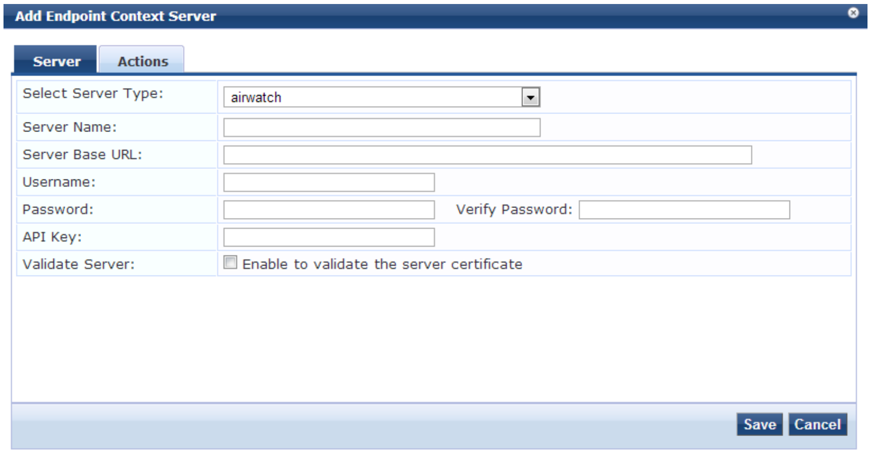
Deleting an endpoint context server just removes its configuration information from Policy Manager. If you think you might want to add it again, export it before you delete it and save the configuration so you can just import it at a later date.

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 Air Watch Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 383: *Add Air Watch Server tab*

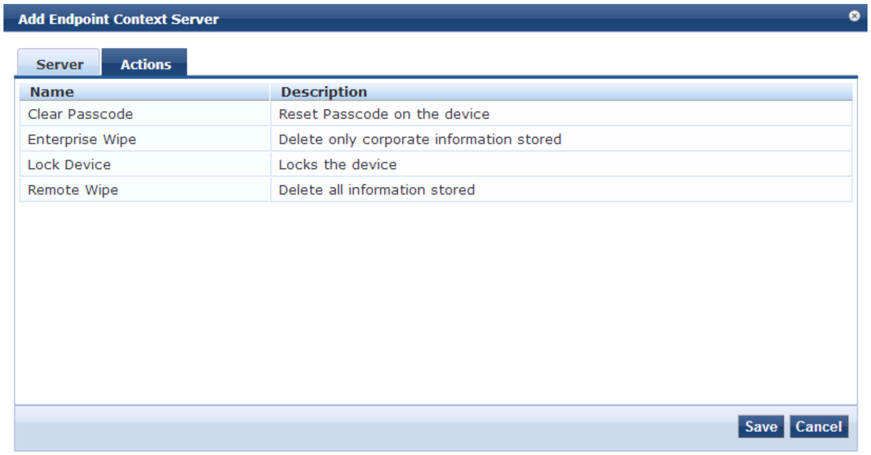


Select Server Type:	airwatch
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
API Key:	
Validate Server:	□ Enable to validate the server certificate

Table 236: *Add Air Watch Server tab Parameters*

Parameter	Description
Select Server Type:	Add Air Watch.
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 384: *Add AirWatch Actions tab*



Name	Description
Clear Passcode	Reset Passcode on the device
Enterprise Wipe	Delete only corporate information stored
Lock Device	Locks the device
Remote Wipe	Delete all information stored

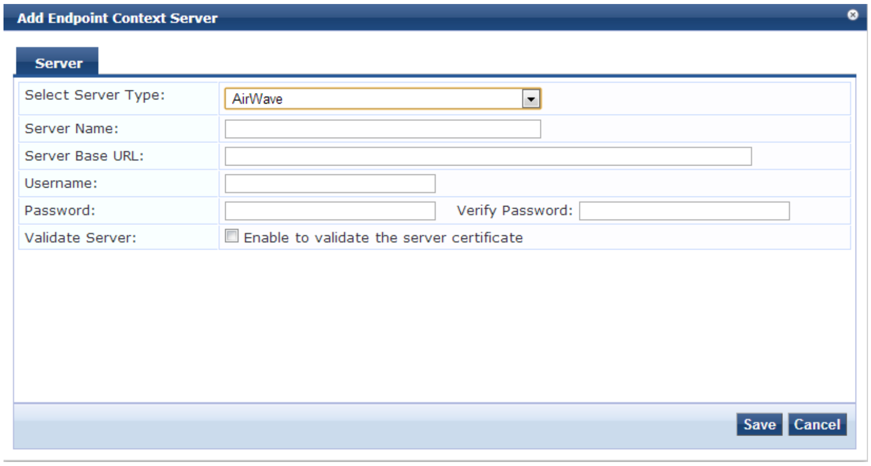
Table 237: *Add Air Watch Actions tab Parameters*

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 Air Wave Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Figure 385: *Add Air Wave Endpoint Context Server tab*



Select Server Type:	AirWave
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Validate Server:	□ Enable to validate the server certificate

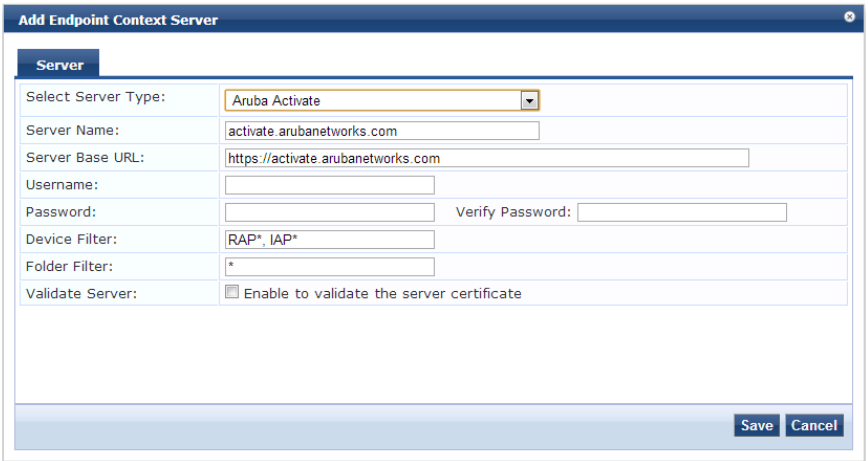
Table 238: *Add Air Wave Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	Air Wave
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 386: *Add Aruba Activate Endpoint Context Server tab*



Add Endpoint Context Server

Server

Select Server Type:	Aruba Activate
Server Name:	activate.arubanetworks.com
Server Base URL:	https://activate.arubanetworks.com
Username:	
Password:	Verify Password:
Device Filter:	RAP*, IAP*
Folder Filter:	*
Validate Server:	□ Enable to validate the server certificate

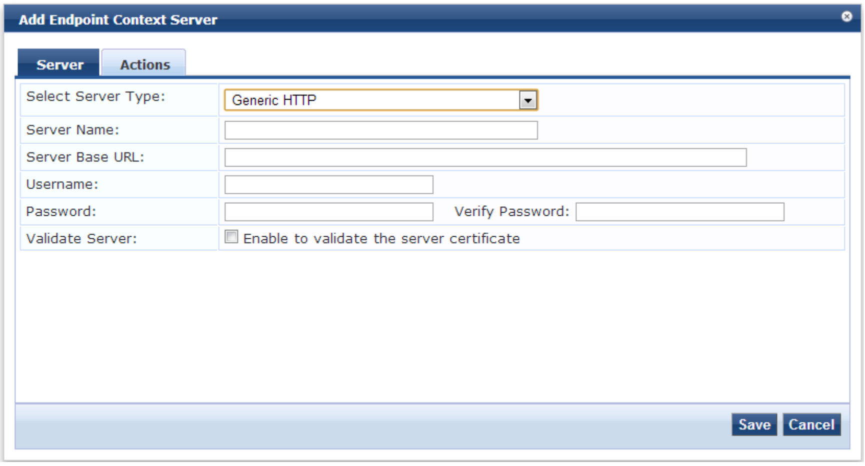
Table 239: *Add Aruba Activate Endpoint Context Server tab Parameter*

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 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 387: *Add Generic HTTP Endpoint Context Server Server tab*

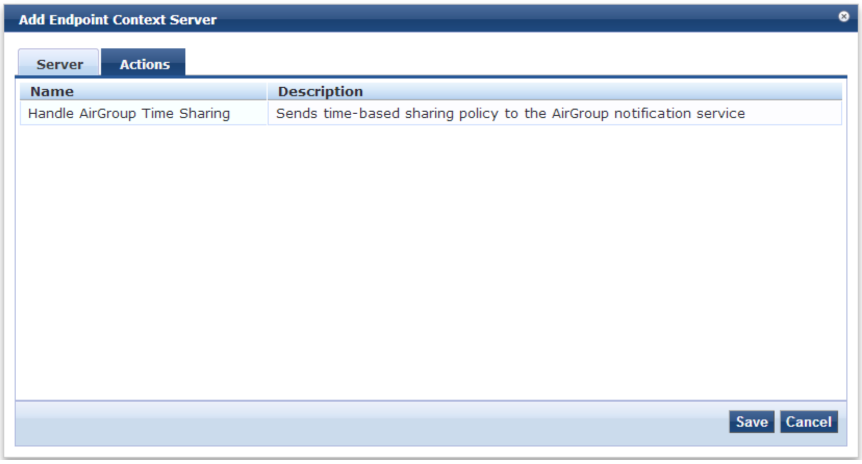


Select Server Type:	Generic HTTP
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Validate Server:	□ Enable to validate the server certificate

Table 240: *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.
Password:	Enter and verify the password.
Verify Password:	
Validate Server:	Click to enable validation of the server certificate.

Figure 388: *Add Generic HTTP Endpoint Context Server Actions tab*



Name	Description
Handle AirGroup Time Sharing	Sends time-based sharing policy to the AirGroup notification service

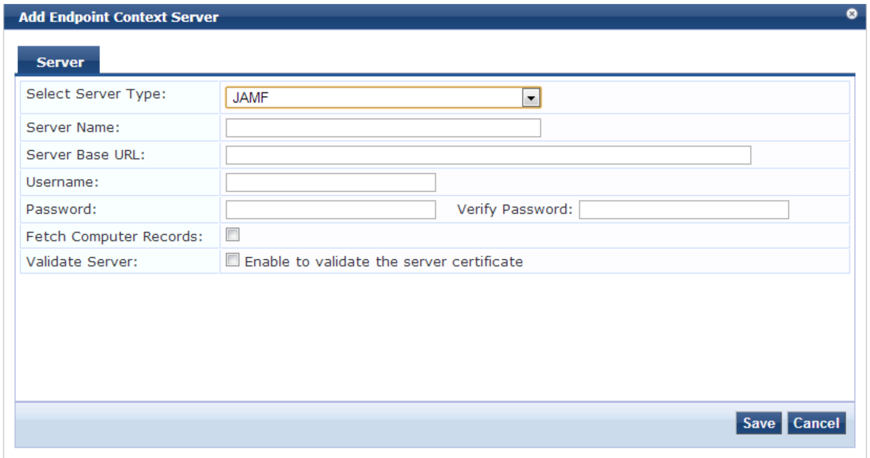
Table 241: *Add Generic HTTP Endpoint Context Server Actions tab Parameters*

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 389: *Add JAMF Endpoint Context Server tab*



Add Endpoint Context Server

Server

Select Server Type: JAMF

Server Name:

Server Base URL:

Username:

Password: Verify Password:

Fetch Computer Records: □

Validate Server: □ Enable to validate the server certificate

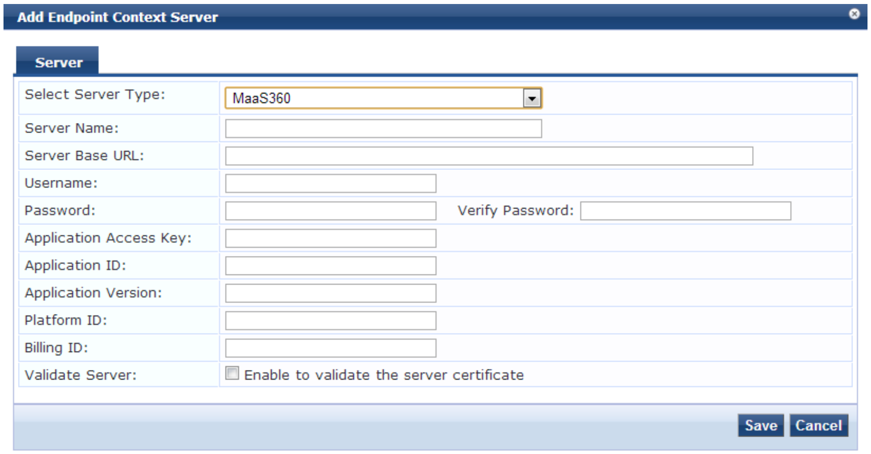
Table 242: *Add JAMF Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	Policy Manager appliance location and contact information.
Server Name:	V1, V2C or V3.
Server Base URL:	Read community string.
Username:	Username to use for SNMP v3 communication.
Password:	One of NOAUTH_NOPRIV (no authentication or privacy), AUTH_NOPRIV (authenticate, but no privacy), or AUTH _PRIV (authenticate and keep the communication private).
Fetch Computer Records	Authentication protocol (MD5 or SHA) and key.
Validate Server:	

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 390: *Add MaaS360 Endpoint Context Server tab*



Select Server Type: MaaS360

Server Name:

Server Base URL:

Username:

Password: Verify Password:

Application Access Key:

Application ID:

Application Version:

Platform ID:

Billing ID:

Validate Server: □ Enable to validate the server certificate

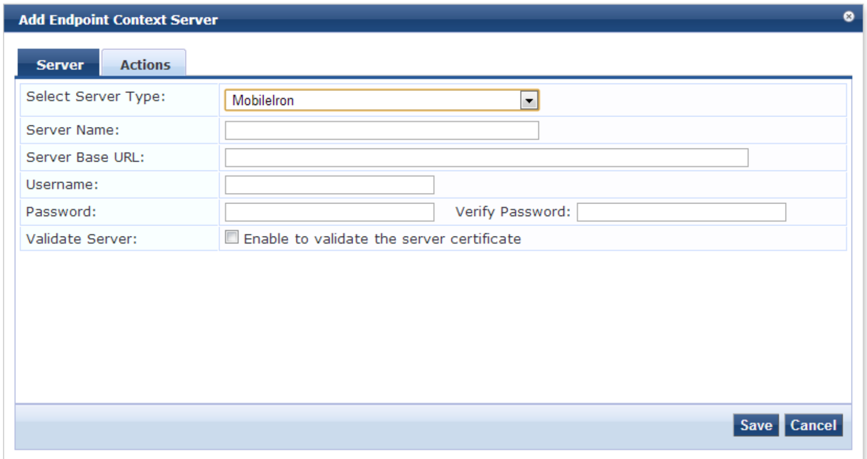
Table 243: *Add MaaS360 Endpoint Context Server tab Parameters*

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.
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 391: *Add MobileIron Endpoint Context Server tab*



Add Endpoint Context Server

Select Server Type: MobileIron

Server Name:

Server Base URL:

Username:

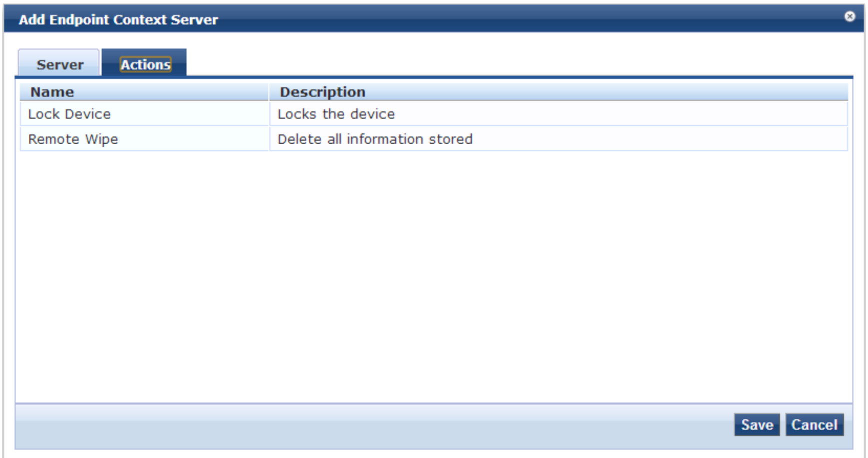
Password: Verify Password:

Validate Server: □ Enable to validate the server certificate

Table 244: *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.
Password:	Enter the password.
Verify Password:	Re-enter the password.
Validate Server:	Click to enable validation of the server.

Figure 392: *Add MobileIron Endpoint Context Server Actions tab*



Name	Description
Lock Device	Locks the device
Remote Wipe	Delete all information stored

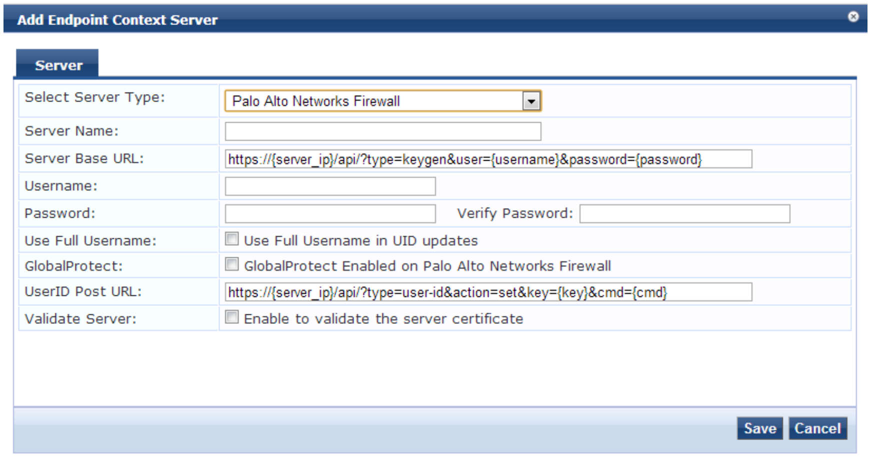
Table 245: *Add MobileIron Endpoint Context Server Actions tab Parameter Description*

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 393: *Add Palo Alto Networks Firewall tab*



Select Server Type:	Palo Alto Networks Firewall
Server Name:	
Server Base URL:	https://{server_ip}/api/?type=keygen&user={username}&password={password}
Username:	
Password:	Verify Password:
Use Full Username:	□ Use Full Username in UID updates
GlobalProtect:	□ GlobalProtect Enabled on Palo Alto Networks Firewall
UserID Post URL:	https://{server_ip}/api/?type=user-id&action=set&key={key}&cmd={cmd}
Validate Server:	□ Enable to validate the server certificate

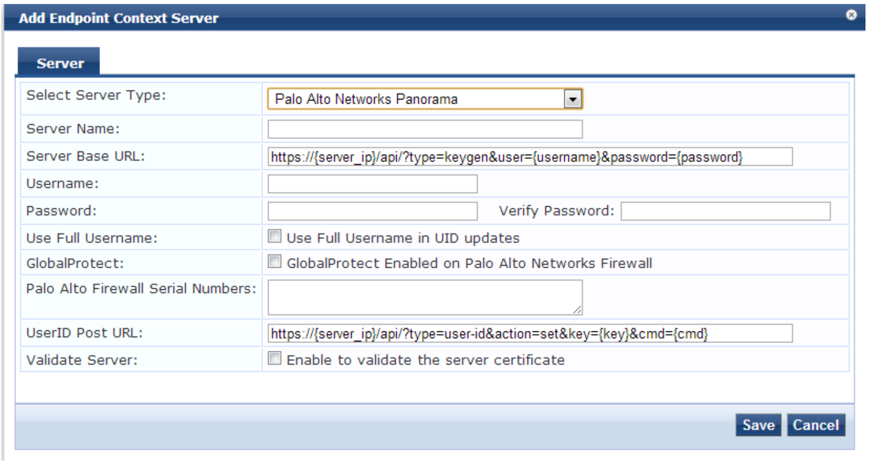
Table 246: *Add Palo Alto Networks Firewall tab Parameters*

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 394: *Palo Alto Networks Panorama Endpoint Context Server tab*



Select Server Type:	Palo Alto Networks Panorama
Server Name:	
Server Base URL:	https://{server_ip}/api/?type=keygen&user={username}&password={password}
Username:	
Password:	Verify Password:
Use Full Username:	□ Use Full Username in UID updates
GlobalProtect:	□ GlobalProtect Enabled on Palo Alto Networks Firewall
Palo Alto Firewall Serial Numbers:	
UserID Post URL:	https://{server_ip}/api/?type=user-id&action=set&key={key}&cmd={cmd}
Validate Server:	□ Enable to validate the server certificate

Table 247: *Palo Alto Networks Panorama Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	Palo Alto Networks Panorama.

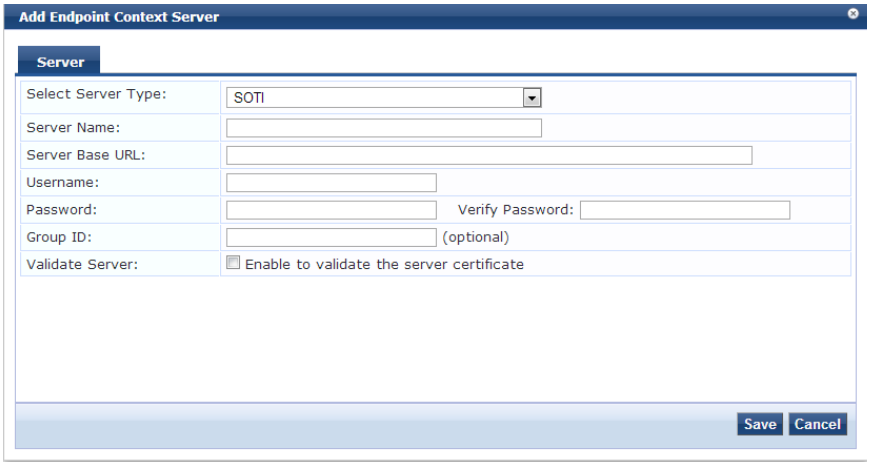
Table 247: *Palo Alto Networks Panorama Endpoint Context Server tab Parameters (Continued)*

Parameter	Description
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 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 395: *Add SOTI Endpoint Context Server tab*



Select Server Type:	SOTI
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Group ID:	(optional)
Validate Server:	□ Enable to validate the server certificate

Table 248: *Add SOTI Endpoint Context Server tab Parameters*

Parameter	Description
Select Server Type:	SOTI.

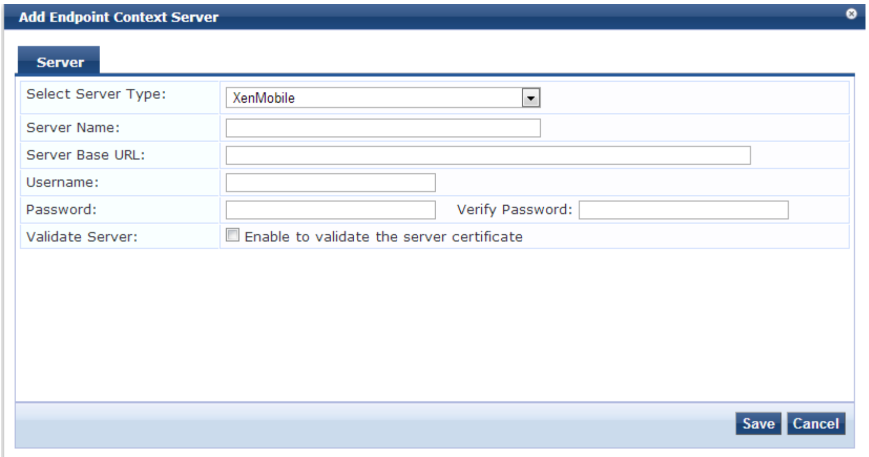
Table 248: *Add SOTI Endpoint Context Server tab Parameters (Continued)*

Parameter	Description
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 396: *Add XenMobile Endpoint Context Server tab*



Add Endpoint Context Server

Server

Select Server Type:	XenMobile
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Validate Server:	☐ Enable to validate the server certificate

Table 249: *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.

Table 249: *Add XenMobile Endpoint Context Server tab Parameter Description (Continued)*

Parameter	Description
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 390
- "Creating a Self-Signed Certificate" on page 392
- "Exporting a Server Certificate" on page 395
- "Importing a Server Certificate" on page 395

Server Certificate Page Overview

The page interface controls that are not dependent on the Server Certificate Type are described below.

Table 250: *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.

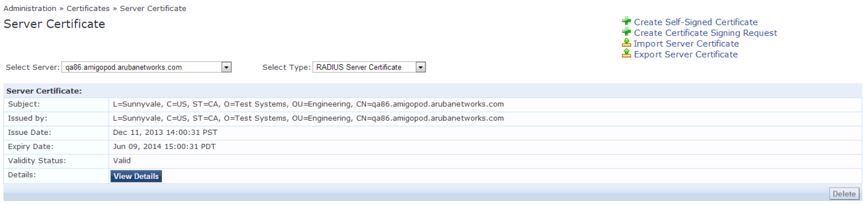
Table 250: *Server Certificate Interfaces (Common) (Continued)*

Parameter	Description
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 397: *Server Certificate Page (RADIUS Server Certificate Type)*



Administration » Certificates » Server Certificate

Server Certificate

Create Self-Signed Certificate
Create Certificate Signing Request
Import Server Certificate
Export Server Certificate

Select Server: qa86.amigopod.arubanetworks.com

Select Type: RADIUS Server Certificate

Server Certificate:

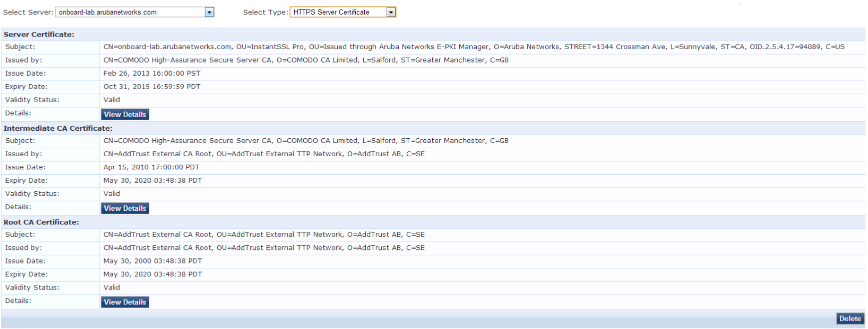
Subject:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issued by:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issue Date:	Dec 11, 2013 14:00:31 PST
Expiry Date:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Details:	View Details

Table 251: *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.



Select Server: onboard-lab.arubanetworks.com

Select Type: HTTPS Server Certificate

Server Certificate:	
Subject:	CN=onboard-lab.arubanetworks.com, OU=InstantSSL Pro, OU=Issued through Aruba Networks E-PKI Manager, O=Aruba Networks, STREET=1344 Crossman Ave, L=Sunnyvale, ST=CA, OID.2.5.4.17=94089, C=US
Issued by:	CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issue Date:	Feb 26, 2013 16:00:00 PST
Expiry Date:	Oct 31, 2015 16:59:59 PDT
Validity Status:	Valid
Details:	View Details
Intermediate CA Certificate:	
Subject:	CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issued by:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issue Date:	Apr 15, 2010 17:00:00 PDT
Expiry Date:	May 30, 2020 03:48:38 PDT
Validity Status:	Valid
Details:	View Details
Root CA Certificate:	
Subject:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issued by:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issue Date:	May 30, 2000 03:48:38 PDT
Expiry Date:	May 30, 2020 03:48:38 PDT
Validity Status:	Valid
Details:	View Details

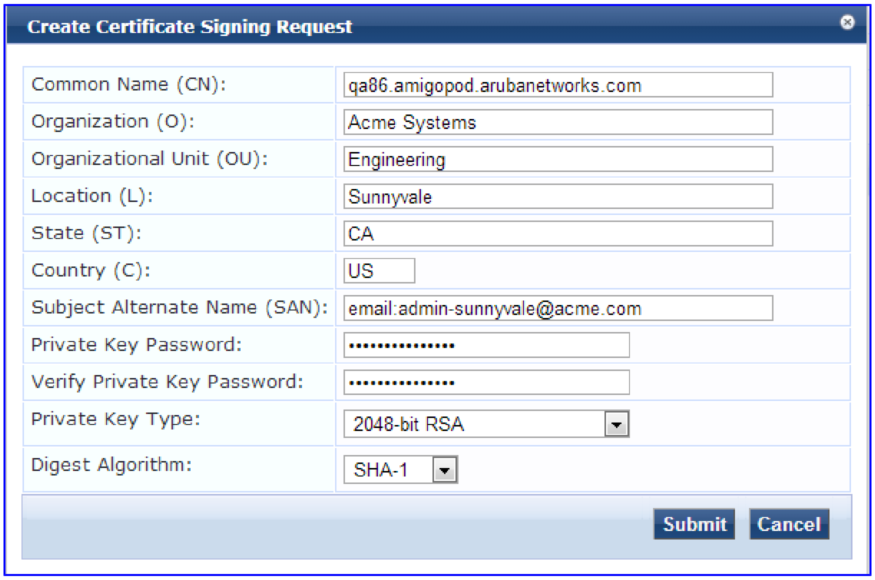
Table 252: *Server Certificate Page (HTTPS Server Certificate Type) Parameters*

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.

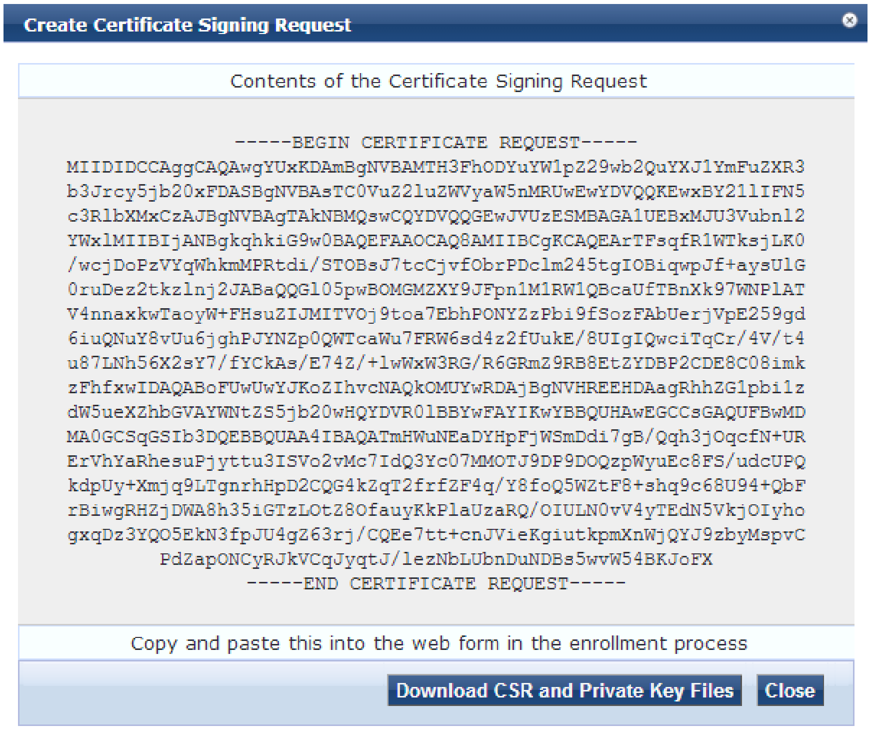
Figure 398: *Create Certificate Signing Request*



Common Name (CN):	qa86.amigopod.arubanetworks.com
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	Sunnyvale
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin-sunnyvale@acme.com
Private Key Password:	•••••••••••••••
Verify Private Key Password:	•••••••••••••••
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-1

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.

Figure 399: *Generated Certificate Signing Request*



Create Certificate Signing Request
Download CSR and Private Key Files
Close

Contents of the Certificate Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDIDCCAggCAQAwgYUxKDAmBgNVBAMTH3FhODYuYW1pZ29wb2QuYXJ1YmFuZXR3
b3Jrcy5jb20xFDASBgNVBAsTC0VuZ2luZWVyaW5nMRUwEwYDVQQKEwxBY21lIFN5
c3RlbXMxCzAJBgNVBAgTAkNBMQswCQYDVQQGEwJVUzESMBAGA1UEBxMJU3Vubnl2
YWxlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArTFsqfR1WTksjLK0
/wcjDoPzVYqWhkmMPRtdi/STOBsJ7tcCjvfObrPDclm245tgIOBiqwpJf+aysUlG
0ruDez2tkzlnj2JABaQQGl05pwBOMGMZXY9JFpn1M1RW1QBcaUfTBnXk97WNPlAT
V4nnaxkwTaoyW+FHsuZIJMITVOj9toa7EbhPONYZzPbi9fSozFAbUerjVpE259gd
6iuQNuY8vUu6jghPJYNZp0QWTcaWu7FRW6sd4z2fUukE/8UIgIQwciTqCr/4V/t4
u87LNh56X2sY7/fYCkAs/E74Z/+lwWxW3RG/R6GRmZ9RB8EtZYDBP2CDE8C08imk
zFhfxwIDAQABoFUwUwYJKoZIhvcNAQkOMUYwRDAjBgNVHREEHDAagRhhZG1pbilz
dW5ueXZhbGVAYWNtZS5jb20wHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMD
MA0GCSqGSIb3DQEBBQUAA4IBAQATmHWuNEaDYHpFjWSmDdi7gB/Qqh3jOqcfN+UR
ErVhYaRhesuPjyttu3ISVo2vMc7IdQ3Yc07MMOTJ9DP9DOQzpWyuEc8FS/udcUPQ
kdpUy+Xmjq9LTgnrhHpD2CQG4kZqT2frfZF4q/Y8foQ5WZtF8+shq9c68U94+QbF
rBiwgRHZjDWA8h35iGTzLOtZ8OfauyKkPlaUzaRQ/OIULN0vV4yTEdN5VkjOIyho
gxqDz3YQO5EkN3fpJU4gZ63rj/CQEe7tt+cnJVieKgiutkpmXnWjQYJ9zbyMspvC
PdZapONCyRJkVCqJyqtJ/lezNbLUbnDuNDBs5wvW54BKJoFX
-----END CERTIFICATE REQUEST-----
```

Copy and paste this into the web form in the enrollment process

Table 253: *Create Certificate Signing Request Parameters*

Parameter	Description
Common Name (CN):	Name associated with this entity. This can be a host name, IP address or other meaningful name. This field is required. The default is the fully-qualified domain name (FQDN).
Organization (O):	Name of the organization. This field is optional.
Organizational Unit (OU):	Name of a department, division, section, or other meaningful name. This field is optional.
Location (L):	State, country, and/or another meaningful location. These fields are optional.
State (ST):	
Country (C):	
Subject Alternate Name (SAN):	Alternative names for the specified Common Name. **NOTE:** If this field is used, then SAN has to be in the form email:*email_address*, URI:*uri*, IP:ip_*address*, dns:*dns_name*, or rid:*id*. This field is optional.

Table 253: *Create Certificate Signing Request Parameters (Continued)*

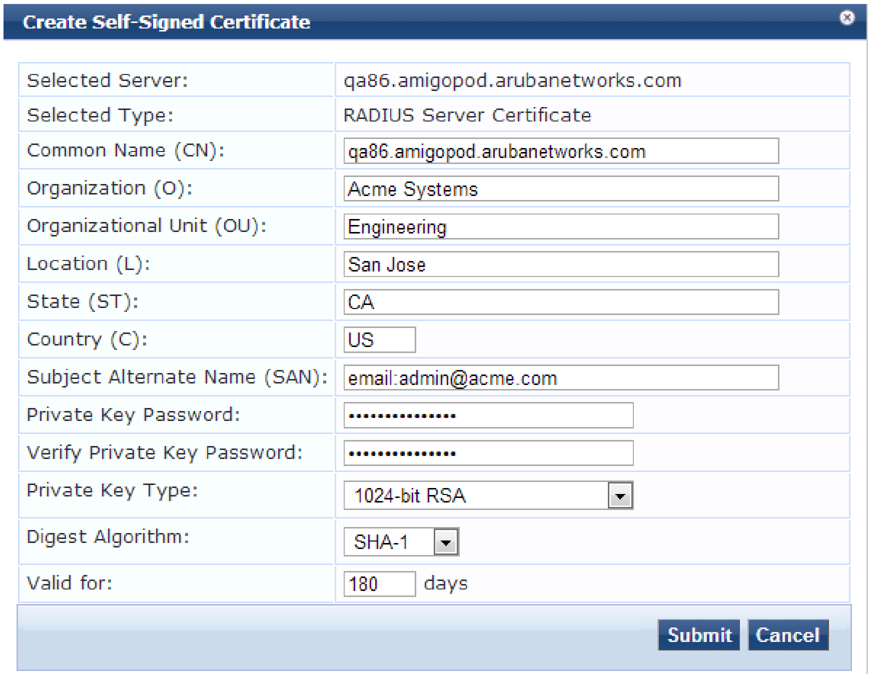
Parameter	Description
Private Key Password:	Specify and verify password. This field is required.
Verify Private Key Password:	
Key Length:	Select length for the generated private key: **512**, **1024**, or **2048**. The default is 2048.
Digest Algorithm:	Select message digest algorithm to use: **SHA-1**, **MD5**, and **MD2**.
Submit:	Click this button to generate a Certificate Signing Request, as shown above.
Download CSR and Private Key Files/Close:	The page displays the contents of the Certificate Signing Request, as shown above. Click **Download CSR and Private Key Files** to save the Certificate Signing Request file and the private key password file.

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, either Backend Services or click the **Create Self-Signed Certificate** link. This opens the **Create Self-Signed Certificate** form.

Figure 400: *Create Self-Signed Certificate Page*



Create Self-Signed Certificate

Selected Server:	qa86.amigopod.arubanetworks.com
Selected Type:	RADIUS Server Certificate
Common Name (CN):	qa86.amigopod.arubanetworks.com
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	San Jose
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin@acme.com
Private Key Password:	•••••••••••••••
Verify Private Key Password:	••••••••••••••
Private Key Type:	1024-bit RSA
Digest Algorithm:	SHA-1
Valid for:	180 days

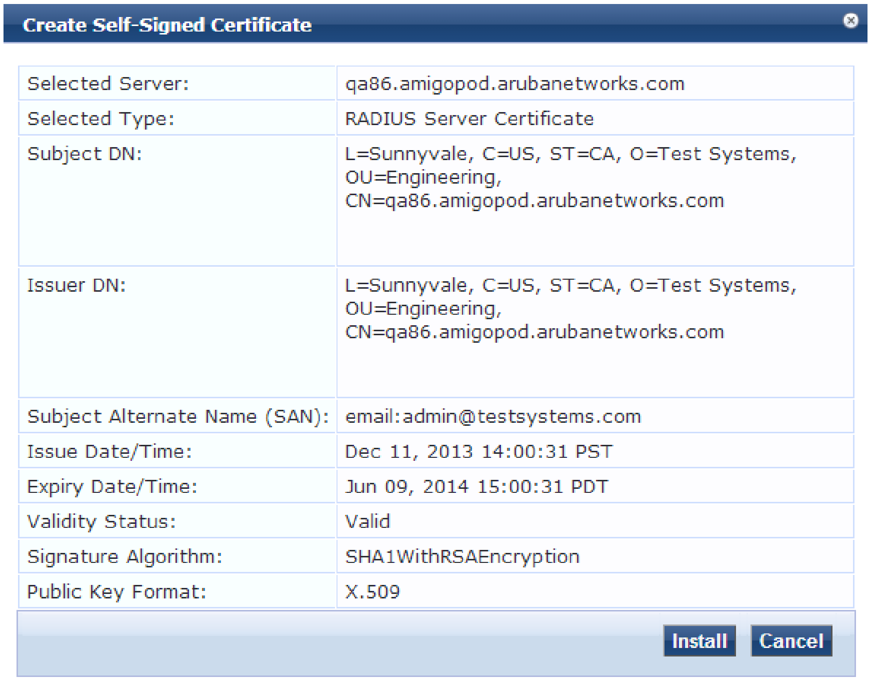
Table 254: *Create Self-Signed Certificate Page Parameters*

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 selected for the server.
Common Name (CN):	Name associated with this entity. This can be a host name, IP address or other meaningful name. This field is required.
Organization (O):	Name of the organization. This field is optional.
Organizational Unit (OU):	Name of a department, division, section, or other meaningful name. This field is optional.
State (ST):	State, country, and/or another meaningful location. These fields are optional.
Country (C):	
Location (L):	
Subject Alternate Name (SAN):	Alternative names for the specified Common Name. **NOTE:** If this field is used, then SAN has to be in the form email:*email_address*, URI:*uri*, IP:ip_*address*, dns:*dns_name*, or rid:*id*. This field is optional.
Private Key Password:	Enter and re-enter the Private Key Password.
Verify Private Key Password:	
Private Key Type:	If you selected the RADIUS Server Certificate type for the server, select from: ● 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 message digest algorithm to use: **SHA-1**, **MD5**, and **MD2**.
Valid for:	Specify duration in days.
Submit/Cancel:	On submit, Policy Manager generates a popup containing the self-signed certificate. Click on the **Install** button to install the certificate on the selected server. **NOTE:** All services are restarted; you must relogin into the UI to continue.

Installing the self-signed certificate

After you click **Submit**, you will be prompted to install the self-signed certificate. The pop-up displays a summary of the values selected on the Create Self-Signed Certificate page.

Figure 401: *Install Self Signed Certificate*



Create Self-Signed Certificate

Selected Server:	qa86.amigopod.arubanetworks.com
Selected Type:	RADIUS Server Certificate
Subject DN:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issuer DN:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Subject Alternate Name (SAN):	email:admin@testsystems.com
Issue Date/Time:	Dec 11, 2013 14:00:31 PST
Expiry Date/Time:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Signature Algorithm:	SHA1WithRSAEncryption
Public Key Format:	X.509

Table 255: *Install Self-Signed Certificate Page Parameters*

Parameter	Description
Selected Server:	Displays the name of the server selected on the first 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 configuration.
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 whether the certificate is valid or invalid.
Signature Algorithm:	Displays the Digest Algorithm and Private Key Type selected during certificate configuration.

Table 255: *Install Self-Signed Certificate Page Parameters (Continued)*

Parameter	Description
Submit/Cancel:	After you click Install, Policy Manager generates a message about the status of the certificate installation. If the installation is successful the page displays "Server Certificate updated successfully. Please login again to continue..." **NOTE:** Because all services are restarted after successful certificate installation, you must click **Logout** and login to the CPPM client to continue.

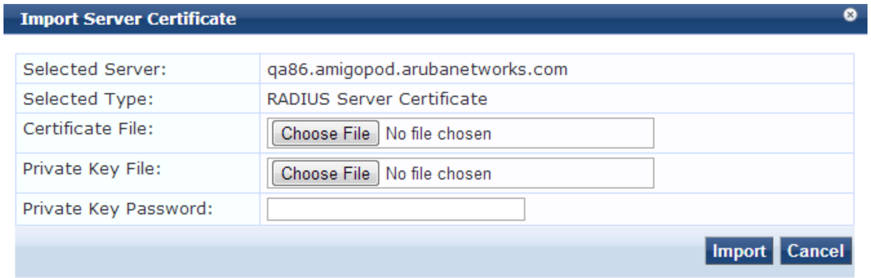
Exporting a Server Certificate

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 402: *Import Server Certificate*



Selected Server:	qa86.amigopod.arubanetworks.com
Selected Type:	RADIUS Server Certificate
Certificate File:	No file chosen
Private Key File:	No file chosen
Private Key Password:	

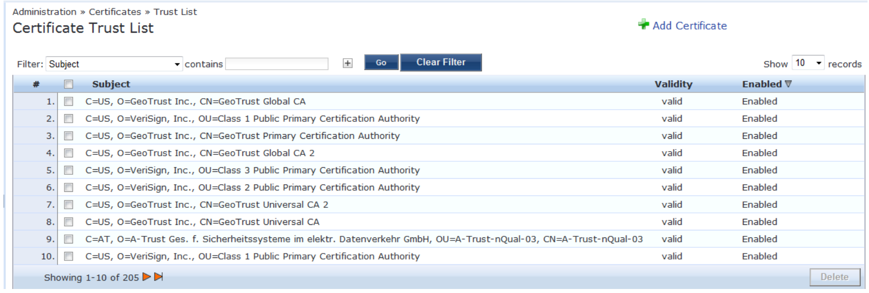
Table 256: *Import Server Certificate Parameters*

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 (CAs), navigate to **Administration** > **Certificates** > **Certificate Trust List**. To add a certificate, click **Add Certificate**; to delete a certificate, select the check box to the left of the certificate and then click **Delete.**

Figure 403: *Certificate Trust List*



Administration » Certificates » Trust List

Certificate Trust List

#	□	Subject	Validity	Enabled ▽
1.	□	C=US, O=GeoTrust Inc., CN=GeoTrust Global CA	valid	Enabled
2.	□	C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority	valid	Enabled
3.	□	C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority	valid	Enabled
4.	□	C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2	valid	Enabled
5.	□	C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority	valid	Enabled
6.	□	C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority	valid	Enabled
7.	□	C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA 2	valid	Enabled
8.	□	C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA	valid	Enabled
9.	□	C=AT, O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, OU=A-Trust-nQual-03, CN=A-Trust-nQual-03	valid	Enabled
10.	□	C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority	valid	Enabled

Showing 1-10 of 205

Table 257: *Certificate Trust List*

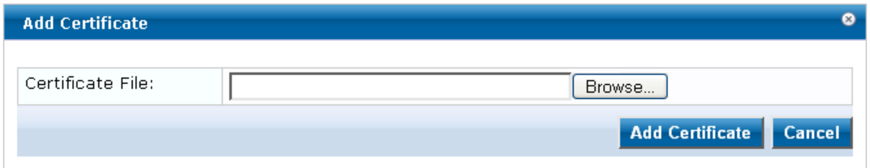
Parameter	Description
Subject	The Distinguished Name (DN) of the subject field in the certificate.
Validity	This indicates whether the CA certificate has expired.
Enabled	Whether this CA certificate is enabled or not.

To view the details of the certificate, click on a certificate row. 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 Certificate** link.

Figure 404: *Add Certificate*



Add Certificate

Certificate File:

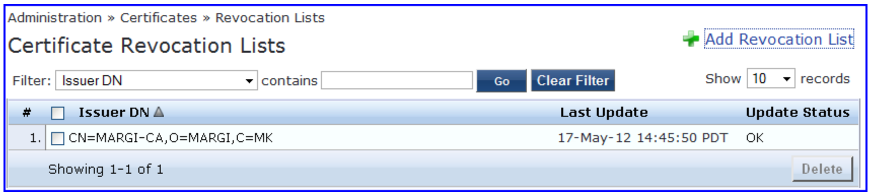
Table 258: *Add Certificate*

Parameter	Description
Certificate File:	Browse to select certificate file.
Add Certificate/Cancel	Click **Add Certificate** to commit, or **Cancel** to dismiss the popup.

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 405: *Revocation Lists*



Administration » Certificates » Revocation Lists

Certificate Revocation Lists

Filter: Issuer DN contains

Show 10 records

#	□	Issuer DN	Last Update	Update Status
1.	□	CN=MARGI-CA,O=MARGI,C=MK	17-May-12 14:45:50 PDT	OK

Showing 1-1 of 1

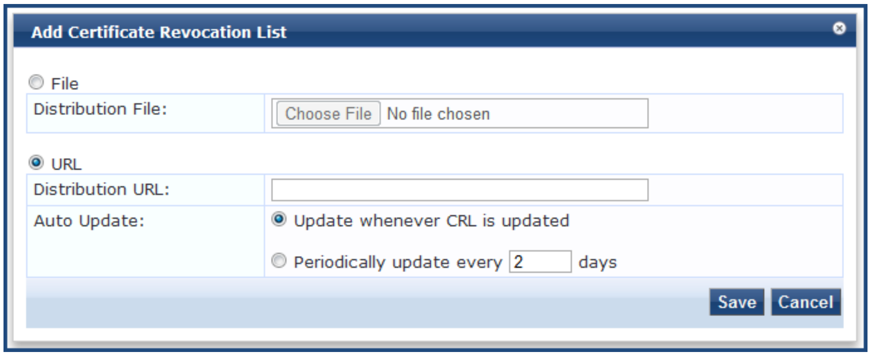
Table 259: *Revocation Lists*

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 406: *Add Certificate Revocation List Page*



Add Certificate Revocation List

○ File

Distribution File: Choose File No file chosen

● URL

Distribution URL:

Auto Update: ● Update whenever CRL is updated

○ Periodically update every 2 days

Table 260: *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.

Parameter	Description
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

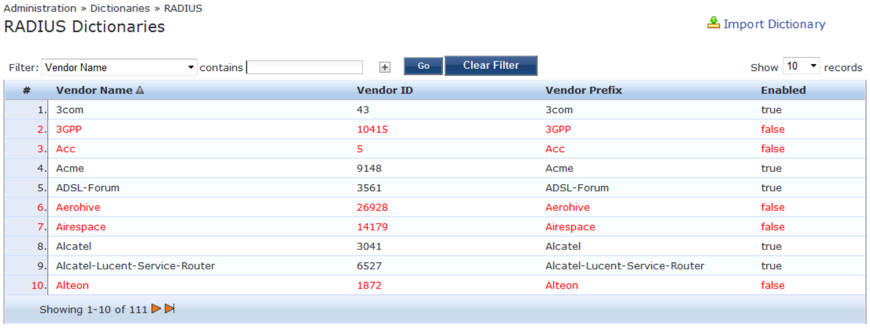
Select one of the following topics to find more information about dictionaries.

- "RADIUS Dictionary" on page 398
- "Posture Dictionary" on page 400
- "TACACS+ Services Dictionary" on page 401
- "Fingerprints Dictionary" on page 402
- "Attributes Dictionary" on page 403
- "Applications Dictionary" on page 406
- "Endpoint Context Server Actions" on page 406

RADIUS Dictionary

RADIUS dictionaries are available on the **Administration > Dictionaries > RADIUS**. This page includes the list of available vendor dictionaries.

Figure 407: *RADIUS Dictionaries*

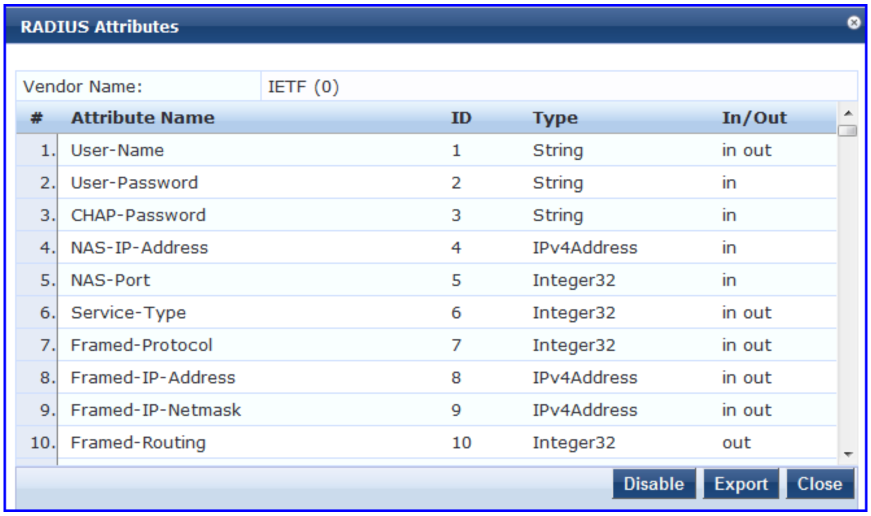


#	Vendor Name	Vendor ID	Vendor Prefix	Enabled
1.	3com	43	3com	true
2.	3GPP	10415	3GPP	false
3.	Acc	5	Acc	false
4.	Acme	9148	Acme	true
5.	ADSL-Forum	3561	ADSL-Forum	true
6.	Aerohive	26928	Aerohive	false
7.	Airespace	14179	Airespace	false
8.	Alcatel	3041	Alcatel	true
9.	Alcatel-Lucent-Service-Router	6527	Alcatel-Lucent-Service-Router	true
10.	Alteon	1872	Alteon	false

Showing 1-10 of 111

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 408: *RADIUS IETF Dictionary Attributes*



Vendor Name:	IETF (0)		

#	Attribute Name	ID	Type	In/Out
1.	User-Name	1	String	in out
2.	User-Password	2	String	in
3.	CHAP-Password	3	String	in
4.	NAS-IP-Address	4	IPv4Address	in
5.	NAS-Port	5	Integer32	in
6.	Service-Type	6	Integer32	in out
7.	Framed-Protocol	7	Integer32	in out
8.	Framed-IP-Address	8	IPv4Address	in out
9.	Framed-IP-Netmask	9	IPv4Address	in out
10.	Framed-Routing	10	Integer32	out

Table 261: *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 Dictionary** 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 409: *Import RADIUS Dictionary*

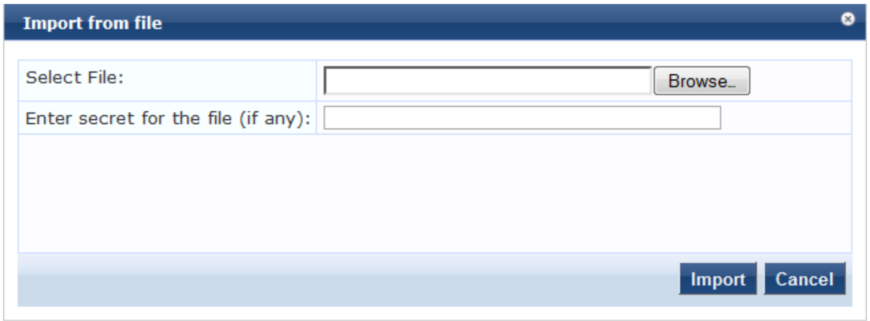


Table 262: *Import RADIUS Dictionary*

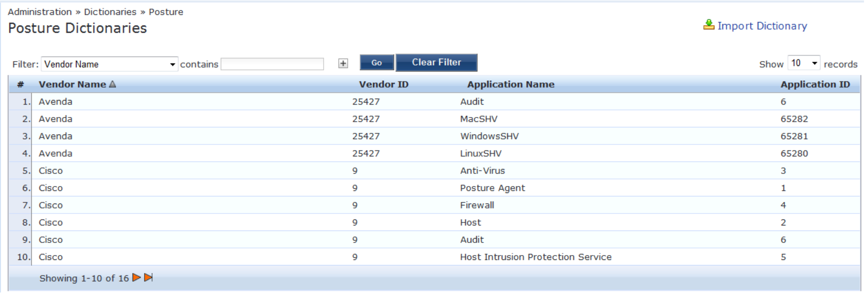
Parameter	Description
Select File	Browse to select the file that you want to import.
Enter secret for the file (if any)	If the file that you want to import is password protected, enter the secret here.

Posture Dictionary

To add a vendor posture dictionary, click on Import Dictionary. 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 410: *Posture Dictionaries*



Administration » Dictionaries » Posture

Posture Dictionaries

Filter: Vendor Name contains

Show 10 records

#	Vendor Name	Vendor ID	Application Name	Application ID
1.	Avenda	25427	Audit	6
2.	Avenda	25427	MacSHV	65282
3.	Avenda	25427	WindowsSHV	65281
4.	Avenda	25427	LinuxSHV	65280
5.	Cisco	9	Anti-Virus	3
6.	Cisco	9	Posture Agent	1
7.	Cisco	9	Firewall	4
8.	Cisco	9	Host	2
9.	Cisco	9	Audit	6
10.	Cisco	9	Host Intrusion Protection Service	5

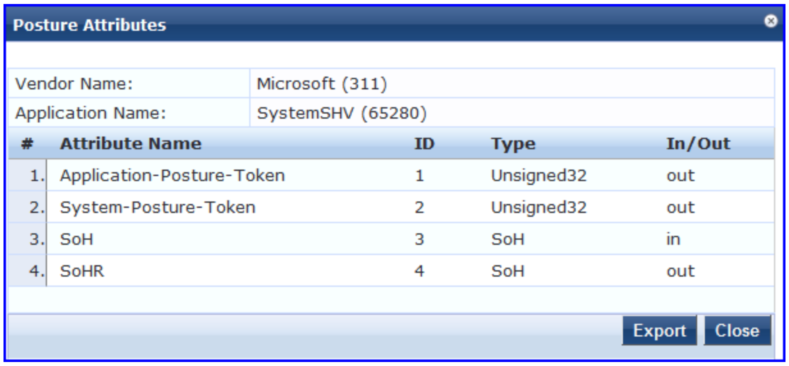
Showing 1-10 of 16

Table 263: *Posture*

Parameter	Description
Import Dictionary	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 411: *Posture Attributes Page*



Posture Attributes

Vendor Name: Microsoft (311)

Application Name: SystemSHV (65280)

#	Attribute Name	ID	Type	In/Out
1.	Application-Posture-Token	1	Unsigned32	out
2.	System-Posture-Token	2	Unsigned32	out
3.	SoH	3	SoH	in
4.	SoHR	4	SoH	out

Table 264: *Posture Attributes Parameters*

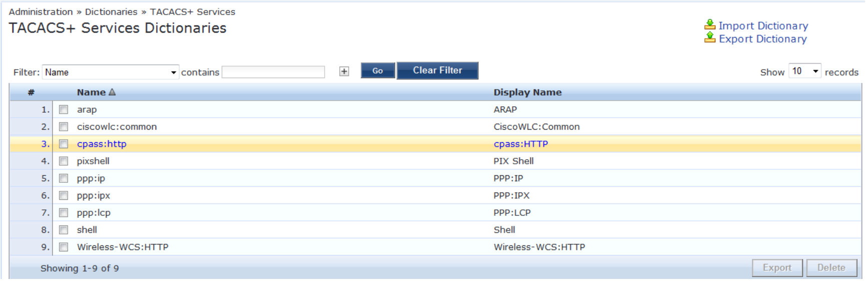
Parameter	Description
Export	Click to save the posture dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.

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 Dictionary** 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 412: *TACACS+ Services Dictionaries Page*



Administration » Dictionaries » TACACS+ Services

TACACS+ Services Dictionaries

#		Name △	Display Name
1.	□	arap	ARAP
2.	□	ciscowlc:common	CiscoWLC:Common
3.	□	cpass:http	cpass:HTTP
4.	□	pixshell	PIX Shell
5.	□	ppp:ip	PPP:IP
6.	□	ppp:ipx	PPP:IPX
7.	□	ppp:lcp	PPP:LCP
8.	□	shell	Shell
9.	□	Wireless-WCS:HTTP	Wireless-WCS:HTTP

Showing 1-9 of 9

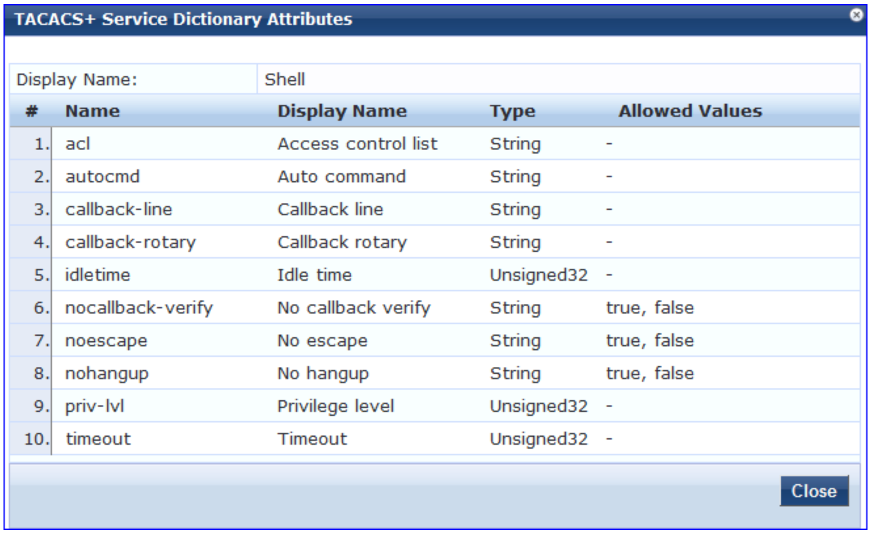
Table 265: *TACACS+ Services Dictionaries Page Parameters*

Parameter	Description
Import Dictionary	Click to open the **Import Dictionary** popup. Import the dictionary (XML file).
Export Dictionary	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 413: *Shell Service Dictionary Attributes*



TACACS+ Service Dictionary Attributes

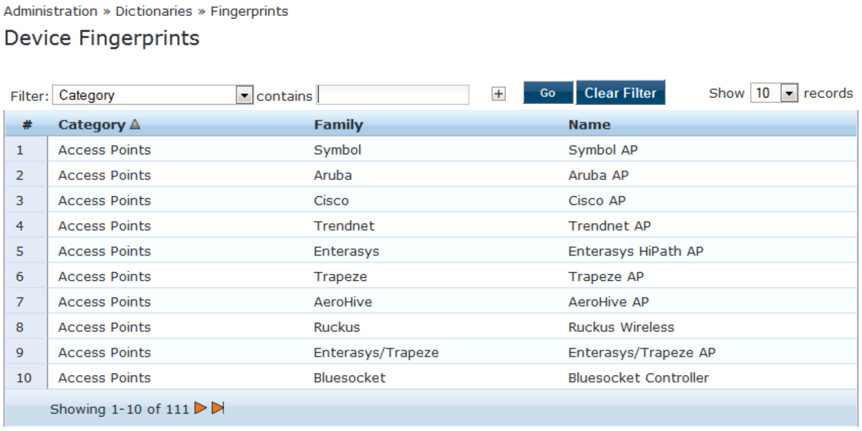
Display Name:	Shell		

#	Name	Display Name	Type	Allowed Values
1.	acl	Access control list	String	-
2.	autocmd	Auto command	String	-
3.	callback-line	Callback line	String	-
4.	callback-rotary	Callback rotary	String	-
5.	idletime	Idle time	Unsigned32	-
6.	nocallback-verify	No callback verify	String	true, false
7.	noescape	No escape	String	true, false
8.	nohangup	No hangup	String	true, false
9.	priv-lvl	Privilege level	Unsigned32	-
10.	timeout	Timeout	Unsigned32	-

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 411 for more information.)

Figure 414: *Device Fingerprints Page*



Administration » Dictionaries » Fingerprints

Device Fingerprints

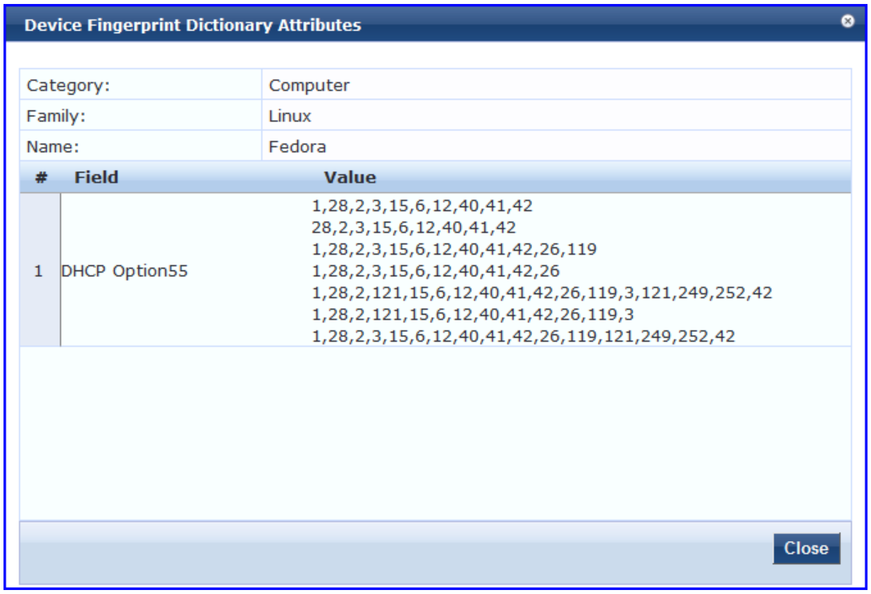
Filter: Category contains

#	Category	Family	Name
1	Access Points	Symbol	Symbol AP
2	Access Points	Aruba	Aruba AP
3	Access Points	Cisco	Cisco AP
4	Access Points	Trendnet	Trendnet AP
5	Access Points	Enterasys	Enterasys HiPath AP
6	Access Points	Trapeze	Trapeze AP
7	Access Points	AeroHive	AeroHive AP
8	Access Points	Ruckus	Ruckus Wireless
9	Access Points	Enterasys/Trapeze	Enterasys/Trapeze AP
10	Access Points	Bluesocket	Bluesocket Controller

Showing 1-10 of 111

You can click on a line in the Device Fingerprints list to drill down and view additional details about the category.

Figure 415: *Device Fingerprint Dictionary Attributes Page*



Device Fingerprint Dictionary Attributes

Category:	Computer
Family:	Linux
Name:	Fedora

#	Field	Value
1	DHCP Option55	1,28,2,3,15,6,12,40,41,42 28,2,3,15,6,12,40,41,42 1,28,2,3,15,6,12,40,41,42,26,119 1,28,2,3,15,6,12,40,41,42,26 1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42 1,28,2,121,15,6,12,40,41,42,26,119,3 1,28,2,3,15,6,12,40,41,42,26,119,121,249,252,42

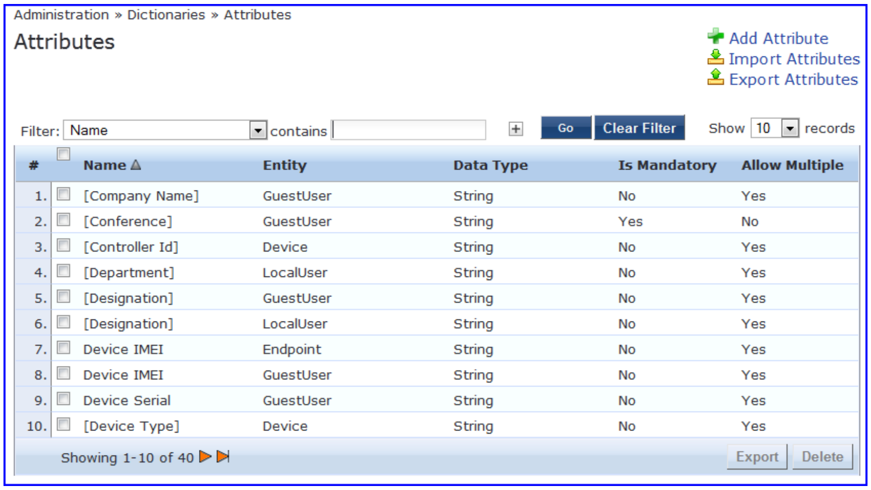
Attributes Dictionary

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:

- "Adding Attributes" on page 404
- "Import Attributes" on page 405
- "Export Attributes" on page 405
- "Export" on page 405

Figure 416: *Attributes page*



Administration » Dictionaries » Attributes

Attributes

Filter: Name contains

Show 10 records

#		Name △	Entity	Data Type	Is Mandatory	Allow Multiple
1.	□	[Company Name]	GuestUser	String	No	Yes
2.	□	[Conference]	GuestUser	String	Yes	No
3.	□	[Controller Id]	Device	String	No	Yes
4.	□	[Department]	LocalUser	String	No	Yes
5.	□	[Designation]	GuestUser	String	No	Yes
6.	□	[Designation]	LocalUser	String	No	Yes
7.	□	Device IMEI	Endpoint	String	No	Yes
8.	□	Device IMEI	GuestUser	String	No	Yes
9.	□	Device Serial	GuestUser	String	No	Yes
10.	□	[Device Type]	Device	String	No	Yes

Showing 1-10 of 40

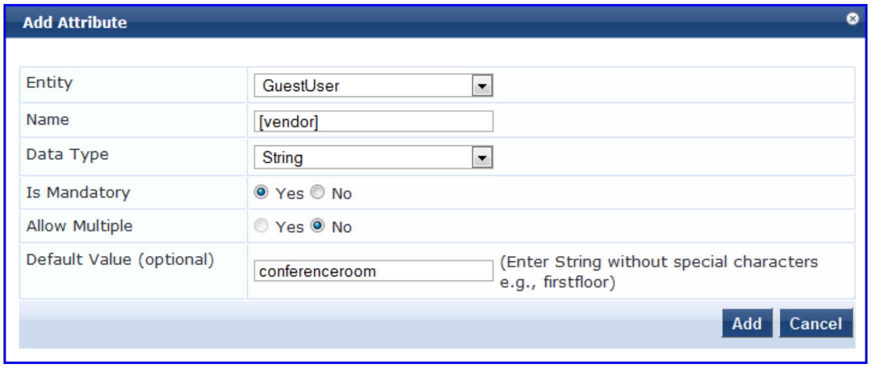
Table 266: *Attributes Page Parameters*

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 Attribute** in the upper right portion of the page.

Figure 417: *Add Attributes Page*



Add Attribute

Entity	GuestUser
Name	[vendor]
Data Type	String
Is Mandatory	● Yes ○ No
Allow Multiple	○ Yes ● No
Default Value (optional)	conferenceroom (Enter String without special characters e.g., firstfloor)

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 267: *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.

Table 267: *Attribute Setting Parameters (Continued)*

Parameter	Description
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**.

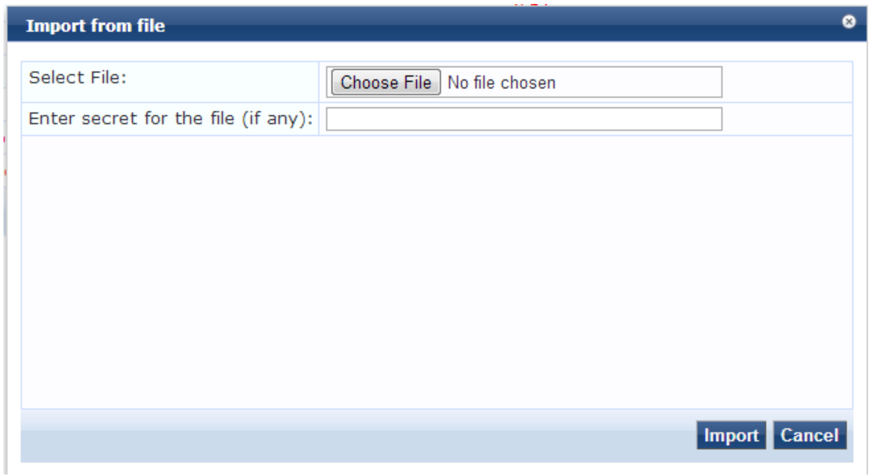
Import Attributes

Select **Import Attributes** on the upper right portion of the page.

NOTE

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 418: *Import from file Page*



Import from file

Select File: Choose File No file chosen

Enter secret for the file (if any):

Table 268: *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 Attributes** 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

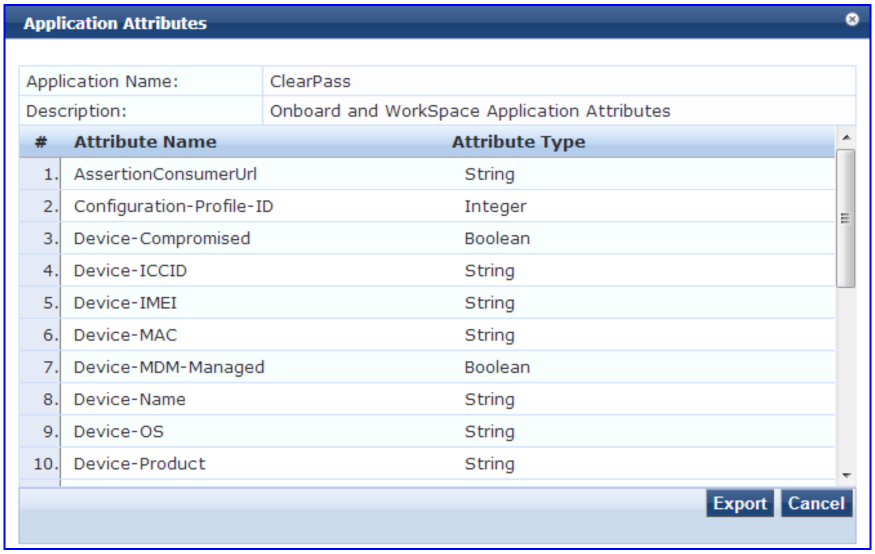
Application dictionaries define the attributes of the Onboard and WorkSpacePolicy Manager applications and the type of each attribute. When Policy Manager is used as the Policy Definition Point (PDP), it uses the information in these dictionaries to validate the attributes and data types sent in a WEB-AUTH request.

You can:

- "View an application dictionary" on page 406
- "Delete an application dictionary" on page 406
- "Importing" on page 21
- "Exporting" on page 22

View an application dictionary

1. Go to **Administration** > **Dictionaries** > **Applications**.
2. Click the name of an application. The Application Attributes dialog box appears.



Application Name:	ClearPass
Description:	Onboard and WorkSpace Application Attributes

#	Attribute Name	Attribute Type
1.	AssertionConsumerUrl	String
2.	Configuration-Profile-ID	Integer
3.	Device-Compromised	Boolean
4.	Device-ICCID	String
5.	Device-IMEI	String
6.	Device-MAC	String
7.	Device-MDM-Managed	Boolean
8.	Device-Name	String
9.	Device-OS	String
10.	Device-Product	String

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

You use the Context Server Actions dictionary to configure actions that are performed on endpoints, such as locking a device, triggering a remote or enterprise wipe, and so forth.

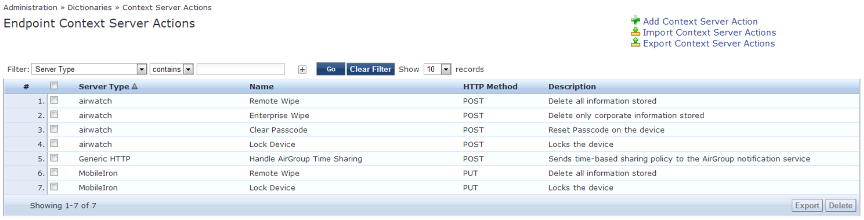
Click **Administration** > **Dictionaries** > **Endpoint Context Server Actions**.

The first page displays a report that shows data about all configured Endpoint Context Server Actions.

For more information, see:

- "Filter an Endpoint Context Server Action Report" on page 407
- "View Details About Endpoint Context Server Actions" on page 407
- "Add an Endpoint Context Server Action Item" on page 407
- "Import Context Server Actions" on page 408
- "Export Context Server Actions" on page 409

Figure 419: *Endpoint Context Server Actions Page*



Administration » Dictionaries » Context Server Actions

Endpoint Context Server Actions

Add Context Server Action
Import Context Server Actions
Export Context Server Actions

Filter: Server Type ▾ contains ▾ ⊞ Go Clear Filter Show 10 ▾ records

#	□	Server Type ▲	Name	HTTP Method	Description
1.	□	airwatch	Remote Wipe	POST	Delete all information stored
2.	□	airwatch	Enterprise Wipe	POST	Delete only corporate information stored
3.	□	airwatch	Clear Passcode	POST	Reset Passcode on the device
4.	□	airwatch	Lock Device	POST	Locks the device
5.	□	Generic HTTP	Handle AirGroup Time Sharing	POST	Sends time-based sharing policy to the AirGroup notification service
6.	□	MobileIron	Remote Wipe	PUT	Delete all information stored
7.	□	MobileIron	Lock Device	PUT	Locks the device

Showing 1-7 of 7

Table 269: *Endpoint Context Server Action Page Parameters*

Parameter	Description
Server Type	The server type configured when the server action was configured.
Name	The name of the action, such as Enterprise Wipe, Lock Device, and more.
HTTP Method	The HTTP method selected when the server action was configured.
Description	A description of the action, such as "Delete all information stored" if the configured action is Remote Wipe.

You can perform the following actions from the first page.

Filter 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. The filters are ServerType, Name, or HTTP method.
2. **Option**: Click the plus icon 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.

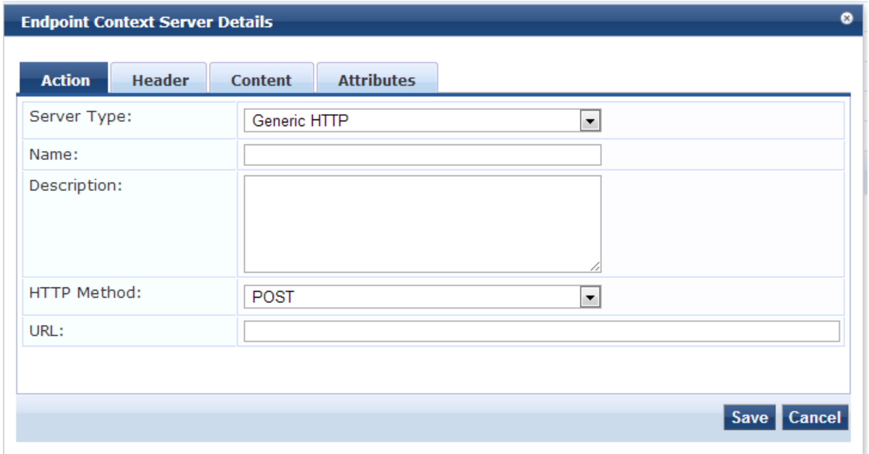
View Details About Endpoint Context Server Actions

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 an explanation of each field on each tab.

Add an Endpoint Context Server Action Item

Enter information in the tabs described in the following table. Click **Add** when you are done. To modify existing Endpoint Context Server Details, select a row and change detail, make any necessary changes, and then click **Save**.

Figure 420: *Endpoint Context Server Details Action tab*



Endpoint Context Server Details

Server Type:	Generic HTTP
Name:	
Description:	
HTTP Method:	POST
URL:	

Table 270: *Endpoint Context Server Action tab Parameters*

Parameter	Description
Action	Specifies the server type, name, description and HTTP Method. Enter the URL of the server.
Header	Specifies the key-value pairs to be included in the HTTP Header.
Content	Specifies a content-Type. Choose from CUSTOM, HTML, JSON, PLAIN, XML.
Attributes	Specifies the mapping for attributes used in the content to parameterized values from the request.

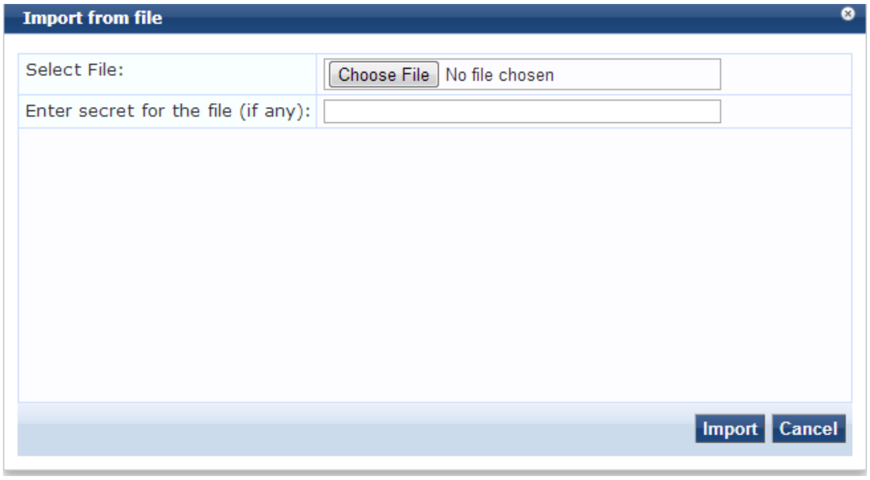
Import Context Server Actions

Select **Import Context Server Actions** on the upper right corner of the page.

NOTE

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 421: *Import Context Server Actions*



Import from file

Select File:	Choose File No file chosen
Enter secret for the file (if any):	

Table 271: *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 Attributes** on the upper right portion of the page.

> NOTE
>
> 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 272: *Export Content Server Action*

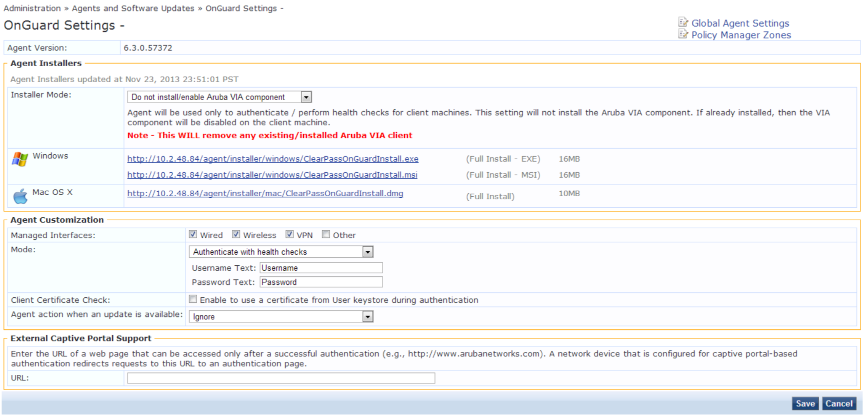
Parameter	Description
Export file with password protection	If you click No, the Secret Key and Verify Secret fields are not available. If you click Yes, enter the Secret Key information in the Secret Key field. The secret key that you enter is the same key that was used during Context Server configuration. Enter the Secret Key in the Verify Secret field.
Export/Cancel	Click **Export** to commit, or **Cancel** to dismiss the popup.

OnGuard Settings

Navigate to the **Administration** > **Agents and Software Updates** > **OnGuard Settings** page.

Use this page 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 placed 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.

Figure 422: *OnGuard Settings*



Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings -

Agent Version: 6.3.0.57372

Agent Installers

Agent Installers updated at Nov 23, 2013 23:51:01 PST

Installer Mode: Do not install/enable Aruba VIA component

Agent will be used only to authenticate / perform health checks for client machines. This setting will not install the Aruba VIA component. If already installed, then the VIA component will be disabled on the client machine.

Note - This WILL remove any existing/installed Aruba VIA client

Windows	http://10.2.48.84/agent/installer/windows/ClearPassOnGuardInstall.exe	(Full Install - EXE)	16MB
	http://10.2.48.84/agent/installer/windows/ClearPassOnGuardInstall.msi	(Full Install - MSI)	16MB
Mac OS X	http://10.2.48.84/agent/installer/mac/ClearPassOnGuardInstall.dmg	(Full Install)	10MB

Agent Customization

Managed Interfaces: ☑ Wired ☑ Wireless ☑ VPN ☐ Other

Mode: Authenticate with health checks

Username Text: Username

Password Text: Password

Client Certificate Check: ☐ Enable to use a certificate from User keystore during authentication

Agent action when an update is available: Ignore

External Captive Portal Support

Enter the URL of a web page that can be accessed only after a successful authentication (e.g., http://www.arubanetworks.com). A network device that is configured for captive portal-based authentication redirects requests to this URL to an authentication page.

URL:

Table 273: *OnGuard Settings*

Container	Description
Global Agent Settings	Configure global parameters for OnGuard agents. Parameters include the following: - **Allowed Subnets for Wired access:** Add a comma-separated list of IP or subnet addresses. - **Allowed Subnets for Wireless access**: Add a 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 ClearPass Policy Servers in a cluster. - **Enable access over Remote Desktop Session:** Enable this option to allow OnGuard access via a Remote Desktop session. - **Enable to hide Logout button:** Enable this option to hide the Logout button. - **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:** The following information when setting the OnGuard Health Check Interval parameter: ▪ OnGuard mode must be set to "health only". ▪ The health check interval is valid only for wired and wireless interface types, and is not applicable for VPN and OTHER interface types. ▪ This parameter is not applicable for the OnGuard Dissolvable Agent. - **Support Team Email Address:** Enter an email address that will automatically populate 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	Current agent version.
Agent Installers	
Installer Mode	Specify the action to take when the Aruba VIA component is used to provide VPN-based access. - Do not install/enable Aruba VIA component. - Install and enable Aruba VIA Component.
Windows	The URLs for the different agent deployment packages for Windows.

Table 273: *OnGuard Settings (Continued)*

Container	Description
Mac OS X	The URLs for the different agent deployment packages 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: ● 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.
Client certificate check	Enable to also perform client certificate based authentication. OnGuard extracts the client certificate from the logged in user’s certificate store and presents this in the TLS exchange with Policy Manager.
Agent action when an update is available	This setting determines what the agent does when an update is available. Options are: ● **Ignore** - CPPM ignores the available update. ● **Notify User** - CPPM notifies the user that an update is available. ● **Download and Install** - CPPM automatically downloads and installs an update as soon as it is available.
External Captive Portal Support	
URL	In a captive portal scenario, the network device presents a captive portal page prior to user authentication. This portal page is presented when the user browses to a URL that is not authorized to be accessed prior to authentication. Enter such a URL here.
Save/Cancel	Commit the update information and generate new deployment packages.

Software Updates

Navigate to **Administration > Agents and Software Updates > Software Updates**.

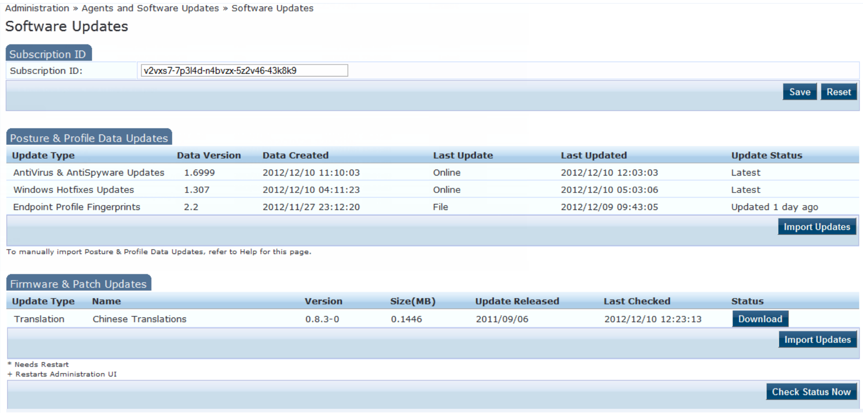
Use the **Software Updates** page to register for and to receive live updates for:

- 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

Updates are stored on the ClearPass webservice server. When a valid Subscription ID is saved, the Dell Networking W-ClearPass Policy Manager server periodically communicates with the webservice about available updates. It downloads any available updates to the Dell Networking W-ClearPass Policy Manager server. The administrator can install these updates directly from this Software Updates page. The first time the Subscription ID is saved, Dell Networking W-ClearPass Policy Manager contacts the webservice to download the latest Posture & Profile Data updates and any available firmware and patch updates. When using an evaluation version, no upgrade Images will be available.

Figure 423: *Software Updates Page*



Subscription ID: v2vxs7-7p3l4d-n4bvzx-5z2v46-43k8k9

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
AntiVirus & AntiSpyware Updates	1.6999	2012/12/10 11:10:03	Online	2012/12/10 12:03:03	Latest
Windows Hotfixes Updates	1.307	2012/12/10 04:11:23	Online	2012/12/10 05:03:06	Latest
Endpoint Profile Fingerprints	2.2	2012/11/27 23:12:20	File	2012/12/09 09:43:05	Updated 1 day ago

To manually import Posture & Profile Data Updates, refer to Help for this page.

Update Type	Name	Version	Size(MB)	Update Released	Last Checked	Status
Translation	Chinese Translations	0.8.3-0	0.1446	2011/09/06	2012/12/10 12:23:13	Download

* Needs Restart
+ Restarts Administration UI

Table 274: *Software Updates Page Parameters*

Parameter	Description
Subscription ID	
Subscription ID	Enter the Subscription ID provided to you in this text box. This text box is enabled only on publisher node. You can at any time opt out of automatic downloads by saving an empty Subscription ID.
Save	Click this button to save the Subscription ID entered in the text box. This button is enabled only on publisher node.
Reset	Performs an "undo" of any unsaved changes made in the Subscription ID field. **NOTE:** This does not clear the text box.
Posture & Profile Data Updates	
Import Updates	Use **Import Updates** to import (upload) the Posture and Profile Data into this server, if this server is not able to reach the webservice server. The data can be downloaded from webservice server by accessing the 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 for authentication. **NOTE:** In a cluster, the **Import Updates** option is only available on the publisher node.

Table 274: *Software Updates Page Parameters (Continued)*

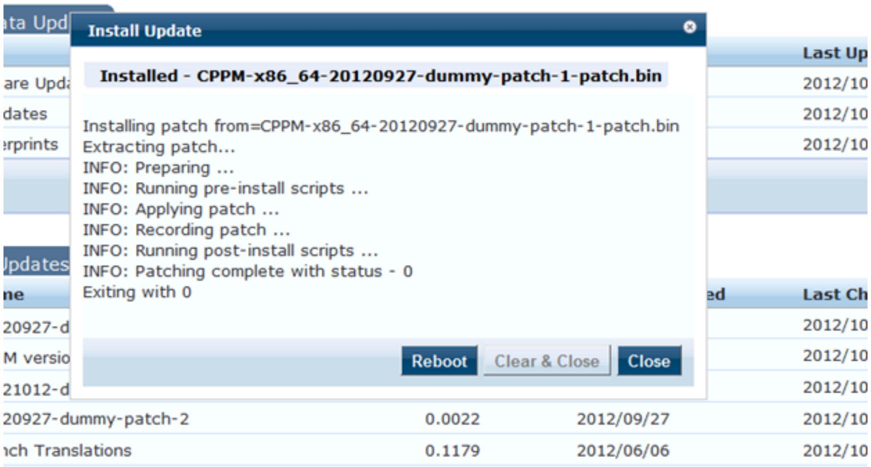
Parameter	Description
Firmware & Patch Updates	
Import Updates	If the server is not able to reach the webservice server, click **Import Updates** to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server. These will show up in the table and can be installed by clicking on the Install button. When logged in as appadmin, the Upgrade and Patch binaries imported can be installed manually 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.
Retry	If the auto-download fails because of connectivity issues or a checksum mismatch, a Retry button will appear. Click on this button to download that update from the webservice server.
Install	This button appears after the update has been downloaded. Clicking on this button starts the installation of the update and displays the Install Update dialog box showing the log messages being generated.
Needs Restart	This 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 showing the log messages generated during the install.
Installed	This link appears when an update has been installed. Clicking on this link displays the Install Update dialog box showing the log messages generated during the install.
Install Error	This link appears when an update install encountered an error. Clicking on this link displays the Install Update dialog box showing the log messages generated during the install.
Other	
Check Status Now	Click on this button to perform an on-demand check for available updates. Applies to updates (only on publisher node) as well as Firmware & Patch Updates.

The Firmware & Patch Updates table will only show the data that is known to webservice. Additionally, it is only visible if the Dell Networking W-ClearPass Policy Manager server is able to communicate with the webservice server.

Install Update dialog box

The Install Update dialog box shows the log messages generated during the install of an update. This popup appears when an Install button is clicked. If the popup is closed, it can be brought up again by clicking the ‘Install in progress…’ link while and installation is in progress or by clicking the ‘Installed’, ‘Install Error’, ‘Needs Restart’ links after the installation is completed.

Figure 424: *Install Update Page*



Installed - CPPM-x86_64-20120927-dummy-patch-1-patch.bin

```
Installing patch from=CPPM-x86_64-20120927-dummy-patch-1-patch.bin
Extracting patch...
INFO: Preparing ...
INFO: Running pre-install scripts ...
INFO: Applying patch ...
INFO: Recording patch ...
INFO: Running post-install scripts ...
INFO: Patching complete with status - 0
Exiting with 0
```

Table 275: *Install Update Page Parameters*

Parameter	Description
Close	Click on this button to close the dialog box.
Clear & Close	Click on this button to delete the log messages and close the popup. This will also remove the corresponding row from the Firmware & Patch Updates table.
Reboot	This button appears only for the updates requiring a reboot to complete the installation. Click on this button to initiate a reboot of the server.

Delete the log messages (using the **Clear & Close** button on the Install Update dialog box) for a failed install. After the log messages are cleared, attempt the install 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 and every day at 4:00 a.m. for a current list of firmware and patch updates. Any new list of firmware and update patches available are downloaded to the Policy Manager server automatically and kept ready for installation. The webservice itself is refreshed with the Antivirus and Antispyware data hourly, with Windows Updates daily, and with Fingerprint data, Firmware & Patches as and when new ones are available. An event is generated (showing up in Event Viewer) with the list of downloaded images. If an SMTP server, any Alert Notification email addresses are configured, an email (from publisher only) is also sent with the list of images downloaded.

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.

MySQL is supported in versions 6.0 and newer. Aruba does not ship MySQL drivers by default. If you require MySQL, contact Aruba 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

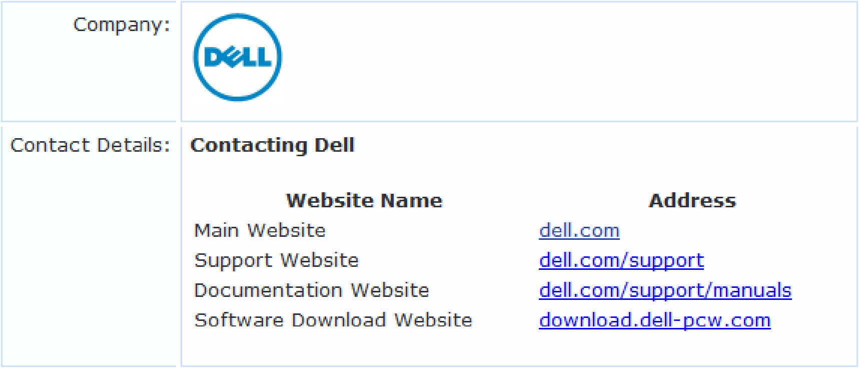
The Administration > Support pages provide information for contacting support, setting up a remote assistance session, and viewing ClearPass documentation. For more information, see:

- "Contact Support" on page 416
- "Remote Assistance" on page 416
- "Documentation" on page 418

Contact Support

The **Administration** > **Support** > **Contact Support** page provides you with information on how to contact Dell Support.

Figure 425: *Contact Support*



Company:

Contact Details: **Contacting Dell**

Website Name	Address
Main Website	dell.com
Support Website	dell.com/support
Documentation Website	dell.com/support/manuals
Software Download Website	download.dell-pcw.com

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 via ssh to the ClearPass Policy Manager server to debug any issues customer is facing or to perform pro-active monitoring of the server.

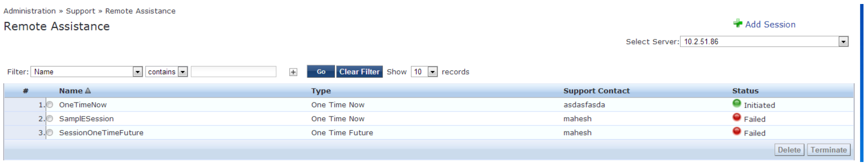
Remote Assistance Process Flow Description

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.

NOTE

Configuring a Remote Assistance session through a CLI can be used if the CPPM UI at the customer site is inaccessible.

Figure 426: *Remote Assistance Session Page*



Administration » Support » Remote Assistance

Remote Assistance

Select Server: 10.2.51.86

Filter: Name contains

Show 10 records

#	Name	Type	Support Contact	Status
1.	OneTimeNow	One Time Now	asdasfasda	● Initiated
2.	SamplESession	One Time Now	mahesh	● Failed
3.	SessionOneTimeFuture	One Time Future	mahesh	● Failed

Table 276: *Remote Assistance Session Page Parameters*

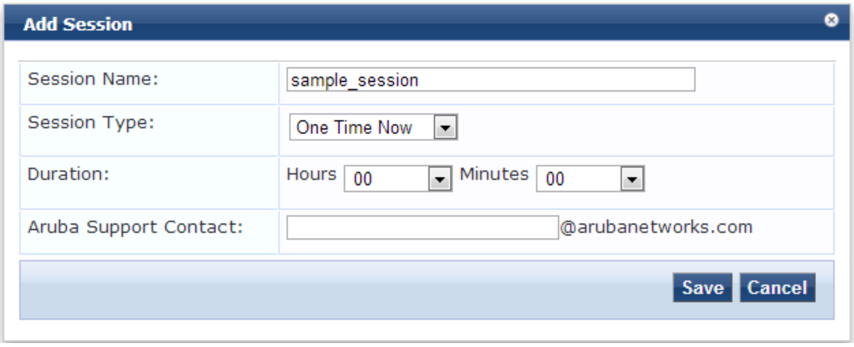
Parameter	Description
Name	Text name of session.
Type	Indicates if the session is a one-time session or a periodic session. Move the cursor over the entry to view the schedule of the session.
Support Contact	The email address of the support contact.
Status	Provides the session state. Available states 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 277: *Add Session Page*



Add Session

Session Name:	sample_session
Session Type:	One Time Now
Duration:	Hours 00 Minutes 00
Aruba Support Contact:	@arubanetworks.com

Table 278: *Add Session Page Parameters*

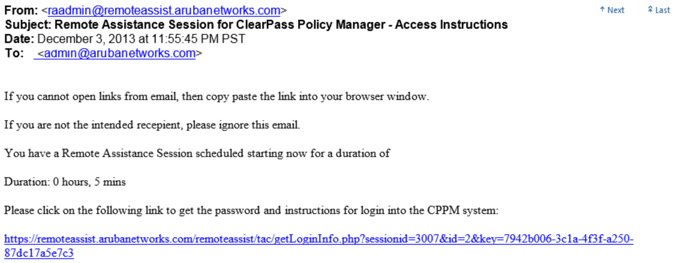
Parameter	Description
Session Name	Text name of session.

Table 278: *Add Session Page Parameters (Continued)*

Parameter	Description
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 427: *Example of a Remote Assistance Session Notification Email*



From: <raadmin@remoteassist.arubanetworks.com>
Subject: Remote Assistance Session for ClearPass Policy Manager - Access Instructions
Date: December 3, 2013 at 11:55:45 PM PST
To: <admin@arubanetworks.com>

If you cannot open links from email, then copy paste the link into your browser window.

If you are not the intended recepient, please ignore this email.

You have a Remote Assistance Session scheduled starting now for a duration of

Duration: 0 hours, 5 mins

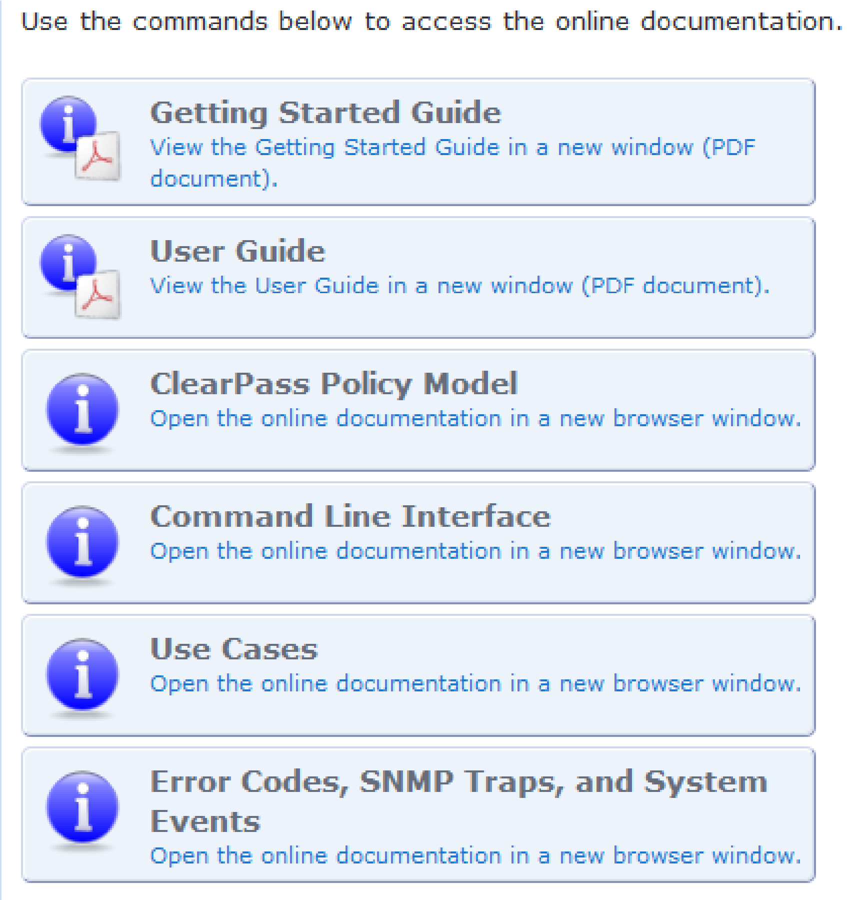
Please click on the following link to get the password and instructions for login into the CPPM system:

https://remoteassist.arubanetworks.com/remoteassist/tac/getLoginInfo.php?sessionid=3007&id=2&key=7942b006-3c1a-4f3f-a250-87dc17a5e7c3

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 6.3 User Guide* and the *Dell Networking W-ClearPass Policy Manager 6.3 Getting Started Guide*.

Figure 428: *Documentation page*



Use the commands below to access the online documentation.

Getting Started Guide
View the Getting Started Guide in a new window (PDF document).

User Guide
View the User Guide in a new window (PDF document).

ClearPass Policy Model
Open the online documentation in a new browser window.

Command Line Interface
Open the online documentation in a new browser window.

Use Cases
Open the online documentation in a new browser window.

Error Codes, SNMP Traps, and System Events
Open the online documentation in a new browser window.

Appendix A
Command Line Interface

Refer to the following sections:

Available Commands

Table 279: *Command Categories*

Command
ad auth See "Miscellaneous Commands" on page 437
ad netleave See "Miscellaneous Commands" on page 437
ad netjoin See "Miscellaneous Commands" on page 437
ad testjoin See "Miscellaneous Commands" on page 437
alias See "Miscellaneous Commands" on page 437
backup See "Miscellaneous Commands" on page 437
cluster drop-subscriber
cluster list
cluster make-publisher
cluster make-subscriber
cluster reset-database
cluster set-cluster-passwd

Table 279: *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 437
dump logs See "Miscellaneous Commands" on page 437
dump servercert See "Miscellaneous Commands" on page 437
exit See "Miscellaneous Commands" on page 437
help See "Miscellaneous Commands" on page 437
krb auth See "Miscellaneous Commands" on page 437
krb list See "Miscellaneous Commands" on page 437
ldapsearch See "Miscellaneous Commands" on page 437
network ip
network nslookup
network ping
network traceroute
network reset
quit See "Miscellaneous Commands" on page 437

Table 279: *Command Categories (Continued)*

Command
restore See "Miscellaneous Commands" on page 437
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 424
- "list" on page 424
- "make-publisher" on page 424
- "make-subscriber" on page 425
- "reset-database" on page 425
- "set-cluster-passwd" on page 425
- "set-local-passwd" on page 426

drop-subscriber

Removes specified subscriber node from the cluster.

Syntax

```
cluster drop-subscriber [-f] [-i <IP Address>] -s
```

Where:

Table 280: *Drop-Subscriber Commands*

Flag/Parameter	Description
-f	Force drop, even for down nodes.
-i <IP Address>	Management IP address of the node. If not specified and the current node is a subscriber, Policy Manager drops the current node.
-s	Do not reset the database on the dropped node. By default, Policy Manager drops the current node (if a subscriber) from the cluster.

Example

```
[appadmin]# cluster drop-subscriber -f -i 192.168.1.1 -s
```

list

Lists the cluster nodes.

Syntax

```
cluster list
```

Example

```
[appadmin]# cluster list
cluster list
Publisher  :
Management port IP=192.168.5.227
Data port IP=None [local machine]
```

make-publisher

Makes this node a publisher.

Syntax

```
cluster make-publisher
```

Example

```
[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

Makes this node a subscriber to the specified publisher node.

Syntax

```
make-subscriber -i <IP Address> [-l]
```

Where:

Table 281: *Make-Subscriber Commands*

Flag/Parameter	Description
-i <IP Address>	Required. Publisher IP address.
-l	Optional. Restore the local log database after this operation.

Example

```
[appadmin]#  cluster make-subscriber –i 192.168.1.1 –p !alore -l
```

reset-database

Resets the local database and erases its configuration.

Syntax

```
cluster reset-database
```

Returns

```
[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

Changes the cluster password on all publisher nodes. Executed on the publisher; prompts for the new cluster password.

Syntax

```
cluster set-cluster-passwd
```

Returns

```
[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

Changes the local password. Executed locally; prompts for the new local password.

Syntax

```
cluster sync-local-password
```

Returns

```
[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" on page 426
- "dns" on page 427
- "hostname" on page 427
- "ip" on page 427
- "timezone" on page 428

date

Sets *System Date, Time* and *Time Zone*.

Syntax

```
configure date -d <date> [-t <time> ] [-z <timezone>]
```

or

```
configure date -s <ntpserver> [-z <timezone>]
```

Where:

Table 282: *Date Commands*

Flag/Parameter	Description
-s <ntpserver>	Optional. Synchronize time with specified NTP server.
-d <date>	Required. *Syntax:* yyyy-mm-dd

Table 282: *Date Commands (Continued)*

Flag/Parameter	Description
-t <time>	Optional. *Syntax:* hh:mm:ss
-z <timezone>	Optional. *Syntax:* To view the list of supported timezone values, enter: show all-timezones.

Example 1

Specify date/time/timezone:

```
[appadmin]#  configure date -d 2007-06-22 -t 12:00:31 -z America/Los_Angeles
```

Example 2

Synchronize with a specified NTP server:

```
[appadmin]# -s <ntpserver>
```

dns

Configure DNS servers. At least one DNS server must be specified; a maximum of three DNS servers can be specified.

Syntax

```
configure dns <primary> [secondary] [tertiary]
```

Example 1

```
[appadmin]# configure dns 192.168.1.1
```

Example 2

```
[appadmin]# configure dns 192.168.1.1 192.168.1.2
```

Example 3

```
[appadmin]# configure dns 192.168.1.1 192.168.1.2 192.168.1.3
```

hostname

Configures the hostname.

Syntax

configure hostname <hostname>

Example

```
[appadmin]#  configure hostname sun.us.arubanetworks.com
```

ip

Configures IP address, netmask and gateway.

Syntax

```
[appadmin]# configure ip <mgmt|data> <ipaddress> netmask <netmask address> gateway <gateway ad
dress>
```

Where:

Table 283: *IP Commands*

Flag/Parameter	Description
ip <mgmt|data> <ip address>	Network interface type: *mgmt* or *data* • Server ip address.
netmask <netmask address>	Netmask address.
gateway <gateway address>	Gateway address.

Example

```
[appadmin]# configure ip data 192.168.5.12 netmask 255.255.255.0 gateway 192.168.5.1
```

timezone

Configures time zone interactively.

Syntax

```
configure timezone
```

Example

```
[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" on page 428
- "nslookup" on page 429
- "ping" on page 430
- "reset" on page 430
- "traceroute" on page 431

ip

Add, delete, or list custom routes to the data or management interface routing table.

Syntax

```
network ip add <mgmt|data> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]>
```

Add a custom routing rule. Where:

Table 284: *IP Commands*

Flag/Parameter	Description
<mgmt|data>	Specify management or data interface
-i <id>	id of the network ip rule. If unspecified, the system will auto-generate an id. Note that the id determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Optional. Specifies the ip address or network (for example, 192.168.5.0/24) or 0/0 (for all traffic) of traffic originator. Only one of SrcAddr or DstAddr must be specified.
`-d <DestAddr>`	Optional. Specifies the destination ip address or network (for example, 192.168.5.0/24) or 0/0 (for all traffic). Only one of SrcAddr or DstAddr must be specified.

Syntax

```
network ip del <-i <id>>
```

Delete a rule. Where:

Table 285: *Network IP Delete Commands*

Flag/Parameter	Description
-i <id>	Id of the rule to delete.

Syntax

```
network ip list
```

List all routing rules.

Syntax

```
network ip reset
```

Reset routing table to factory default setting. All custom routes are removed.

Example 1

```
[appadmin]# network ip add data -s 192.168.5.0/24
```

Example 2

```
[appadmin]# network ip add data -s 192.168.5.12
```

Example 3

```
[appadmin]# network ip list
```

nslookup

Returns IP address of host using DNS.

Syntax

```
nslookup -q <record-type> <host>
```

Where:

Table 286: *Nslookup Commands*

Flag/Parameter	Description
<record-type>	Type of DNS record. For example, A, CNAME, PTR
<host>	Host or domain name to be queried.

Example 1

```
[appadmin]# nslookup sun.us.arubanetworks.com
```

Example 2

```
[appadmin]# nslookup -q SRV arubanetworks.com
```

ping

Tests reachability of the network host.

Syntax

```
network ping [-i <SrcIpAddr>] [-t] <host>
```

Where:

Table 287: *Ping Commands*

Flag/Parameter	Description
-i <SrcIpAddr>	Optional. Originating IP address for ping.
-t	Optional. Ping indefinitely.
<host>	Host to be pinged.

Example

```
[appadmin]# network ping -i 192.168.5.10 -t sun.us.arubanetworks.com
```

reset

Reset network data port.

Syntax

```
network reset <port>
```

Where:

Table 288: *Reset Commands*

Flag/Parameter	Description
<port>	Required. Name of network port to reset.

Example

```
[appadmin]# network reset data
```

traceroute

Prints route taken to reach network host.

Syntax

```
network traceroute <host>
```

Where:

Table 289: *Traceroute Commands*

Flag/Parameter	Description
<host>	Name of network host.

Example

```
[appadmin]#  network traceroute sun.us.arubanetworks.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>

Activates the specified Policy Manager service.

Syntax

```
service <action> <service-name>
```

Where:

Table 290: *Action Commands*

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" on page 432
- "date" on page 432
- "dns" on page 433
- "domain" on page 433
- "hostname" on page 433
- "ip" on page 433
- "license" on page 434
- "timezone" on page 434
- "version" on page 434

all-timezones

Interactively displays all available timezones

Syntax

```
show all-timezones
```

Example

```
[appadmin]#  show all-timezones
Africa/Abidjan
Africa/Accra
.....
WET
Zulu
```

date

Displays *System Date, Time,* and *Time Zone* information.

Syntax

```
show date
```

Example

```
[appadmin]#  show date
Wed Oct 31 14:33:39 UTC 2012
```

dns

Displays DNS servers.

Syntax

```
show dns
```

Example

```
[appadmin]#  show dns
show dns
===========================================
          DNS Information
-------------------------------------------
Primary   DNS  :   192.168.5.3
Secondary DNS  :   <not configured>
Tertiary  DNS  :   <not configured>
===========================================
```

domain

Displays *Domain Name, IP Address,* and *Name Server* information.

Syntax

```
show domain
```

Example

```
[appadmin]#  show domain
```

hostname

Displays hostname.

Syntax

```
show hostname
```

Example

```
[appadmin]#  show hostname
show hostname
wolf
```

ip

Displays IP and DNS information for the host.

Syntax

```
show ip
```

Example

```
[appadmin]#  show ip
show ip
===========================================
Device Type    :   Management Port
-------------------------------------------
IP Address     :   192.168.5.227
```

```
Subnet Mask     :   255.255.255.0
Gateway         :   192.168.5.1
===========================================
Device Type     :   Data Port
-------------------------------------------
IP Address      :   <not configured>
Subnet Mask     :   <not configured>
Gateway         :   <not configured>
===========================================
          DNS Information
-------------------------------------------
Primary   DNS   :   192.168.5.3
Secondary DNS   :   <not configured>
Tertiary  DNS   :   <not configured>
===========================================
```

license

Displays the license key.

Syntax

```
show license
```

Example

```
[appadmin]#  show license
show license
```

timezone

Displays current system timezone.

Syntax

```
show timezone
```

Example

```
[appadmin]#  show timezone
show timezone
```

version

Displays Policy Manager software version hardware model.

Syntax

```
show version
```

Example

```
[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 includes the following *system* commands:

- "boot-image" on page 435
- "gen-support-key" on page 435

- "install-license" on page 435
- "restart" on page 436
- "shutdown" on page 436
- "update" on page 436
- "upgrade" on page 437

boot-image

Sets system boot image control options.

Syntax

```
system boot-image [-l] [-a <version>]
```

Where:

Table 291: *Boot-Image Commands*

Flag/Parameter	Description
-l	Optional. List boot images installed on the system.
-a <version>	Optional. Set active boot image version, in *A.B.C.D* syntax.

Example

```
[appadmin]#  system boot-image
```

gen-support-key

Generates the support key for the system.

Syntax

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

Example

```
[appadmin]#  system gen-support-key
system gen-support-key
Support key='01U2FsdGVkX1+/WS9jZKQajERyzXhM8mF6zAKrzxrHvaM='
```

install-license

Replace the current license key with a new one.

Syntax

```
system install-license <license-key>
```

Where:

Table 292: *Install-License Commands*

Flag/Parameter	Description
<license-key>	Mandatory. This is the newly issued license key.

Example

```
[appadmin]#  system install-license
```

morph-vm

Converts an evaluation VM to a production VM. With this command, licenses are still required to be installed after the morph operation is complete.

Syntax

```
system morph-vm <vm-version>
```

Where:

Table 293: *Install-License Commands*

Flag/Parameter	Description
<vm-version>	Mandatory. This is the updated ClearPass version.

restart

Restart the system

Syntax

```
system restart
```

Example

```
[appadmin]#  system restart
system restart
*********************************************************

* WARNING: This command will shutdown all applications *
* and reboot the system                                *
********************************************************
Are you sure you want to continue? [y|Y]: y
```

shutdown

Shutdown the system

Syntax

```
system shutdown
```

Example

```
[appadmin]#  system shutdown
********************************************************
* WARNING: This command will shutdown all applications *
* and power off the system                             *
********************************************************
Are you sure you want to continue? [y|Y]: y
```

update

Manages updates.

Syntax

```
system update [-i user@hostname:/<filename> | http://hostname/<filename>]
system update [-l]
```

Where:

Table 294: *Update Commands*

Flag/Parameter	Description
-i user@hostname:/<filename> | http://hostname/<filename>	Optional. Install the specified patch on the system.
-l	Optional. List the patches installed on the system.

NOTE: This command supports only SCP and http uploads.

Example

```
[appadmin]# system update
```

upgrade

Upgrades the system.

Syntax

```
system upgrade <filepath>
```

Where:

Table 295: *Upgrade Commands*

Flag/Parameter	Description
<filepath>	Required. Enter filepath, using either syntax provided in the two examples provided.

NOTE: This command supports only SCP and http uploads.

Example 1

```
[appadmin]# system upgrade admin@sun.us.arubanetworks.com:/tmp/PolicyManager-x86-64-upgrade-71.tgz
```

Example 2

```
[appadmin]# system upgrade http://sun.us.arubanetworks.com/downloads/PolicyManager-x86-64-upgrade-71.tgz
```

Miscellaneous Commands

The Policy Manager command line interface includes the following *miscellaneous* commands:

- "ad auth" on page 438
- "ad netjoin" on page 438

ad auth

Authenticate the user against AD.

Syntax

```
ad auth --username=<username>
```

Where:

Table 296: *Ad Auth Commands*

Flag/Parameter	Description
<username>	Required. username of the authenticating user.

Example

```
[appadmin]#  ad auth --username=mike
```

ad netjoin

Joins host to the domain.

Syntax

```
ad netjoin <domain-controller.domain-name> [domain NETBIOS name]
```

Where:

Table 297: *Ad Netjoin Commands*

Flag/Parameter	Description
<domain-controller. domain-name>	Required. Host to be joined to the domain.
[domain NETBIOS name]	Optional.

Example

```
[appadmin]#  ad netjoin atlas.us.arubanetworks.com
```

ad netleave

Removes host from the domain.

Syntax

```
ad netleave
```

Example

```
[appadmin]#  ad netleave
```

ad testjoin

Tests if the netjoin command succeeded. Tests if Policy Manager is a member of the AD domain.

Syntax

```
ad testjoin
```

Example

```
[appadmin]#  ad testjoin
```

alias

Creates or removes aliases.

Syntax

```
alias <name>=<command>
```

Where:

Table 298: *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

Creates 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]
```

Where:

Table 299: *Backup Commands*

Flag/Parameter	Description
-f <filename>	Optional. Backup target. If not specified, Policy Manager will auto-generate a filename.
-L	Optional. Do not backup the log database configuration
-P	Optional. Do not backup password fields from the configuration database

Example

```
[appadmin]#  backup -f PolicyManager-data.tar.gz
Continue? [y|Y]:  y
```

dump certchain

Dumps certificate chain of any SSL secured server.

Syntax

```
dump certchain <hostname:port-number>
```

Where:

Table 300: *Dump Certchain Commands*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1

```
[appadmin]#  dump certchain ldap.acme.com:636
dump certchain
```

dump logs

Dumps 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]
```

Where:

Table 301: *Dump Logs Commands*

Flag/Parameter	Description
-f <output-file-name>	Specifies target for concatenated logs.
-s yyyy-mm-dd	Optional. Date range start (default is today).
-e yyyy-mm-dd	Optional. Date range end (default is today).
-n <days>	Optional. Duration in days (from today).
-t <log-type>	Optional. Type of log to collect.
-h	Specify (print help) for available log types.

Example 1

```
[appadmin]#  dump logs -f tips-system-logs.tgz -s 2007-10-06 -e 2007-10-17 -t SystemLogs
```

Example 2

```
[appadmin]#  dump logs -h
```

dump servercert

Dumps server certificate of SSL secured server.

Syntax

```
dump servercert <hostname:port-number>
```

Where:

Table 302: *Dump Servercert Commands*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1

```
[appadmin]#  dump servercert ldap.acme.com:636
```

exit

Exits shell.

Syntax

```
exit
```

Example

```
[appadmin]#  exit
```

help

Display the list of supported commands

Syntax

```
help <command>
```

Example

```
[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

Does a kerberos authentication against a kerberos server (such as Microsoft AD)

Syntax

```
krb auth <user@domain>
```

Where:

Table 303: *Kerberos Authentication Commands*

Flag/Parameter	Description
<user@domain>	Specifies the username and domain.

Example

```
[appadmin]#  krb auth mike@corp-ad.acme.com
```

krb list

Lists the cached kerberos tickets

Syntax

```
krb list
```

Example

```
[appadmin]#  krb list
```

ldapsearch

The Linux ldapsearch command to find objects in an LDAP directory. (Note that only the Policy Manager-specific command line arguments are listed below. For other command line arguments, refer to ldapsearch man pages on the Internet).

Syntax

```
ldapsearch -B <user@hostname>
```

Where:

Table 304: *LDAP Search commands*

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

```
[appadmin]#  ldapsearch -B admin@corp-ad.acme.com
```

quit

Exits shell.

Syntax

```
quit
```

Example

```
[appadmin]# quit
```

restore

Restores Policy Manager configuration data from the backup file.

Syntax

```
restore user@hostname:/<backup-filename> [-l] [-i] [-c|-C] [-p] [-s]
```

Where:

Table 305: *Restore Commands*

Flag/Parameter	Description
user@hostname:/<backup-filename>	Specify filepath of restore source.
-c	Restore configuration database (default).
-C	Do not restore configuration database.
-l	Optional. If it exists in the backup, restore log database.
-i	Optional. Ignore version mismatch errors and proceed.
-p	Optional. Force restore from a backup file that does not have password fields present.
-s	Optional. Restore cluster server/node entries from the backup. (Node entries disabled on restore.)

Example

```
[appadmin]# restore user@hostname:/tmp/tips-backup.tgz -l -i -c -s
```

system start-rasession

Allows administrators to configure and begin a Remote Assistance session through the CPPM CLI. Configuring a Remote Assistance session through a CLI can be used if the CPPM UI at the customer site is inaccessible.

Syntax

```
system start-rasession <duration_hours> <duration_mins> <contact> <server_ip>
```

Where:

Table 306: *Start Remote Session Commands*

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>	The name of the TAC engineer.
<server_ip>	Gives the ip of a CPPM in the cluster.

system terminate-rasession

Allows administrators to terminate the session on the CPPM where the Remote Assistance session is running.

Syntax

```
system terminate-rasession <sessionid>
```

Where:

Table 307: *Terminate Remote Session Command*

Flag/Parameter	Description
<sessionid>	Provides the sessionid that can be used to terminate-session.

system status-rasession

Allows administrators to acquire the status on the CPPM in the cluster where the remote session is running.

Syntax

```
system status-rasession <sessionid>
```

Where:

Table 308: *Terminate Remote Session Command*

Flag/Parameter	Description
<sessionid>	The id returned when system status-rasession command was run.

Appendix B
Rules Editing and Namespaces

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 in more detail:

- "Namespaces" on page 445
- "Variables" on page 455
- "Operators" on page 456

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 446

- "Audit Namespaces" on page 447
- "Authentication Namespaces" on page 447
- "Authorization Namespaces" on page 449
- "Certificate Namespaces" on page 450
- "Connection Namespaces" on page 451
- "Date Namespaces" on page 452
- "Device Namespaces" on page 452
- "Endpoint Namespaces" on page 453
- "Guest User Namespaces" on page 453
- "Host Namespaces" on page 453
- "Local User Namespaces" on page 453
- "Posture Namespaces" on page 454
- "RADIUS Namespaces" on page 454
- "Tacacs Namespaces" on page 455
- "Tips Namespaces" on page 455

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
- WorkSpace
- 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 233 for more information.

The Avenda Systems:Audit namespace appears when editing post-audit rules for NESSUS and NMAP audit servers.

Table 309: *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 that was used, or what the status of the authentication is.

Authentication namespace editing context

Role mapping policies

Table 310: *Authentication Namespace Attributes*

Attribute Name	Values
InnerMethod	- CHAP - EAP-GTC - EAP-MD5 - EAP-MSCHAPv2 - EAP-TLS - MSCHAP - PAP
OuterMethod	- CHAP - EAP-FAST - EAP-MD5 - EAP-PEAP - EAP-TLS - EAP-TTLS - MSCHAP - PAP
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 131).
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 - **AuthSource-Unreachable** - The authentication source was unreachable

Table 310: *Authentication Namespace Attributes (Continued)*

Attribute Name	Values
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 149 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 149).

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 311: *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.

Table 311: *Certificate Namespace Attributes (Continued)*

Attribute Name	Values
• Issuer-C • Issuer-CN • Issuer-DC • Issuer-DN • Issuer-emailAddress • Issuer-GN • Issuer-L • Issuer-O • Issuer-OU • Issuer-SN • Issuer-ST • Issuer-UID	Attributes associated with the issuer (Certificate Authorities or the enterprise CA). Not all of these fields are populated in a certificate.
• 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 312: *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.

Table 312: *Connection Namespace Pre-defined Attributes (Continued)*

Attribute	Description
NAD-IP-Address	IP address of the network device from which the request originated.
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.

NOTE

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.

NOTE

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.

NOTE

> 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 400) 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 398 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 313: *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 149.
%{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

NOTE

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 314: *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

Table 314: *Attribute Operators (Continued)*

Attribute Type	Operators
Time or Date	- EQUALS NOT_EQUALS - GREATER_THAN - GREATER_THAN_OR_EQUALS - LESS_THAN - 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 315: *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-"`

Operator	Description
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`
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`

Operator	Description
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*`

Error Codes, SNMP Traps, and System Events

This appendix contains listings of Dell Networking W-ClearPass Policy Manager error codes, SNMP traps, and important system events.

- "Error Codes" on page 461
- "SNMP Trap Details" on page 464
- "Important System Events" on page 474

Error Codes

The following table shows the CPPM error codes.

Table 316: *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 316: *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
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
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

Table 316: *CPPM Error Codes (Continued)*

Code	Description	Type
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
9006	Received error TLV from client	RADIUS Protocol
9007	Received failure TLV from client	RADIUS Protocol
9008	Phase2 PAC not found	RADIUS Protocol

Table 316: *CPPM Error Codes (Continued)*

Code	Description	Type
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

SNMP Trap Details

CPPM 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 464
- "CPPM Processes Stop and Start Events" on page 464
- "Network Interface up and Down Events" on page 465
- "Disk Utilization Threshold Exceed Events" on page 465
- "CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds" on page 465
- "SNMP Daemon Traps" on page 465
- "Process Status Traps" on page 465
- "Network Interface Status Traps" on page 473
- "Disk Space Threshold Traps" on page 473
- "CPU Load Average Traps" on page 473

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

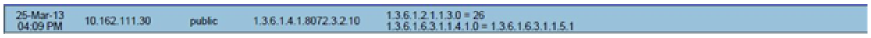
SNMP Daemon Traps

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 429: *SNMP daemon traps example*



25-Mar-13 04:09 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 = 26 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1

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.

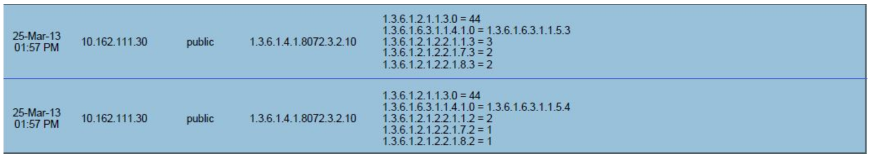
Network Interface Status Traps

.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 430: *Network interface status traps example*



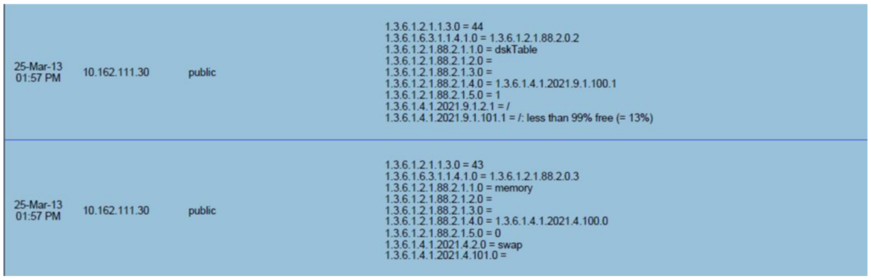
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3 1.3.6.1.2.1.2.2.1.1.3 = 3 1.3.6.1.2.1.2.2.1.7.3 = 2 1.3.6.1.2.1.2.2.1.8.3 = 2
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 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 431: *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 =

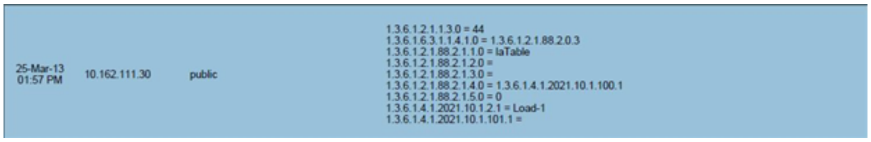
CPU Load Average Traps

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 432: *CPU load-1 average example*

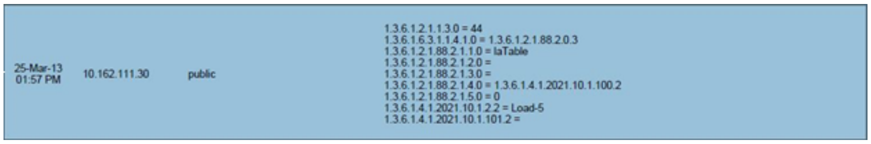


25-Mar-13 01:57 PM	10.162.111.30	public		1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3 1.3.6.1.2.1.88.2.1.1.0 = laTable 1.3.6.1.2.1.88.2.1.2.0 = 1.3.6.1.2.1.88.2.1.3.0 = 1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.1 1.3.6.1.2.1.88.2.1.5.0 = 0 1.3.6.1.4.1.2021.10.1.2.1 = Load-1 1.3.6.1.4.1.2021.10.1.101.1 =

.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 433: *CPU load-5 average example*

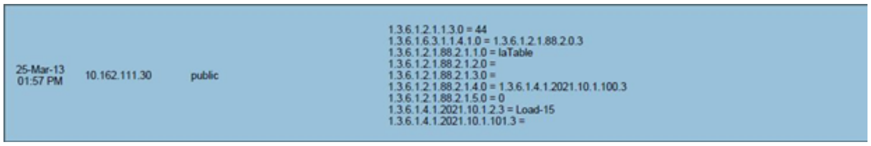


```
25-Mar-13    10.162.111.30    public    1.3.6.1.2.1.1.3.0 = 44
01:57 PM                                1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3
                                        1.3.6.1.2.1.88.2.1.1.0 = laTable
                                        1.3.6.1.2.1.88.2.1.2.0 =
                                        1.3.6.1.2.1.88.2.1.3.0 =
                                        1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.2
                                        1.3.6.1.2.1.88.2.1.5.0 = 0
                                        1.3.6.1.4.1.2021.10.1.2.2 = Load-5
                                        1.3.6.1.4.1.2021.10.1.101.2 =
```

.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 434: *CPU load-15 average example*



```
25-Mar-13    10.162.111.30    public    1.3.6.1.2.1.1.3.0 = 44
01:57 PM                                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 = laTable
                                        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 = 1.3.6.1.4.1.2021.10.1.100.3
                                        1.3.6.1.2.1.88.2.1.5.0 = 0
                                        1.3.6.1.4.1.2021.10.1.2.3 = Load-15
                                        1.3.6.1.4.1.2021.10.1.101.3 =
```

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 478 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

Appendix D
Use Cases

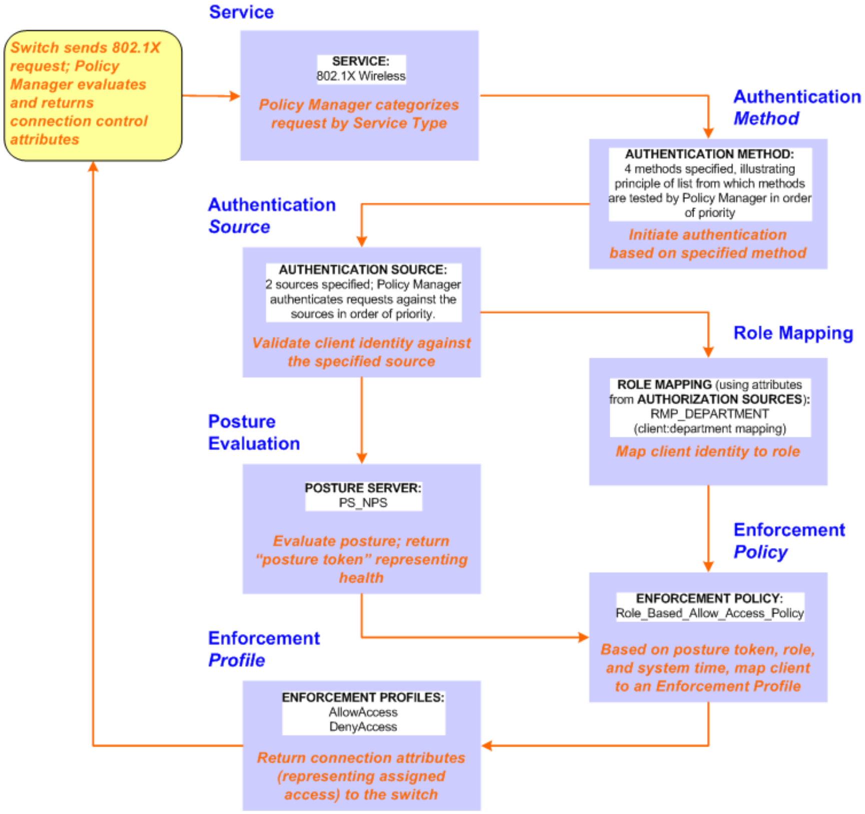
This appendix contains several specific Dell Networking W-ClearPass Policy Manager use cases. Each one explains what it is typically used for, and then describes how to configure Policy Manager for that use case.

- "802.1X Wireless Use Case" on page 479
- "Web Based Authentication Use Case" on page 485
- "MAC Authentication Use Case" on page 492
- "TACACS+ Use Case" on page 495
- "Single Port Use Case" on page 497

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 435: *Flow of Control, Basic 802.1X Configuration Use Case*



Service
Switch sends 802.1X request; Policy Manager evaluates and returns connection control attributes
SERVICE: 802.1X Wireless
Policy Manager categorizes request by Service Type
Authentication Method
AUTHENTICATION METHOD: 4 methods specified, illustrating principle of list from which methods are tested by Policy Manager in order of priority
Initiate authentication based on specified method
Authentication Source
AUTHENTICATION SOURCE: 2 sources specified; Policy Manager authenticates requests against the sources in order of priority.
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (using attributes from AUTHORIZATION SOURCES): RMP_DEPARTMENT (client:department mapping)
Map client identity to role
Posture Evaluation
POSTURE SERVER: PS_NPS
Evaluate posture; return "posture token" representing health
Enforcement Policy
ENFORCEMENT POLICY: Role_Based_Allow_Access_Policy
Based on posture token, role, and system time, map client to an Enforcement Profile
Enforcement Profile
ENFORCEMENT PROFILES: AllowAccess DenyAccess
Return connection attributes (representing assigned access) to the switch

Configuring the Service

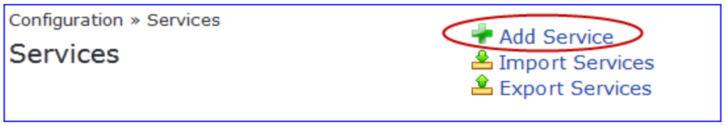
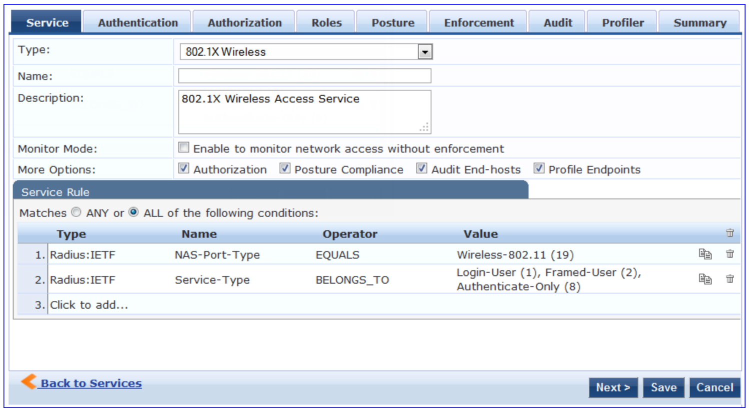
Follow the steps below to configure this basic 802.1X service:

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 317: *802.1X - Create Service Navigation and Settings*

Navigation	Settings
Create a new Service: ● **Services** > ● **Add Service** (link) >	 Configuration » Services Services Add Service Import Services Export Services
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)	 Service | Authentication | Authorization | Roles | Posture | Enforcement | Audit | Profiler | Summary Type: 802.1X Wireless Name: Description: 802.1X Wireless Access Service Monitor Mode: □ Enable to monitor network access without enforcement More Options: ☑ Authorization ☑ Posture Compliance ☑ Audit End-hosts ☑ Profile Endpoints Service Rule Matches ○ ANY or ● ALL of the following conditions: Type | Name | Operator | Value 1. Radius:IETF | NAS-Port-Type | EQUALS | Wireless-802.11 (19) 2. Radius:IETF | Service-Type | BELONGS_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) 3. Click to add... Back to Services Next > | Save | Cancel

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.

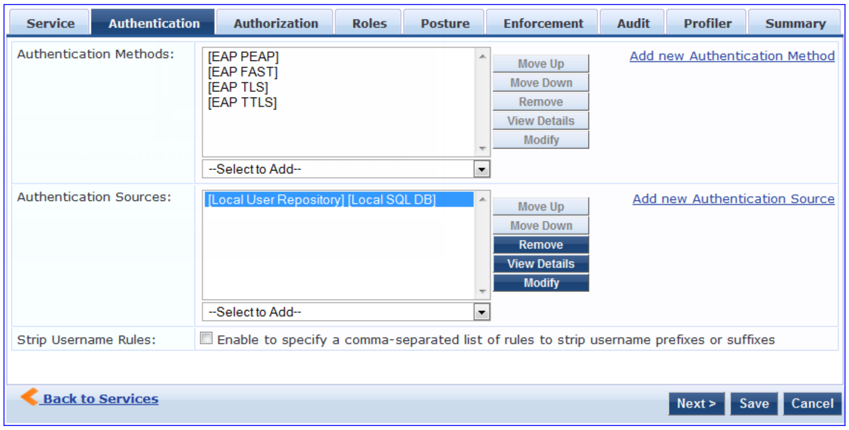
2. Configure Authentication.

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.

NOTE

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 318: *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)	 Service | **Authentication** | Authorization | Roles | Posture | Enforcement | Audit | Profiler | Summary Authentication Methods: [EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] --Select to Add-- Add new Authentication Method Authentication Sources: [Local User Repository] [Local SQL DB] --Select to Add-- Add new Authentication Source Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes Back to Services

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.

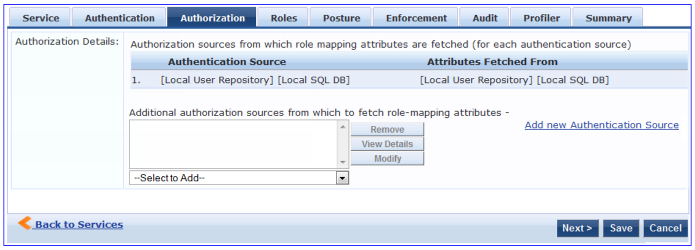
NOTE

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 319: *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).	 Authorization Details: Authorization sources from which role mapping attributes are fetched (for each authentication source) Authentication Source: 1. [Local User Repository] [Local SQL DB] — Attributes Fetched From: [Local User Repository] [Local SQL DB] Additional authorization sources from which to fetch role-mapping attributes - --Select to Add-- Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Remove View Details Modify Add new Authentication Source Back to Services Next > Save Cancel

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 320: *Role Mapping Navigation and Settings*

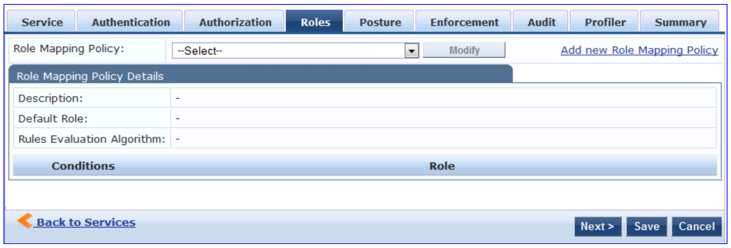
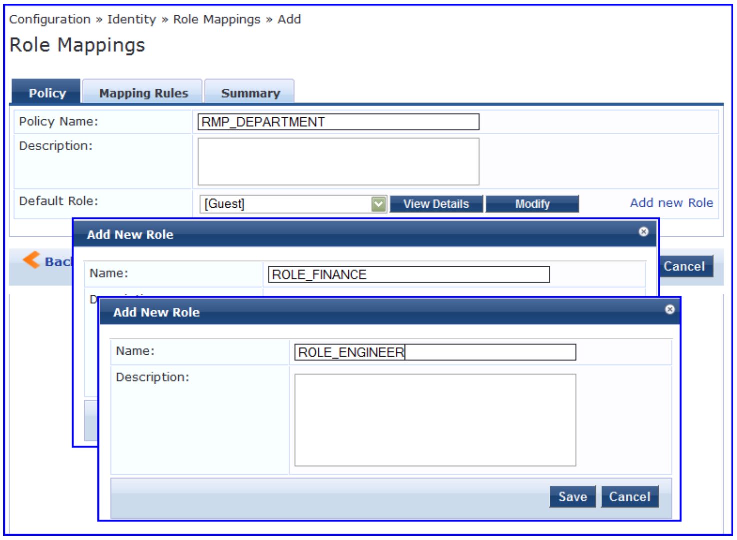
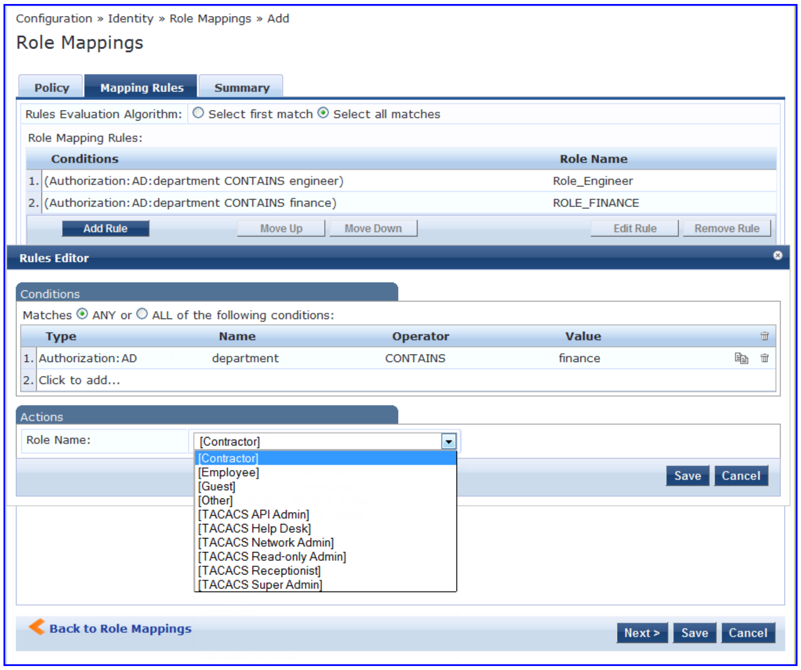
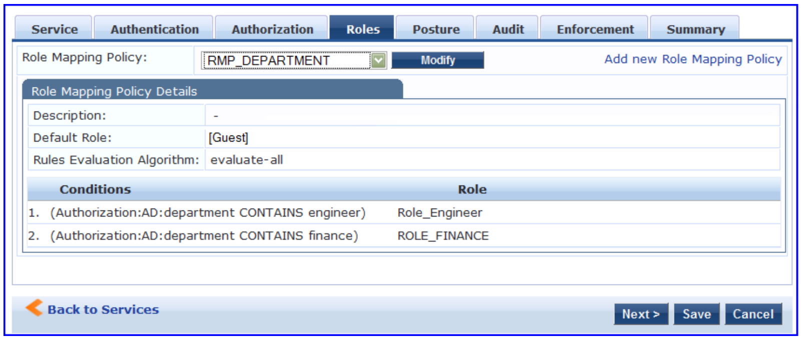
Navigation	Settings
Create the new Role Mapping Policy: - Roles (tab) > - Add New Role Mapping Policy (link) >	 Role Mapping Policy: --Select-- Role Mapping Policy Details Description: - Default Role: - Rules Evaluation Algorithm: - Conditions / Role Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Modify Add new Role Mapping Policy Back to Services Next > Save Cancel
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)	 Configuration » Identity » Role Mappings » Add Role Mappings Policy Name: RMP_DEPARTMENT Description: Default Role: [Guest] Add New Role Name: ROLE_FINANCE Add New Role Name: ROLE_ENGINEER Description: Policy Mapping Rules Summary View Details Modify Add new Role Cancel Save Cancel

Table 320: *Role Mapping Navigation and Settings (Continued)*

Navigation	Settings
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)	 Configuration » Identity » Role Mappings » Add Role Mappings Policy | Mapping Rules | Summary Rules Evaluation Algorithm: ○ Select first match ● Select all matches Role Mapping Rules: Conditions | Role Name 1. (Authorization:AD:department CONTAINS engineer) | Role_Engineer 2. (Authorization:AD:department CONTAINS finance) | ROLE_FINANCE Add Rule | Move Up | Move Down | Edit Rule | Remove Rule Rules Editor Conditions Matches ● ANY or ○ ALL of the following conditions: Type | Name | Operator | Value 1. Authorization:AD | department | CONTAINS | finance 2. Click to add... Actions Role Name: [Contractor] [Contractor] [Employee] [Guest] [Other] [TACACS API Admin] [TACACS Help Desk] [TACACS Network Admin] [TACACS Read-only Admin] [TACACS Receptionist] [TACACS Super Admin] Save | Cancel Back to Role Mappings Next > | Save | Cancel
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)	 Service | Authentication | Authorization | Roles | Posture | Audit | Enforcement | Summary Role Mapping Policy: RMP_DEPARTMENT | Modify | Add new Role Mapping Policy Role Mapping Policy Details Description: - Default Role: [Guest] Rules Evaluation Algorithm: evaluate-all Conditions | Role 1. (Authorization:AD:department CONTAINS engineer) | Role_Engineer 2. (Authorization:AD:department CONTAINS finance) | ROLE_FINANCE Back to Services Next > | Save | Cancel

5. Configure a Posture Server.

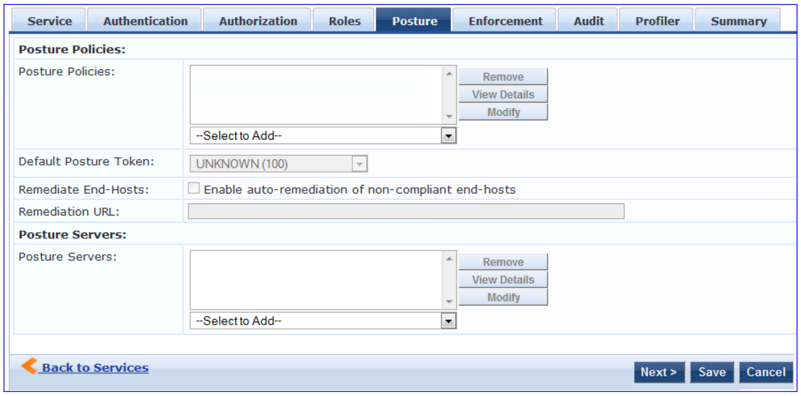
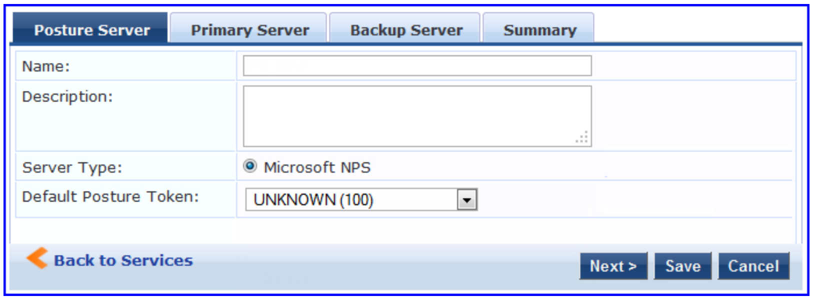
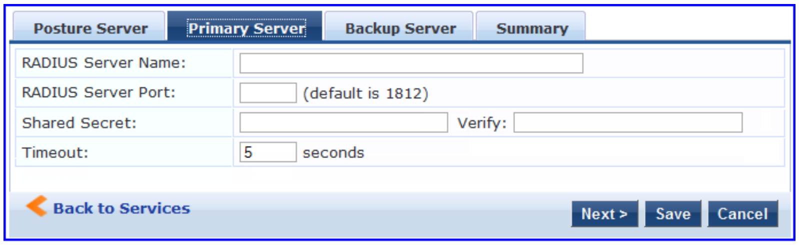
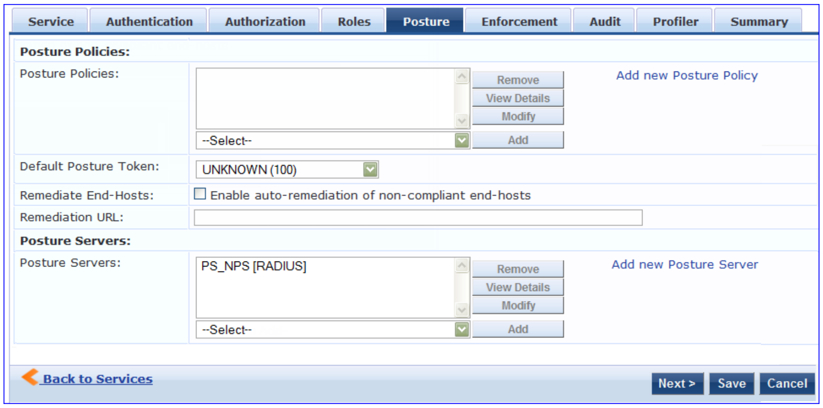
NOTE

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:

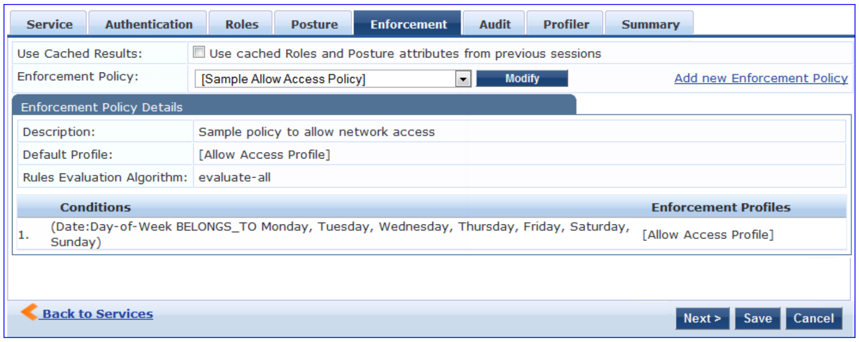
Table 321: *Posture Navigation and Settings*

Navigation	Setting
Add a new Posture Server: - **Posture** (tab) > - **Add new Posture Server** (button) >	 Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Remove View Details Modify Remove View Details Modify Back to Services Next > Save Cancel**Posture Policies:** Posture Policies: --Select to Add-- Default Posture Token: UNKNOWN (100) Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts Remediation URL: **Posture Servers:** Posture Servers: --Select to Add--
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)	 Posture Server Primary Server Backup Server Summary Back to Services Next > Save CancelName: Description: Server Type: ● Microsoft NPS Default Posture Token: UNKNOWN (100)
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.	 Posture Server Primary Server Backup Server Summary Back to Services Next > Save CancelRADIUS Server Name: RADIUS Server Port: (default is 1812) Shared Secret: Verify: Timeout: 5 seconds
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.	 Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary Remove View Details Modify Add Add new Posture Policy Remove View Details Modify Add Add new Posture Server Back to Services Next > Save Cancel**Posture Policies:** Posture Policies: --Select-- Default Posture Token: UNKNOWN (100) Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts Remediation URL: **Posture Servers:** Posture Servers: PS_NPS [RADIUS] --Select--

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 322: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Configure the Enforcement Policy: - **Enforcement** (tab) > - **Enforcement Policy** (selector): **Role_Based_ Allow_Access_ Policy**	 Service Authentication Roles Posture Enforcement Audit Profiler Summary Modify Add new Enforcement Policy Back to Services Next > Save Cancel Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: [Sample Allow Access Policy] Enforcement Policy Details Description: Sample policy to allow network access Default Profile: [Allow Access Profile] Rules Evaluation Algorithm: evaluate-all Conditions — Enforcement Profiles 1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) — [Allow Access Profile]

For instructions about how to build such an Enforcement Policy, refer to "Configuring Enforcement Policies" on page 277.

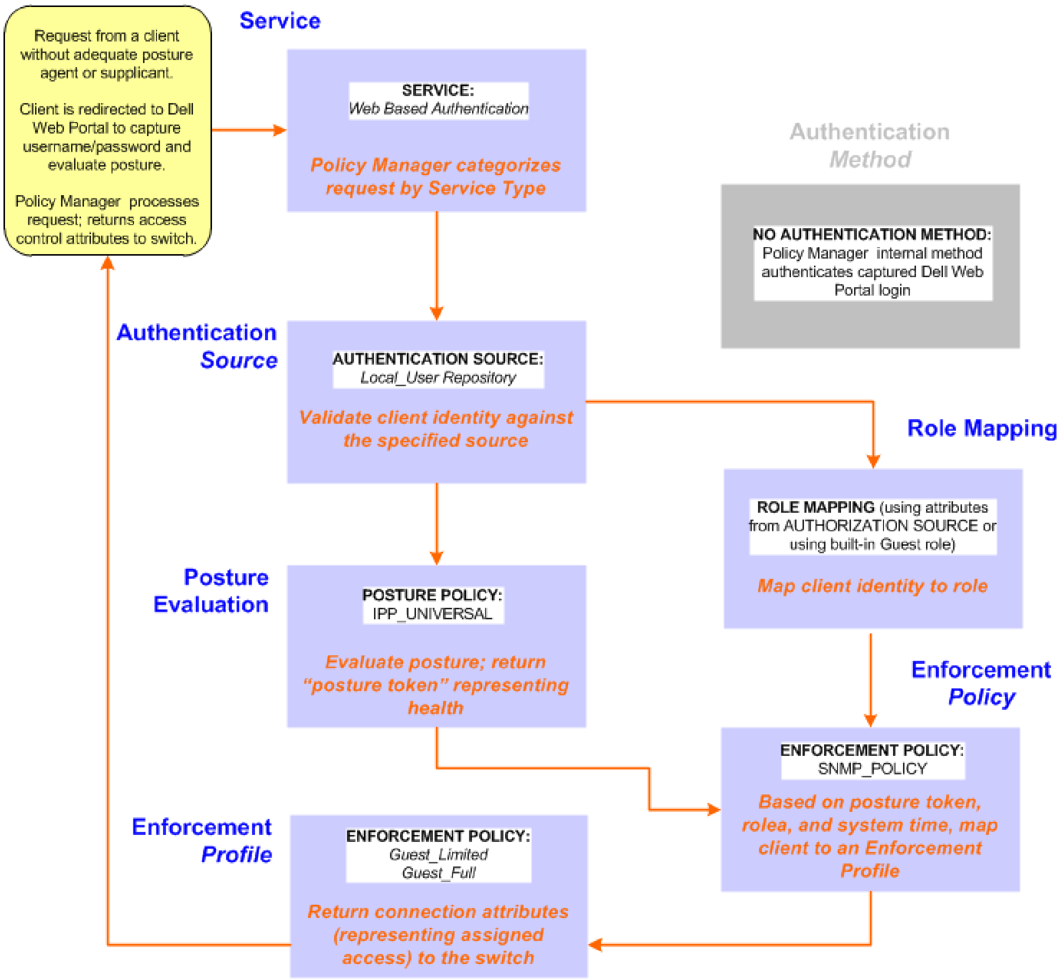
7. Save the Service.

   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 436: *Flow-of-Control of Web-Based Authentication for Guests*


Request from a client without adequate posture agent or supplicant.
Client is redirected to Dell Web Portal to capture username/password and evaluate posture.
Policy Manager processes request; returns access control attributes to switch.
Service
SERVICE:
Web Based Authentication
Policy Manager categorizes request by Service Type
Authentication Method
NO AUTHENTICATION METHOD: Policy Manager internal method authenticates captured Dell Web Portal login
Authentication Source
AUTHENTICATION SOURCE:
Local_User Repository
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (using attributes from AUTHORIZATION SOURCE or using built-in Guest role)
Map client identity to role
Posture Evaluation
POSTURE POLICY:
IPP_UNIVERSAL
Evaluate posture; return "posture token" representing health
Enforcement Policy
ENFORCEMENT POLICY:
SNMP_POLICY
Based on posture token, rolea, and system time, map client to an Enforcement Profile
Enforcement Profile
ENFORCEMENT POLICY:
Guest_Limited
Guest_Full
Return connection attributes (representing assigned access) to the switch

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 323: *Service Navigation and Settings*

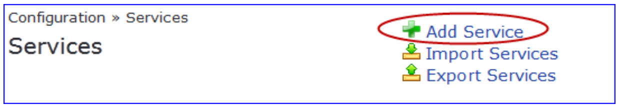
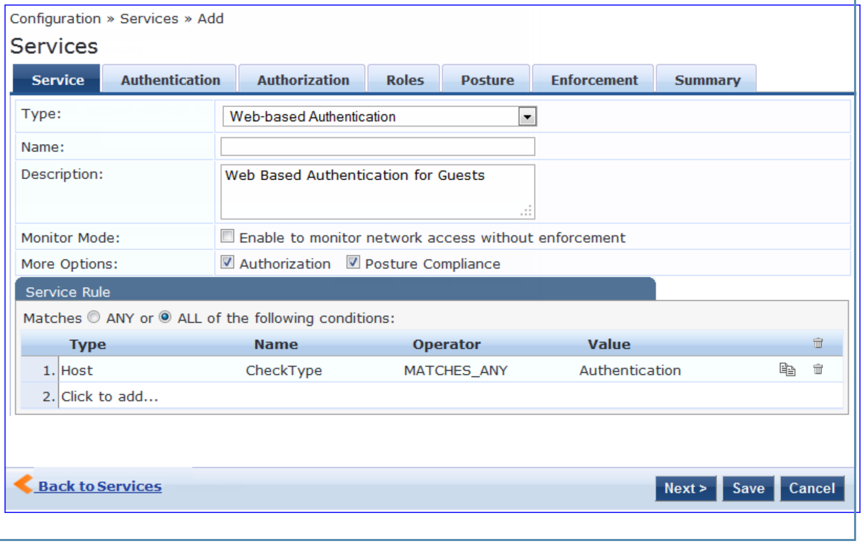
Navigation	Settings
Create a new Service: ● **Services** > ● **Add Service** >	 Configuration » Services Services Add Service Import Services Export Services

Table 323: *Service Navigation and Settings (Continued)*

Navigation	Settings
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**.	

Configuration » Services » Add

Services

Type:	Web-based Authentication
Name:	
Description:	Web Based Authentication for Guests
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☑ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ANY	Authentication
2.	Click to add...			

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.

NOTE 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 324: *Local Policy Manager Database Navigation and Settings*

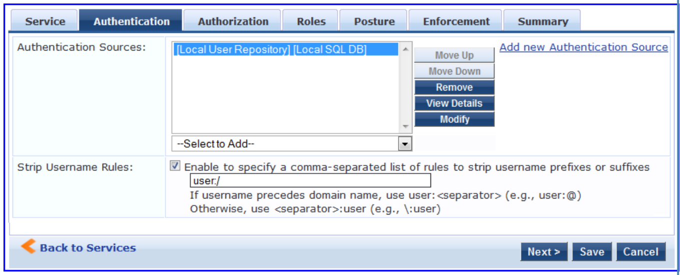
Navigation	Settings
Select the local Policy Manager database: - **Authentication** (tab) > - **Sources** (**Select** drop-down list): **[Local User Repository]** > - **Add** > - **Strip Username Rules** (check box) > - Enter an example of preceding or following separators (if any), with the phrase “user” 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).	 Service | Authentication | Authorization | Roles | Posture | Enforcement | Summary Authentication Sources: [Local User Repository] [Local SQL DB] --Select to Add-- Move Up | Move Down | Remove | View Details | Modify Add new Authentication Source Strip Username Rules: ☑ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes user:/ If username precedes domain name, use user:<separator> (e.g., user:@) Otherwise, use <separator>:user (e.g., \:user) Back to Services Next > | Save | Cancel

Table 325: *Posture Policy Navigation and Settings*

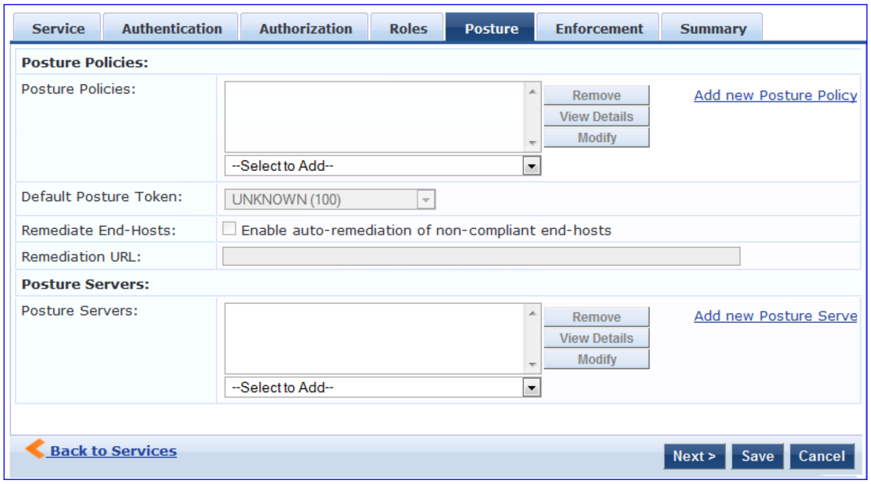
Navigation	Setting
Create a Posture Policy: - **Posture** (tab) > - Enable **Validation Check** (check box) > - **Add new Internal Policy** (link) >	 Service | Authentication | Authorization | Roles | Posture | Enforcement | Summary **Posture Policies:** Posture Policies: --Select to Add-- Remove | View Details | Modify Add new Posture Policy Default Posture Token: UNKNOWN (100) Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts Remediation URL: **Posture Servers:** Posture Servers: --Select to Add-- Remove | View Details | Modify Add new Posture Serve Back to Services Next > | Save | Cancel

Table 325: *Posture Policy Navigation and Settings (Continued)*

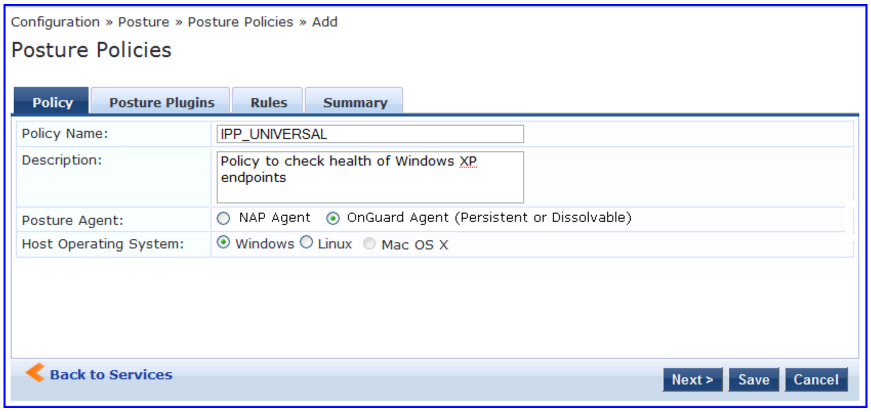
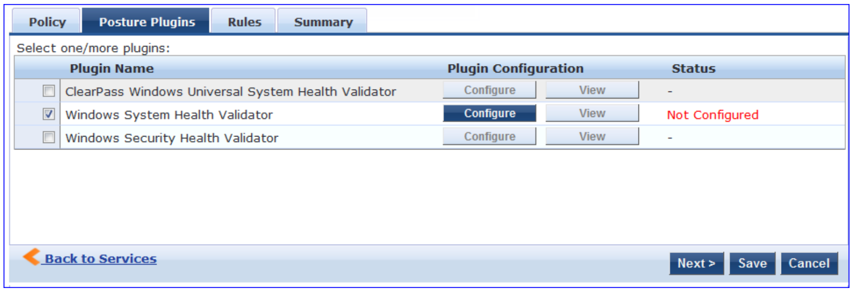
Navigation	Setting
Name the Posture Policy and specify a general class of operating system: • **Policy** (tab) > • **Policy Name** (freeform): *IPP_ UNIVERSAL* > • **Host Operating System** (radio buttons): **Windows** > • When finished working in the **Policy** tab, click **Next** to open the Posture Plugins tab	 Configuration » Posture » Posture Policies » Add Posture Policies Policy | Posture Plugins | Rules | Summary Policy Name: IPP_UNIVERSAL Description: Policy to check health of Windows XP endpoints Posture Agent: ○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable) Host Operating System: ● Windows ○ Linux ○ Mac OS X Back to Services · Next > · Save · Cancel
Select a Validator: • **Posture Plugins** (tab) > • Enable **Windows Health System Validator** > • **Configure** (button) >	 Policy | Posture Plugins | Rules | Summary Select one/more plugins: Plugin Name · Plugin Configuration · Status ☐ ClearPass Windows Universal System Health Validator · Configure · View · - ☑ Windows System Health Validator · Configure · View · Not Configured ☐ Windows Security Health Validator · Configure · View · - Back to Services · Next > · Save · Cancel

Table 325: *Posture Policy Navigation and Settings (Continued)*

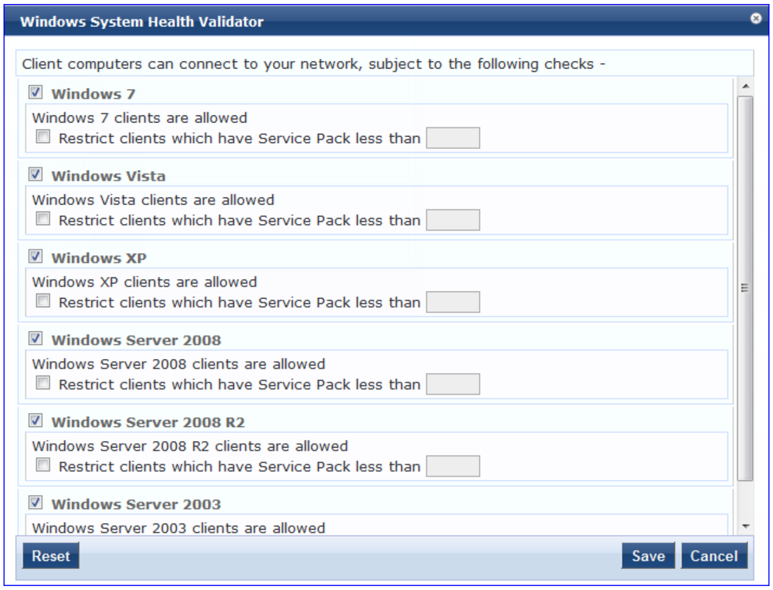
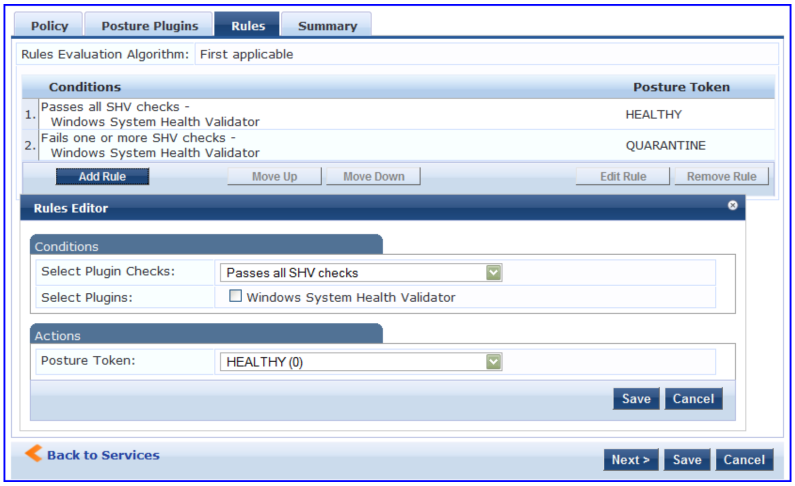
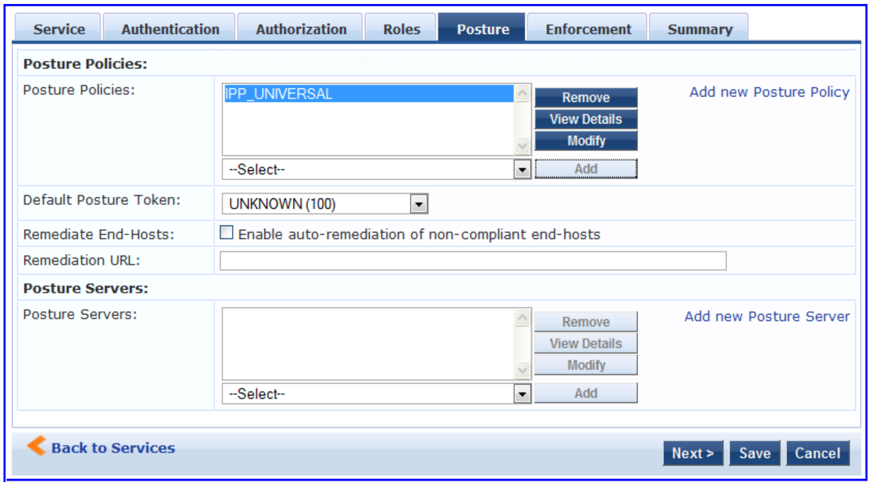
Navigation	Setting
Configure the Validator: - **Windows System Health Validator** (popup) > - **Enable all Windows operating systems** (check box) > - Enable Service Pack levels for Windows 7, Windows Vista®, Windows XP Windows Server® 2008, Windows Server 2008 R2, and Windows Server 2003 (check boxes) > - **Save** (button) > - When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)	 Windows System Health Validator Client computers can connect to your network, subject to the following checks - ☑ Windows 7 Windows 7 clients are allowed ☐ Restrict clients which have Service Pack less than ☑ Windows Vista Windows Vista clients are allowed ☐ Restrict clients which have Service Pack less than ☑ Windows XP Windows XP clients are allowed ☐ Restrict clients which have Service Pack less than ☑ Windows Server 2008 Windows Server 2008 clients are allowed ☐ Restrict clients which have Service Pack less than ☑ Windows Server 2008 R2 Windows Server 2008 R2 clients are allowed ☐ Restrict clients which have Service Pack less than ☑ Windows Server 2003 Windows Server 2003 clients are allowed

Table 325: *Posture Policy Navigation and Settings (Continued)*

Navigation	Setting
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.	 Rules Evaluation Algorithm: First applicable Conditions — Posture Token 1. Passes all SHV checks - Windows System Health Validator — HEALTHY 2. Fails one or more SHV checks - Windows System Health Validator — QUARANTINE Rules Editor Conditions Select Plugin Checks: Passes all SHV checks Select Plugins: ☐ Windows System Health Validator Actions Posture Token: HEALTHY (0)
Add the new Posture Policy to the Service: Back in **Posture** (tab) > **Internal Policies** (selector): **IPP_ UNIVERSAL_XP,** then click the **Add** button	 Posture Policies: Posture Policies: IPP_UNIVERSAL Default Posture Token: UNKNOWN (100) Remediate End-Hosts: ☐ Enable auto-remediation of non-compliant end-hosts Remediation URL: Posture Servers: Posture Servers: --Select--

The following fields deserve special mention:

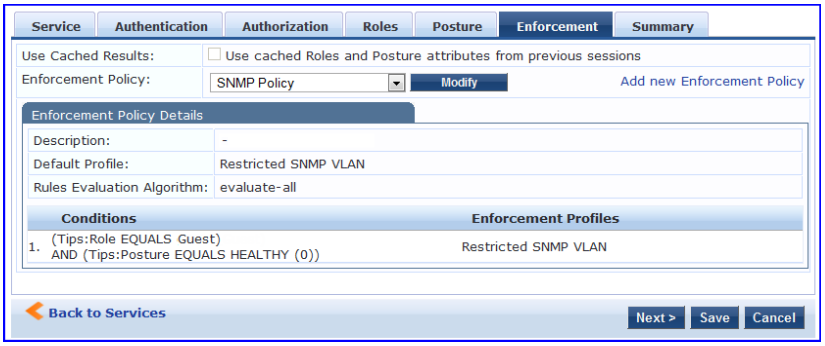
- **Default Posture Token.** Value of the posture token to use if health status is not available.
- **Remediate End-Hosts.** When a client does not pass posture evaluation, redirect to the indicated server for remediation.
- **Remediation URL.** URL of remediation server.

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 326: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Add a new Enforcement Policy: ● **Enforcement** (tab) > ● Enforcement Policy (selector): **SNMP_ POLICY** ● Upon completion, click **Save**.	Service | Authentication | Authorization | Roles | Posture | Enforcement | Summary Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: SNMP Policy ▾ Modify — Add new Enforcement Policy Enforcement Policy Details Description: - Default Profile: Restricted SNMP VLAN Rules Evaluation Algorithm: evaluate-all Conditions — Enforcement Profiles 1. (Tips:Role EQUALS Guest) AND (Tips:Posture EQUALS HEALTHY (0)) — Restricted SNMP VLAN Back to Services — Next > | Save | Cancel

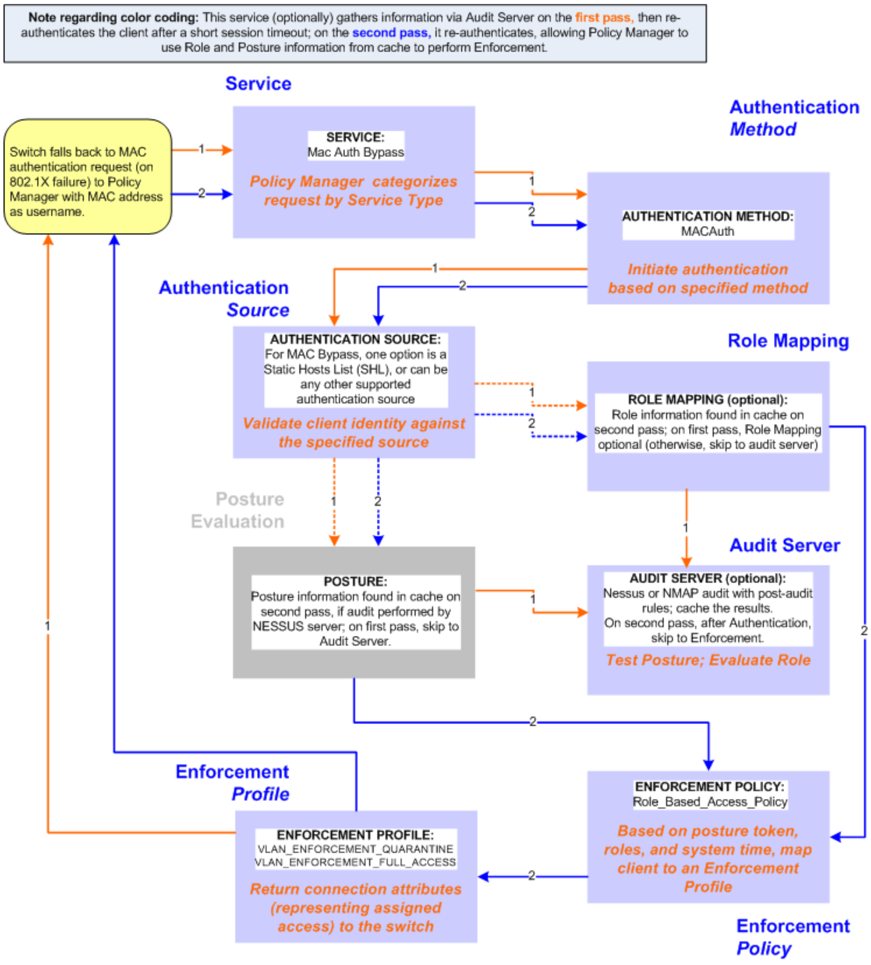
6. Save the Service.

   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 437: *Flow-of-Control of MAC Authentication for Network Devices*


Note regarding color coding: This service (optionally) gathers information via Audit Server on the first pass, then re-authenticates the client after a short session timeout; on the second pass, it re-authenticates, allowing Policy Manager to use Role and Posture information from cache to perform Enforcement.
Service
Switch falls back to MAC authentication request (on 802.1X failure) to Policy Manager with MAC address as username.
1
2
SERVICE: Mac Auth Bypass
Policy Manager categorizes request by Service Type
Authentication Method
1
2
AUTHENTICATION METHOD: MACAuth
Initiate authentication based on specified method
Authentication Source
AUTHENTICATION SOURCE: For MAC Bypass, one option is a Static Hosts List (SHL), or can be any other supported authentication source
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (optional): Role information found in cache on second pass; on first pass, Role Mapping optional (otherwise, skip to audit server)
Posture Evaluation
POSTURE: Posture information found in cache on second pass, if audit performed by NESSUS server; on first pass, skip to Audit Server.
Audit Server
AUDIT SERVER (optional): Nessus or NMAP audit with post-audit rules; cache the results. On second pass, after Authentication, skip to Enforcement.
Test Posture; Evaluate Role
Enforcement Profile
ENFORCEMENT PROFILE: VLAN_ENFORCEMENT_QUARANTINE VLAN_ENFORCEMENT_FULL_ACCESS
Return connection attributes (representing assigned access) to the switch
ENFORCEMENT POLICY: Role_Based_Access_Policy
Based on posture token, roles, and system time, map client to an Enforcement Profile
Enforcement Policy

Configuring the Service

Follow these steps to configure Policy Manager for MAC-based Network Device access.

1. Create a MAC Authentication Service.

Table 327: *MAC Authentication Service Navigation and Settings*

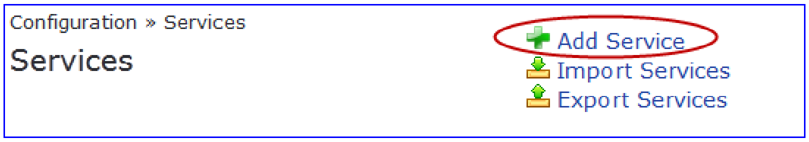
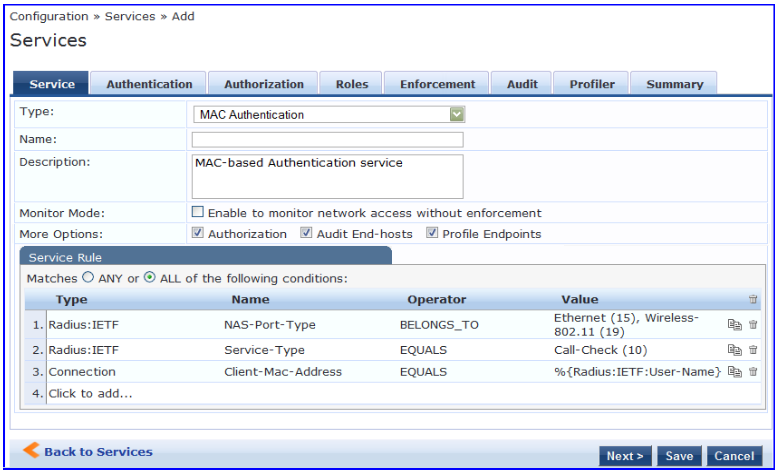
Navigation	Settings
Create a new Service: ● **Services** > ● **Add Service** (link) >	 Configuration » Services Services Add Service Import Services Export Services

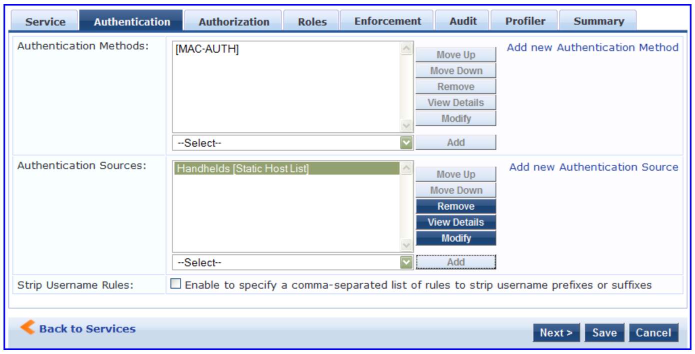
Table 327: *MAC Authentication Service Navigation and Settings (Continued)*

Navigation	Settings
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	 Configuration » Services » Add Services Service Authentication Authorization Roles Enforcement Audit Profiler Summary Type: MAC Authentication Name: Description: MAC-based Authentication service Monitor Mode: ☐ Enable to monitor network access without enforcement More Options: ☑ Authorization ☑ Audit End-hosts ☑ Profile Endpoints Service Rule Matches ○ ANY or ● ALL of the following conditions: Type | Name | Operator | Value 1. Radius:IETF | NAS-Port-Type | BELONGS_TO | Ethernet (15), Wireless-802.11 (19) 2. Radius:IETF | Service-Type | EQUALS | Call-Check (10) 3. Connection | Client-Mac-Address | EQUALS | %{Radius:IETF:User-Name} 4. Click to add...

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 187 for more information. You can also select any other supported type of authentication source.

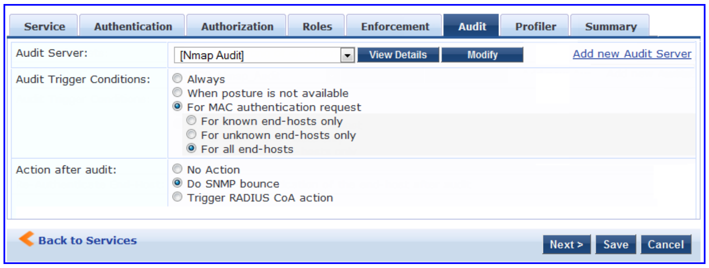
Table 328: *Authentication Method Navigation and Settings*

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)	 Service Authentication Authorization Roles Enforcement Audit Profiler Summary Authentication Methods: [MAC-AUTH] --Select-- Move Up Move Down Remove View Details Modify Add Add new Authentication Method Authentication Sources: Handhelds [Static Host List] --Select-- Move Up Move Down Remove View Details Modify Add Add new Authentication Source Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes Back to Services Next > Save Cancel

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.

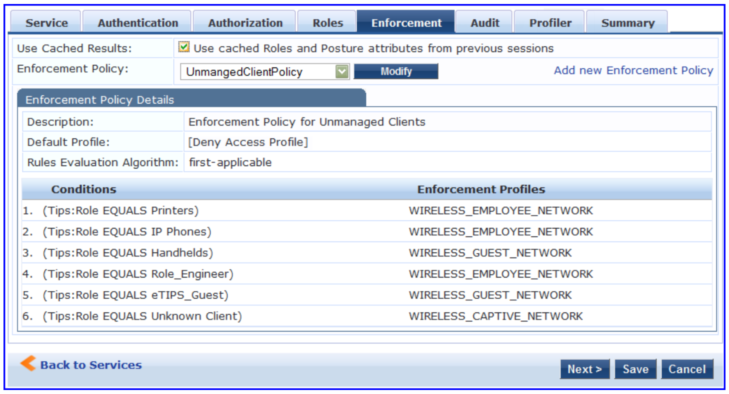
Table 329: *Audit Server Navigation and Settings*

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**	 Audit Server: [Nmap Audit] Audit Trigger Conditions: ○ Always ○ When posture is not available ● For MAC authentication request ○ For known end-hosts only ○ For unknown end-hosts only ● For all end-hosts Action after audit: ○ No Action ● Do SNMP bounce ○ Trigger RADIUS CoA action Service Authentication Authorization Roles Enforcement Audit Profiler Summary View Details Modify Add new Audit Server Back to Services Next > Save Cancel

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 330: *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**.	 Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: UnmangedClientPolicy Enforcement Policy Details Description: Enforcement Policy for Unmanaged Clients Default Profile: [Deny Access Profile] Rules Evaluation Algorithm: first-applicable Conditions — Enforcement Profiles 1. (Tips:Role EQUALS Printers) — WIRELESS_EMPLOYEE_NETWORK 2. (Tips:Role EQUALS IP Phones) — WIRELESS_EMPLOYEE_NETWORK 3. (Tips:Role EQUALS Handhelds) — WIRELESS_GUEST_NETWORK 4. (Tips:Role EQUALS Role_Engineer) — WIRELESS_EMPLOYEE_NETWORK 5. (Tips:Role EQUALS eTIPS_Guest) — WIRELESS_GUEST_NETWORK 6. (Tips:Role EQUALS Unknown Client) — WIRELESS_CAPTIVE_NETWORK Service Authentication Authorization Roles Enforcement Audit Profiler Summary Modify Add new Enforcement Policy Back to Services Next > Save Cancel

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).

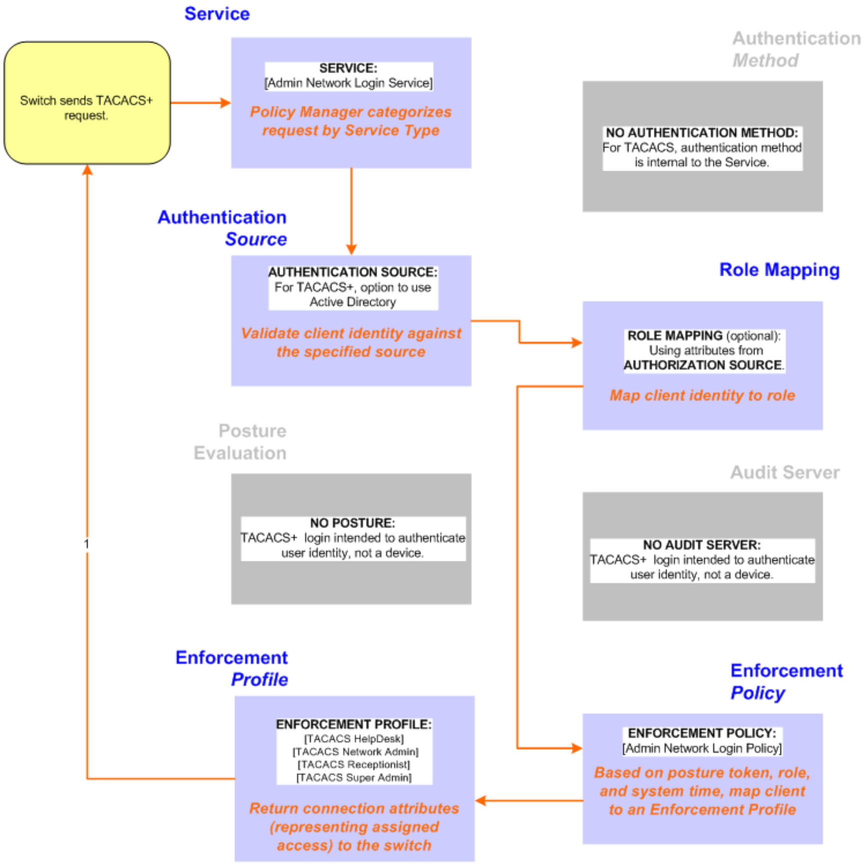
5. Save the Service.

   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 438: *Administrator connections to Network Access Devices via TACACS+*



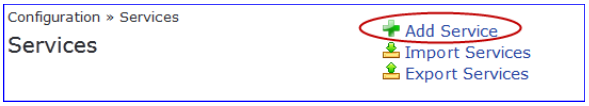
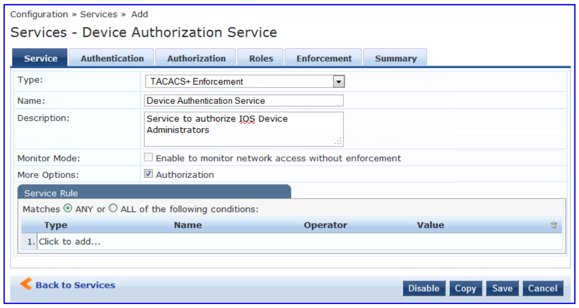
Service
Switch sends TACACS+ request.
SERVICE:
[Admin Network Login Service]
Policy Manager categorizes request by Service Type
Authentication Method
NO AUTHENTICATION METHOD:
For TACACS, authentication method is internal to the Service.
Authentication Source
AUTHENTICATION SOURCE:
For TACACS+, option to use Active Directory
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (optional):
Using attributes from AUTHORIZATION SOURCE.
Map client identity to role
Posture Evaluation
NO POSTURE:
TACACS+ login intended to authenticate user identity, not a device.
Audit Server
NO AUDIT SERVER:
TACACS+ login intended to authenticate user identity, not a device.
1
Enforcement Profile
ENFORCEMENT PROFILE:
[TACACS HelpDesk]
[TACACS Network Admin]
[TACACS Receptionist]
[TACACS Super Admin]
Return connection attributes (representing assigned access) to the switch
Enforcement Policy
ENFORCEMENT POLICY:
[Admin Network Login Policy]
Based on posture token, role, and system time, map client to an Enforcement Profile

Configuring the Service

Perform the following steps to configure Policy Manager for TACACS+-based access:

1. Create a TACACS+ Service.

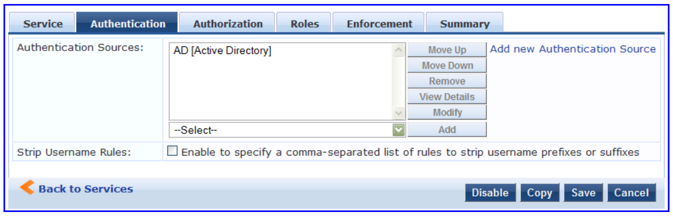
Table 331: *TACACS+ Navigation and Settings*

Navigation	Settings
Create a new Service: ● **Services** > ● **Add Service** (link) >	 Configuration » Services Services Add Service Import Services Export Services
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)	 Configuration » Services » Add Services - Device Authorization Service Service | Authentication | Authorization | Roles | Enforcement | Summary Type: TACACS+ Enforcement Name: Device Authentication Service Description: Service to authorize IOS Device Administrators Monitor Mode: □ Enable to monitor network access without enforcement More Options: ☑ Authorization Service Rule Matches ● ANY or ○ ALL of the following conditions: Type | Name | Operator | Value 1. Click to add... Back to Services Disable | Copy | Save | Cancel

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.

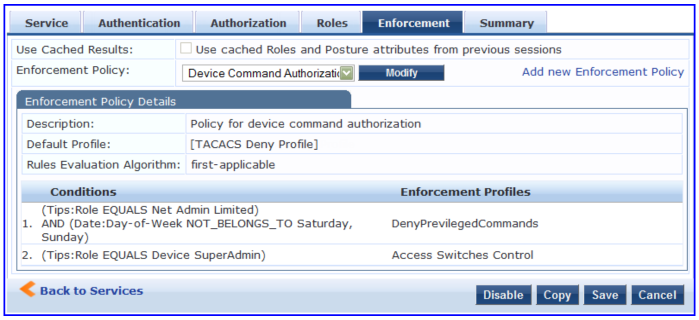
Table 332: *Active Directory Navigation and Settings*

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)	 Authentication Sources: AD [Active Directory] --Select-- Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes Service Authentication Authorization Roles Enforcement Summary Move Up Move Down Remove View Details Modify Add Add new Authentication Source Back to Services Disable Copy Save Cancel

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 333: *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**.	 Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: Device Command Authorizatio Enforcement Policy Details Description: Policy for device command authorization Default Profile: [TACACS Deny Profile] Rules Evaluation Algorithm: first-applicable Conditions — Enforcement Profiles 1. (Tips:Role EQUALS Net Admin Limited) AND (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday) — DenyPrevilegedCommands 2. (Tips:Role EQUALS Device SuperAdmin) — Access Switches Control Service Authentication Authorization Roles Enforcement Summary Modify Add new Enforcement Policy Back to Services Disable Copy Save Cancel

4. Save the Service.

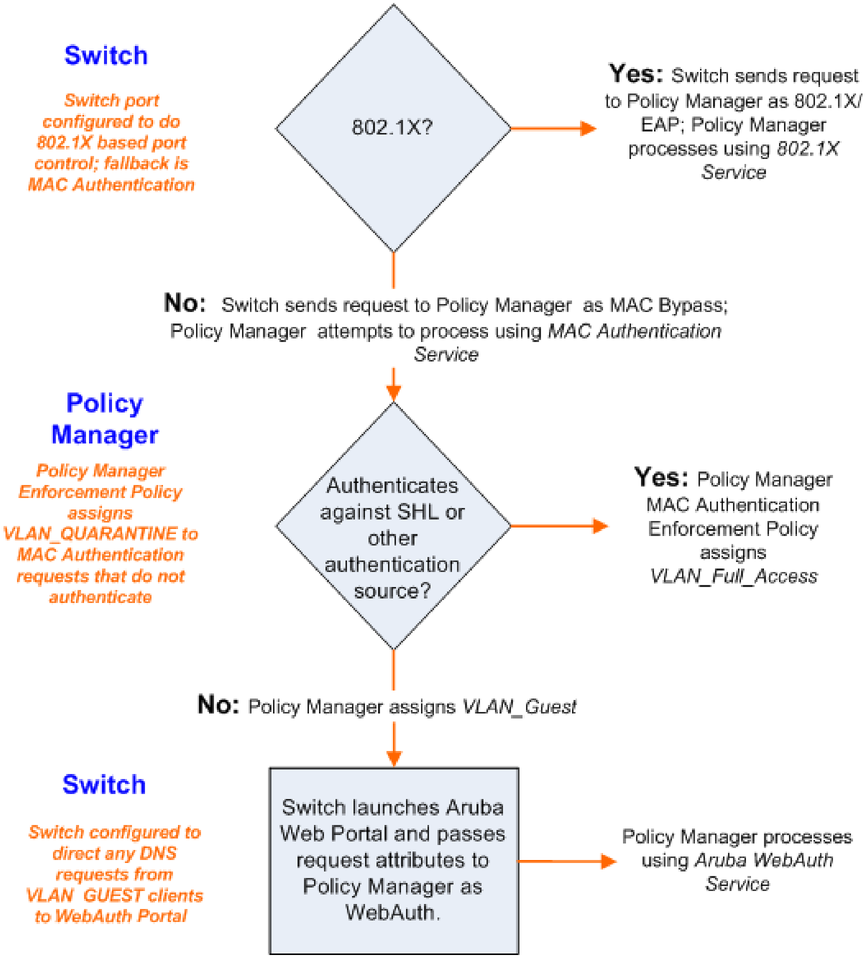
   Click **Save.** The Service now appears at the bottom of the **Services** list.

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 439: *Flow of the Multiple Protocol Per Port Case*


Switch
Switch port configured to do 802.1X based port control; fallback is MAC Authentication
802.1X?
Yes: Switch sends request to Policy Manager as 802.1X/ EAP; Policy Manager processes using 802.1X Service
No: Switch sends request to Policy Manager as MAC Bypass; Policy Manager attempts to process using MAC Authentication Service
Policy Manager
Policy Manager Enforcement Policy assigns VLAN_QUARANTINE to MAC Authentication requests that do not authenticate
Authenticates against SHL or other authentication source?
Yes: Policy Manager MAC Authentication Enforcement Policy assigns VLAN_Full_Access
No: Policy Manager assigns VLAN_Guest
Switch
Switch configured to direct any DNS requests from VLAN GUEST clients to WebAuth Portal
Switch launches Aruba Web Portal and passes request attributes to Policy Manager as WebAuth.
Policy Manager processes using Aruba WebAuth Service

Supported Browsers and Java Versions

The table below provides a list of supported browsers and java versions for the OnGuard Dissolvable Agent. These versions were tested in house and are current as of the time of this release.

Table 334: *Supported Browsers and Java Versions*

Operating System	Browser	Java Version	Known Issues
Windows XP SP3	Firefox 26.x	Java plugin 10.45.2.18 or JRE-1.7_Update 45-b18 Java hotspot(	
Windows XP SP3	IE 8.0.6001	Java plugin 10.40.2.43 or JRE-1.7_Update 40-b43 Java hotspot	Cannot view health scan of endpoints.

Table 334: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Known Issues
Windows XP SP3	Chrome 31.0.1650.63	Java plugin 10.45.2.18 or JRE-1.7_Update 45-b18	
Windows 7 32-bit	Chrome 29.x	Java plugin 10.25.2.17 or JRE-1.7_Update25-b17	
Windows 7 32-bit	IE 8.0.7600	Java plugin 10.45.2.18 or JRE-1.7_45-b18	
Windows 7 32-bit	Firefox 26.x	Java plugin 10.45.2.18 or JRE-1.7_45-b18	
Windows 7 64-bit	Chrome 29.x	Java plugin 10.25.2.16 or JRE-1.7_Update25-b16	
Windows 7 64-bit	IE 10.0.9	Java plugin 10.25.2.16 or JRE-1.7_Update25-b16	Cannot view health scan of endpoints.
Windows 7 64-bit	Firefox 25.01	Java plugin 10.45.2.18 or JRE-1.7 update 45-b18	
Windows Vista	Firefox 26.x	Java plugin 10.45.2.18 or JRE-1.7 update 45-b18	
Windows Vista	Chrome 31.x	Java plugin 10.45.2.18 or JRE-1.7 update 45-b18	
Windows Vista	IE 7.x	Java plugin 10.45.2.18 or JRE-1.7 update 45-b18	Cannot view health scan of endpoints.
Windows 8 32-bit	Chrome 31.0.1650.x	Java plugin 10.45.2.18 or JRE_1.7-Update 45-b18	
Windows 8 32-bit	Firefox 23.x	Java-1.7 or JRE_1.7 update 45-b18	
Windows 8 32-bit	IE 10.0.9	Java plugin 10.45.2.18 or JRE_1.7-Update 45-b18	Cannot view health scan of endpoints.
Windows 8 64-bit	Chrome 31.x	Java plugin 10.45.2.18 or JRE_1.7-Update 45-b18	
Windows 8 64-bit	Firefox 25.x	Java plugin 10.45.2.18 or JRE_1.7-Update 45-b18	
Windows 8 64-bit	IE 10.0.9	Java plugin 10.45.2.18 or JRE_1.7-Update 45-b18	Cannot view health scan of endpoints.

Table 334: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Known Issues
Windows 2008 R2 64-bit	IE 10.0.x	Java 10.5.0.-06 or JRE_1.7-Update05-b06	Cannot view health scan of endpoints.
Windows 2008 R2 64-bit	Firefox 26.x	Java plugin 10.5.0.06 or JRE-1.7_Update05_b06	
Windows 2003	Firefox 11.x	Java plugin 10.45.2.18 or JRE-1.7_Update45-b18	
Mac 10.9	Firefox 26.x	Java plugin 10.45.2.18 or JRE-1.7_Update45-b18	
Mac 10.9	Chrome 29.0.1547	JRE_7 update 40	The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 installed.
Mac 10.9	Safari 6.0.5	JRE-1.7_Update 40	The OnGuard applet needs to run in "Unsafe mode" on Safari in order to perform health checks.
Mac 10.8.1	Firefox 24.x	Java plugin 10.40.2.43 or JRE_1.7_40-b43	
Mac 10.8.1	Chrome 29.0.1547	JRE-1.7 update 40	The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 installed.
Mac 10.8.1	Safari 6.0.5	Java plugin 10.40.2.43 or JRE-1.7 Update 40-b43(TM) 64 bit	
Mac 10.7.5	Firefox 23.x	Java plugin 10.40.2.43 or JRE-1.7_Update40-b43	
Mac 10.7.5	Chrome 28.x	Java plugin 10.40.2.43 or JRE-1.7_Update40-b43	The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 installed.
Mac 10.7.5	Safari 6.0.x	Java plugin 10.40.2.43 or JRE-1.7_Update40-b43	
Mac 10.6	Firefox 25.0.1	JRE 10.6 Update 16 or Java-1.6_51	
Mac 10.6	Chrome 29.x	JRE 10.6 Update 16 or Java-1.6_51	The OnGuard Web Agent does not work with Chrome on Mac OS X with Java 7 installed.
Mac 10.6	Safari 5.1.9	JRE 10.6 Update 16 or Java-1.6_51	