Dell Networking W-ClearPass Policy Manager 6.2

User Guide

Copyright Information

Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include the Aruba Networks logo, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

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

Contents

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.

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.

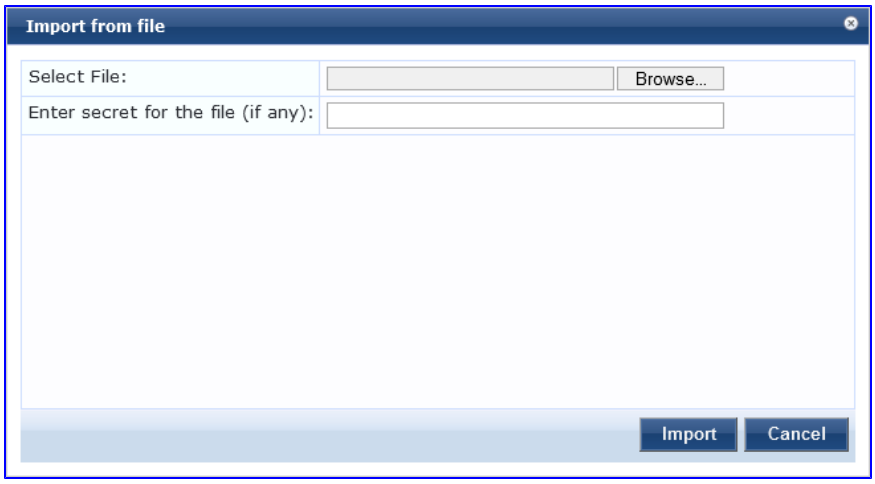
- "Importing" on page 12
- "Exporting" on page 13.

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.

To import into Policy Manager

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



2. Click **Browse** and select the file you want to import from your hard drive.

   The file 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. The API Guide contains more information about the format and contents of these XML files.

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

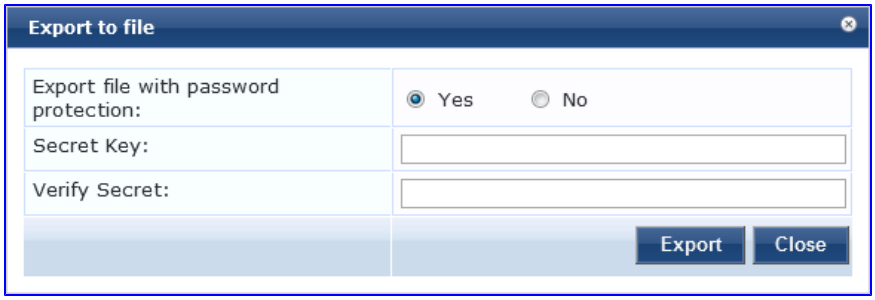
Exporting

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. You can:

- Export all the items.
- Export one or more items.

To export all the items in a list

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

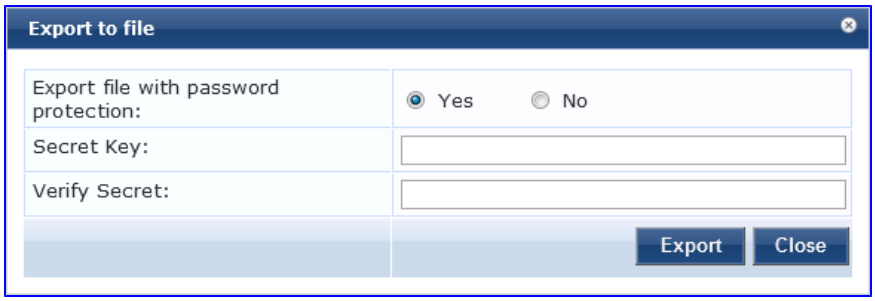


2. If you want the file password protected, select **Yes** and enter a password twice (in the Secret Key and Verify Secret fields). If you do not want the file passowrd protected, select **No**.
3. Click **Export**.

Depending on which browser you use, the file is automatically saved to your hard drive or you are asked to save it, and you may be asked where.

To export one or more items in a list

1. Select the check box next to the items you want to export.
2. Click the **Export** button at the bottom of the list. The Export to File dialog box appears.



3. 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 passowrd protected, select **No**.
4. Click **Export**.

Depending on which browser you use, the file is automatically saved to your hard drive or you are asked to save it, and you may be asked where.

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

Server Port Overview

Figure 1 *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 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 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)	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 290 for more information.

Powering Off the System

Perform the following 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 Passwords to Factory Default

Administrator passwords in Policy Manager can be reset to factory defaults by logging into 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 "Server Port Configuration " on page 15 for details.
2. Reboot the system. See the `restart` command.
3. 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 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 (or 3, if you want to generate a support key, as well).
5. Once the password recovery key is generated, email the key to Dell technical support. A unique password will be generated from the recovery key and emailed back to you.
6. Enter the following 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 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 for details.

2. Connect to the Policy Manager appliance via the front serial port (using any terminal program). See "Server Port Configuration " on page 15 for details.
3. Reboot the system. See the `restart` command.
4. When the system restarts it waits at the following prompt for 10 seconds:

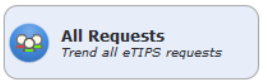
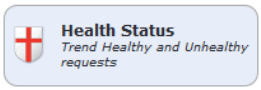
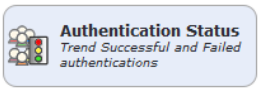
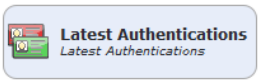
   ```
   Generate support keys? [y/n]:
   ```

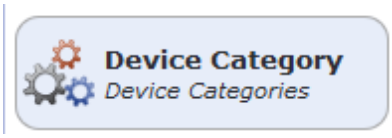
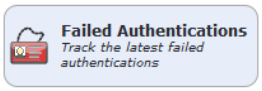
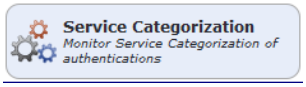
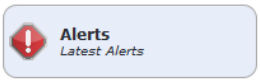
   Enter ‘y’ at the prompt. The system prompts with the following choices:

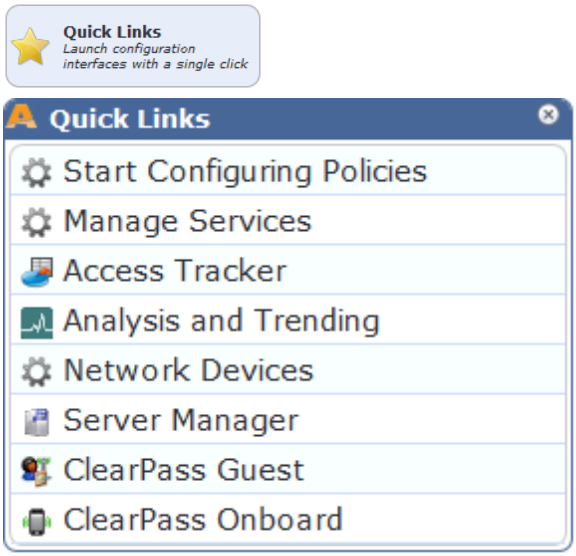
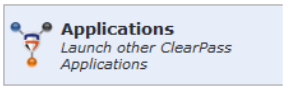
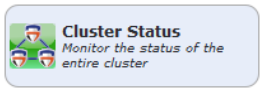
   ```
   Please select a support key generation option.
   1) Generate password recovery key
   2) Generate a support key
   3) Generate password recovery and support keys
   Enter the option or press any key to quit:
   ```

5. To generate the support key, select option 2 (or 3, if you want to generate a password recovery key, as well).
6. Once 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.

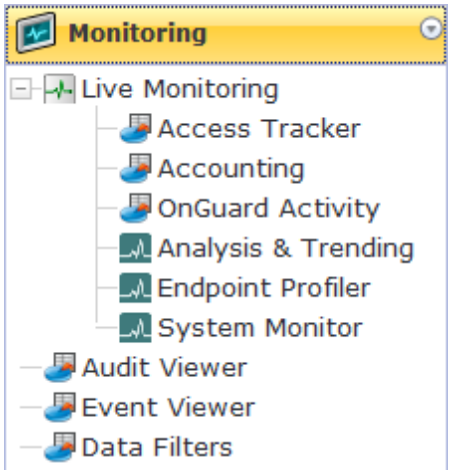
The Policy Manager **Dashboard** menu allows you to display system health and other request related statistics. Policy Manager comes pre-configured with different dashboard elements. The screen on the right of the dashboard menu is partitioned into five fixed slots. You can drag and drop any of the dashboard elements into the five slots. The dashboard elements are listed below:

	This shows a graph of all requests processed by Policy Manager over the past week. This includes 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.
	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.
	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.
	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.

	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.
	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 smartdevices identified by Profile.
	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.
	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.
	This shows a bar chart with each bar representing an 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.
	This shows a table of last few system level events. Clicking on a row drills down into the Event Viewer

	Quick Links shows links to common configuration tasks: • **Start Configuring Policies** links to the Start Here Page under Configuration menu. Start configuring Policy Manager Services from here. • **Manage Services** links to the Services page under 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 Configuration menu. Configure network devices from here. • **Server Manager** links to the Server Configuration screen under Administration menu. • **ClearPass Guest** links to the ClearPass Guest application. This application opens in a new tab. • **ClearPass Onboard** links to the ClearPass Onboard screen within the ClearPass Guest application. This application opens in a new tab.
	This shows links to the Dell applications that are integrated with Policy Manager, such as Guest or Insight.
	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** menu provides the following interfaces:



- Live Monitoring
  - "Access Tracker" on page 24
  - "Accounting" on page 26
  - "OnGuard Activity " on page 33
  - "Analysis and Trending" on page 35
  - "Endpoint Profiler " on page 36
  - "System Monitor" on page 37
- "Audit Viewer" on page 39
- "Event Viewer " on page 41
- "Data Filters " on page 42

Access Tracker

The Access Tracker provides a real-time display of system activity, with optional auto-refresh, at: **Monitoring > Live Monitoring > Access Tracker.** Click on **Edit** to change the Access Tracker display parameters.

Figure 2 *Access Tracker (Edit Mode)*

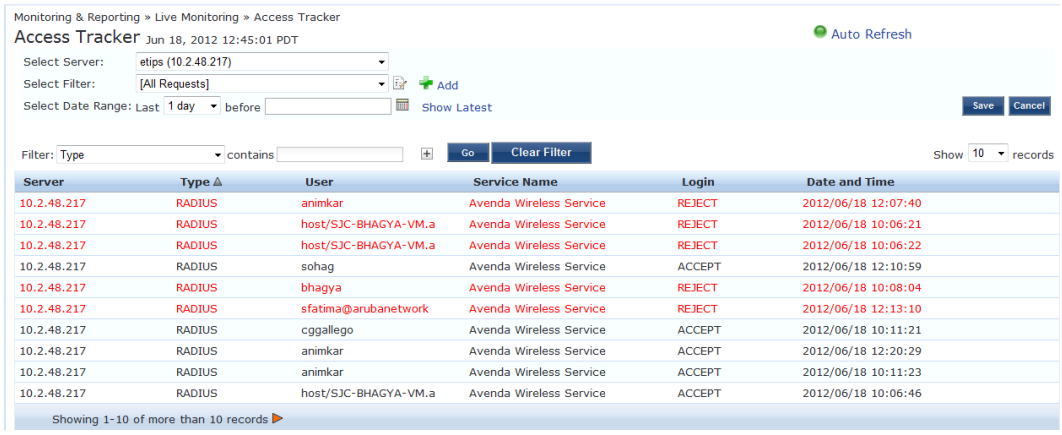
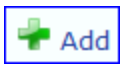


Table 3: *Access Tracker Display Parameters*

Container	Description
Select Server	Select server for which to display dashboard data. Select All to display transactions from all nodes in the Policy Manager cluster.
Auto Refresh	Click to toggle On/Off.

Container	Description
Select Filter	Select filter to constrain data display.
	Modify the currently displayed data filter
 **Add**	Go to **Data Filters** page to create a new data filter.
Select Date Range	Select the number of days prior to the configured date for which Access Tracker 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.
Save/Cancel	Save or cancel edit operation

To display a specific set of records, use the simple filter controls. The filter controls enable you to filter by Protocol Type, User, Service Name, MAC Address, or Status. Note that this filter is applied on top of the display constraints configured previously (See table above).

Table 4: *Access Tracker Simple Filter*

Container	Description
Filter	Select a filter type from the drop down list: Type, User, Service Name, MAC Address, Login
contains	Enter the string to search for.
Clear Filter	Clear the currently applied filter and show all entries.
Show n Records	Show 10, 20, 50 or 100 rows. Once selected, this setting is saved and available in subsequent logins.

Table 5: *Access Tracker Session Types*

Container	Description
RADIUS	All RADIUS transactions (802.1X, MAC-Auth, generic RADIUS)
TACACS+	All TACACS+ transactions
WebAuth	Web authentication transactions (Dissolvable Agent, OnGuard)
Application	All Dell application authentications (Insight, Guest)

Viewing Session Details

To view details for a session, click on the row containing any entry. Policy Manager divides the view into multiple tabs. Depending on the type of authentication - RADIUS, WebAuth, TACACS, Application - the view displays

different tabs.

- Summary - This tab shows a summary view of the transaction, including policies applied.
- Input - 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.
- Output - This tab shows the attributes that were sent to the network device and the (posture capable) endpoint.
- Alerts - This tab shows the reason for authentication or authorization failure.
- Accounting - This tab is only available for RADIUS sessions. This shows the RADIUS accounting details for the session, including re authentication details.
- Authorizations - This tab is only available for TACACS+ sessions. This shows the commands entered at the network device, and the authorization status.
- RADIUS CoA - 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.

Table 6: *Session Details Popup Actions*

Container	Description
Change Status	This button allows you to change the access control status of a session. This function is only available for RADIUS and WebAuth. • Agent - This type of control is available for a session where the endpoint has the OnGuard Agent installed. Actions allowed are: Bounce, Send Message and tagging the status of the endpoint as Disabled or Known. • SNMP - This type of 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 that, for this type of control, SNMP read and write community strings have to be configured for the network device; furthermore, Policy Manager must be configured as an SNMP trap receiver to receive link up/down traps. • RADIUS CoA - This type of control is available for any session where access was previously controlled by a RADIUS transaction. Note that 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 color coded in red. Warning messages are color coded in orange.
Close	RADIUS response attributes sent to the device

Accounting

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

Figure 3 *Accounting (Edit Mode)*

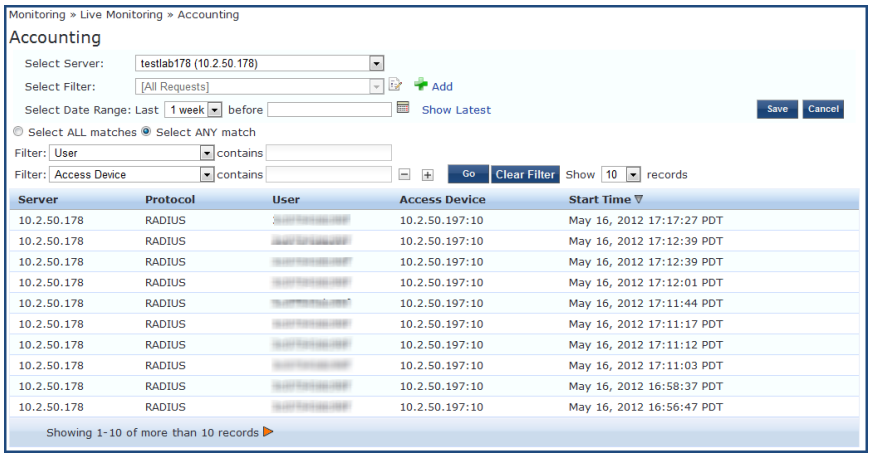
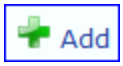


Table 7: *Accounting*

Container	Description
Select Server	Select server for which to display dashboard data.
Select Filter	Select filter to constrain data display.
Modify 	Modify the currently displayed data filter
Add 	Go to Data Filters page to create a new data filter.
Select Date Range	Select the number of days prior to the configured date for which 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.
Save/Cancel	Save or cancel edit operation
Show <n> records	Show 10, 20, 50 or 100 rows. Once selected, this setting is saved and available in subsequent logins.

Click on any row to display the corresponding Accounting Record Details.

Figure 4 *RADIUS Accounting Record Details (Summary tab)*

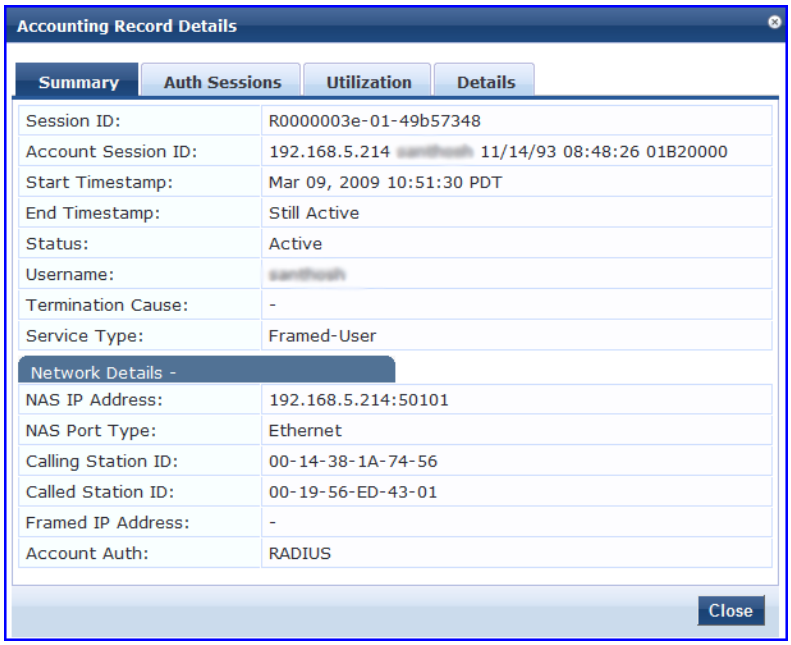


Figure 5 *RADIUS Accounting Record Details (Auth Sessions tab)*

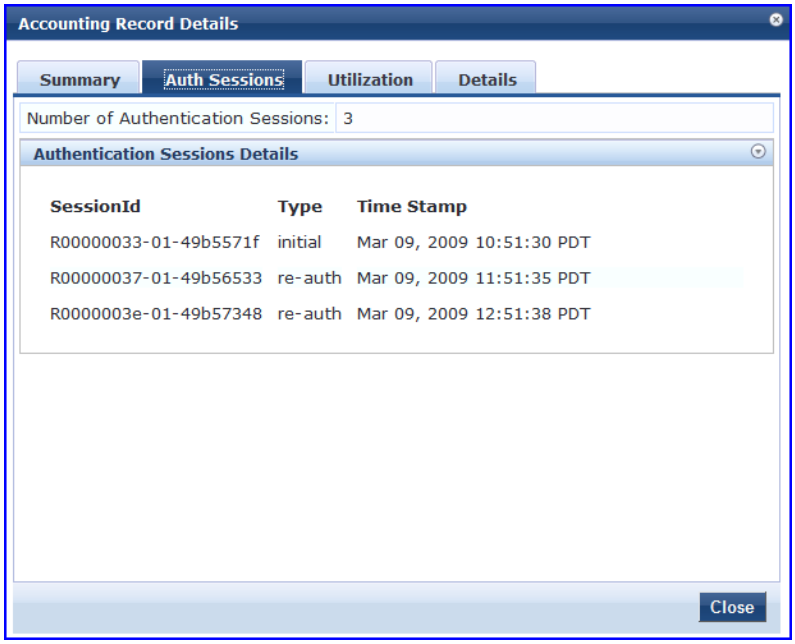


Figure 6 *RADIUS Accounting Record Details (Utilization tab)*

Figure 7 *RADIUS Accounting Record Details (Details tab)*

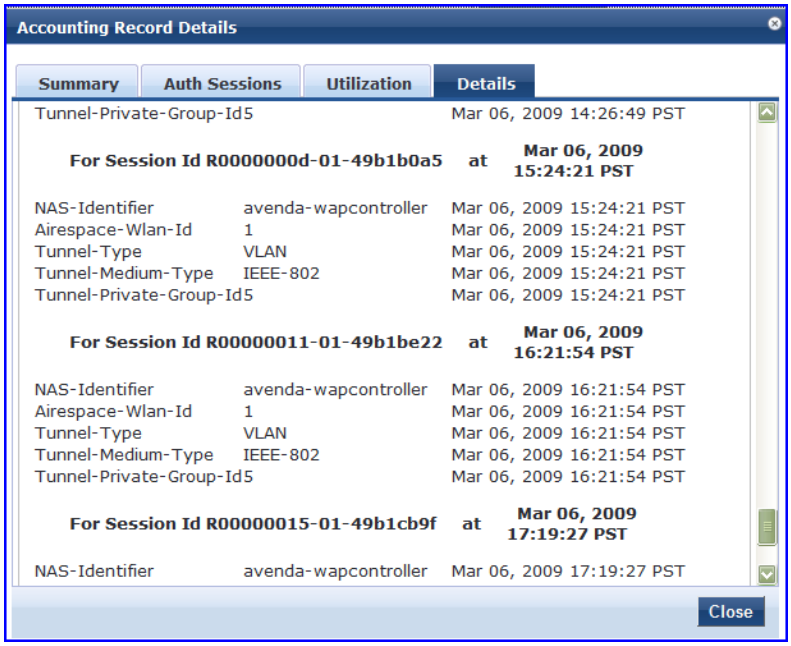


Table 8: *RADIUS Accounting Record Details*

Tab	Container	Description
Summary	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

Tab	Container	Description
	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
	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.
Auth Sessions	Session ID	Policy Manager session ID
	Type	Initial authentication or a re-authentication
	Time Stamp	When the event occurred
Utilization	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)

Tab	Container	Description
	Account Input Octets	Octets sent 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	
Details		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.

Figure 8 *TACACS+ Accounting Record Details (Request tab)*

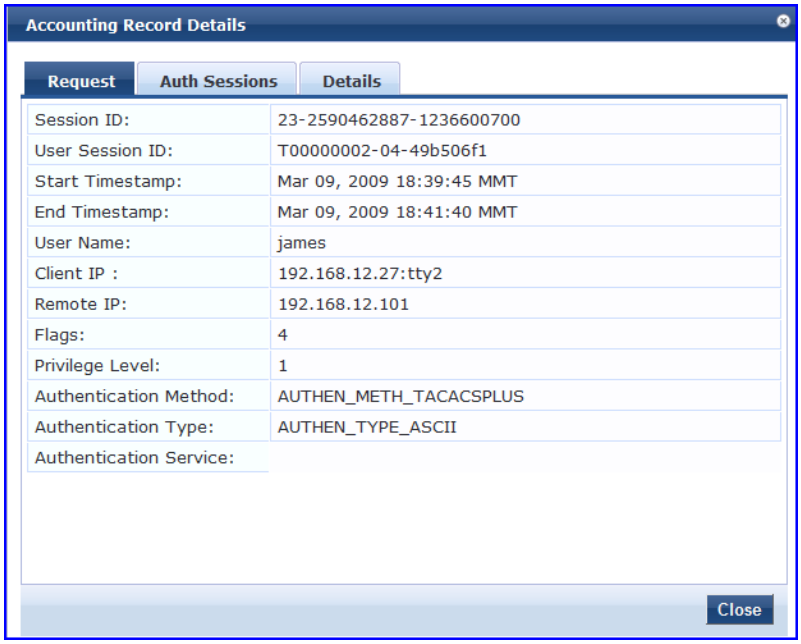


Figure 9 *TACACS+ Accounting Record Details (Auth Sessions tab)*

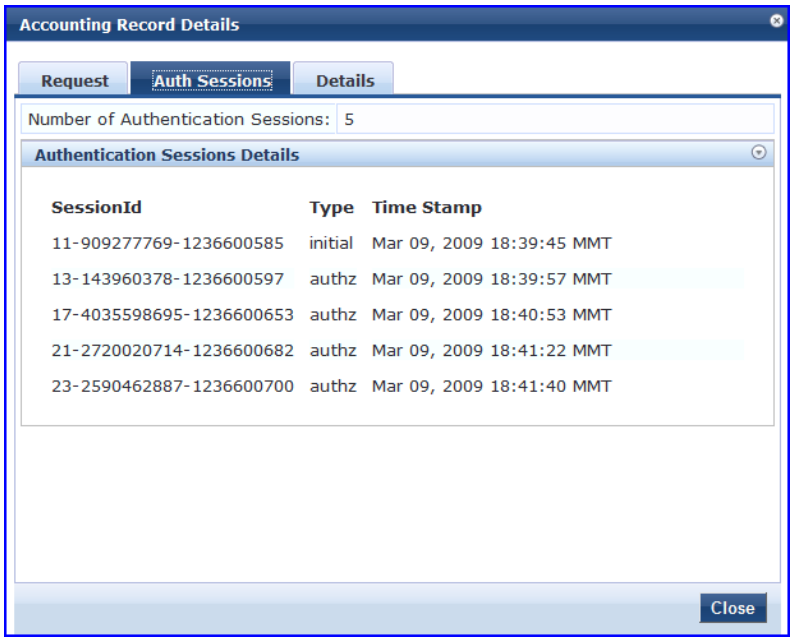


Figure 10 *TACACS+ Accounting Record Details (Details tab)*

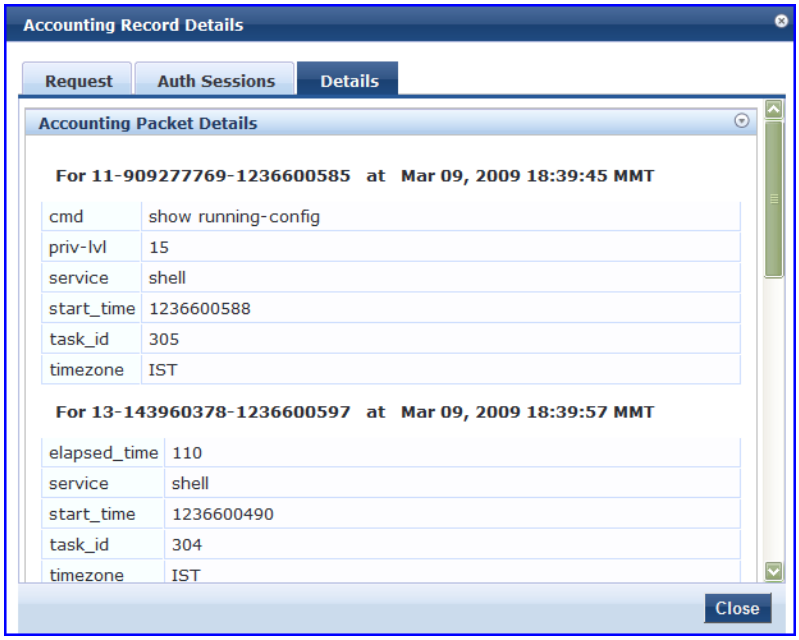


Table 9: *TACACS+ Accounting Record Details*

Tab	Container	Description
Request	Session ID	Unique ID associated with a request
	User Session ID	A session ID that correlates authentication, authorization and accounting records

Tab	Container	Description
	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	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.
Auth Sessions	Number of Authentication Sessions	Total number of authentications (always 1) and authorizations in this session
	Authentication Session Details	For each request ID, denotes whether it is an authentication or authorization request, and the time at which the request was sent
Details		For each authorization request, shows: cmd (command typed), priv-lvl (privilege level of the administrator executing the command), service (shell), etc.

OnGuard Activity

The OnGuard Activity screen shows the realtime status of all endpoints that have Dell W-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 that bouncing of endpoints will only work with endpoints running the persistent agent.

Figure 11 *Fig: OnGuard Activity*

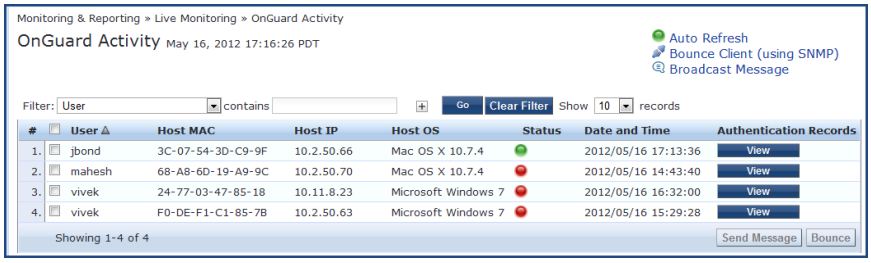
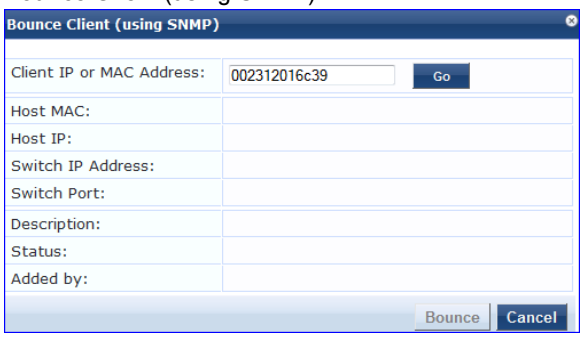
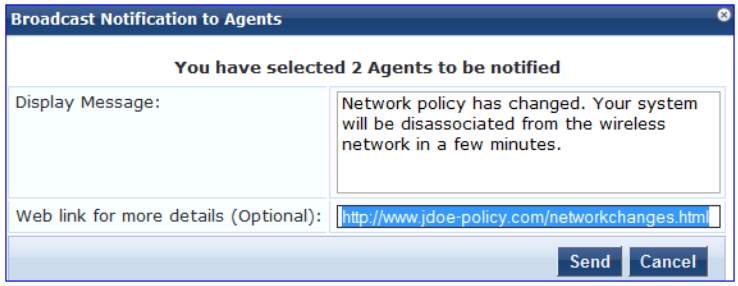
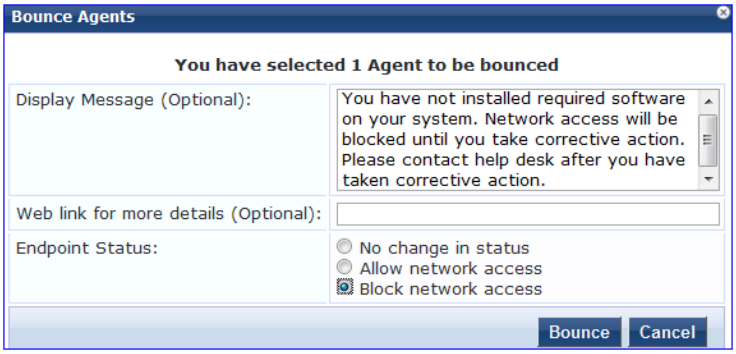


Table 10: *OnGuard Activity*

Container	Description
Auto Refresh	Toggle auto-refresh. If this is turned on, all endpoint activities are refreshed automatically.
Bounce 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. Note that, for this operation to work: • 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 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.
Broadcast Message 	Send a message to all active endpoints
Send Message	Send a message to the selected endpoints.

Container	Description
Bounce  	Initiate a bounce on the managed interface on the endpoint. • Display Message - An optional message to display on the endpoint (via the OnGuard interface). • Web link - An optional clickable URL that is displayed along with the Display Message. • Endpoint Status - No change - 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 that this action just sets the status of the endpoint as "Known". You need to configure Enforcement Policy Rules to allow access to "Known" endpoints. Block network access - Always block network access. Blacklist this endpoint. Note that this action just sets the status of the endpoint as "Disabled". You need to configure Enforcement Policy Rules to allow access to "Disabled" endpoints. This action results in tags being created for the specified endpoint in the Endpoints table (**Configuration > Identity > Endpoints**). One or more of the following tags are created: Disabled by, Disabled Reason, Enabled by, Enabled Reason, Info URL.

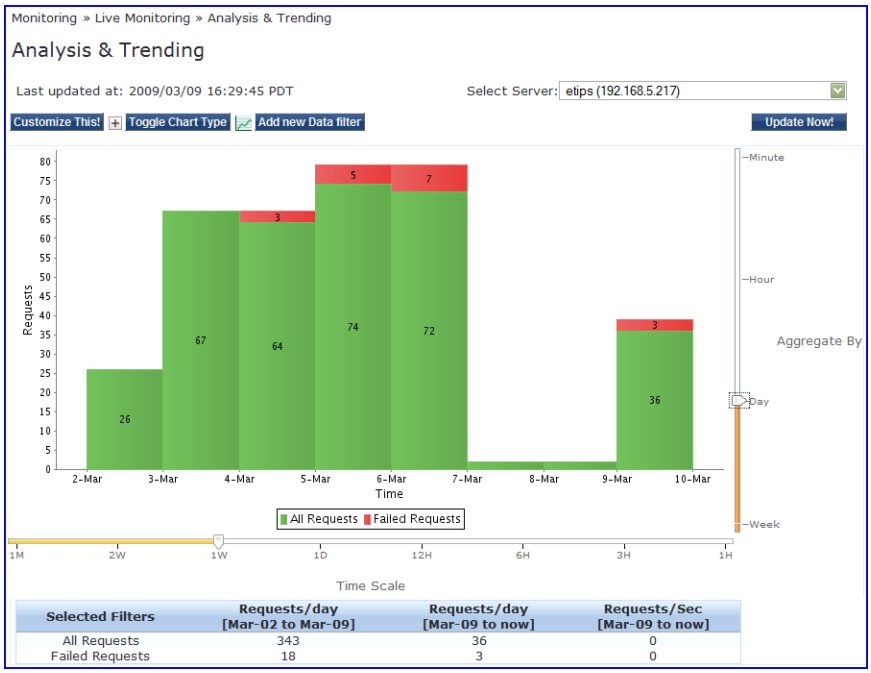
Analysis and Trending

Monitoring > Live Monitoring > Analysis & 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 summary table at the bottom shows the per-filter count for the aggregated data.

Each bar (corresponding to each filter) in the bar graph is clickable. Clicking on the bar drills down into the "Access Tracker" on page 24, showing session data for that time slice (and for that many requests). Similarly, for a line graph, clicking on the circle (corresponding to each plotted point in the graph) drills down into Access Tracker.

Figure 12 *Analysis and Trending*



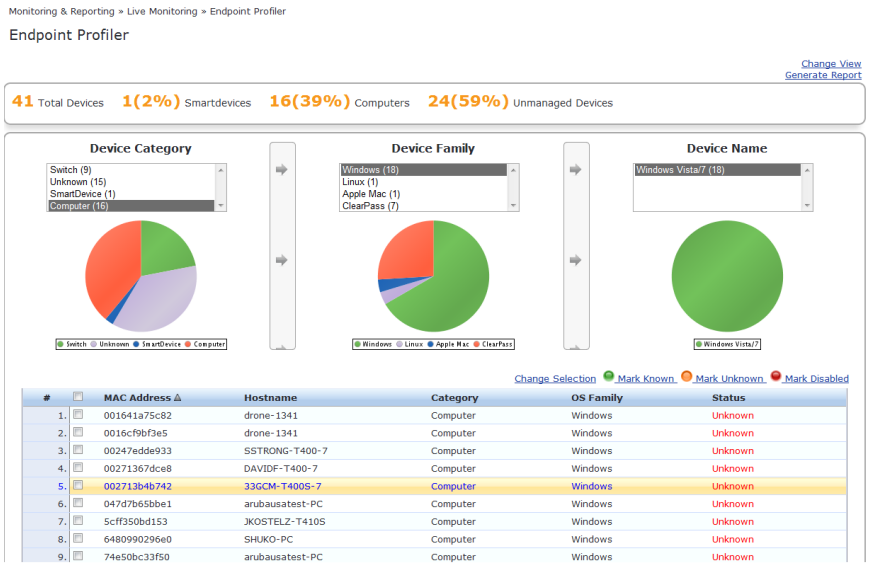
To add additional filters, refer to "Data Filters " on page 42.

- **Select Server** - Select a node from the cluster for which data is to be displayed.
- **Update Now**- Click on this button to update the display with the latest available data.
- **Customize This**- Click on this link to customize the display by adding filters (up to a maximum of 4 filters)
- **Toggle Chart Type**- Click on this link to toggle chart display between line and bar type.
- **Add New Data Filter** - Click on this to add a new 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 on the Change Selection link to change the selection criteria used to list the devices.

Figure 13 *Endpoint Profiler*



You can view endpoint details about a specific device by clicking on a device in the table below the graphs. Select the **Cancel** button to return to the **Endpoint Profiler** page.

Figure 14 *Fig: Endpoint Profiler Details*

System Monitor

The System Monitor is available by navigating to **Monitoring > Live Monitoring > System Monitor**.

- **Select Server**- Select a node from the cluster for which data is to be displayed.
- **Update Now**- Click on this button to update the display with the latest available data.

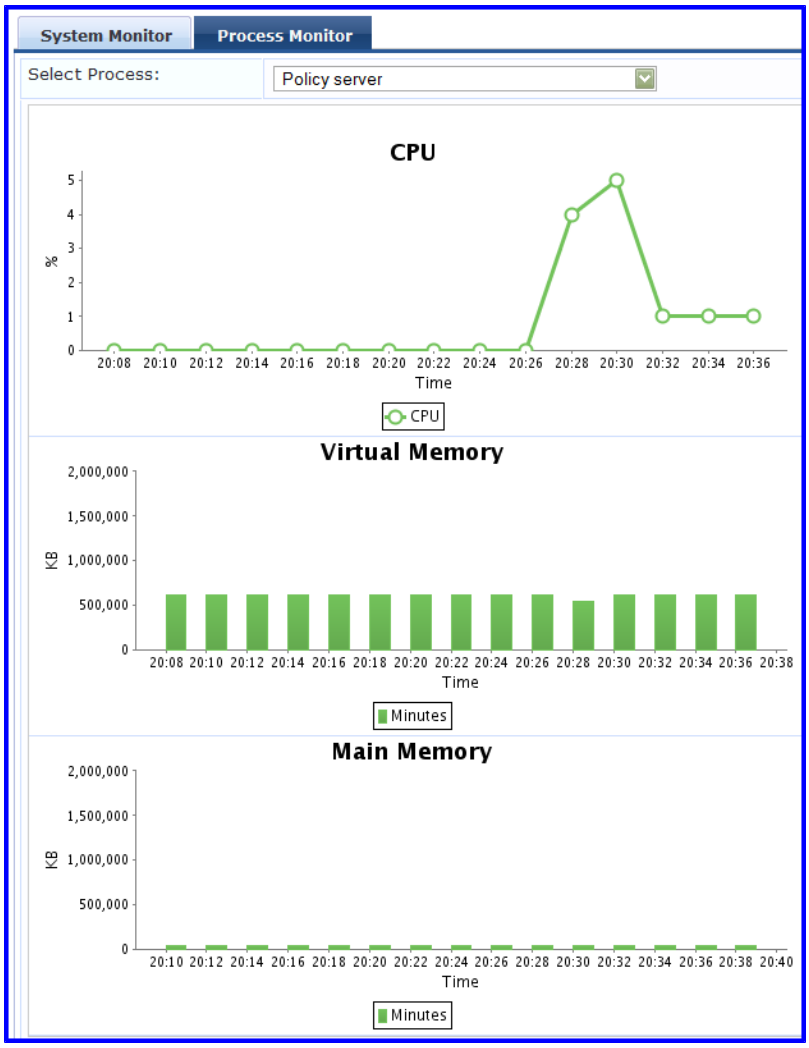
The **System Monitor Page** includes two tabs:

- **System Monitor**- For the selected server, provides load statistics, including CPU, memory, swap memory, physical disk space, and swap disk space:

Figure 15 *System Monitor Graphs*

- **Process Monitor**- For the selected server and process, provides critical usage statistics, including CPU, Virtual Memory, and Main Memory. Use **Select Process** to select the process for which you want to see the usage statistics.

Figure 16 *Figure Process Monitor Graphs*



Audit Viewer

The Audit Viewer display provides a dynamic report of Actions, filterable by Action, Name and Category (of policy component), and User, at: **Monitoring > Audit Viewer**.

Figure 17 *Audit Viewer*

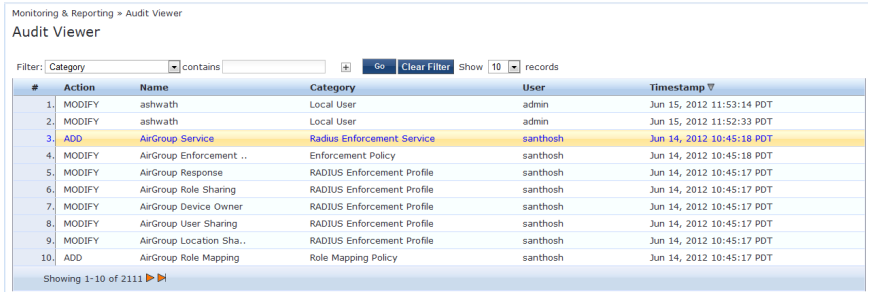


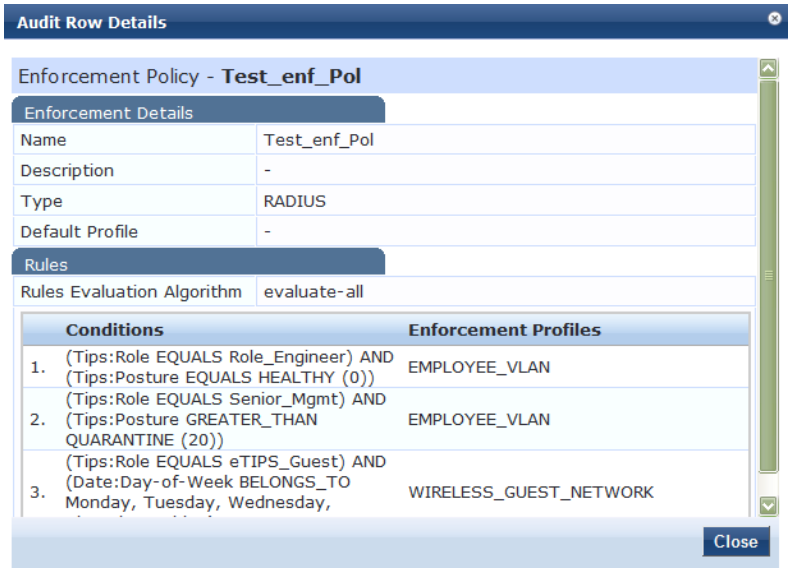
Table 11: *Audit Viewer*

Container	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. Once selected, this setting is saved and available in subsequent logins.

Click on any row to display the corresponding Audit Row Details:

- For **Add** Actions, a single popup displays, containing the new data.

Figure 18 *Audit Row Details (Old Data tab)*



For **Modify** Actions, a popup with three tabs displays, comparing the old data and the new.

Figure 19 *Audit Row Details (Old Data tab)*

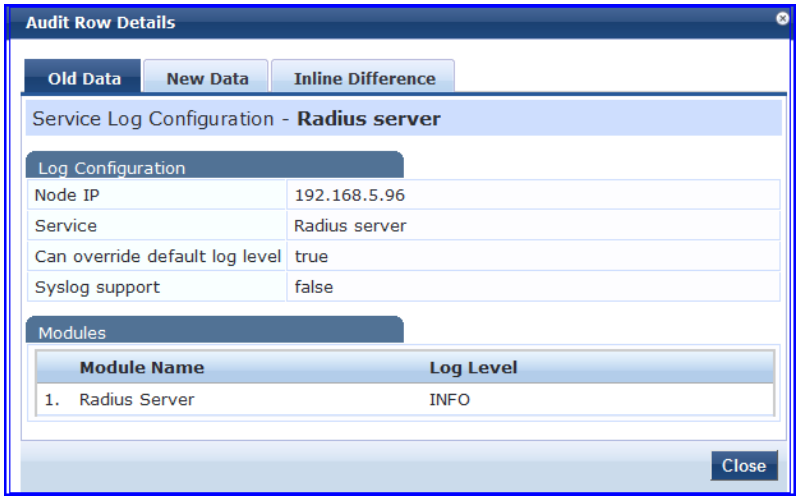


Figure 20 *Audit Row Details (New Data tab)*

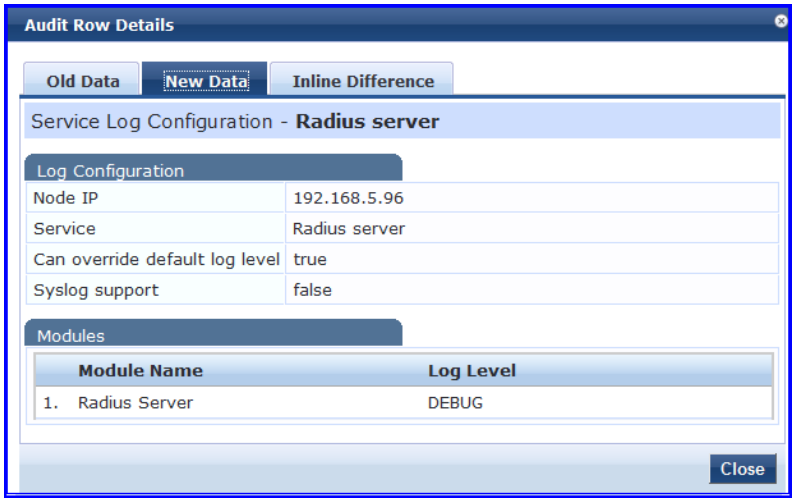
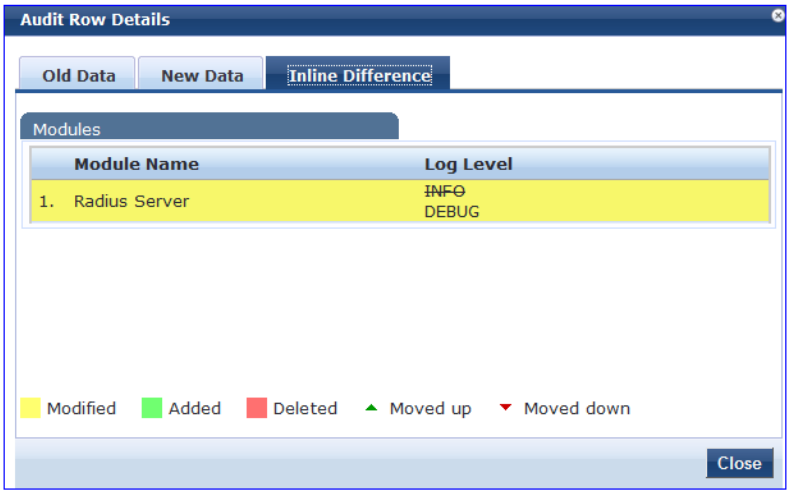


Figure 21 *Audit Row Details (Inline Difference tab)*



For **Remove** Actions, a popup displays the removed data.

Event Viewer

The Event Viewer display provides a dynamic report of system level (not request-related) Events, filterable by Source, Level, Category, and Action, at: **Monitoring > Event Viewer**.

Figure 22 *Event Viewer*

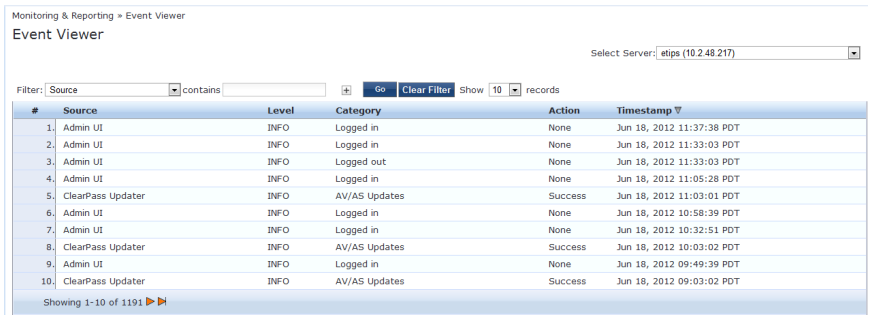
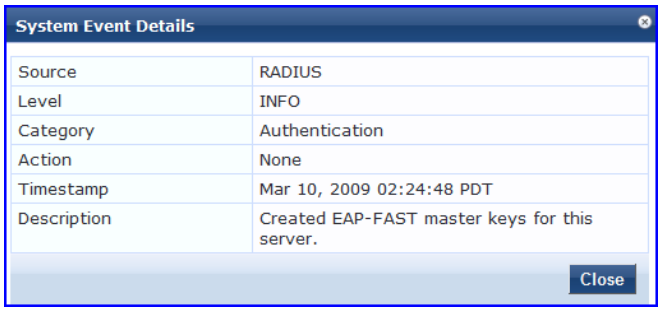


Table 12: *Event Viewer*

Container	Description
Select Server	Select the server for which to display accounting data.
Filter	Select the filter by which to constrain the display of accounting data.
Show <n> records	Show 10, 20, 50 or 100 rows. Once selected, this setting is saved and available in subsequent logins.

Click on any row to display the corresponding System Event Details.

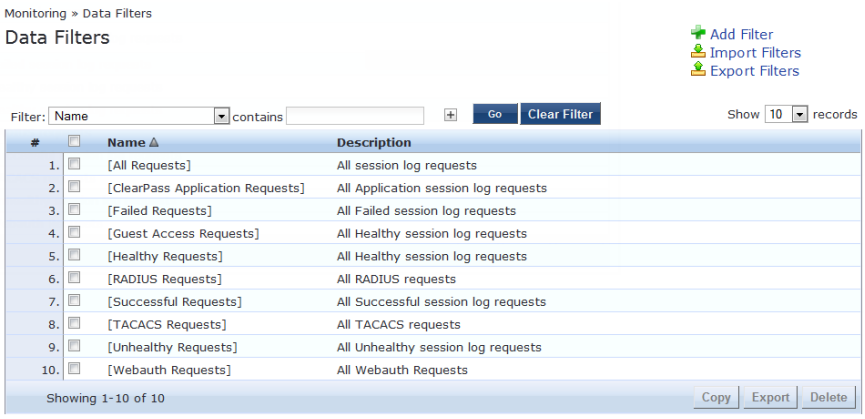
Figure 23 *System Event Details*



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 "Access Tracker" on page 24, "Syslog Export Filters " on page 262, "Analysis and Trending" on page 35, and "Accounting" on page 26 components in Policy Manager. It is available at: **Monitoring> Data Filters**.

Figure 24 *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).

Table 13: *Data Filters*

Container	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 25 *Add Filter (Filter tab)*

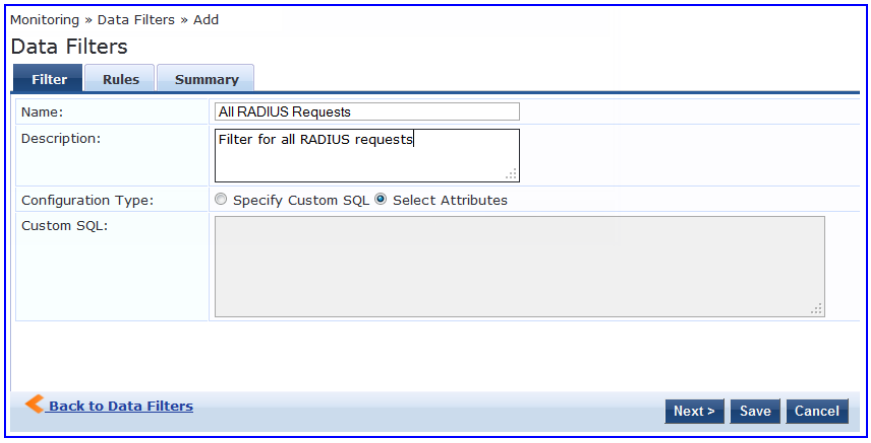


Table 14: *Add Filter (Filter tab)*

Container	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 when **Select Attributes** is selected on the Filter tab.

Figure 26 *Add Filter (Rules tab)*

Table 15: *Add Filter (Rules tab)*

Container	Description
Rule Evaluation Algorithm	**Select first 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 27 *Add Filter (Rules tab) - Rules Editor*

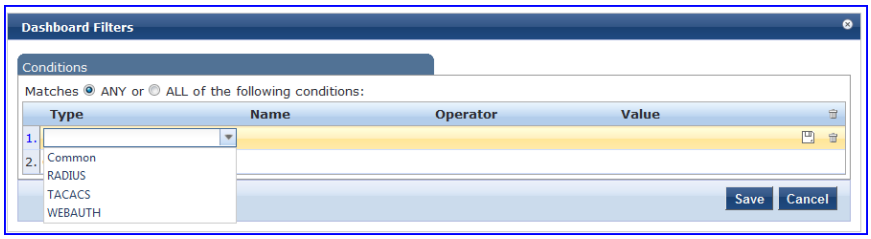


Table 16: *Add Filter (Rules tab) - Rules Editor*

Container	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

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.

Refer to the following topics for additional information.

Services Paradigm

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

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

Policy Manager 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.

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

Figure 28 *Generic Policy Manager Service Flow of Control*

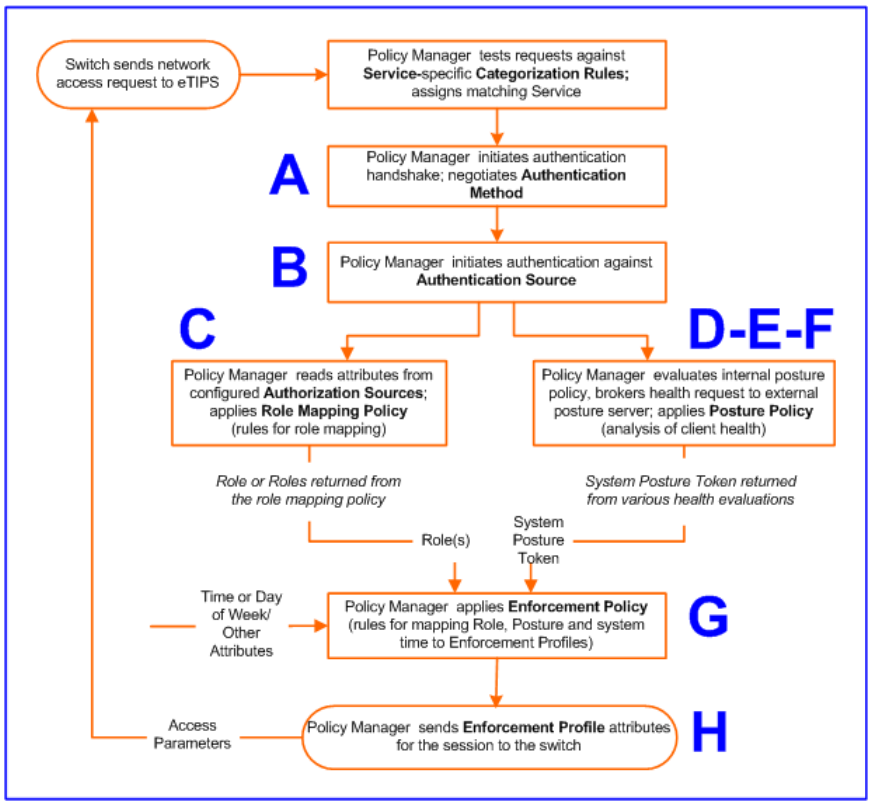


Table 17: *Policy Manager Service Components*

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.

Component	Service: component ratio	Description
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® • any 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.
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: *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, system time and other contextual attributes against Enforcement Policy rules to return one or more matching Enforcement Policy Profiles (that define scope of access for the client).

Component	Service: component ratio	Description
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.

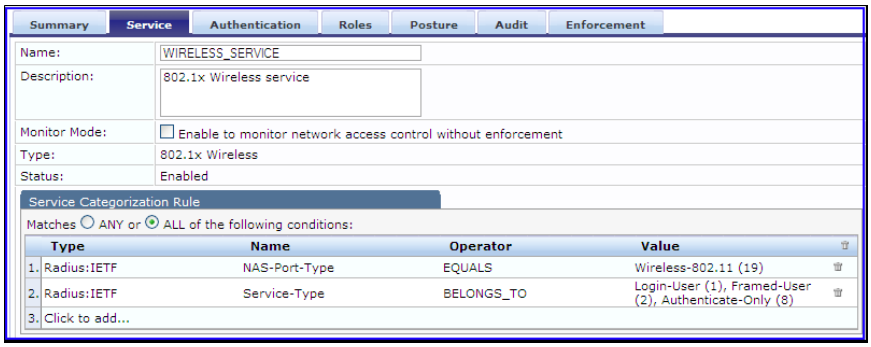
Viewing Existing Services

You can view all configured services in a list or drill down into individual services:

- View and manipulate the list of current services.

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

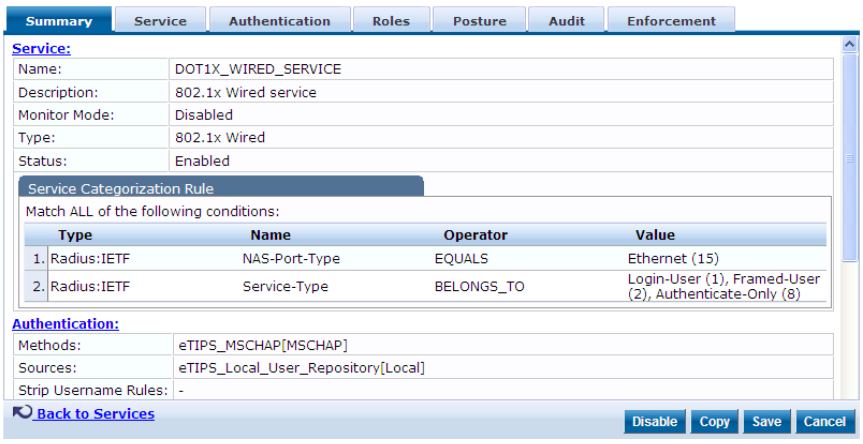
Figure 29 *List of services with sorting tool*



- Drill down to view details for an individual service.

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

Figure 30 *Details for an individual service*



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 filepath. Later, you can import this service by clicking **Import a Service** and providing the filepath.

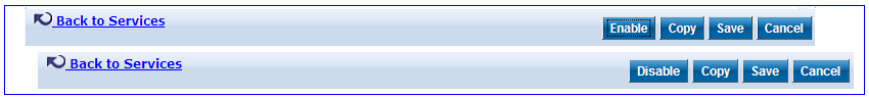
- **Create a new service** that you will configure from scratch.

  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 31 *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 18: *Policy Component Use Cases and Configuration Instructions*

Policy Component	Illustrative Use Cases	Configuration Instructions
Service	• "802.1x Wireless Use Case" on page 336 • "Dell Web Based Authentication Use Case " on page 344. • "MAC Authentication Use Case" on page 350. • "TACACS+ Use Case" on page 354.	"Adding Services " on page 81
Authentication Method	"802.1x Wireless Use Case" on page 336 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. "Dell Web Based Authentication Use Case " on page 344 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 90

Policy Component	Illustrative Use Cases	Configuration Instructions
Authentication Source	• "802.1x Wireless Use Case" on page 336 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. • "Dell Web Based Authentication Use Case " on page 344 uses the local Policy Manager repository, as this is common practice among administrators configuring Guest Users. • "MAC Authentication Use Case" on page 350 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 354 uses the local Policy Manager repository. Other authentication sources would also be fine.	"Adding and Modifying Authentication Sources " on page 107
Role Mapping	"802.1x Wireless Use Case" on page 336 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 137 • "Adding and Modifying Roles " on page 140 • "Adding and Modifying Local Users " on page 141 • "Adding and Modifying Guest Users " on page 142 • "Adding and Modifying Static Host Lists " on page 147
Posture Policy	"Dell Web Based Authentication Use Case " on page 344 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 and Modifying Posture Policies " on page 152
Posture Server	"802.1x Wireless Use Case" on page 336 appends a third-party posture server to evaluate health policies based on vendor-specific posture credentials.	"Adding and Modifying Posture Servers " on page 177
Audit Server	"MAC Authentication Use Case" on page 350, uses an Audit Server to provide port scanning for health.	"Configuring Audit Servers" on page 180

Policy Component	Illustrative Use Cases	Configuration Instructions
Enforcement Policy and Profiles	All Use Cases have an assigned Enforcement Policy and corresponding Enforcement Rules.	• "Configuring Enforcement Profiles " on page 193 • "Configuring Enforcement Policies " on page 204

Policy Simulation

Once 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.

Figure 32 *Policy Simulation*

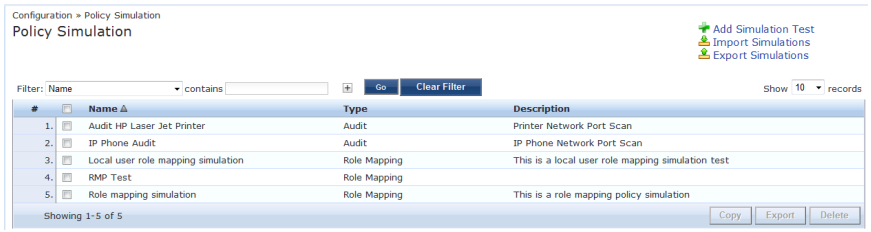


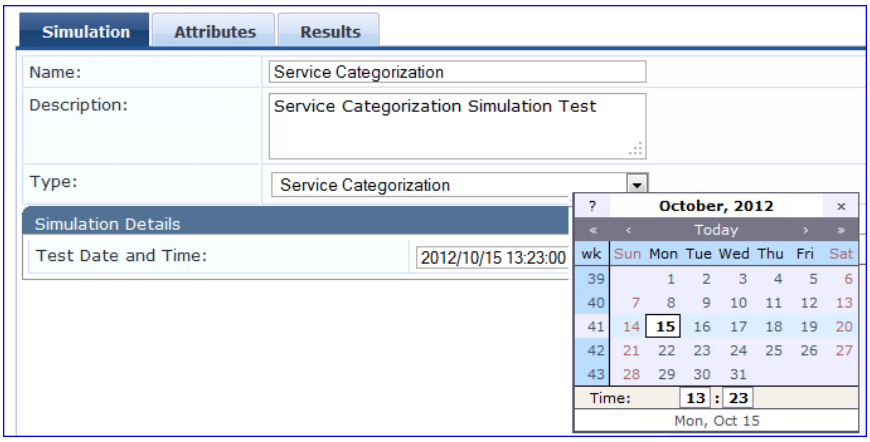
Table 19: *Policy Simulation*

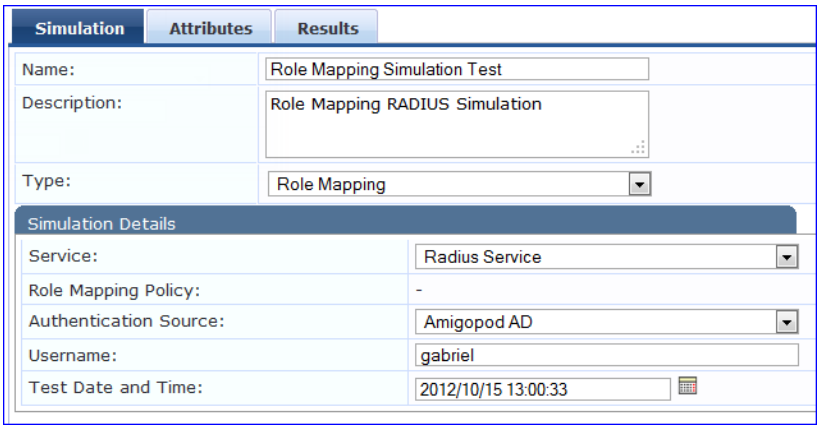
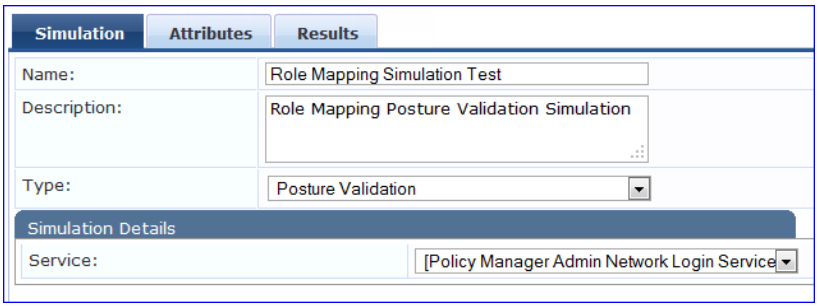
Container	Description
Add Simulation Test	Opens the **Add Simulation Test** page.
Import Simulations	Opens the **Import Simulations** popup.
Export Simulations	Opens the **Export Simulations** popup.
Filter	Select the filter by which to constrain the display of simulation data.
Copy	Make a copy the selected 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.

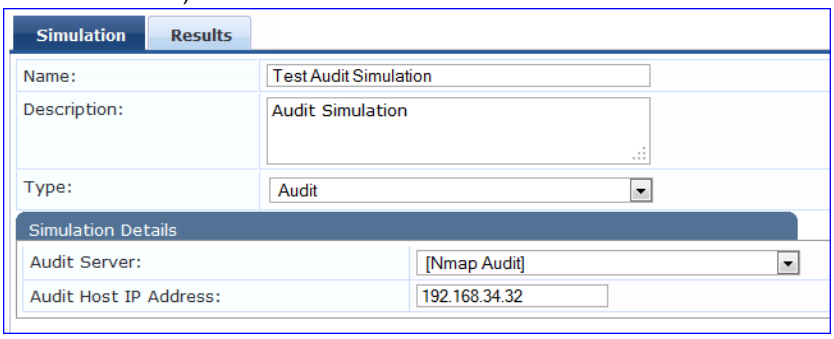
Add Simulation Test

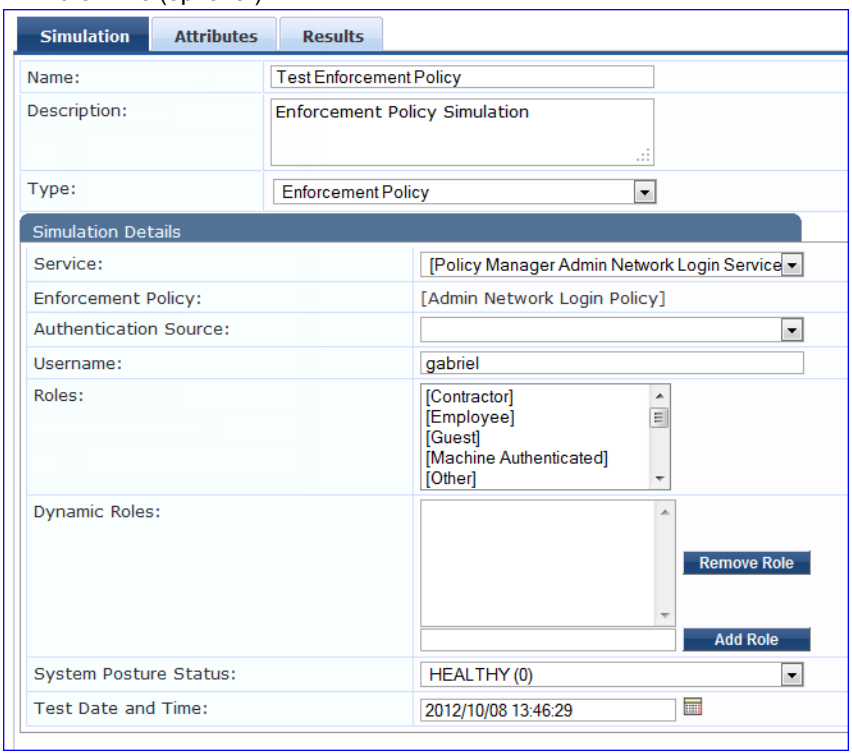
Navigate to **Configuration > Policy Simulation** and click on the **Add Simulation** link. Depending on the simulation type selected the contents of the **Simulation** tab changes.

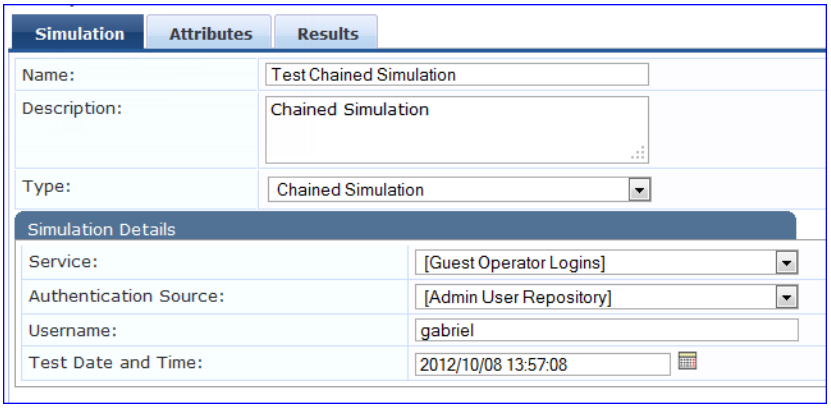
Table 20: *Add Policy Simulation (Simulation Tab)*

Container	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)  • 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)

Container	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**.  • 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).  • 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*.

Container	Description
Type **Audit.**	• Input (**Simulation** tab): Select the **Audit Server** and host to be Audited (IP address or hostname)  • Returns (**Results** tab): *Summary Posture Status*, *Audit Attributes* and *Status* **NOTE:** Audit simulations can take a while; an AuditInProgress status is shown until the audit completes.

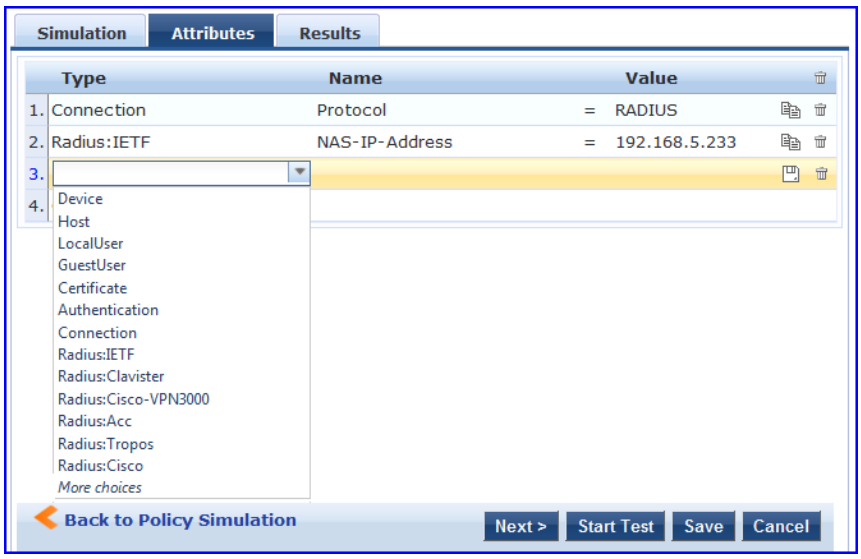
Container	Description
Type **Enforcement Policy.**	• Input (**Simulation** tab): Select **Service** (Enforcement Policy is implicit by its association with the Service), Authentication Source (optional), User Name (optional), Roles, Dynamic Roles (optional), System Posture Status, and Date/Time (optional).  • 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 "Generic LDAP or Active Directory " on page 108for more information.

Container	Description
Type **Chained Simulations.**	• Input (**Simulation** tab): Select **Service**, **Authentication Source**, **User Name**, and **Date/Time**.  • 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).

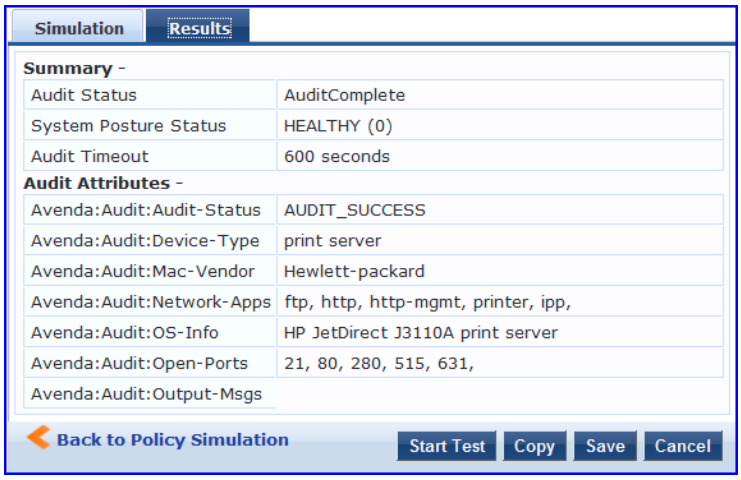
The **Attributes** tab will not display if you select the **Audit Policy** component in the **Simulation** tab.

Figure 33 *Add Simulation (Attributes Tab)*



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 34 *Add Simulation (Results Tab)*



Import and Exporting Simulations

Import Simulations

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

Figure 35 *Import Simulations*

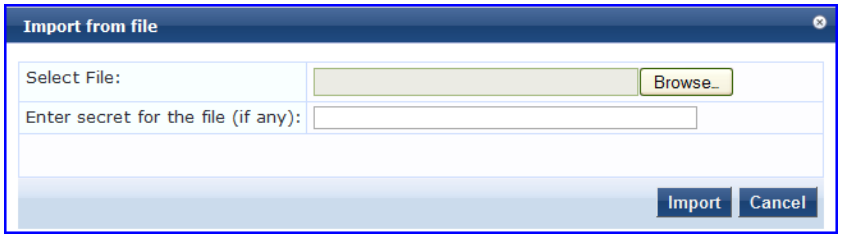


Table 21: *Import Simulations*

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

Export Simulations

Navigate to **Configuration > Policy Simulation** and select 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 just one simulation, select it (using the check box at the 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.

Profile is a ClearPass Policy Manager module that automatically classifies endpoints using attributes obtained from software components called Collectors. It can be used to implement “Bring Your Own Device” (BYOD) flows, where access has to 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 versus 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 minimal amount of configuration.

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 the 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. The following collectors send endpoint attributes to Profile.

- DHCP
- ClearPass Onboard
- HTTP User Agent
- MAC OUI - Acquired via various authentication mechanisms such as 802.1X, MAC authentication, etc.
- ActiveSync plugin
- CPPM OnGuard
- SNMP
- Subnet Scanner

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 (future)

Configuration

Navigate to the **Administrator > Network Setup > ClearPass** page to configure ClearPass Onboard and ClearPass Guest to send HTTP User Agent string to Profile. The screenshot below shows how the CPPM publisher and Profile nodes configured in ClearPass Guest.

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 which may be configured with static IP addresses.

ActiveSync Plugin

ActiveSync plugin is software 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 is send to CPPM profiler. Profiler uses dictionaries to derive profiles from these attributes.

CPPM OnGuard

ClearPass Onguard agents perform advanced endpoint posture assessment. It could collect and send OS details from endpoints during authentication. Profiler uses 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 neighbour 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 neighbour devices connected to switch/controller configured in CPPM
- ARPtable read from network devices is used as a means to discover endpoints in the network.

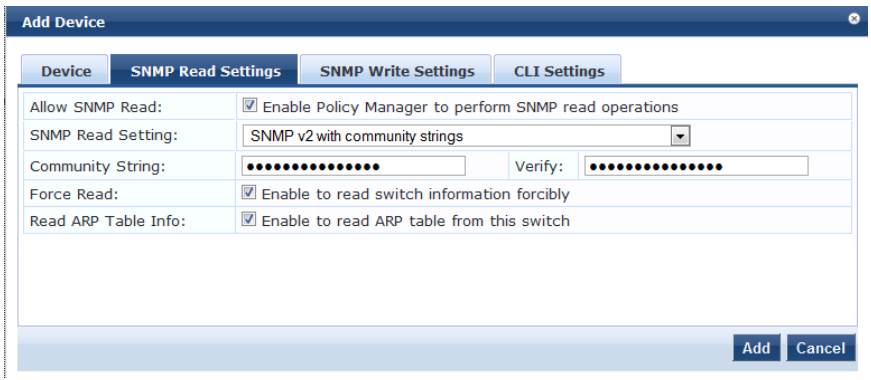
Note that the SNMP based mechanism is only capable of profiling devices if they respond to SNMP, or if the device advertises its capability via LLDP. When performing SNMP reads for a device, CPPM uses SNMP Read credentials configured in Network Devices, or defaults to using SNMP v2c with "public" community 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 have been introduced for 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 36 *SNMP Read/Write Settings Tabs*

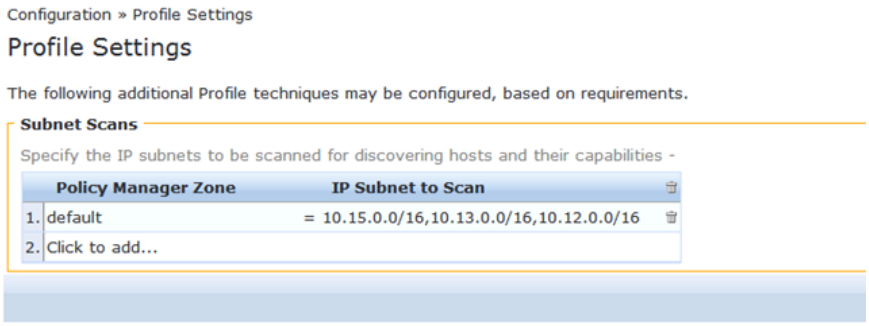


In large or geographically spread cluster deployments you do not want all CPPM nodes to probe all SNMP configured devices. The default behaviour is for a CPPM node in the cluster to read network device information only for devices configured to send traps to that CPPM node.

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.

Figure 37 *Configuration > Profile Settings*



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 attributes available, it will lookup dhcp, http, active_sync, MAC oui, and SNMP dictionaries and derives multiple matching profiles. When 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 which 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.

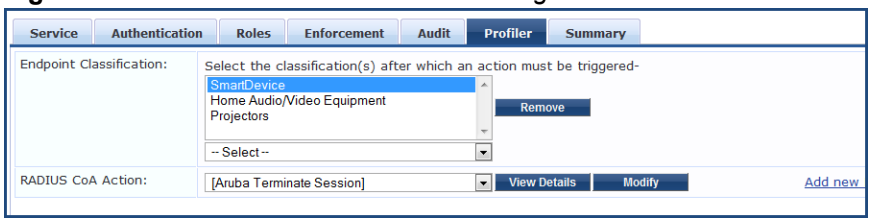
Example

With DHCP options Stage-1 can identify that a device is Android. Stage-2 uses rules to combine this with MAC OUI to further classify an android device as Samsung Android, HTC Android etc.

Post Profile Actions

After profiling an endpoint, profiler can be configured 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 38 *Services > Edit > Profiler tab settings*



Fingerprint Dictionaries

CPPM uses a set of dictionaries and built-in rules to perform device fingerprinting. The following dictionaries are used by CPPM:

- DHCP
- HTTP User-Agent
- ActiveSync Attributes
- SNMP Attributes
- MAC OUI

Refer to Fingerprints for more information.

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. Refer to Update Portal for more information.

The Profiler User Interface

CPPM provides admin interfaces to search and view profiled endpoints. It also provides basic statistics on the profiled endpoints. The Cluster Status Dashboard widget shows basic distribution of device types. (See Policy Manager Dashboard fore more information on Dashboard widgets.) In addition, the Monitoring and Reporting > Live Monitoring > Endpoint Profiler page detailed device distribution information along with a list of endpoints. From this page, you can also search for endpoint profiles based on category, family, name, etc. Refer to Endpoint Profiler for more information.

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. Dell offers the following default services:

- 802.1X Wireless
- 802.1X Wired
- MAC Authentication
- Web-based Authentication
- Web based Health Check Only
- Web-based Open Network Access
- 802.1X Wireless - Identity Only
- 802.1X Wired - Identity Only
- RADIUS Enforcement (Generic)
- RADIUS Proxy
- TACACS+ Enforcement
- Dell Application Authentication
- Dell Application Authorization
- Cisco Web Authentication Proxy

Refer to the following sections for more detailed information:

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 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.

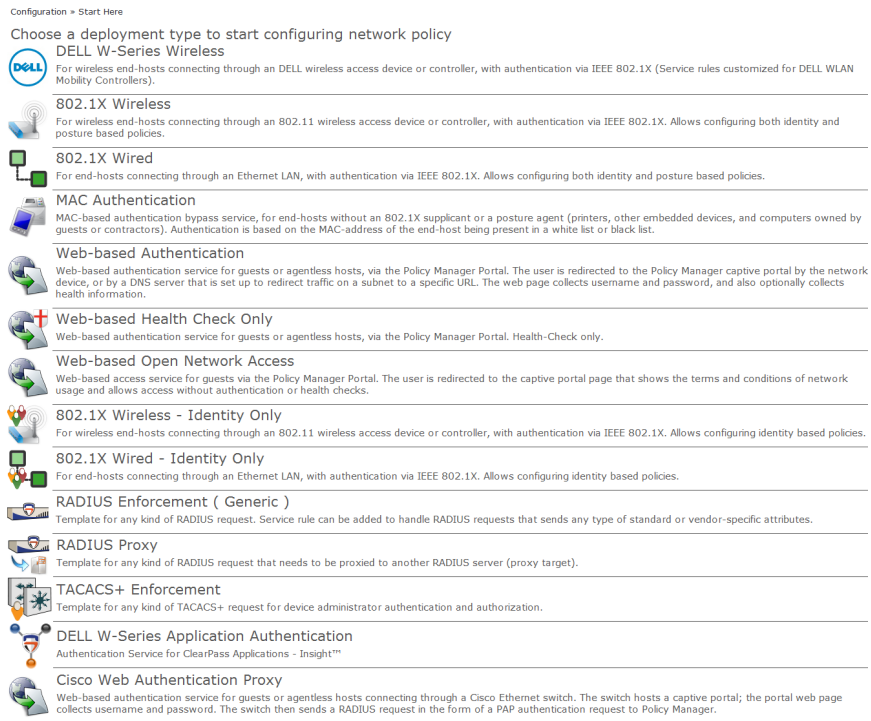
To help you get started, Policy Manager comes pre-configured with 14 different Service types or templates. If these service types do not suit your needs, you can roll your own service with custom service rules.

Start Here Page

From the **Configuration > Start Here** page, you can create a new service by clicking on any of the pre-configured Policy Manager Service Types.

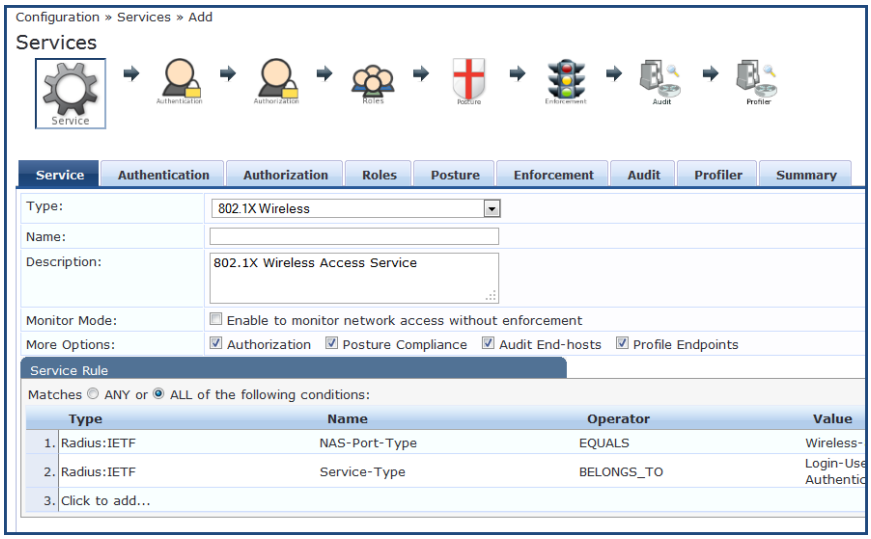
Each of the service types is listed in a graphical list, with a description of each type:

Figure 39 *Start Here page*



After you select a service type, the associated service wizard is displayed with a clickable diagram that shows on top of the wizard. The following image displays the flow with all available configuration options for 802.1X Wireless:

Figure 40 *Service Wizard with Clickable Flow*

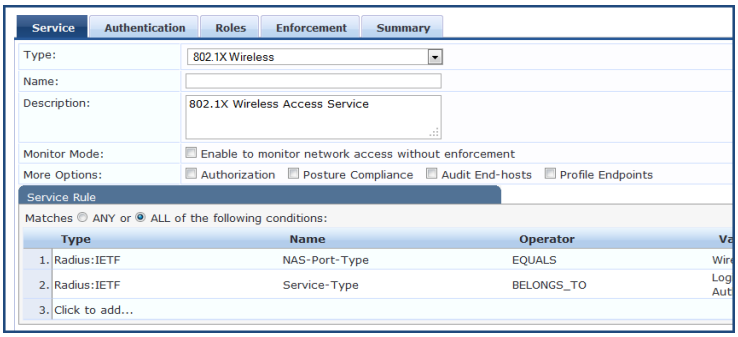
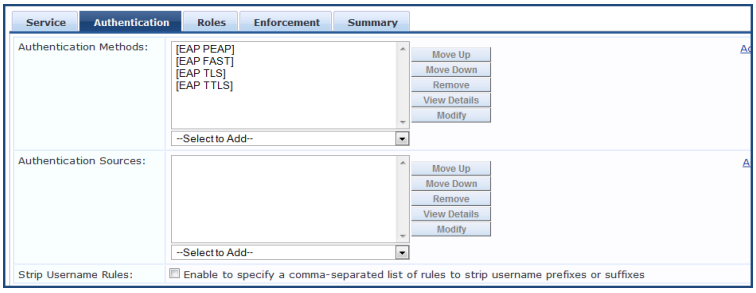


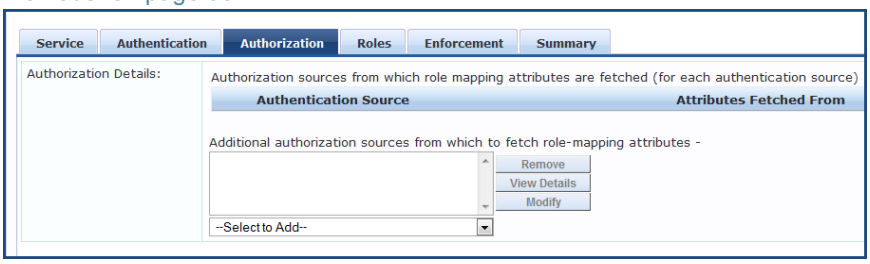
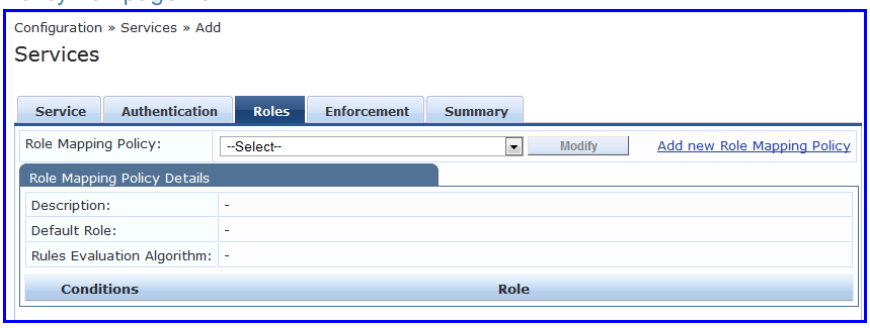
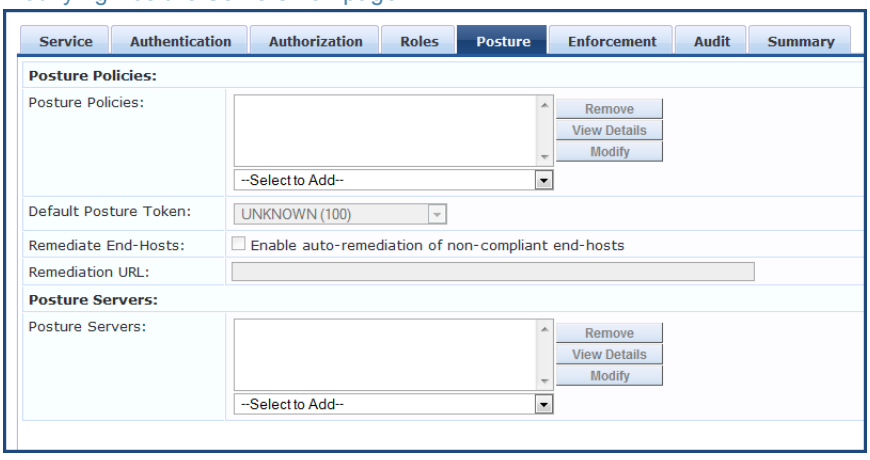
The rest of the service configuration flow is as described in Policy Manager Service Types.

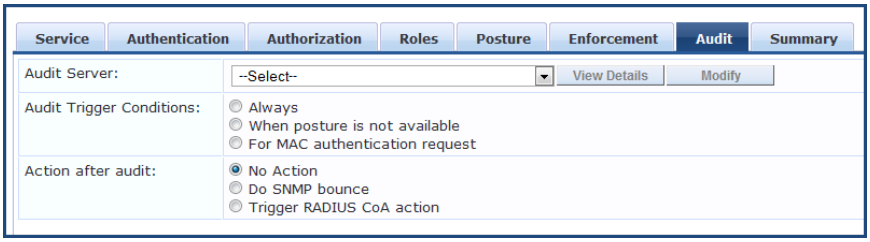
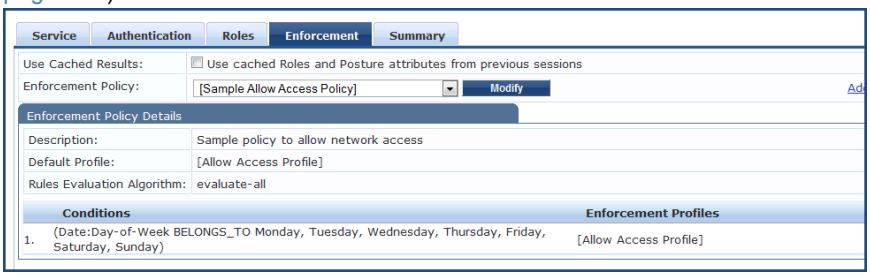
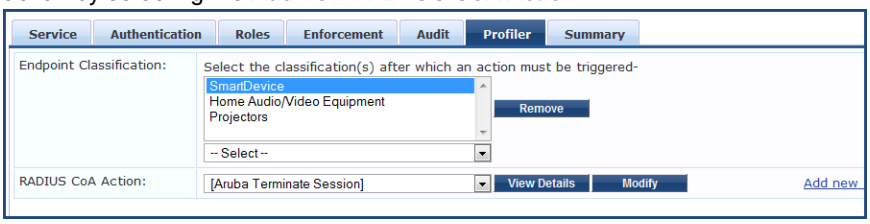
Policy Manager Service Types

The following service types come preconfigured on Policy Manager:

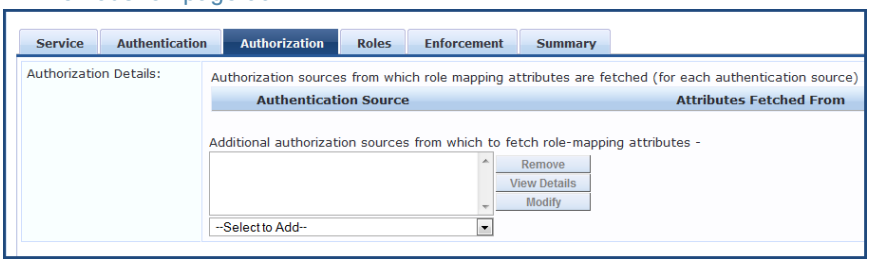
Table 22: *Policy Manager Service Types*

Service Type	Description
DellW-Series Wireless	Template for wireless hosts connecting through a Dell W-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. Refer to the "802.1X Wireless " on page 69 service type for a description of the different tabs.
802.1X Wireless	For wireless clients connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. By default, the template displays with the Service, Authentication, Roles, Enforcement, and Summary tabs. In the **More Options** section, click on Authorization, Posture Compliance, Audit End Hosts, or Profile Endpoints to enable additional tabs.  To configure authentication methods and authentication source, click on the **Authentication** tab. The *Authentication methods* used for this service depend on the 802.1X supplicants and the type of authentication methods you choose to deploy. The common types are PEAP, EAP-TLS, EAP-FAST or EAP-TTLS (These methods are automatically selected). Non-tunneled EAP methods such as EAP-MD5 can also be used as authentication methods. 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 more information on configuring authentication sources, refer to "Adding and Modifying Authentication Sources " on page 107. You can enable **Strip Username Rules** to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source. 

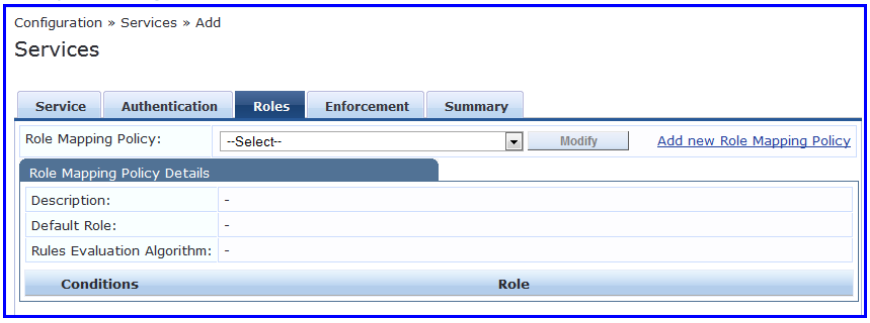
Service Type	Description
	To create an authorization source for this service click on the **Authorization** tab. This tab is not visible by default. To enable Authorization for this service select the **Authorization** check box on the **Service** tab. Policy Manager fetches role mapping attributes from the authorization sources associated with 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 service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 90.  To associate a role mapping policy with this service click on the Roles tab. For information on configuring role mapping policies, refer to "Configuring a Role Mapping Policy " on page 137.  By default, this type of service does not have Posture checking enabled. 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 aDell 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). For more information on configuring *Posture Polices* and *Posture Servers* refer to topics: "Adding and Modifying Posture Policies " on page 152 and "Adding and Modifying Posture Servers " on page 177. 

Service Type	Description
	By default, this type of service does not have Audit checking enabled. To 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. Refer to "Configuring Audit Servers" on page 180 for audit server configuration steps. 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 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. • **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager. You must select an enforcement policy (see "Configuring Enforcement Policies " on page 204) for a service.  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.  To create an authorization source for this service click on the **Authorization** tab. This tab is not visible by default. To enable Authorization for this service select the **Authorization** check box on the **Service** tab. Policy Manager fetches role mapping attributes from the authorization sources associated with 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:

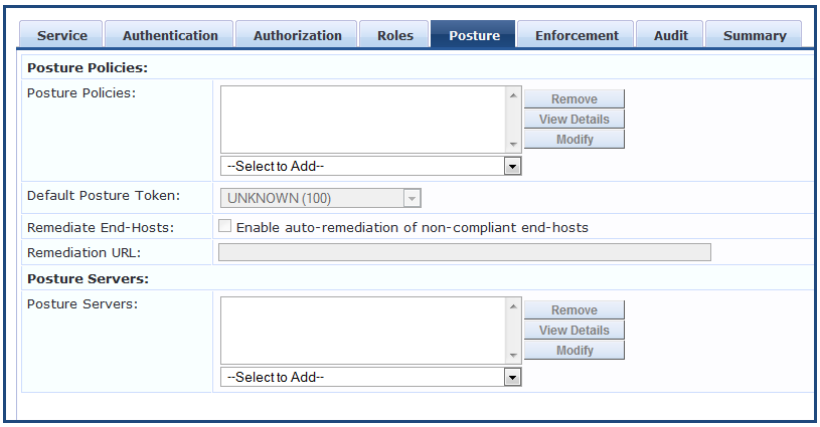
Service Type	Description
	• The authorization sources associated with the authentication source • The authorization sources associated with the service. For more information on configuring authorization sources, refer to "Adding and Modifying Authentication Methods" on page 90.



To associate a role mapping policy with this service click on the **Roles** tab. For information on configuring role mapping policies, refer to "Configuring a Role Mapping Policy " on page 137.



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

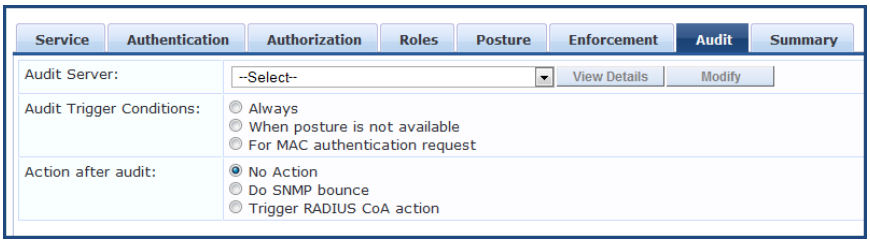


You can enable posture checking for this kind of service if you are deploying Policy Manager in a Microsoft NAP or Cisco NAC framework environment, or if you are deploying a Dell hosted captive portal that does posture checks through a dissolvable agent. You can also choose to **Enable auto-remediation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

For more information on configuring *Posture Polices* and *Posture Servers* refer to topics: "Adding and Modifying Posture Policies " on page 152 and "Adding and Modifying Posture Servers " on page 177.

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

Service Type	Description

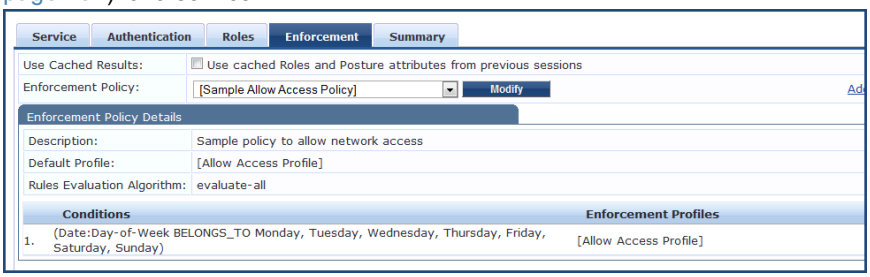


Select an **Audit Server** - either built-in or customized. Refer to "Configuring Audit Servers" on page 180 for audit server configuration steps.

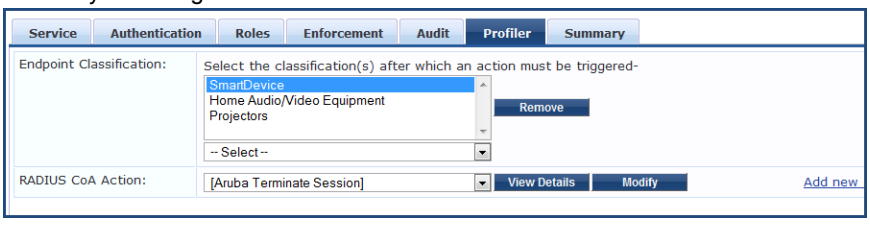
You can specify to trigger an audit always, when posture is not available, or for MAC authentication requests. If **For MAC authentication requests** is specified, then you can perform an audit **For known end-hosts only** or **For unknown end hosts only**, or **For all end hosts**. Known end hosts are 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:

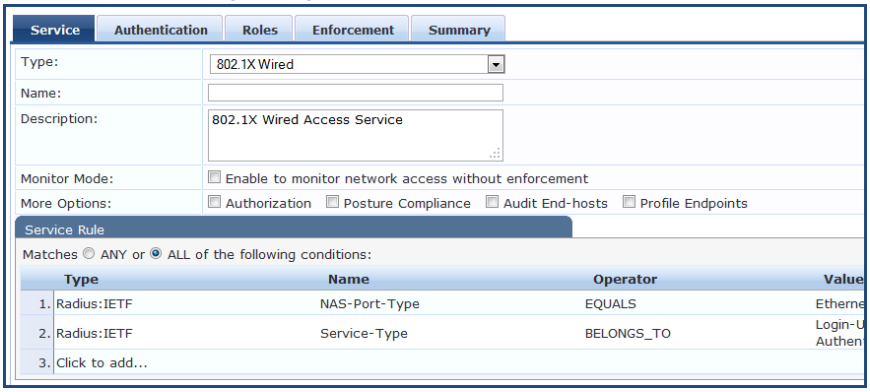
- **No Action:** The audit will not apply policies on the network device after this audit.
- **Do SNMP bounce:** This option will bounce the switch port or to force an 802.1X reauthentication (both done via SNMP).Note: Bouncing the port triggers a new 802.1X/MAC authentication request by the client. 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.
- **Trigger RADIUS CoA action:** This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.

You must select an enforcement policy (see "Configuring Enforcement Policies " on page 204) for a service.

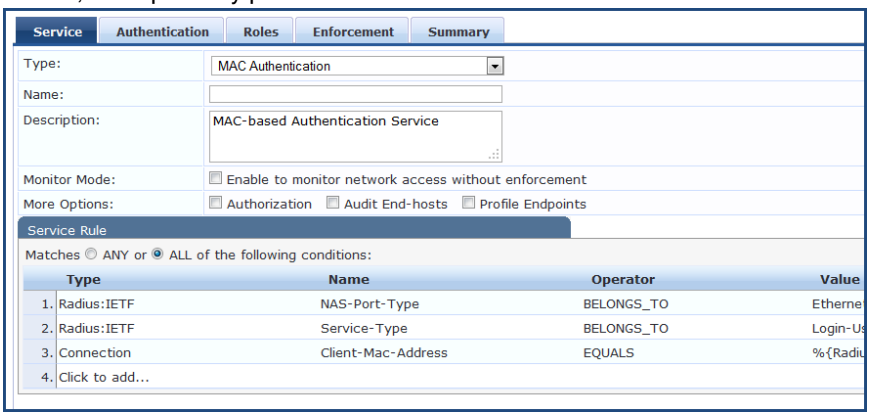


Optionally configure **Profiler** settings. Select one or more Endpoint Classification items from the drop down list, then select the RADIUS CoA action. You can also create a new action by selecting the **Add new RADIUS CoA Action** link.

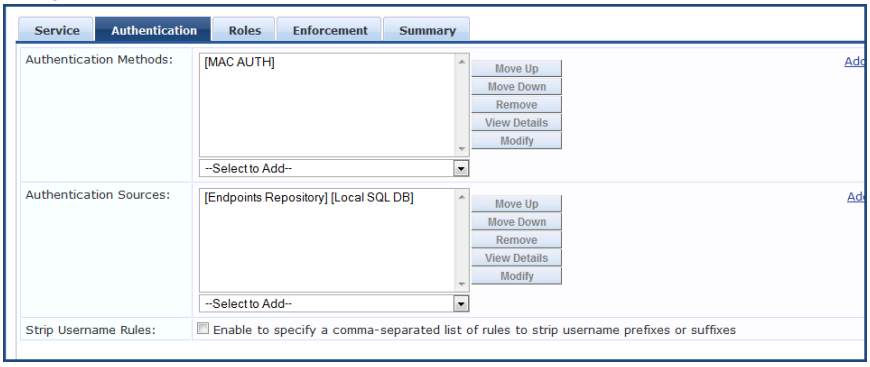


Service Type	Description
 802.1X Wired	For clients connecting through an Ethernet LAN, with authentication via IEEE 802.1X.  Except for the service rules shown above, configuration for the rest of the tabs is similar to the 802.1X Wireless Service. **NOTE:** If you want to administer the same set of 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. Refer to the "802.1X Wireless " on page 69 service type for a description of the different tabs.

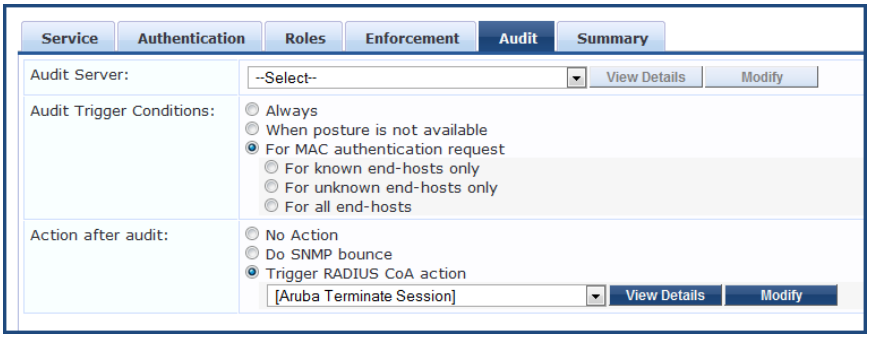
Service Type	Description
 MAC Authentication	MAC-based authentication service, for clients without an 802.1X supplicant or a posture agent (printers, other embedded devices, and computers owned by guests or contractors). The network access device sends a MAC authentication request to Policy Manager. 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.



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 (refer to Adding and Modifying Static Host Lists), 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.

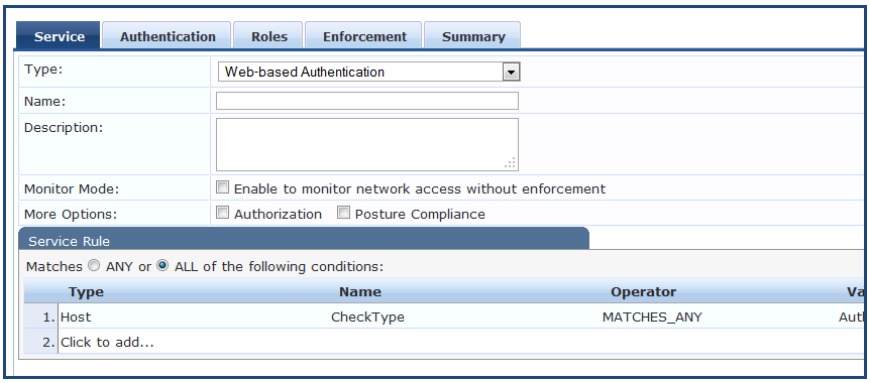
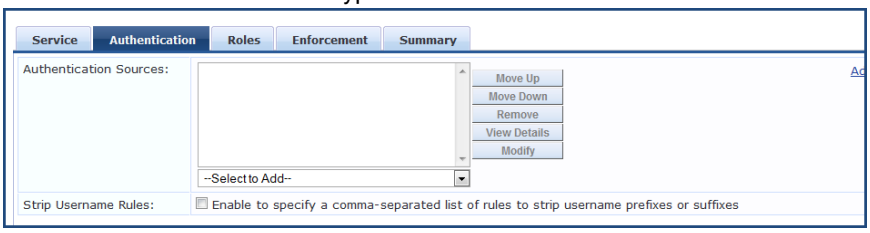


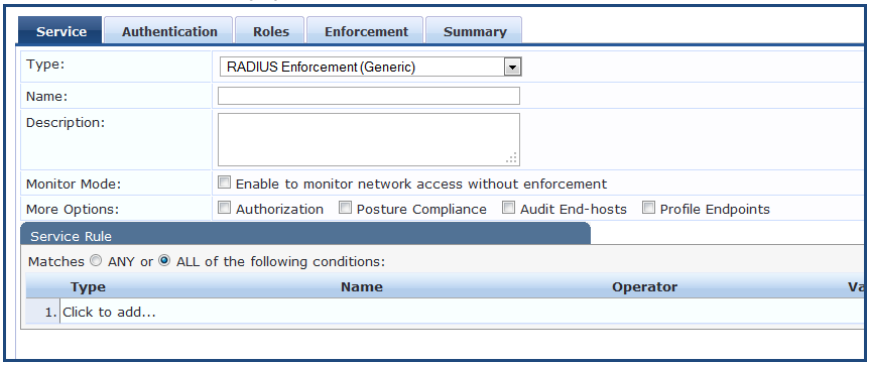
NOTE: You cannot configure Posture for this type of service.
Audit can optionally be enabled for this type of service by checking the **Audit End-hosts** check box on the **Service** tab.

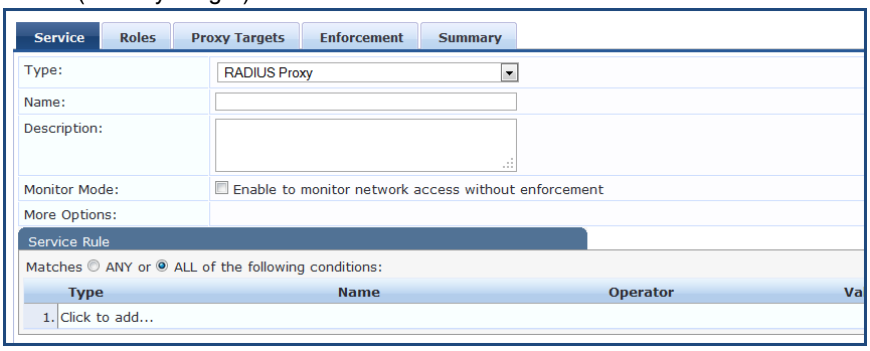
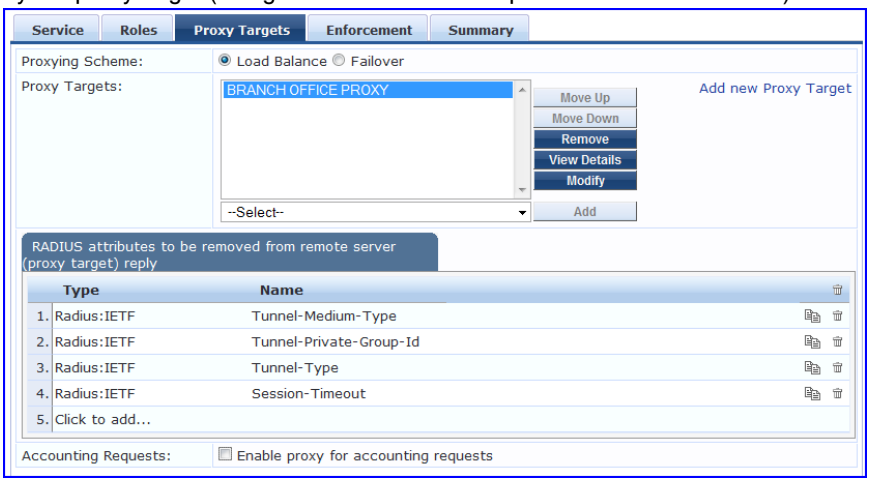


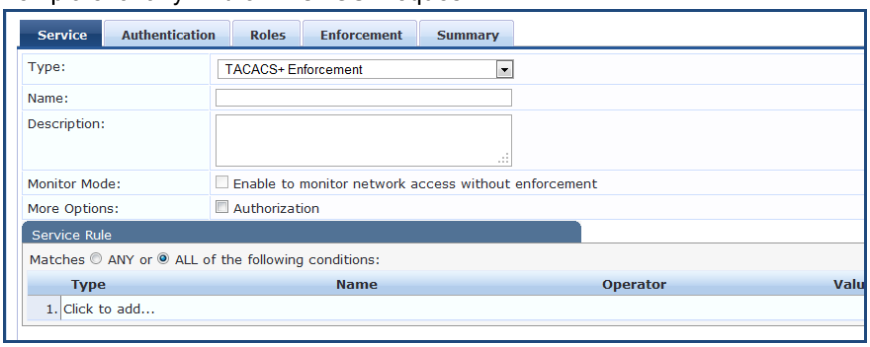
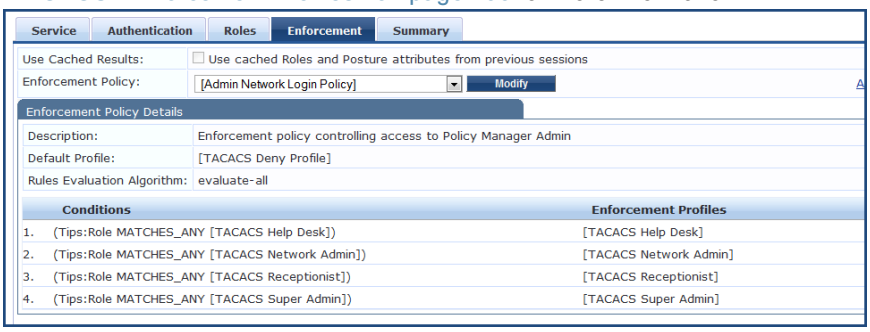
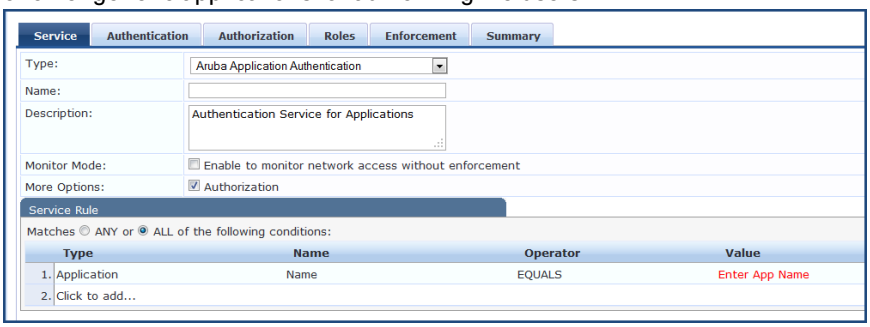
You can perform audit For known end-hosts only or For unknown end hosts only or For all end hosts. Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service. Performing audit on a client is an asynchronous task, which means the audit can 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:

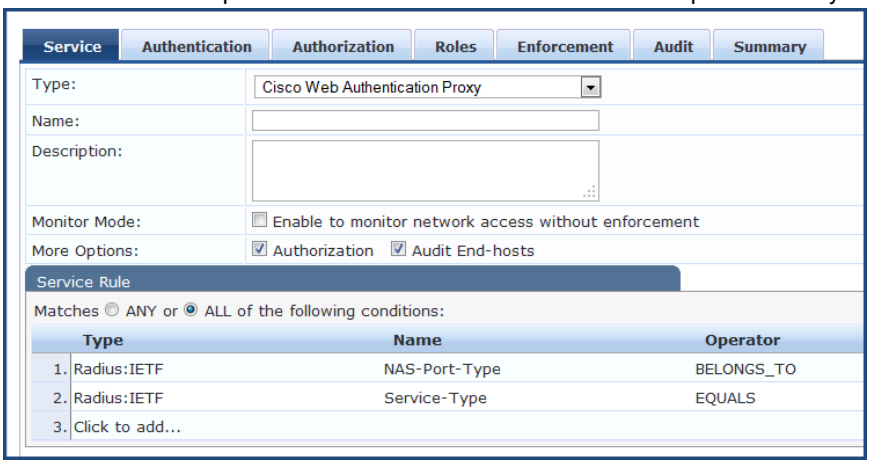
- **No Action:** The audit will not apply policies on the network device after this audit.
- **Do SNMP bounce:** This option will bounce the switch port or to force an 802.1X reauthentication (both done via SNMP).Note: Bouncing the port triggers a new

Service Type	Description
 Web-based Authentication	Web-based authentication service for guests or agentless hosts, 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, popular Linux systems). There is an internal service rule (*Connection:Protocol EQUALS WebAuth*) that categorizes request into this type of service. You can add other rules, if needed.  There is no authentication method associated with this type of service (Authentication methods are only relevant for RADIUS requests). You can select any type of authentication source with this type of service.  Note that when you configure posture policies, only those that are configured for the OnGuard Agent are shown in list of posture policies. Refer to the "802.1X Wireless " on page 69 service type for a description of the other tabs.
 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 request 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*.
 Web-based Open Network Access	This type of service is similar to other Web-based services, except that authentication and health checking are 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 click on the submit action on the page.

Service Type	Description
 802.1X Wireless - Identity Only	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.
 802.1X Wired - Identity Only	This type of service is the same as regular 802.1X Wired Service, except that posture and audit policies are not configurable when you use this template.
 RADIUS Enforcement [Generic]	Template for any kind of RADIUS request. Rules can be added to handle RADIUS requests that sends any type of standard or vendor-specific attributes.  **NOTE:** No default rule 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). You can click on the **Authorization**, **Posture Compliance**, **Audit End-hosts** and **Profile Endpoints** options to enable additional tabs. Refer to the "802.1X Wireless " on page 69 service type for a description of the other tabs.

Service Type	Description
 RADIUS Proxy	Template for any kind of RADIUS request that needs to be proxied to another RADIUS server (a Proxy Target).  **NOTE:** No default rule is 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 domain of the user trying to access the network. **NOTE: Authentication**, **Posture**, and **Audit** tabs are not available for this service type. Role mapping rules can be created based on the RADIUS attributes that are returned by the proxy target (using standard or vendor-specific RADIUS attributes).  The servers to which requests are proxied are called *Proxy Targets*. Requests can be dispatched to the proxy targets randomly; over time these requests are *Load Balanced*. Instead, 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, sequentially, if the prior requests failed. When you **Enable proxy for accounting requests** accounting requests are also sent to the proxy targets.

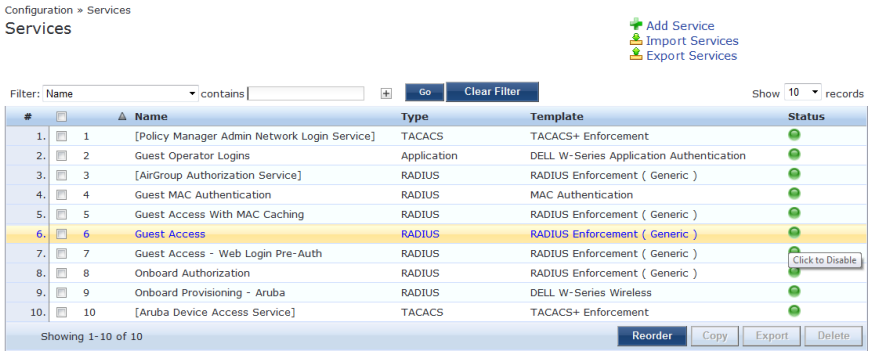
Service Type	Description
 TACACS+ Enforcement	Template for any kind of TACACS+ request.  **NOTE:** No default rule is associated with this service type. Rules can be added to filter the request based on the Date and Connection namespaces. See "Rules Editing and Namespaces" on page 314 for more information. 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+ Enforcement Profiles " on page 199 for more information. 
 Dell W-Series Application Authentication	This type of service provides authentication and authorization to users of Dell applications: Guest and Insight. Application Enforcement Profiles can be sent to these or other generic applications for authorizing the users. 

Service Type	Description
 Cisco Web-Authentication Proxy	Web-based authentication service for guests or agentless hosts. The Cisco switch hosts a captive portal; the portal web page collects username and password. The switch then sends a RADIUS request in the form of a PAP authentication request to Policy Manager.  By default, this service uses the Authentication Method [PAP] [PAP] You can click on the **Authorization** and **Audit End-hosts** options to enable additional tabs. Refer to the "802.1X Wireless " on page 69 service type for a description of these tabs.

Services

You can use these service types as configured, or you can edit their settings.

Figure 41 *Service Listing Page*



The **Services** page includes the following fields.

Table 23: *Services page*

Label	Description
Add Service	Add a service
Import Services	Import previously exported services

Label	Description
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 that when 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

For additional information, refer to the following sections:

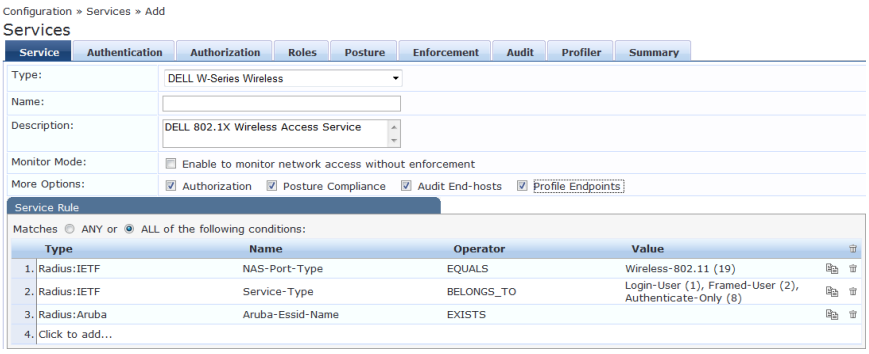
- "Adding Services " on page 81
- "Modifying Services" on page 84
- "Reordering Services " on page 85

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 42 *Add Service Page*

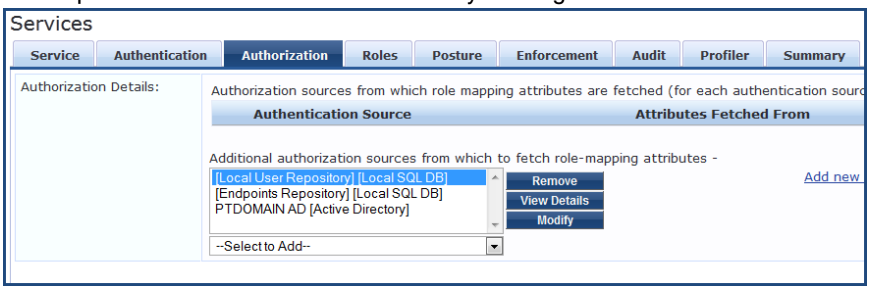


The **Add Service** tab includes the following fields.

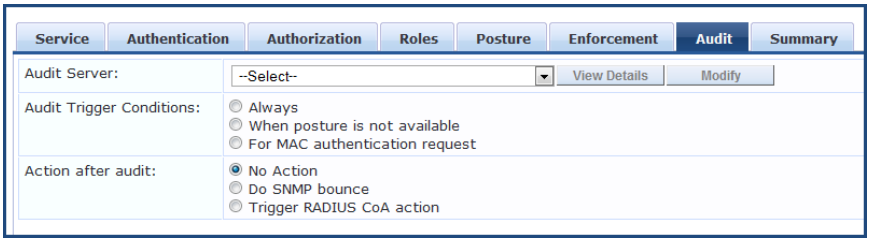
Table 24: *Service Page (General Parameters)*

Label	Description
Type	Select the desired service type from the drop down menu. 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 "Namespaces" on page 314 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).
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.

Label	Description
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 menu 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 menu 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 menu or add a new server by clicking the **Add new Posture Server** link.



- **Audit End-hosts:** Select an Audit Server, either built-in or customized. Refer to "Configuring Audit Servers" on page 180 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**.

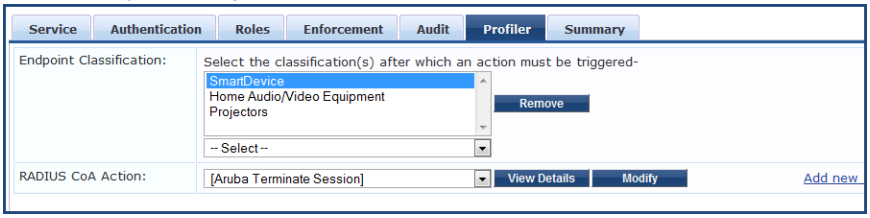


  You can specify to trigger an audit always, when posture is not available, or for MAC authentication requests. If **For MAC authentication requests** is specified, then you can perform an audit **For known end-hosts only** or **For unknown end hosts only**, or **For all end hosts**. Known end hosts are 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 to 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.

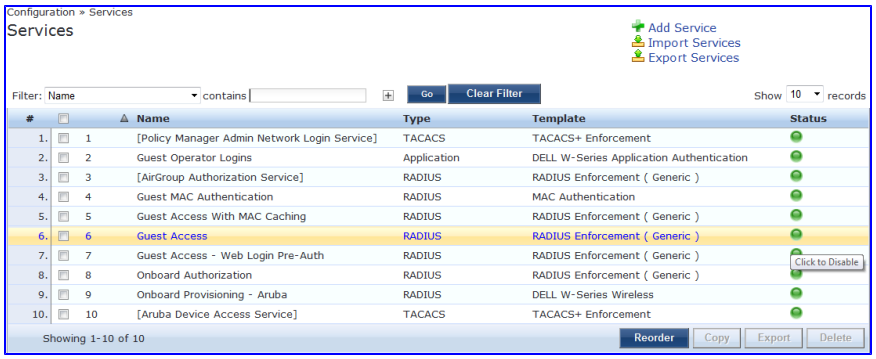
- Optionally configure **Profiler** settings. Select one or more Endpoint Classification items from the drop down list, then select the RADIUS CoA action. You can also create a new action by selecting the **Add new RADIUS CoA Action** link.



Modifying Services

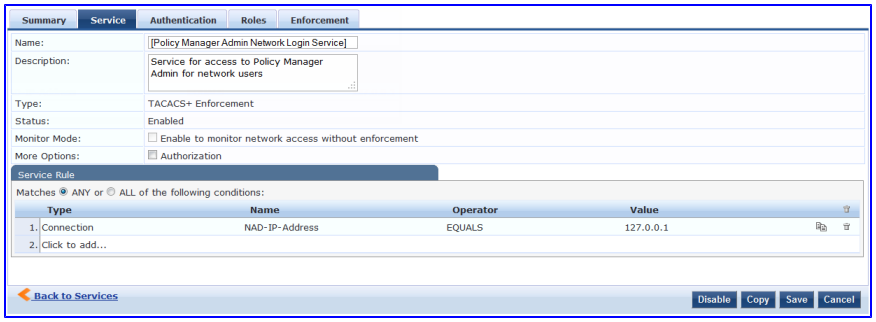
Navigate to the **Configuration > Services** page to view available services. You can use these service types as configured, or you can edit their settings.

Figure 43 *Service Listing Page*



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 44 *Services Configuration*



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

Table 25: *Service Page (General Parameters)*

Label	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.

Label	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 26: *Service Page (Rules Editor)*

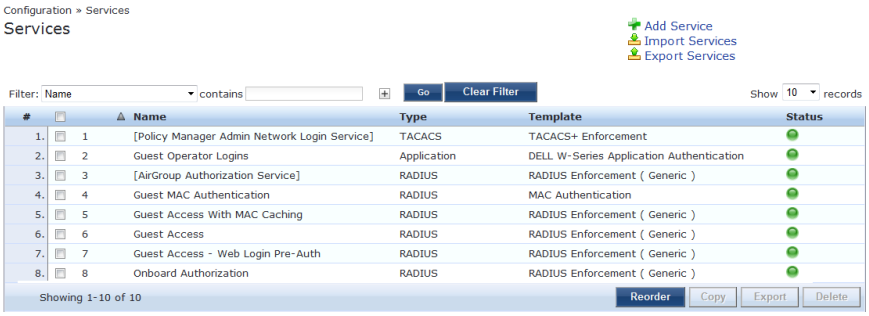
Label	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on Service type. When working with service rules, you can select from the following namespace dictionaries: • **Application**: The type of application for this 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 "Namespaces" on page 314 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 "Operators" on page 320 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. The following page displays.

Figure 45 *Service Reorder Button*



2. Click the **Reorder** button located on the lower-right portion of the page to open the Reordering Services form.

Figure 46 *Reordering Services*

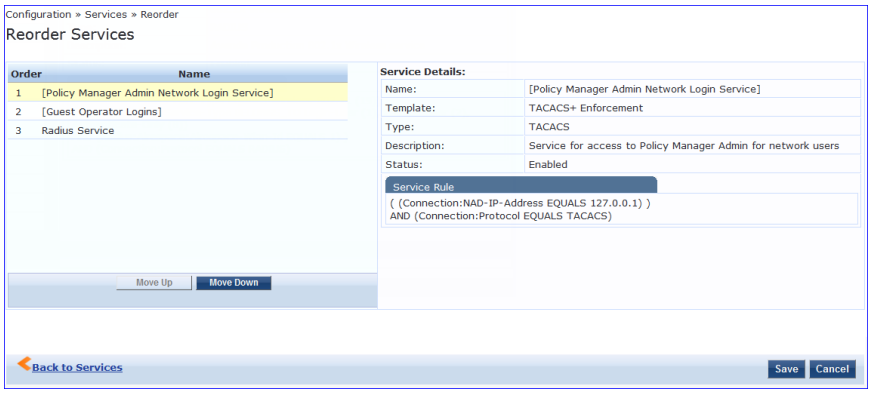


Table 27: *Reordering Services*

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

As the first step in Service-based processing, Policy Manager uses an Authentication Method to authenticate the user or device against an Authentication Source. Once the user or device is authenticated, Policy Manager fetches attributes for role mapping policies from the Authorization Sources associated with this Authentication Source.

Architecture and Flow

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

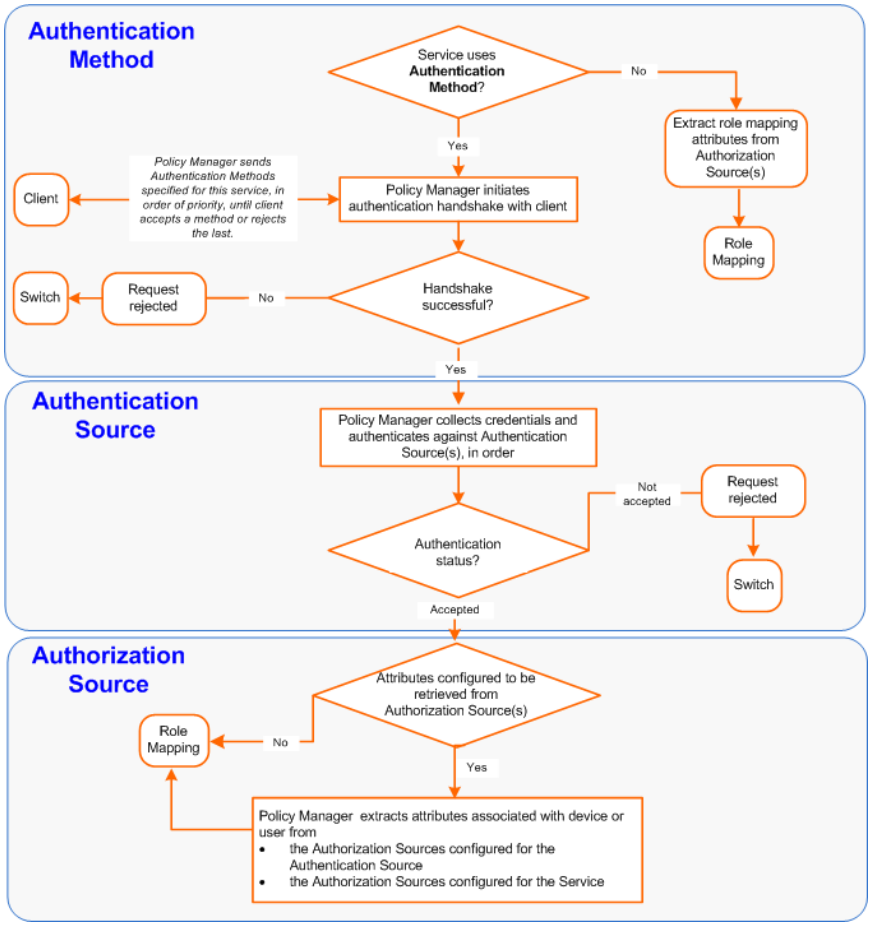
- *Authentication Method*. Policy Manager initiates the authentication handshake by sending available methods, in priority order, until the client accepts a methods or until it NAKs the last method, with the following possible outcomes:
  - Successful negotiation returns a method, for use in authenticating the client against the Authentication Source.
  - Where no method is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this Service.
  - Policy Manager rejects the connection.

An Authentication Method is only configurable for some service types (Refer to "Policy Manager Service Types" on page 69). 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. Once 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.
  - Once 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 47 *Authentication and Authorization Flow of Control*

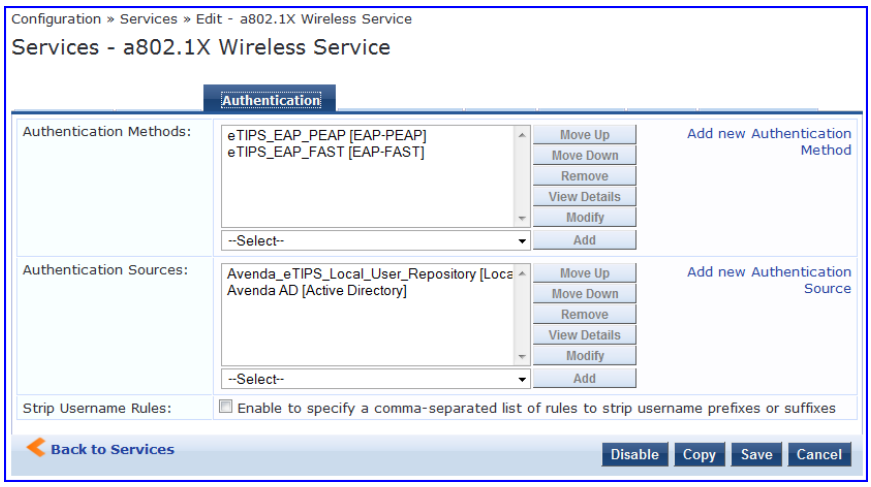


Configuring Authentication Components

The following summarizes the methods for configuring authentication:

- For an existing Service, you can add or modify 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 by itself: **Configuration > Authentication > Methods or Configuration > Authentication > Sources**.

Figure 48 *Authentication Components*



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

Table 28: *Authentication Features at the Service Level*

Configurable 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.) ▪ To add a previously configured *Authentication Method*, select from the **Select** drop down list, then click **Add**. ▪ To configure a new *Method*, click the **Add New Authentication Method** link. Refer to "Adding and Modifying Authentication Methods" on page 90for information about Authentication Methods. Note that an Authentication Method is only configurable for some service types. Refer to "Policy Manager Service Types" on page 69 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. ▪ To add a previously configured *Authentication Source*, select from the **Select** drop down list, then click **Add**. ▪ To configure a new *Authentication Source*, click the Add New Authentication Source link. Refer to "Adding and Modifying Authentication Sources " on page 107 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.

Table 29: *Policy Manager Supported Authentication Methods*

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

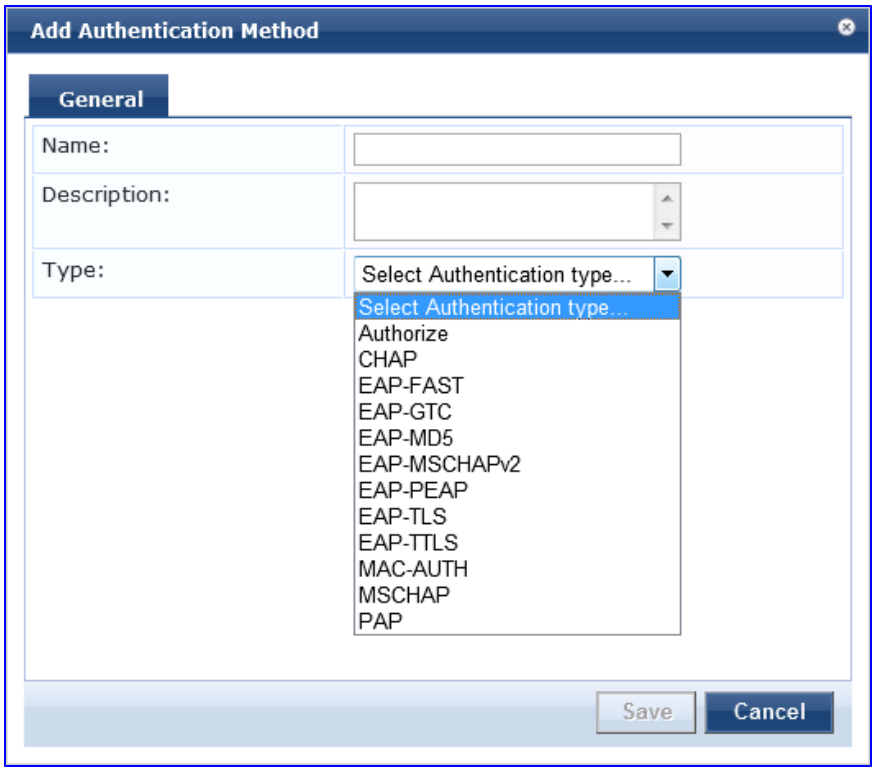
In tunneled EAP methods, authentication and posture credential exchanges occur inside of a protected outer tunnel.

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

From the **Services** page (**Configuration > Service**), 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).

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

Figure 49 *Add Authentication Method dialog box*



Depending on the **Type** selected, different tabs and fields appear. Refer to the following:

- "PAP " on page 92
- "MSCHAP " on page 93
- "EAP-MSCHAP v2 " on page 94
- "EAP-GTC " on page 94
- "EAP-TLS " on page 95
- "EAP-TTLS " on page 97
- "EAP-PEAP " on page 98
- "EAP-FAST " on page 100
- "MAC-AUTH " on page 105
- "CHAP and EAP-MD5 " on page 105
- Authorize

PAP

The PAP method contains one tab.

General Tab

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

Figure 50 *PAP General Tab*

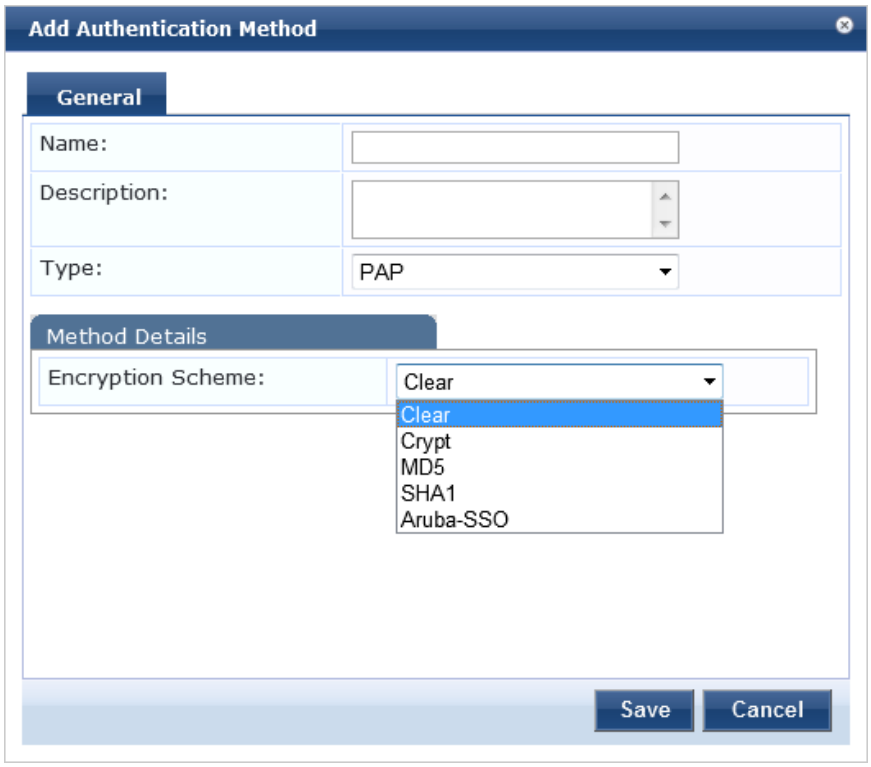


Table 30: *PAP General Tab*

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 or Aruba-SSO.

MSCHAP

The MSCHAP method contains one tab.

General Tab

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

Figure 51 *MSCHAP General Tab*

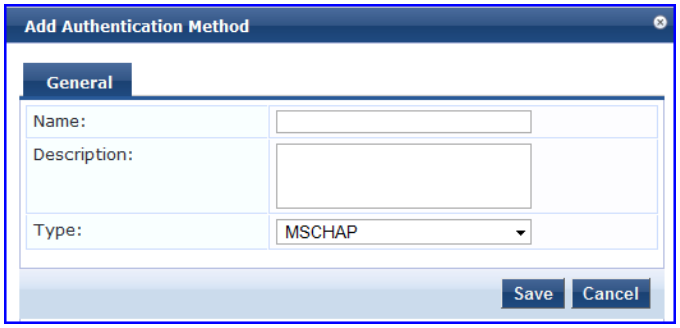


Table 31: *MSCHAP General Tab*

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

EAP-MSCHAP v2

The EAP-MSCHAPv2 method contains one tab.

General Tab

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

Figure 52 *EAP-MSCHAPv2 General Tab*

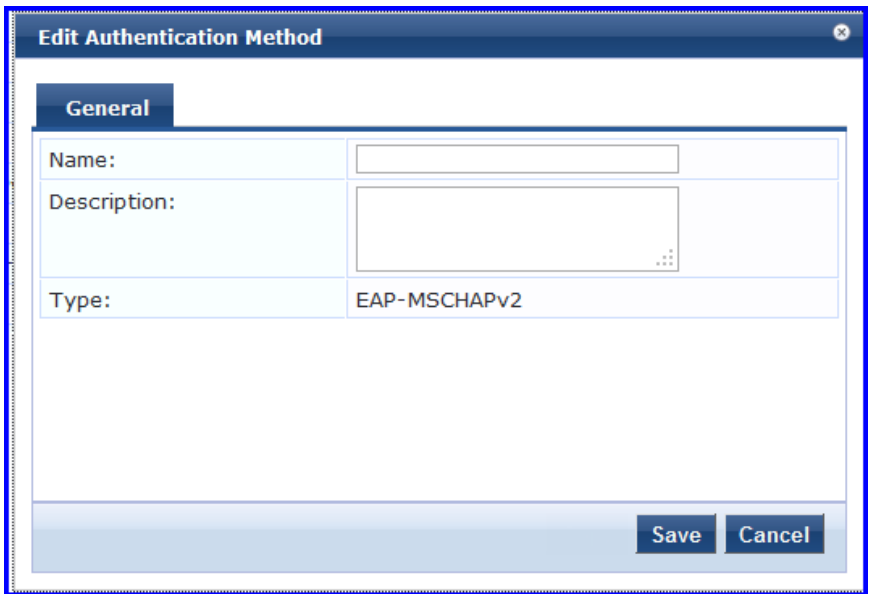


Table 32: *EAP-MSCHAPv2 General Tab*

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

EAP-GTC

The EAP-GTC method contains one tab.

General Tab

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

Figure 53 *EAP-GTC General Tab*

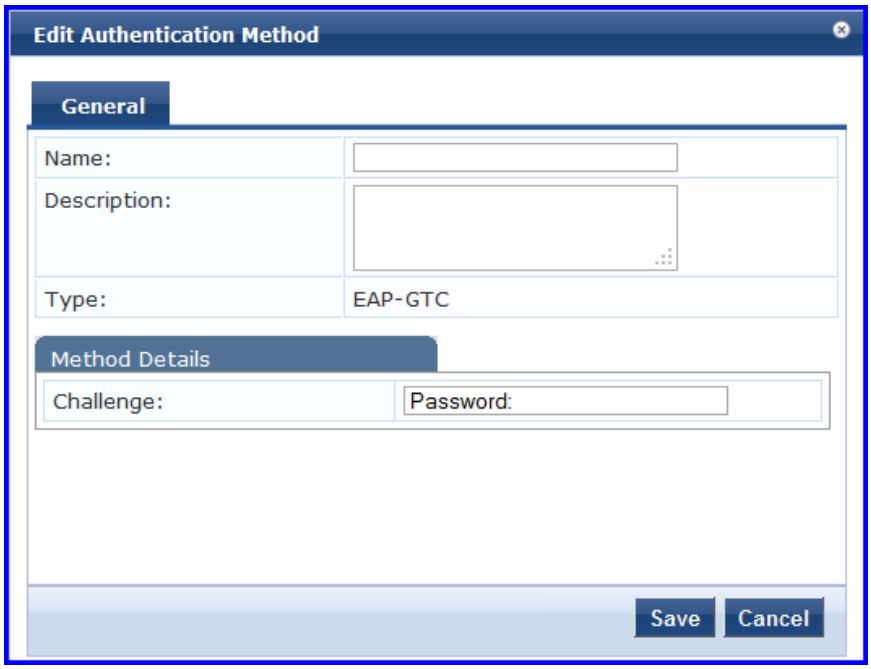


Table 33: *EAP-GTCGeneral Tab*

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

EAP-TLS

The EAP-TLS method contains one tab.

General Tab

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

Figure 54 *EAP_TLS General Tab*

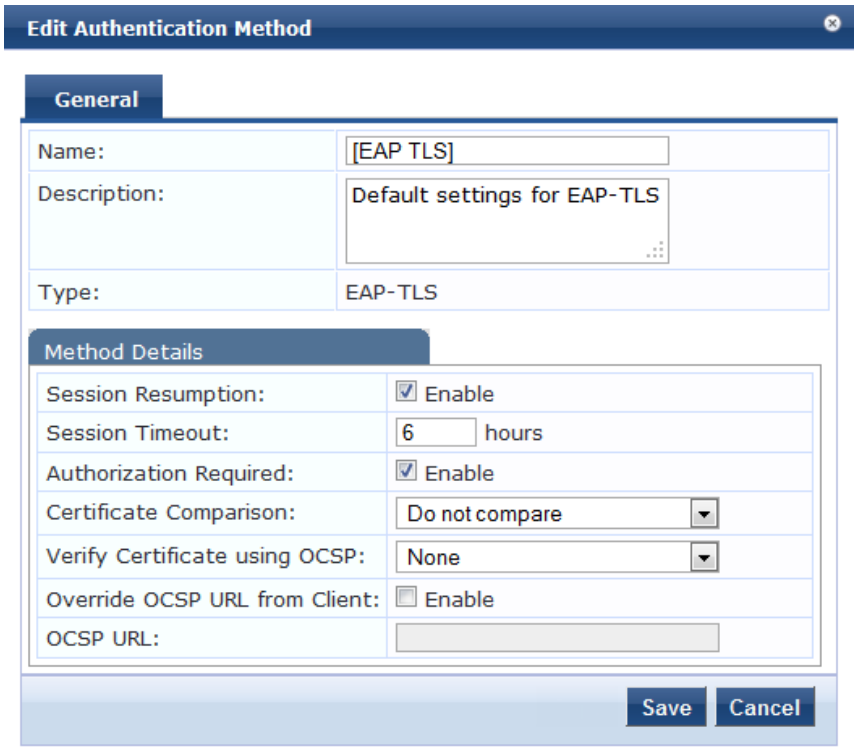


Table 34: *EAP_TLS General Tab*

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 Common Name (CN)**, **Compare Subject Alternate Name (SAN)**, or **Compare CN or SAN**. • To perform a binary comparison of the stored (in the client record in Active Directory or another LDAP-compliant directory) and presented certificates, choose **Compare Binary**.
Verify Certificate using OCSP	Select **Optional** or **Required** if the certificate should be verified by the Online Certificate Status Protocol (OCSP). Select **None** to not verify the certificate.

Parameter	Description
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 Tab

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

Figure 55 *EAP-TTLS General Tab*

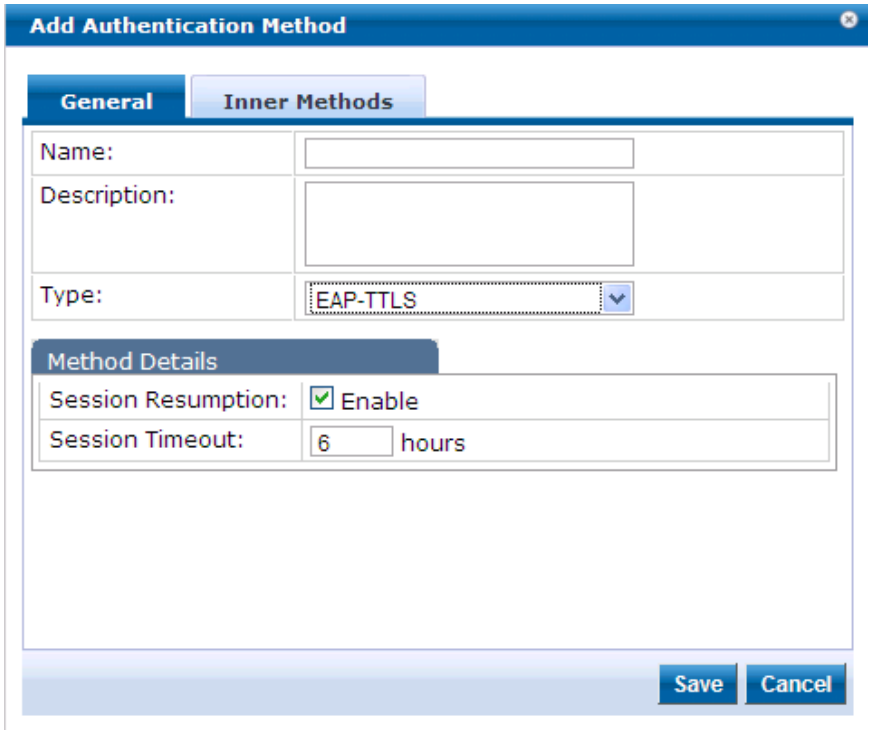


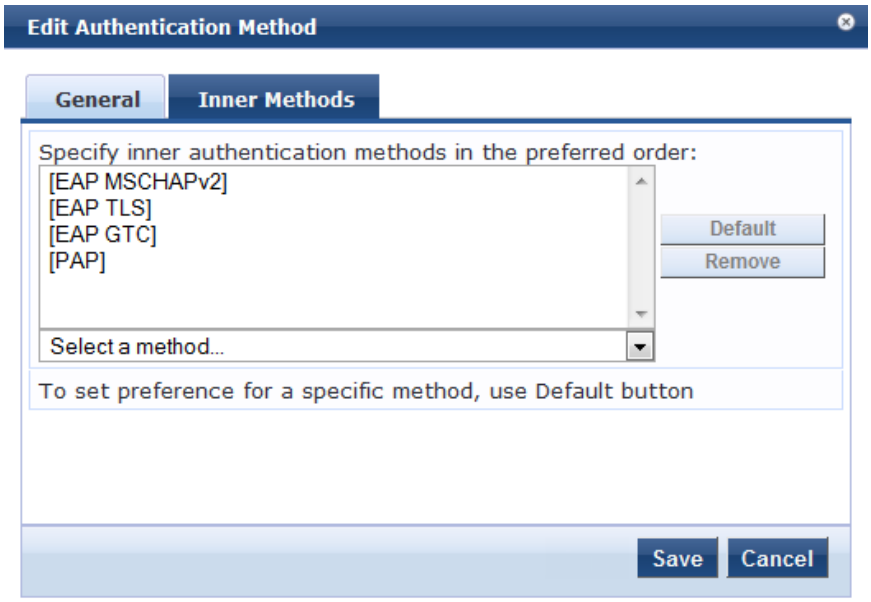
Table 35: *EAP-TTLS General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **EAP-TTLS**.
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 methods for the EAP-TTLS method:

Figure 56 *EAP_TTLS Inner Methods Tab*



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

- To append an inner method to the displayed list, select it from the drop-down list, 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-PEAP

The EAP-PEAP method contains two tabs:

General Tab

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

Figure 57 *EAP-PEAP General Tab*

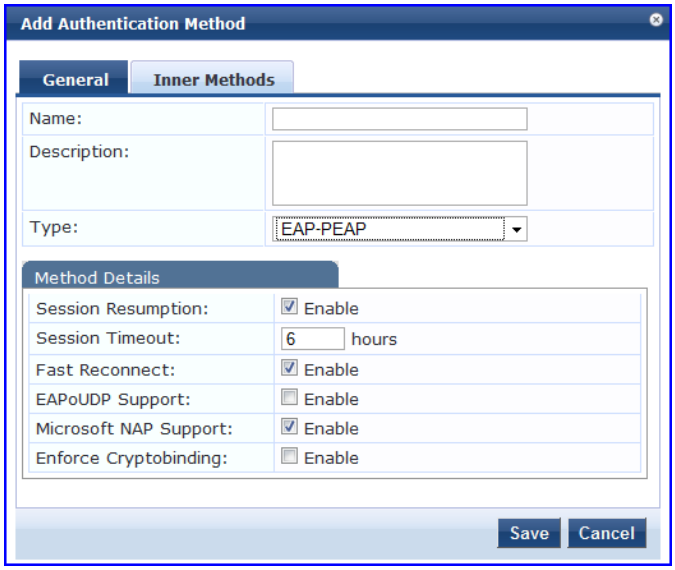


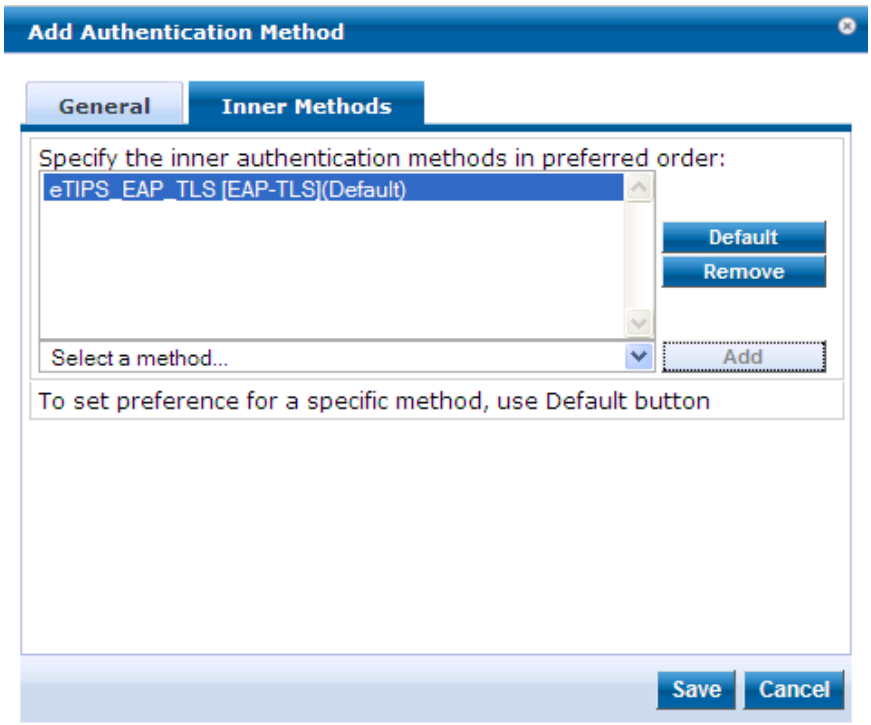
Table 36: *EAP-PEAP General Tab*

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.
EAPoUDP Support	Enable EAPoUDP support. When EAPoUDP support is enabled Policy Manager does not expect user authentication to happen within the protected tunnel.
Microsoft NAP Support	Enable while Policy Manager establishes the protected PEAP tunnel with a Microsoft NAP-enabled client. When enabled, Policy Manager prompts the client for Microsoft Statement of Health (SoH) credentials.
Enforce 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 58 *EAP-PEAP Inner Methods Tab*



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

- To append an inner method to the displayed list, select it from the drop-down list, 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-FAST

The EAP-FAST method contains four tabs:

General Tab

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

Figure 59 *EAP-FAST General Tab*

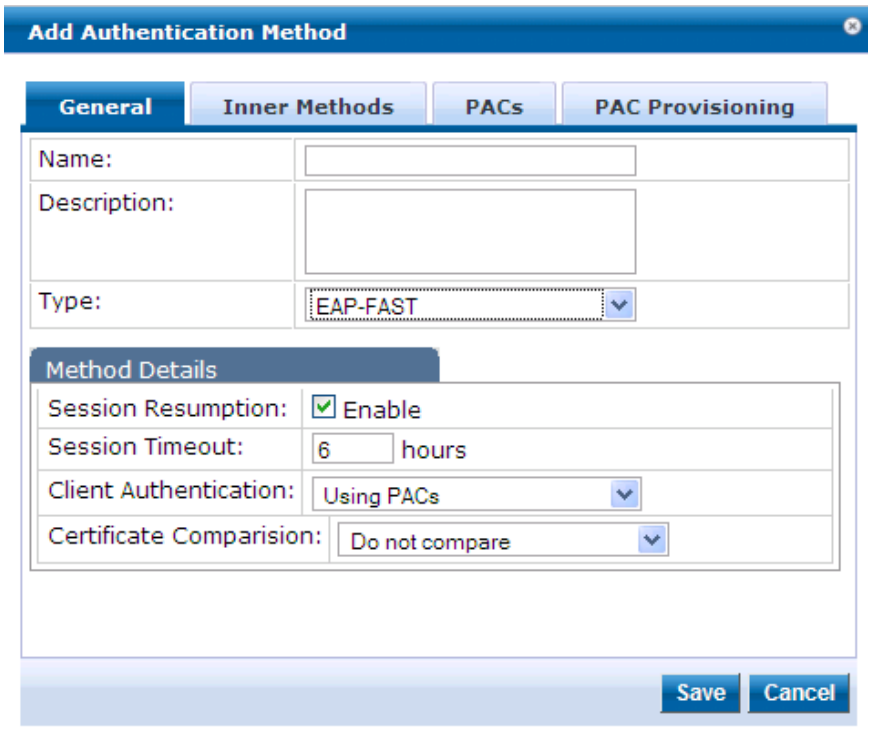


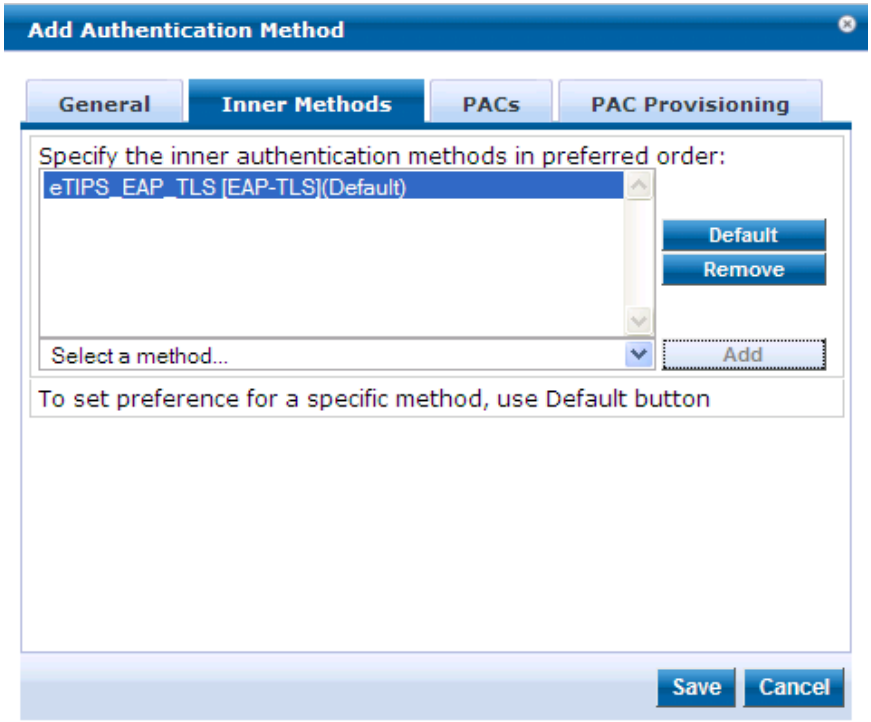
Table 37: *EAP_FAST General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always **EAP_FAST**.
Session Resumption	Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to Policy Manager within the session timeout interval.
Session Timeout	Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to Policy Manager within the session timeout interval. If session timeout value is set to 0, the cached sessions are not purged.
Fast Reconnect	Enable to allow fast reconnect. When enabled, the inner method of 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.
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.
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 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 60 *Inner Methods Tab*

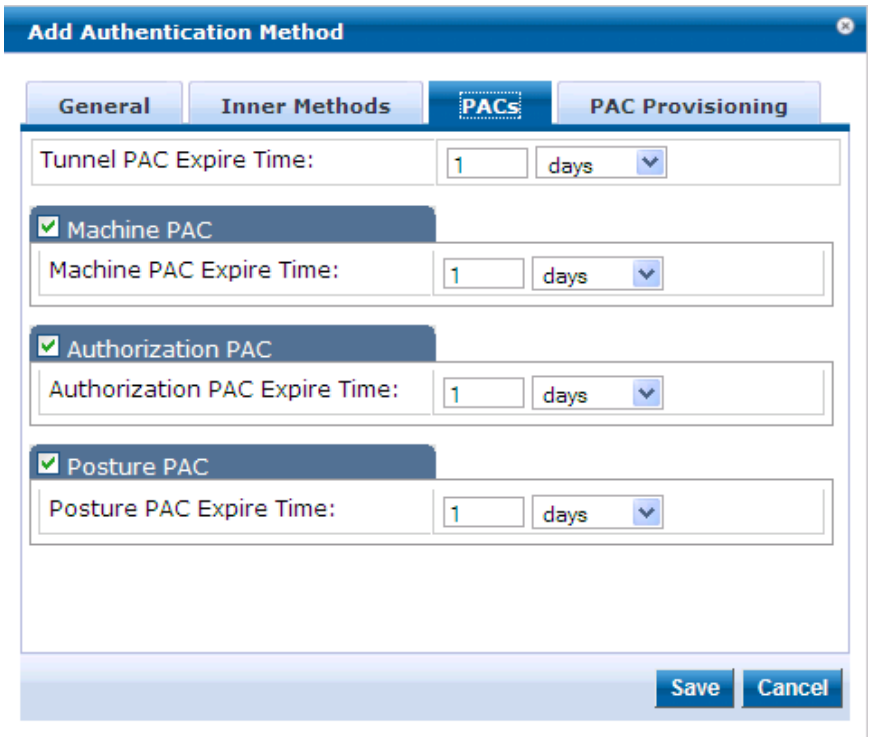


- To append an inner method to the displayed list, select it from the drop-down list, then click **Add**. The list can contain multiple inner methods, which Policy Manager will send, in priority order, until negotiation succeeds.
- To remove an inner method from the displayed list, select the method and click **Remove.**
- To set an inner method as the default (the method tried first), select it and click **Default.**

PACs Tab

The **PACs** tab enables/disables PAC types:

Figure 61 *EAP_FAST PACs Tab*



- 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. When presented with a valid Authorization PAC, Policy Manager skips the inner user authentication handshake within EAP-FAST. Specify the **Authorization PAC Expire Time** (the time until the PAC expires and must be replaced, by automatic or manual provisioning) in hours, days, weeks, months, or years. This is typically a short-lived PAC (specified in hours, 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 62 *EAP_FAST PAC Provisioning tab*

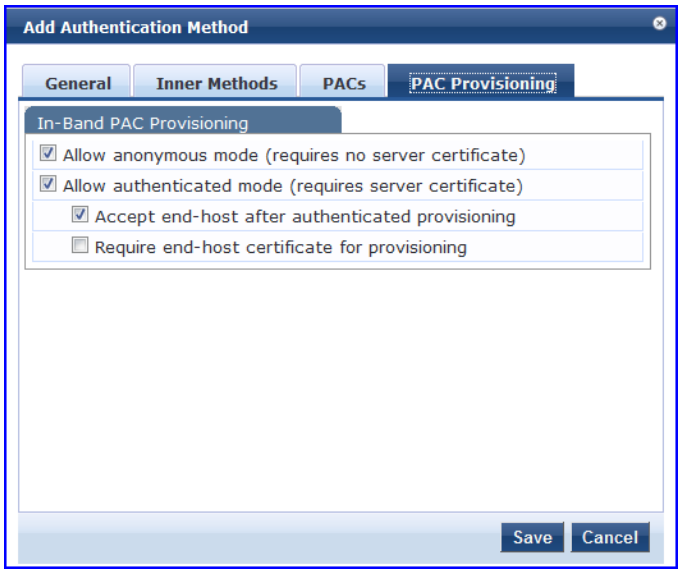


Table 38: *EAP_FAST PAC Provisioning Tab*

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). Once 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. Once 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.	
Accept end-host after authenticated provisioning	Once 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.	

Parameter	Description	Considerations
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.	

MAC-AUTH

The MAC-AUTH method contains one tab.

General Tab

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

Figure 63 *MAC-AUTH General Tab*

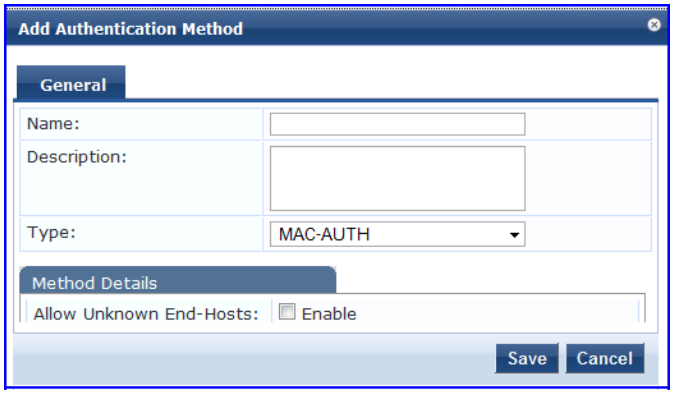


Table 39: *MAC-Auth General Tab*

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 180), you can trigger an audit of an unknown client.

CHAP and EAP-MD5

In addition the methods listed above, Policy Manager also comes packaged with CHAP and EAP-MD5 methods. These are named [CHAP] and [EAP-MD5], respectively. You can add methods of this type with a custom name. These methods can also be associated to a *Service* as authentication methods.

Figure 64 *CHAP General Tab*

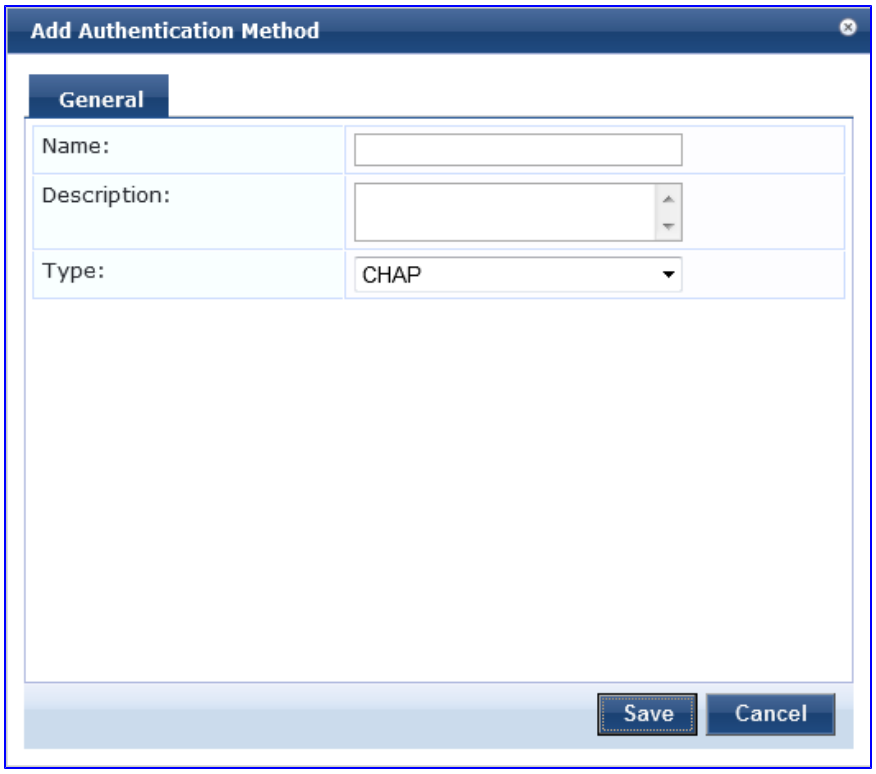


Figure 65 *EAP-MD5 General Tab*

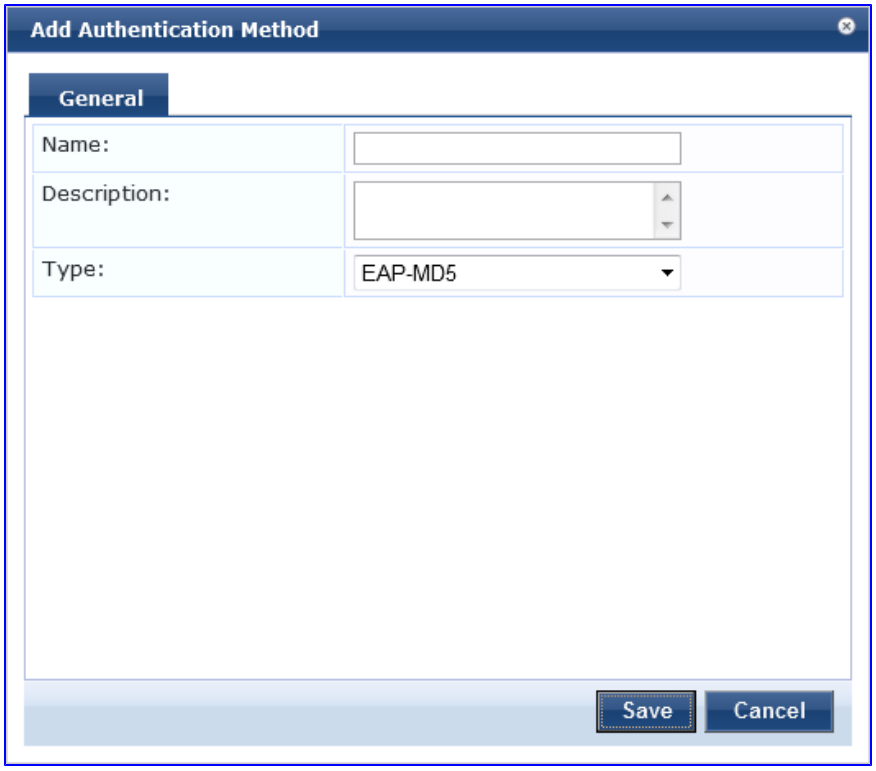


Table 40: *CHAP and EAP-MD5 General Tab Parameters*

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

Authorize

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

Figure 66 *Authorize General Tab*

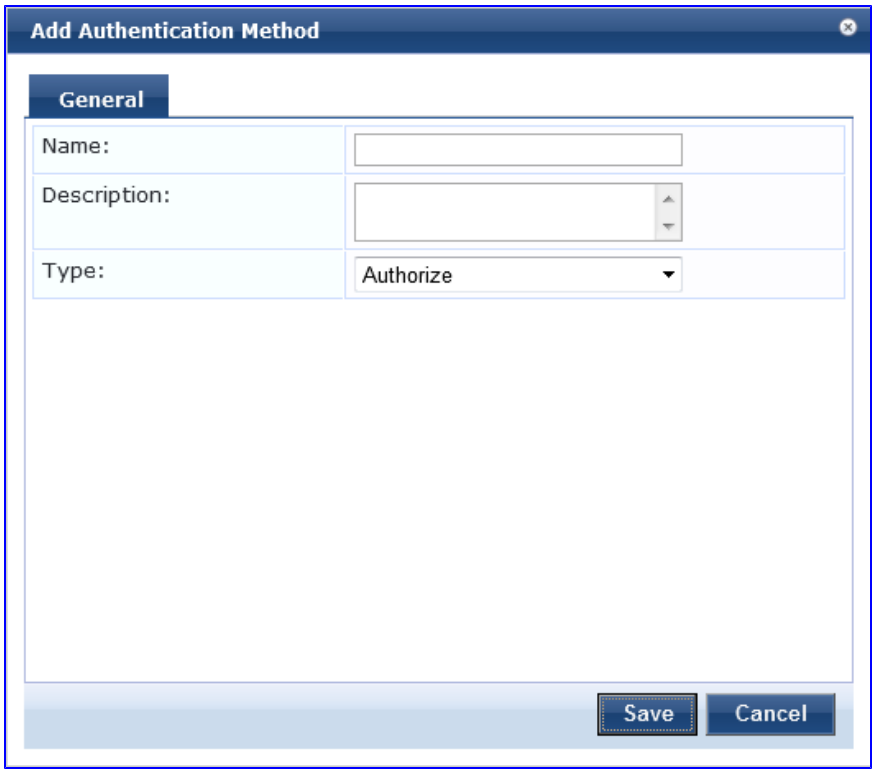


Table 41: *Authorize General Tab Parameters*

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

Adding and Modifying Authentication Sources

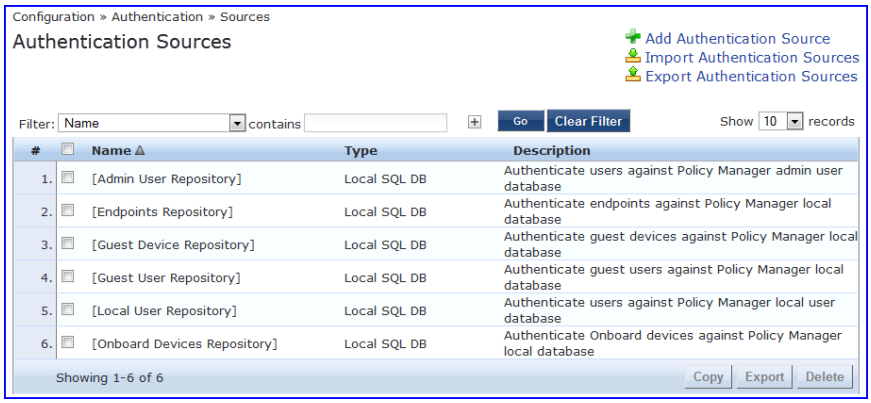
Policy Manager supports the following Authentication Sources:

- "Generic LDAP or Active Directory " on page 108
- "Generic SQL DB (Open Data Base Connectivity (ODBC) compliant SQL Databases) " on page 120
- "HTTP" on page 123

- "Kerberos " on page 126
- "Okta" on page 128
- "Static Host List " on page 130
- "Token Server " on page 132

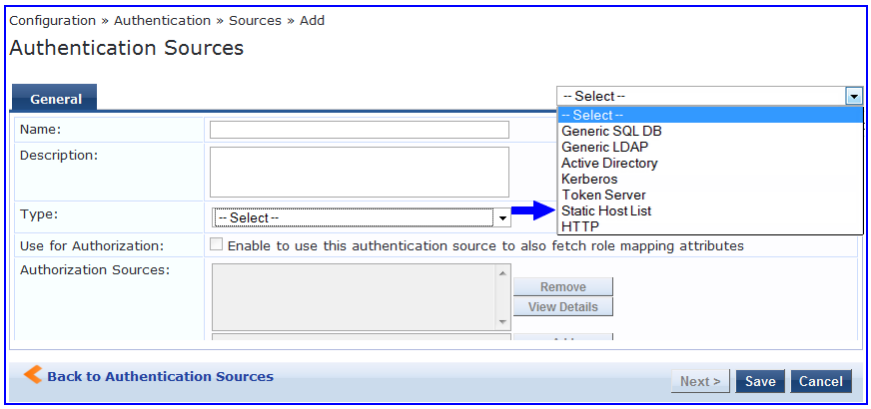
From the **Services** page (**Configuration > Service**), you can configure authentication source for a new service (as part of the flow of the **Add Service** wizard), or modify an existing authentication source directly (**Configuration > Authentication > Sources**, then click on its name in the listing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

Figure 67 *Authentication Sources Listing Page*



When you click **Add New Authentication Source** from any of these locations, Policy Manager displays the **Add** page.

Figure 68 *Add Authentication Source Page*



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

Generic LDAP or 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. See "Adding and Modifying Role Mapping Policies " on page 137

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
- Primary Tab

- Attributes Tab

General Tab

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

Figure 69 *Generic LDAP or Active Directory (General Tab)*

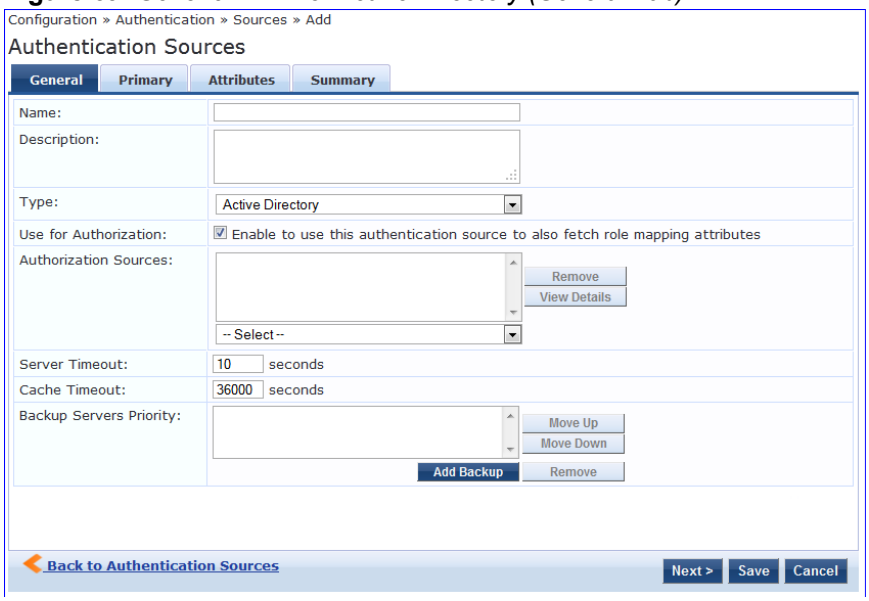


Table 42: *Generic LDAP or Active Directory (General Tab)*

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
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 66, 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.

Parameter	Description
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 if the primary server is unreachable.

Primary Tab

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

Figure 70 *Generic LDAP or Active Directory (Primary Tab)*

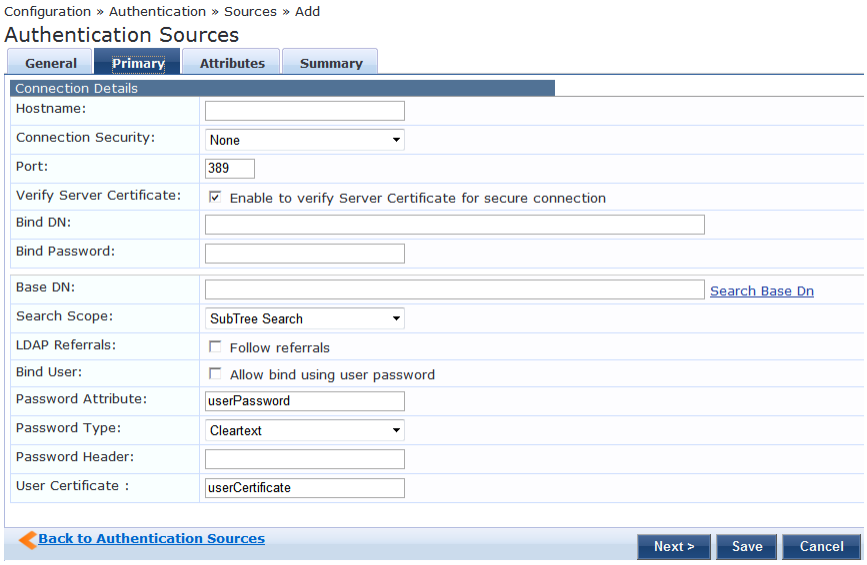
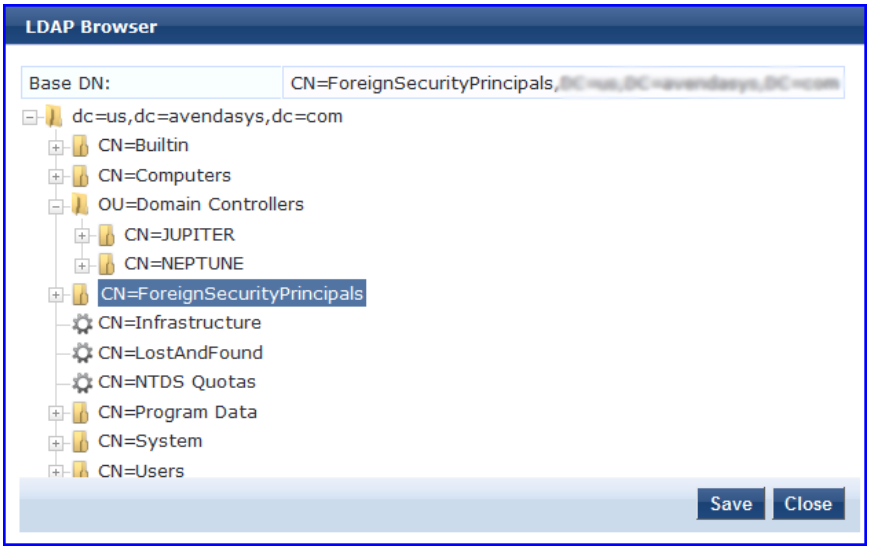


Table 43: *Generic LDAP or active Directory (Primary Tab)*

Parameter	Description
Host Name/Port	• Hostname or IP address of the LDAP or Active Directory server. • 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).
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.

Parameter	Description
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). 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.
Verify Server Certificate	Select this checkbox if you want to verify the Server Certificate as part of the authentication.
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 is popped up. You can navigate to the DN that you want to use as the Base DN.  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. • **Subtree Search** allows you to search the entire subtree under the base DN (including at the base DN level). • **One Level Search** allows you to search up to one level below (immediate children of) the base DN.
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.

Parameter	Description
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** directory)	Enter the name of the attribute in the user record from which user password can be retrieved. This is not available for Active Directory.
Password Header	Oracle's LDAP implementation prepends a header to a hashed password string. When 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 71 *Active Directory Attributes Tab (with default data)*

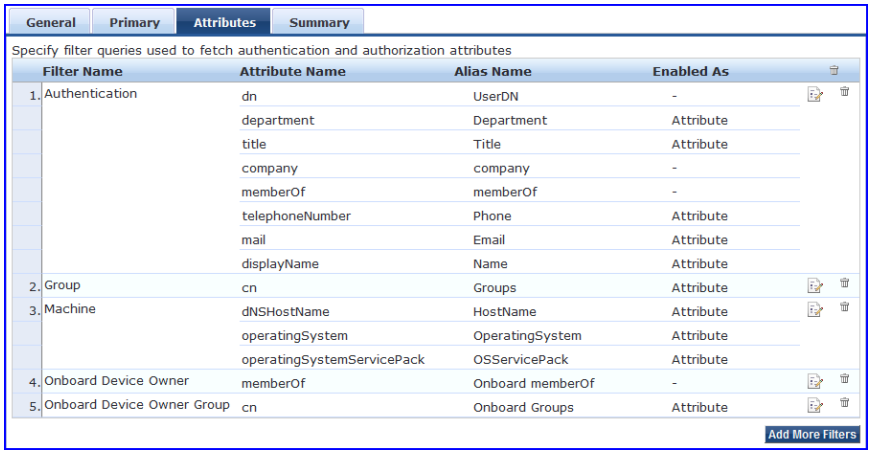


Figure 72 *Generic LDAP Directory Attributes Tab*

Table 44: *AD/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. This is described in the next image.

The following table describes the available directories.

Table 45: *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}))`
	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 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**
	• **Group**: This is 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 name of the connecting host (if available). dNSHostName, operatingSystem and operatingSystemServicePack attributes are fetched with this filter query.
	• **Onboard Device Owner:** This is the filter for retrieving the name of the owner the onboard device belongs to. This query finds the user in the ACtive Directory.
	`(&(sAMAccountName=%{Onboard:Owner})(objectClass=user))`
	%{Onboard:Owner} is populated by Policy Manager with the name of the onboarded user.
	• **Onboard Device Owner Group:** This filter is used for retrieving the name of the group the onboarded device owner belongs to.
	`(distinguishedName=%{Onboard memberOf})`
	This query fetches all group records where the distinguished name is the value returned by the Onboard memberOf variable. The attribute fetched with this filter query is cn, which is the name of the Onboard group

Generic LDAP Directory	**Authentication**: This is the filter used for authentication.
	`(&(objectClass=*)(uid=%{Authentication:Username}))`
	When a request arrives, Policy Manager populates %{Authentication:Username} with the authenticating user or machine. This filter is also set up to fetch the following attributes based on this filter query:
	▪ **dn** (aliased to UserDN): This is an internal attribute that is populated with the user record's Distinguished Name (DN)
	Group: This is filter used for retrieving the name of the groups a user belongs to.
	`(&(objectClass=groupOfNames)(member=%{UserDn}))`
	▪ This query fetches all group records (of objectClass groupOfNames), where 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)

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.

AD/LDAP Configure Filter 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 73 *AD/LDAP Configure Filter (Browse Tab)*

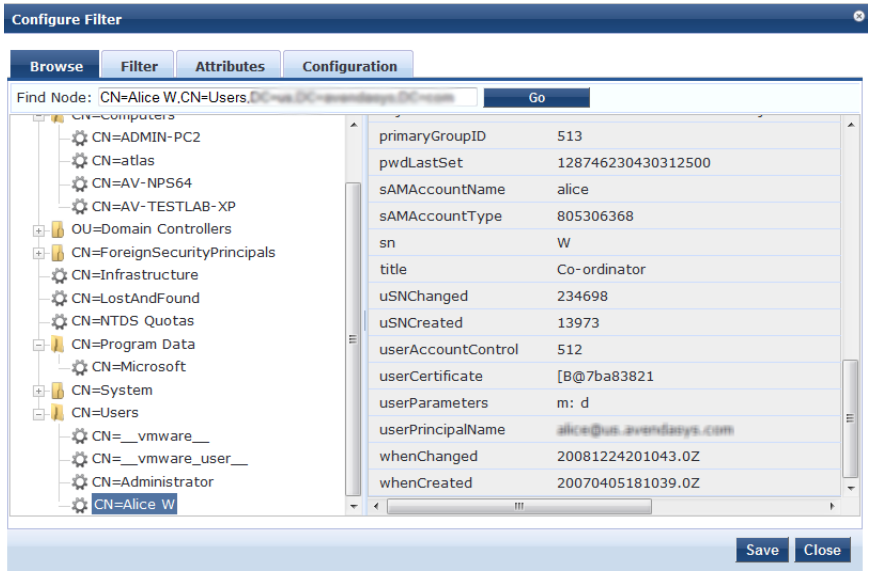


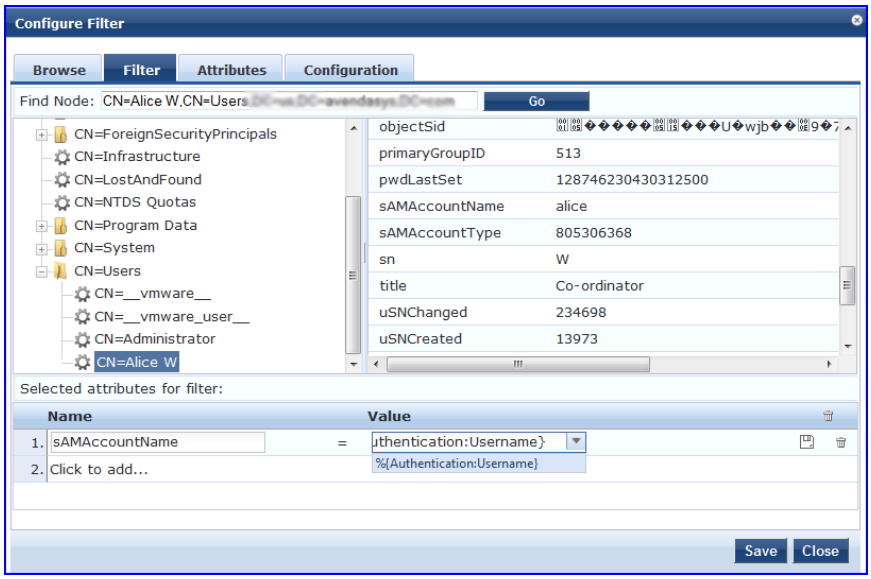
Table 46: *AD/LDAP Configure Filter Popup (Browse Tab)*

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

AD/LDAP Configure Filter, 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 74 *AD/LDAP Create Filter Popup (Filter Tab)*



NOTE

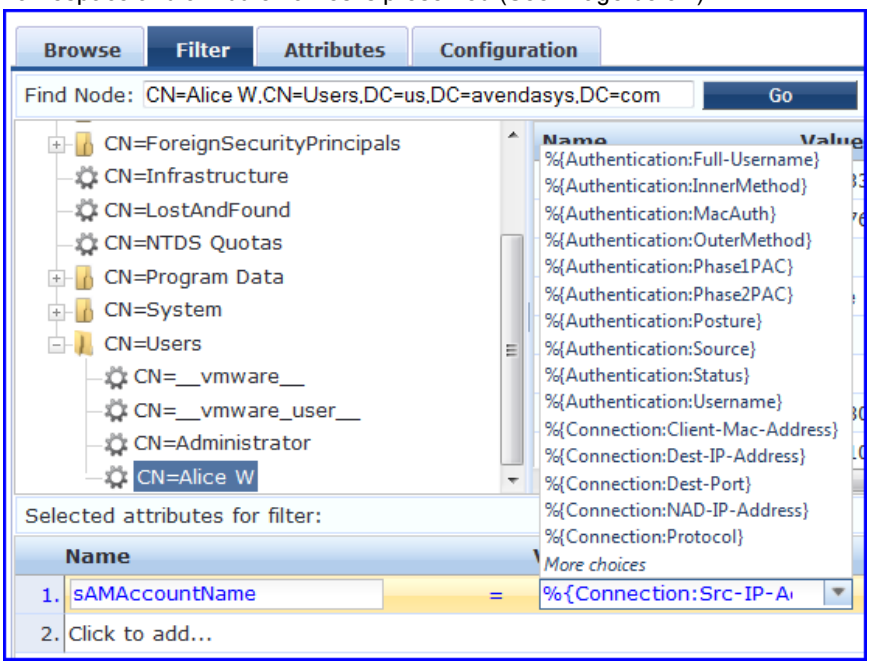
Policy Manager comes pre-populated with filters and selected attributes for Active Directory and generic LDAP directory. New filters need to be created only if you need Policy Manager to fetch role mapping attributes from a new type of record

NOTE

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 47: *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.

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). 

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

Table 48: *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).

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.

AD/LDAP Configure Filter 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 204.)

Figure 75 *AD/LDAP Configure Filter Attributes Tab*

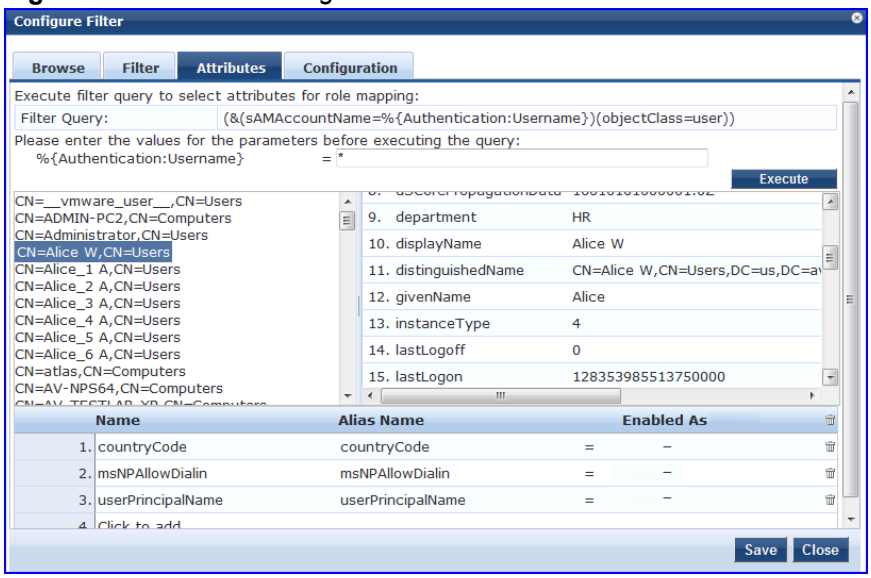


Table 49: *AD/LDAP Configure Filter Popup (Attributes Tab)*

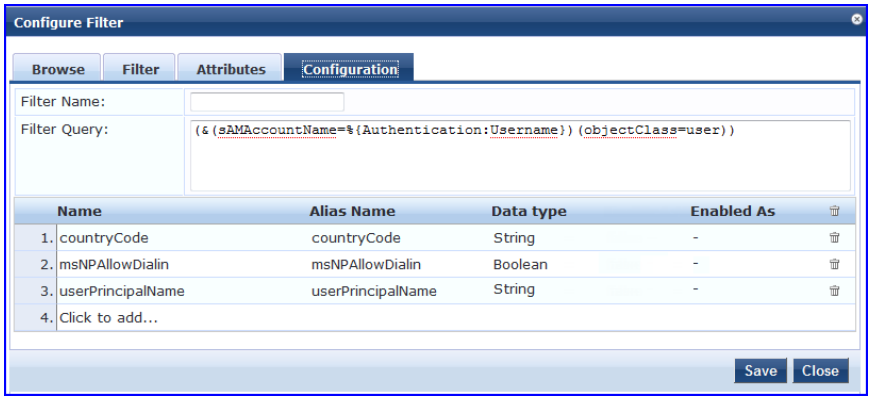
Parameter	Description
Enter values for parameters	Policy Manager parses the filter query (created in the **Filter** tab and shown at the top of the **Attributes** tab) and prompts to enter the values for all dynamic session parameters in the query. For example, if you have %{Authentication:Username} 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.
Execute	Once you have entered the values for all dynamic parameters, click on **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.

Parameter	Description
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.

AD/LDAP Configure Filter 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 76 *Configure Filter Popup (Configuration Tab)*



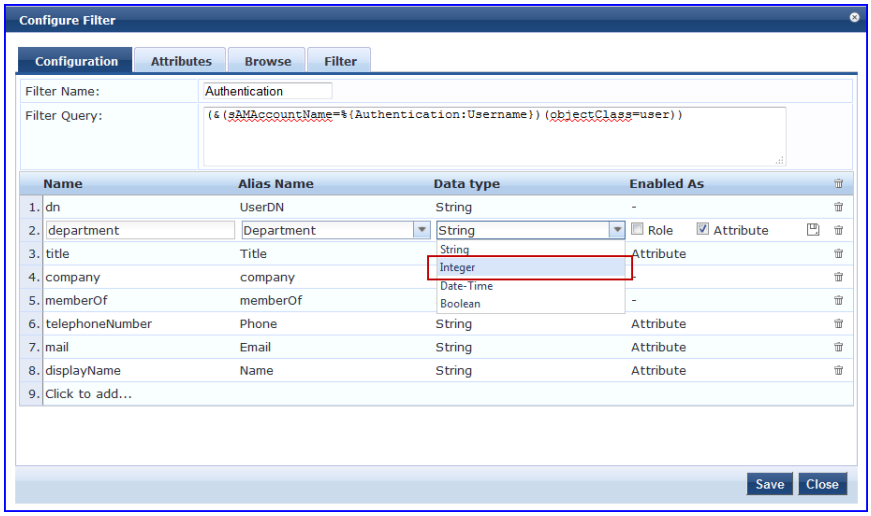
Modify Default Filters

When you add a new authentication source of type Active Directory or LDAP, a few default filters and attributes are 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 77 *Modify Default Filters*



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.

At least one 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 (Open Data Base Connectivity (ODBC) compliant SQL Databases)

Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against any ODBC-compliant database (for example, 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
- Primary Tab
- Attributes Tab

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 78 *Generic SQL DB (General Tab)*

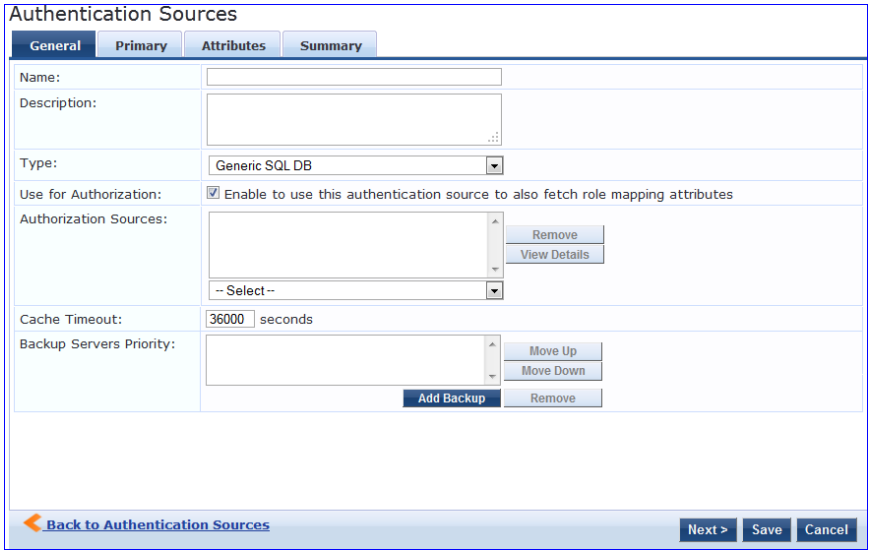


Table 50: *General SQL DB (General Tab)*

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**. 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.
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 79 *General SQL DB (Primary Tab)*

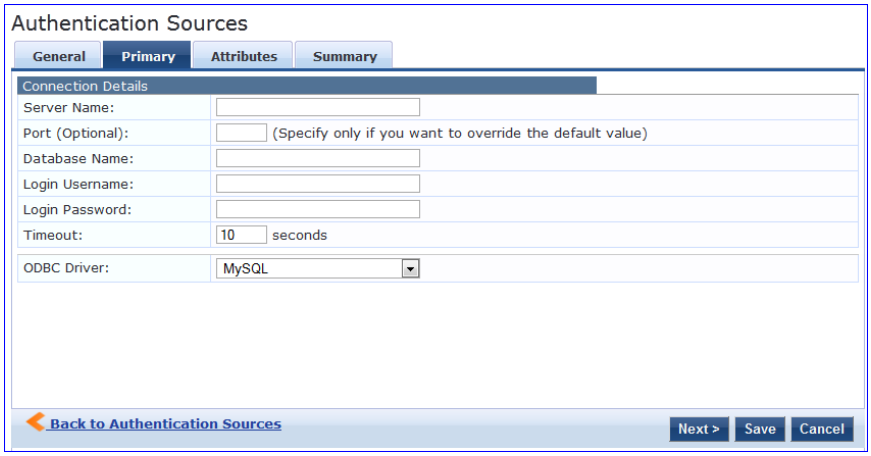


Table 51: *Generic SQL DB (Primary Tab)*

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, Oracle,or MSSQL in this release) to connect to database. **NOTE:** 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.

Attributes Tab

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

Figure 80 *Generic SQL DB (Attributes Tab)*

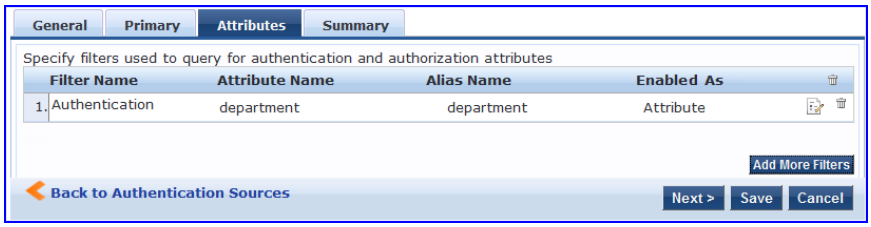


Table 52: *Generic SQL DB Attributes Tab (Filter List)*

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. • **Enabled As**: Indicates whether the filter is enabled as a role or attribute type. Note that this can also be blank.
Add More Filters	Brings up the filter creation popup.

Configure Filter Popup

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

Figure 81 *Generic SQL DB Filter Configure Popup*

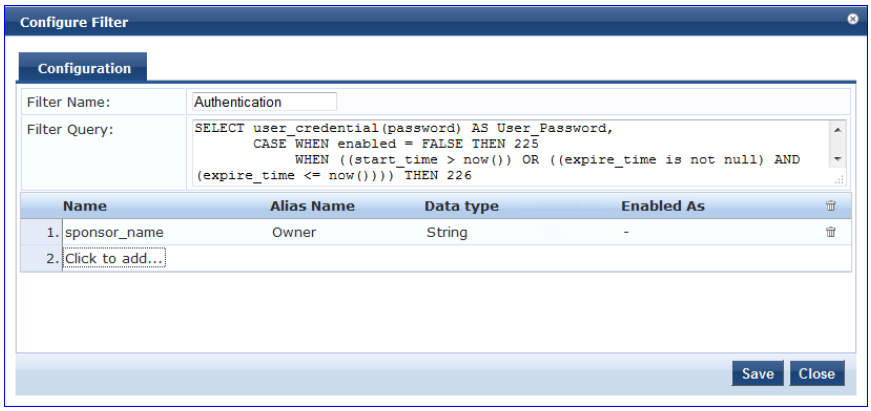


Table 53: *Generic SQL DB Configure Filter Popup*

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
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 of Generic SQL authentication sources on the following tab:

- General Tab
- Primary Tab
- Attributes Tab

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details.

Figure 82 *HTTP (General Tab)*

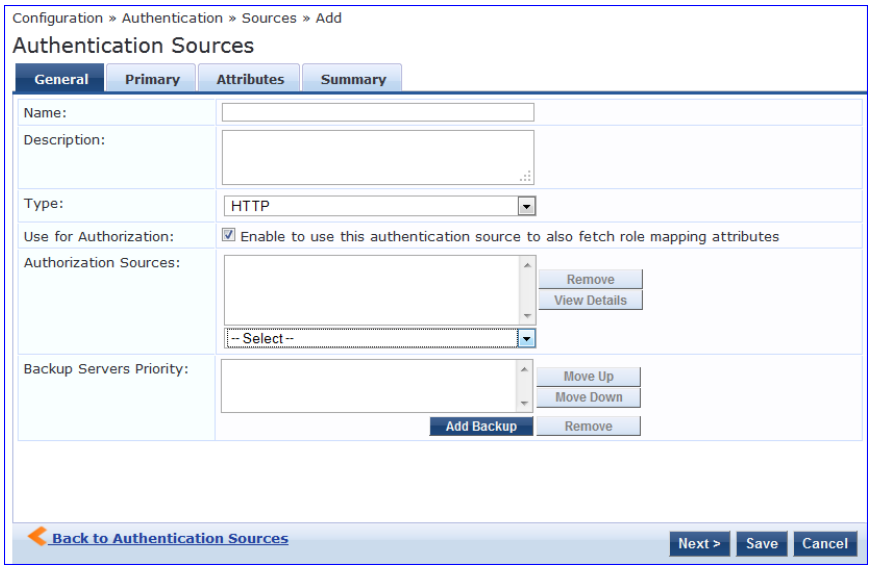


Table 54: *HTTP (General Tab)*

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 83 *HTTP (Primary Tab)*

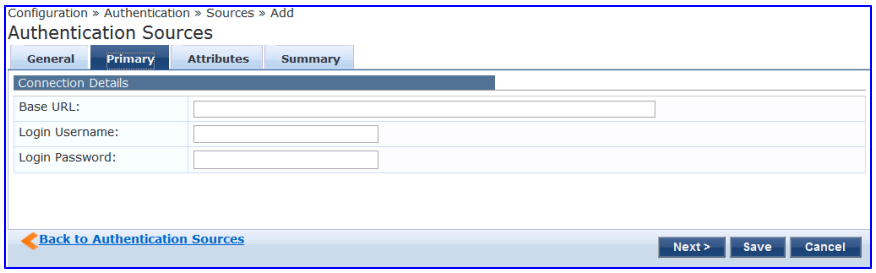


Table 55: *HTTP (Primary Tab)*

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 84 *HTTP (Attributes Tab)*

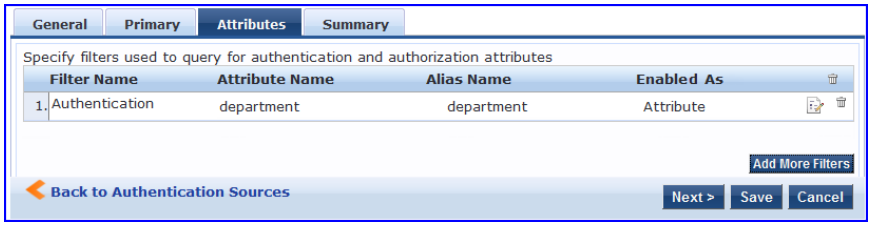


Table 56: *HTTP Attributes Tab (Filter List)*

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.

Configure Filter Popup

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

Figure 85 *HTTP Filter Configure Popup*

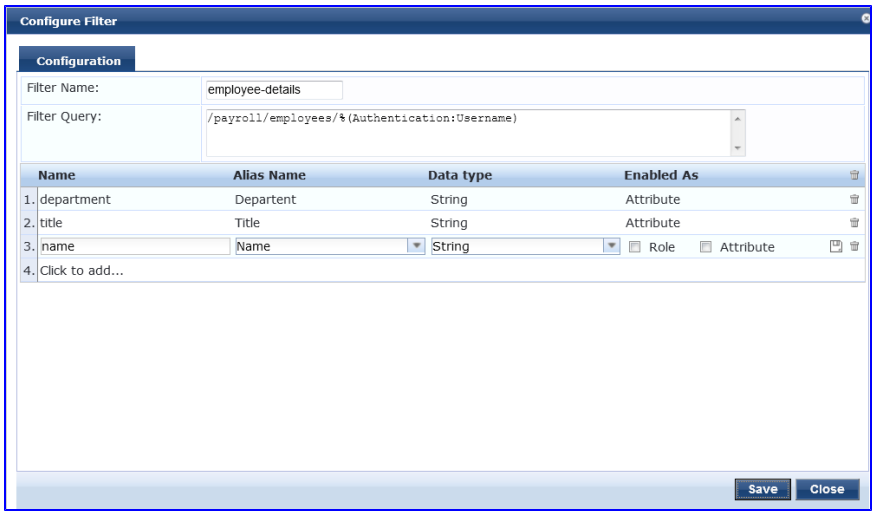


Table 57: *HTTP Configure Filter Popup*

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 pathname 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
- Primary Tab

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details.

Figure 86 *Kerberos General Tab*

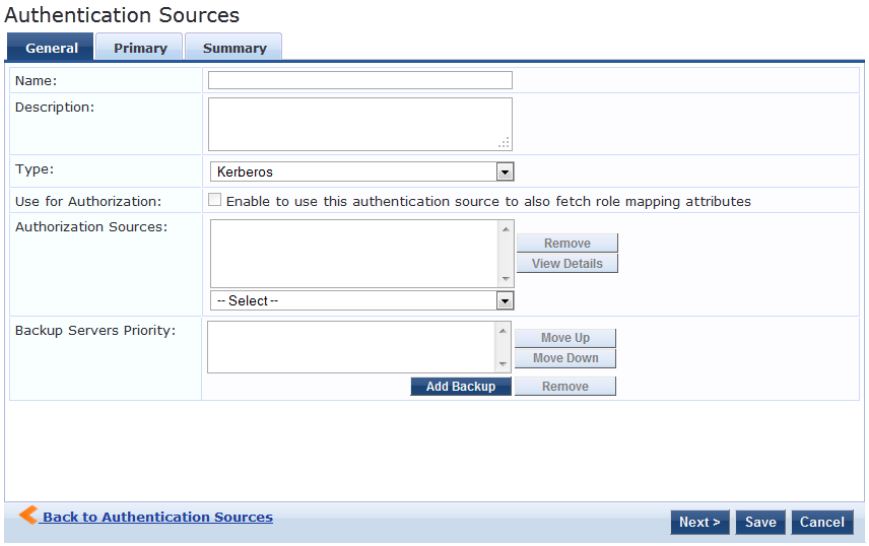


Table 58: *Kerberos (General Tab)*

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 87 *Kerberos (Primary Tab)*

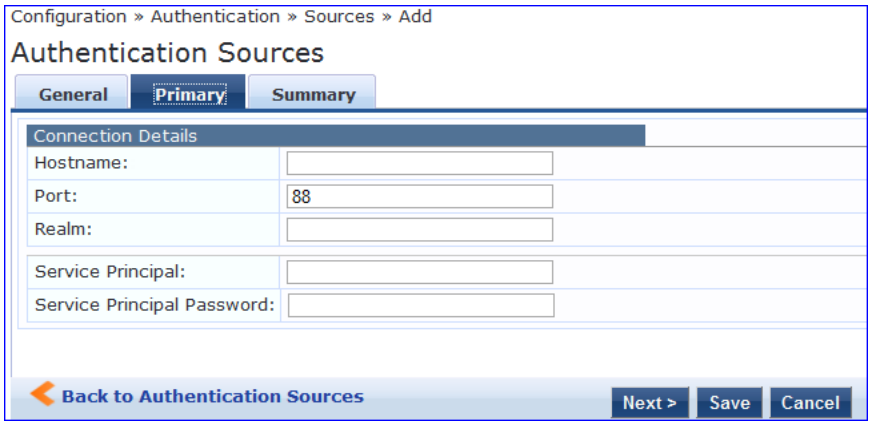


Table 59: *Kerberos (Primary Tab)*

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 Active Directory, this is the AD 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
- Primary Tab
- Attributes Tab

General Tab

Figure 88 *Okta General Tab*

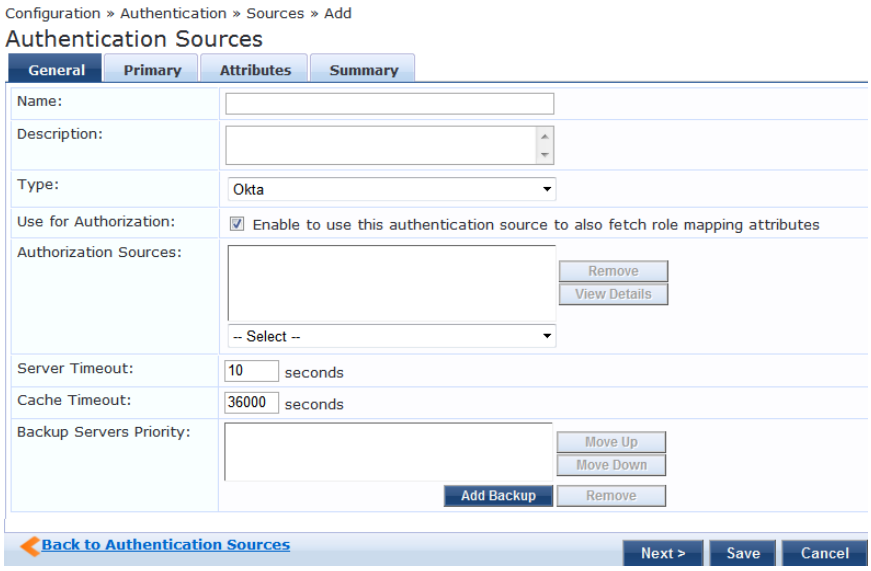


Table 60: *Okta (General Tab)*

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 89 *Okta Primary Tab*

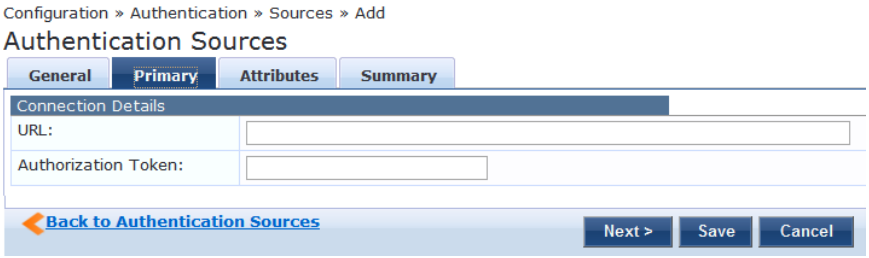


Table 61: *Okta (Primary Tab)*

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

Attributes Tab

Figure 90 *Okta Attribu tes Tab*

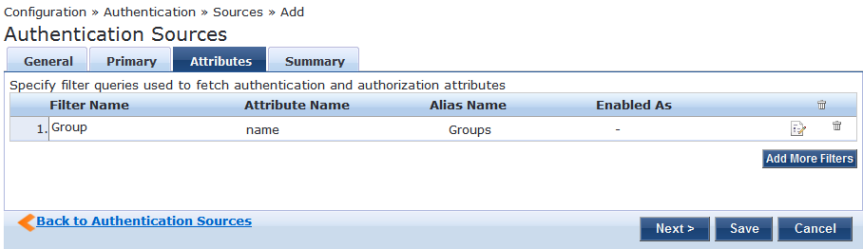


Table 62: *Okta (Attributes Tab)*

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. This is described in the next image.

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
- Static Host ListsTab

General Tab

The **General** Tab labels the authentication source.

Figure 91 *Static Host List (General Tab)*

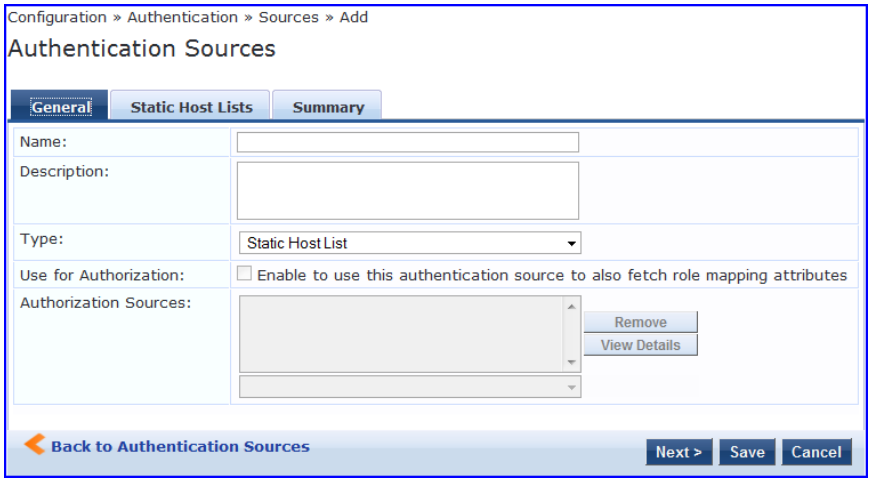


Table 63: *Static Host List (General Tab)*

Parameter	Description
Name/ Description	Freeform label
Type	**Static Host List**, in this context.
Use for Authorization/Authorization Sources	Not configurable

Static Host ListsTab

The Static Hosts List tab defines the list of static hosts to be included as part of the authorization source.

Figure 92 *Static Host List (Static Host Lists Tab)*

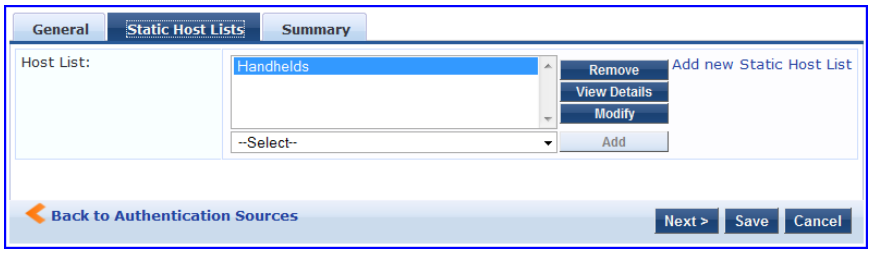


Table 64: *Static Hosts List (Static Host Lists Tab)*

Parameter	Description
Host List	Select a Static Host List from the drop down and **Add** to add it to the list.Click on **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 147 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 314.

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
- Primary Tab
- Attributes Tab

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details.

Figure 93 *Token Server (General Tab)*

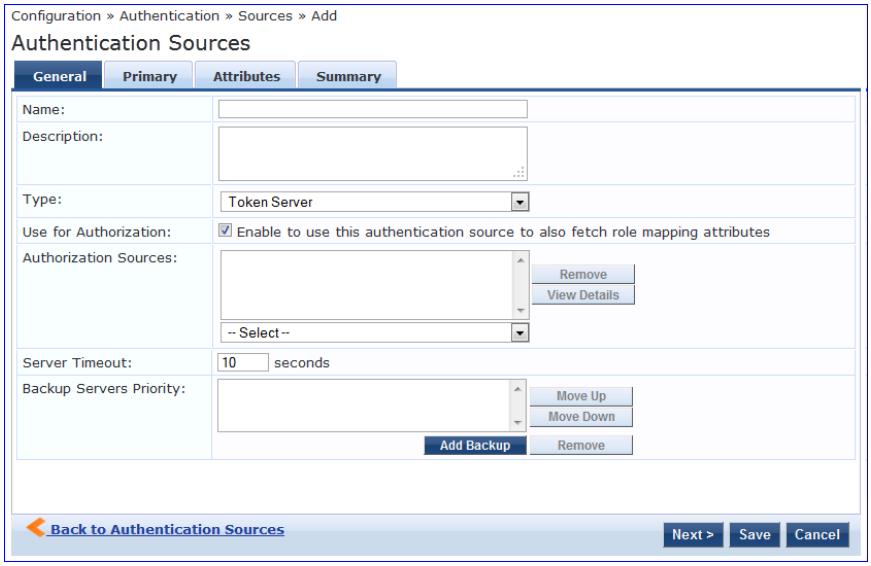


Table 65: *Token Server General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, **Token Server**
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: 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 94 *Token Server (Primary Tab)*

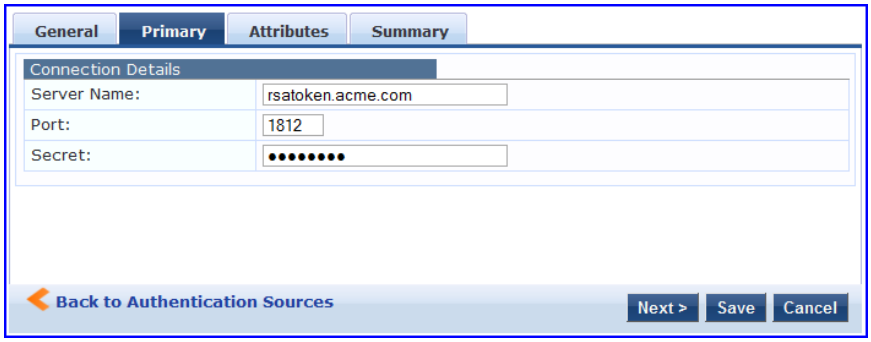


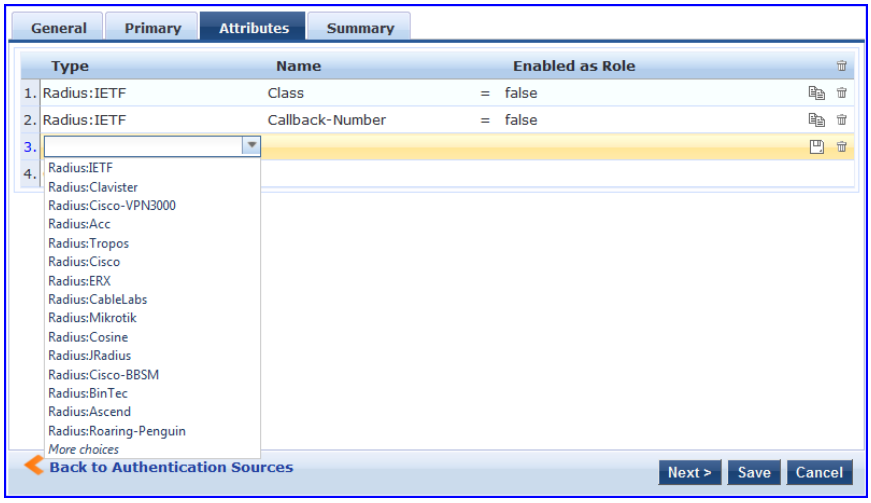
Table 66: *Token Server (Primary Tab)*

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 136for more information.) Policy Manager load all RADIUS vendor dictionaries in the type drop down to help select the attributes.

Figure 95 *Token Server (Attributes Tab)*



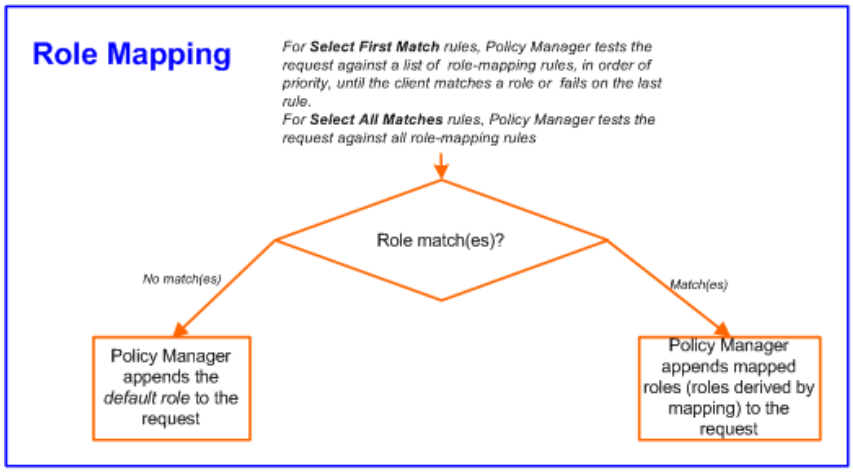
A Role Mapping Policy reduces client (user or device) identity or attributes associated with the request to *Role(s)* for Enforcement Policy evaluation. The roles ultimately determine differentiated access.

Architecture and Flow

Roles 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 users. A role can be:

- Discovered by Policy Manager through *role mapping* (Adding and Modifying Role Mapping Policies). 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. ("Adding and Modifying Authentication Sources " on page 107)
- Associated directly with a user in the Policy Manager *local user* database ("Adding and Modifying Local Users " on page 141 and "Adding and Modifying Guest Users " on page 142).
- Associated directly with a *static host list*, again through *role mapping* ("Adding and Modifying Static Host Lists " on page 147).

Figure 96 *Role Mapping Process*



Configuring a Role Mapping Policy

After authenticating a request, an 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 with the following pre-configured roles:

- [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

You can also configure other roles. Refer to Adding and Modifying Roles .

Configuring a Role Mapping Policy

After authenticating a request, an 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 with the following pre-configured roles:

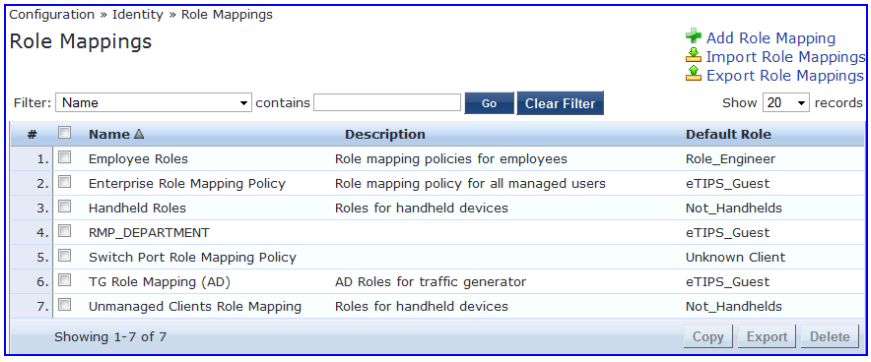
- [Guest] - Role for guest access
- [TACACS Help Desk] - Policy Manager Admin Role, limited to views of the Monitoring screens
- [TACACS Network Admin] - Policy Manager Admin Role, limited to Configuration and Monitoring UI screens
- [TACACS Receptionist] - Policy Manager Guest Provisioning Role
- [TACACS Super Admin] - Policy Manager Admin Role with unlimited access to all UI screens

You can also configure additional roles. Refer to "Adding and Modifying Roles " on page 140 for more information.

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 97 *Role Mapping Policies*



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 98 *Role Mapping (Policy Tab)*

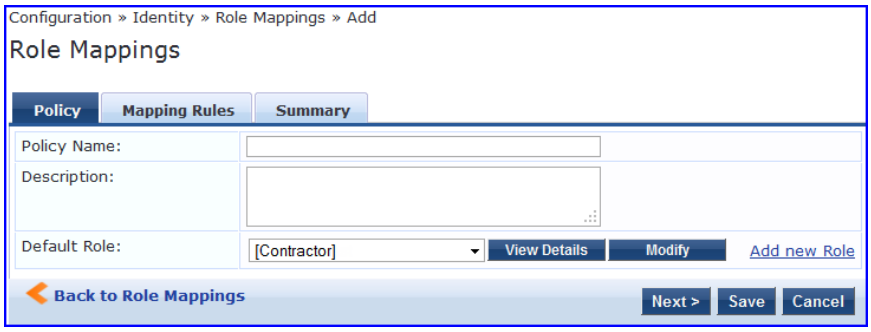


Table 67: *Role Mapping (Policy tab)*

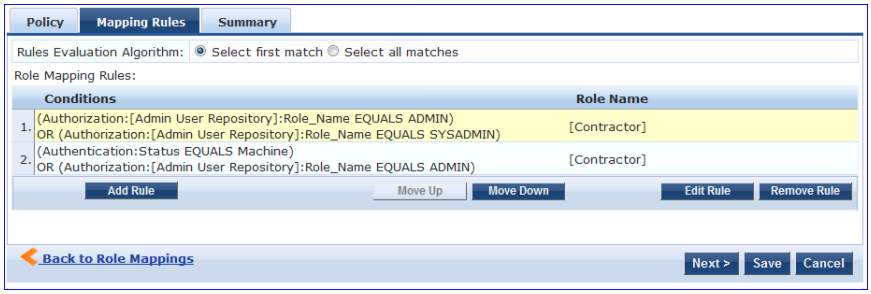
Parameter	Description
Policy Name /Description	Freeform label and description.
Default Role	Select the role to which Policy Manager will default when the role mapping policy does not produce a match.
View Details / Modify / Add new Role	Click on **View Details** to view the details of the default role. 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 99 *Role Mapping (Mapping Rules Tab)*



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

Figure 100 *Rules Editor*

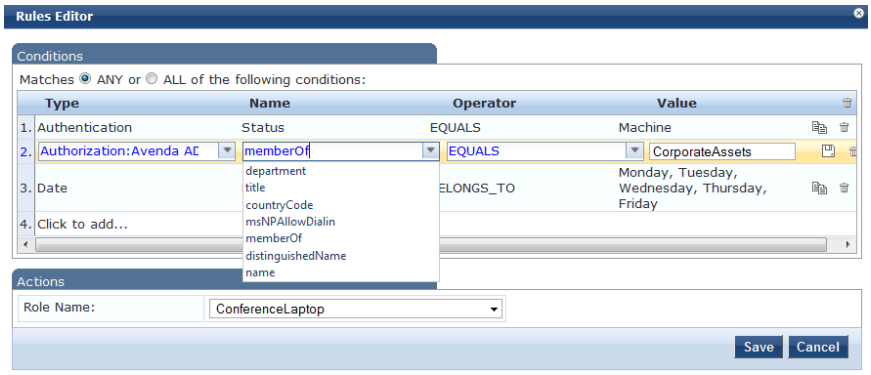


Table 68: *Role Mappings Page (Rules Editor)*

Label	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to "Namespaces" on page 314.) In the role mapping context, Policy Manager allows attributes from following namespaces: • Application • Authentication • Authorization • Authorization:<authorization_source_instance> - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. ("Adding and Modifying Authentication Sources " on page 107). Only those attributes that have been configured to fetched are shown in the attributes dropdown. • 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 320.
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.

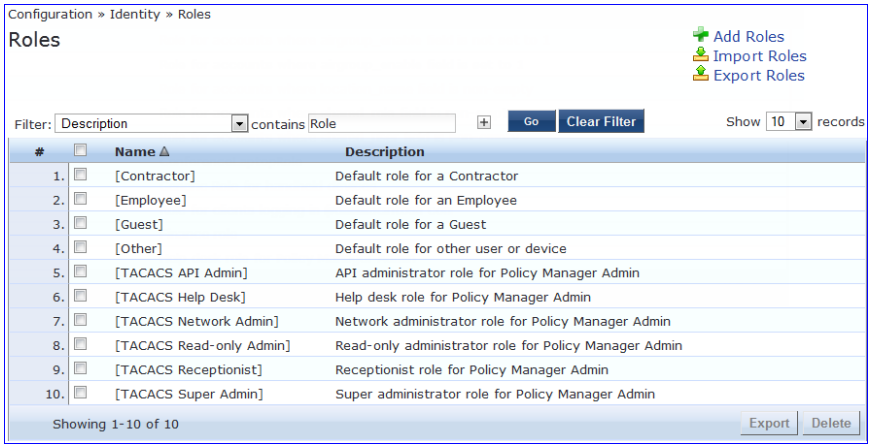
The Operator values that display for each Type and Name are based on the data type specified for the Authentication Source (from the **Configuration > Authentication > Sources** page). If, for example, you modify the UserDN Data type on the Authentication Sources page to be an Integer rather than a string,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

When you save your Role Mapping configuration, it appears in the **Mapping Rules** tab list. In this interface, you can select a rule (click and the background changes color), and then use the various widgets to Move Up, Move Down, Edit the rule, or Remove the rule.

Adding and Modifying Roles

Policy Manager lists all available roles in the Roles page. From the menu, select **Configuration > Identity > Roles**.

Figure 101 *Roles*



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 102 *Add New Role*

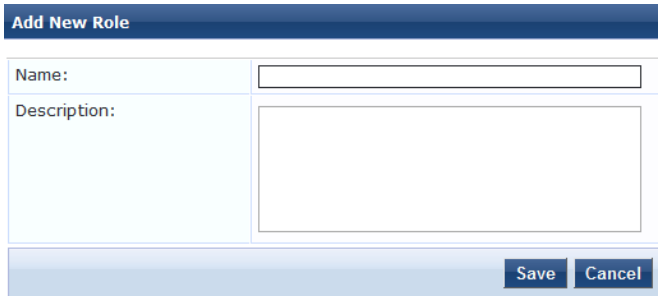


Table 69: *Add New Role*

Parameter	Description
Role Name /Description	Freeform label and description.

Local Users, Guest Users, Onboard Devices, Endpoints, and Static Host List Configuration

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 **endpoints** table 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.

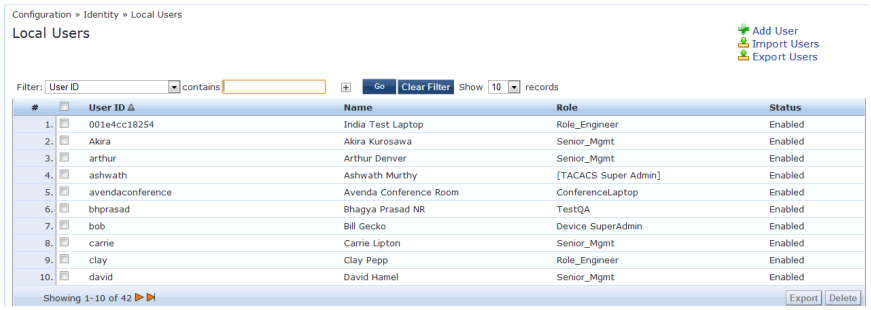
A **static host list** comprises of list of MAC and IP addresses. These can be used as white or black lists to control access to the network.

Refer to "Adding and Modifying Local Users " on page 141 for information on how to configure Local Users.

Adding and Modifying Local Users

Policy Manager lists all local users in the **Local Users** page (**Configuration > Identity > Local Users**):

Figure 103 *Fig: Local Users Listing*



To add a local user, click **Add User** to display the **Add Local User** popup.

Figure 104 *Add Local User*

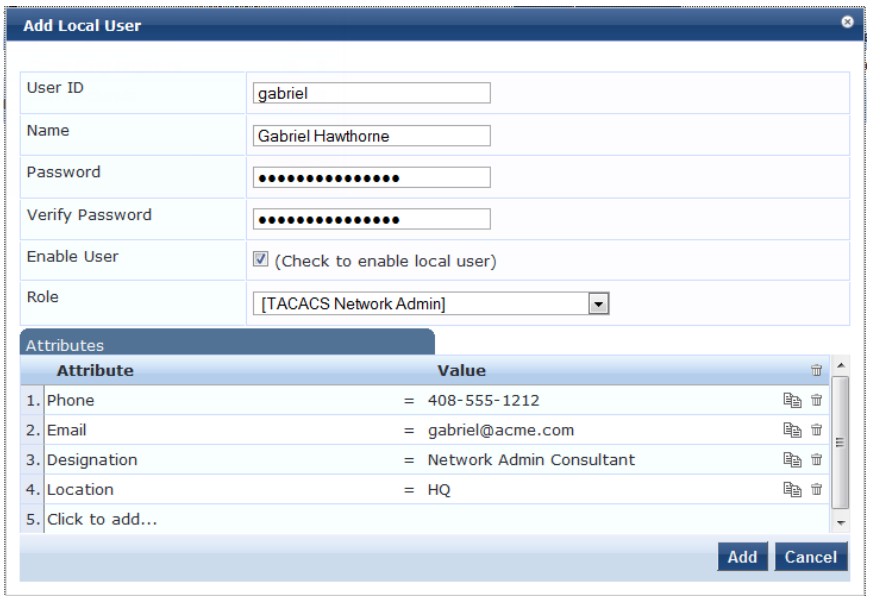


Table 70: *Add Local User*

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.
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 dropdown: 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 Attribute dropdown for all local users. **NOTE:** All attributes entered for a local user are available in the role mapping rules editor under the LocalUser namespace.

Additional Available Tasks

- 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.**

Adding and Modifying Guest Users

An administrator with the Policy Manager *Receptionist* role provisions users specifically as *Guests* (local users with a pre-defined role of Guest). From the menu, select **Configuration > Identity > Guest Users**.

Figure 105 *Guest Users Listing*

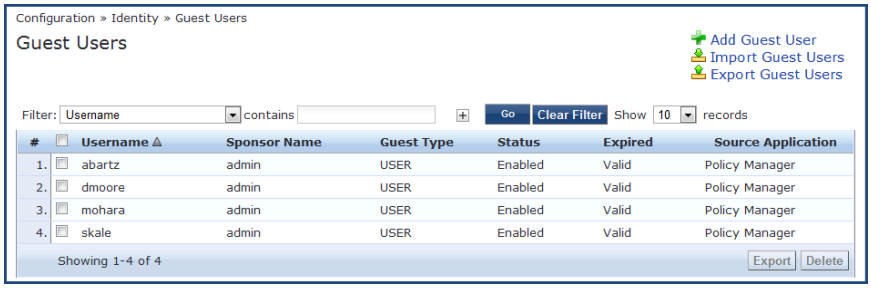


Table 71: *Guest Users Listing*

Parameter	Description
User Name	Guest user name.

Parameter	Description
Sponsor Name	Sponsor who sponsored the guest.
Guest Type	USER (for guest users) and DEVICE (for devices registered from the Guest product).
Status	Enabled/Disabled status.
Expired	Whether the guest/device account has expired
Source Application	Where this account was created: From Policy Manager or the Guest guest provisioning product.

In the **Guest Users** listing:

- To add a guest user or device, click **Add User**. This opens the **Add New Guest User** popup.

Figure 106 *Add New Guest User*

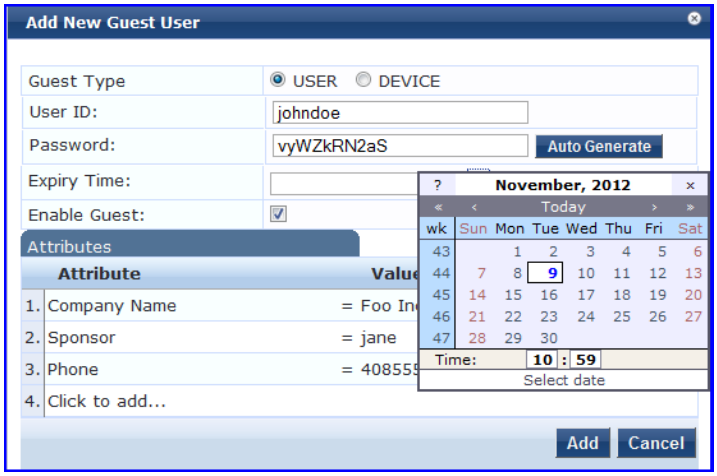


Figure 107 *Add New Guest Device*

Table 72: *Add New Guest User/Device*

Parameter	Description
Guest Type	Add a guest user or a guest device

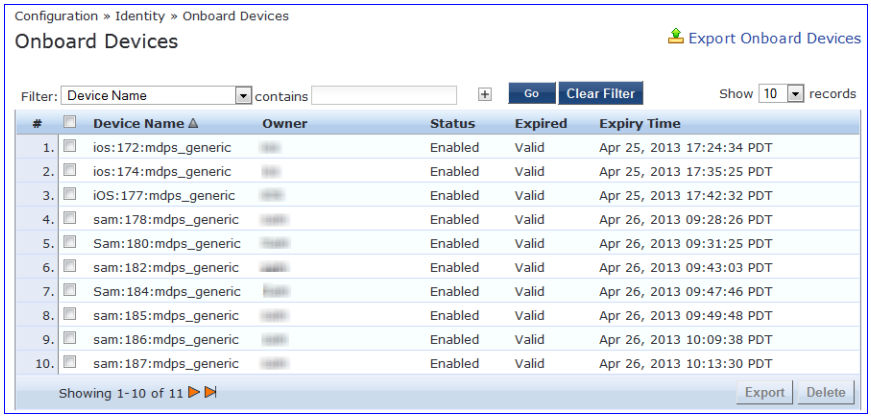
Parameter	Description
User ID/ Name /Password/ Verify Password (Guest User only)	Freeform labels and password. Click **Auto Generate** to auto-generate a password for the guest user.
MAC Address (Guest Device only)	MAC address of the guest device.
Enable Guest	Check to enable guest user.
Expiry Time	Use the date widget to select the date and time on which this Guest User's access expires.
Attributes	Add custom attributes for this guest user. Click on the "Click to add..." row to add custom attributes. By default, six custom attributes appear in the Attribute dropdown: Company-Name, Location, 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 **Attribute** drop down for all guest users. **NOTE:** All attributes entered for a guest user are available in the role mapping rules editor under the GuestUser namespace.

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

Onboard Devices

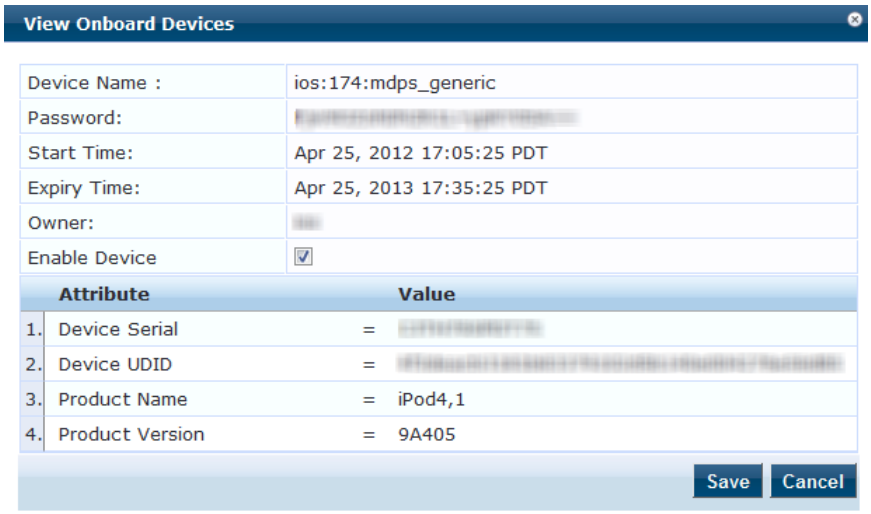
The **Configuration > Identity > Onboard Devices** page lists all devices that have authenticated. The information within this page includes the device name, owner, status, whether the device is expired, and the expiry time.

Figure 108 *Onboard Devices*



Click on a device name within a row to drill down and view detailed information about the device, including the device password, start and expiry times, owner, serial number, UUID, product name, and product version. You can also use the **Enable Device** check box to enable or disable the device.

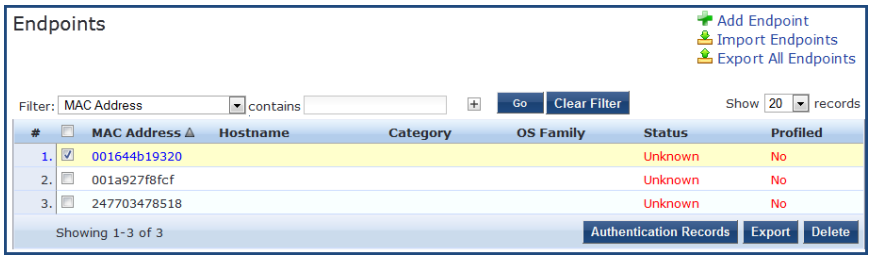
Figure 109 *View Onboard Devices*



Adding and Modifying Endpoints

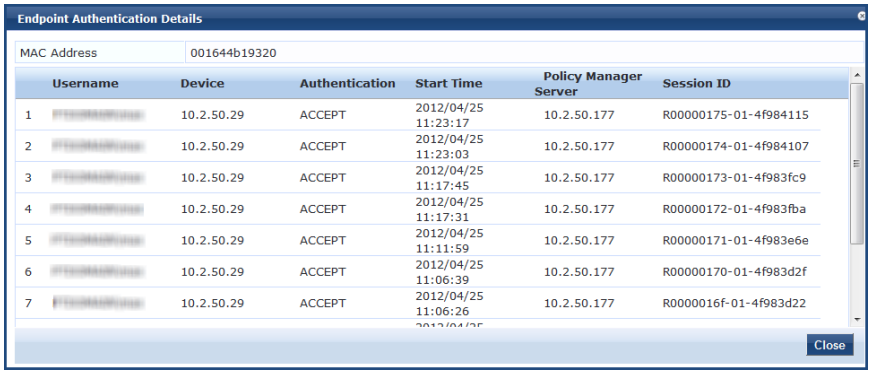
Policy Manager automatically lists all endpoints (that have authenticated) in the **Endpoints** page (**Configuration > Identity > Endpoints**):

Figure 110 *Endpoints Listing*



- *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 111 *Endpoint Authentication Details*



To manually add an endpoint, click **Add Endpoint** to display the **Add Endpoint** popup.

Figure 112 *Add Endpoint*

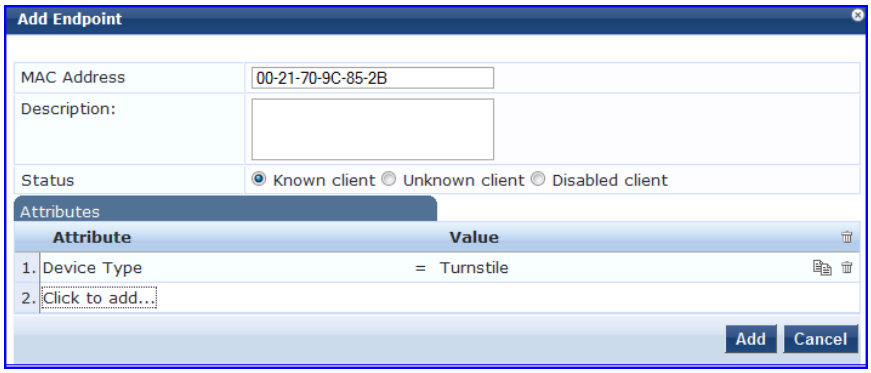


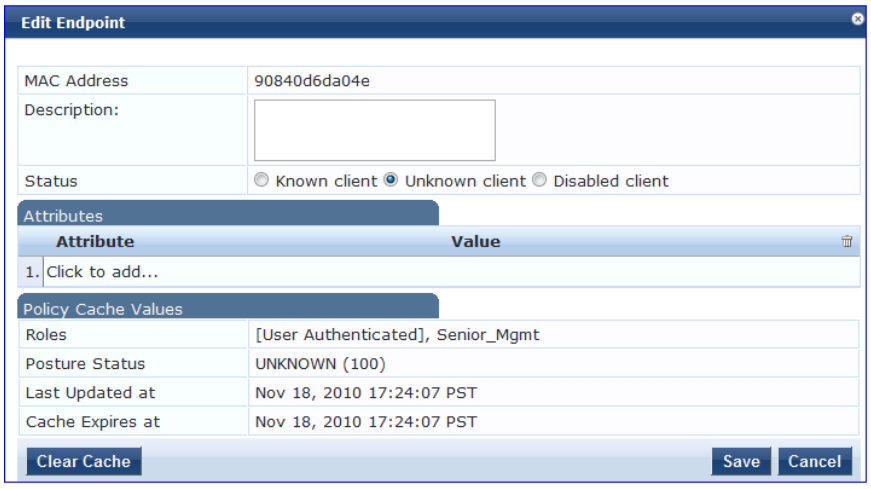
Table 73: *Add Endpoint*

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 Attribute dropdown 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 113 *Endpoint Popup*



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.

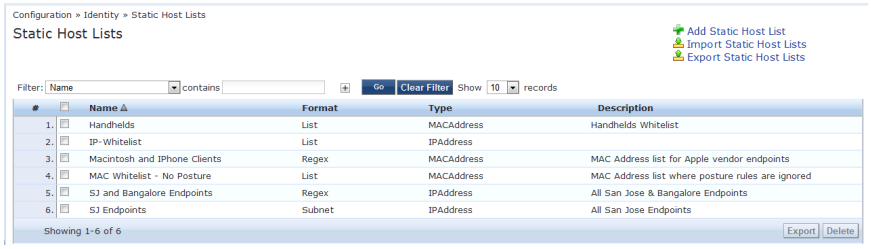
Adding and Modifying Static Host Lists

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.

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 114 *Static Host Lists (Listing Page)*



To add a Static Host List, click the **Add Static Host List** link. This opens the **Add Static Host List** popup.

Figure 115 *Add Static Host List*

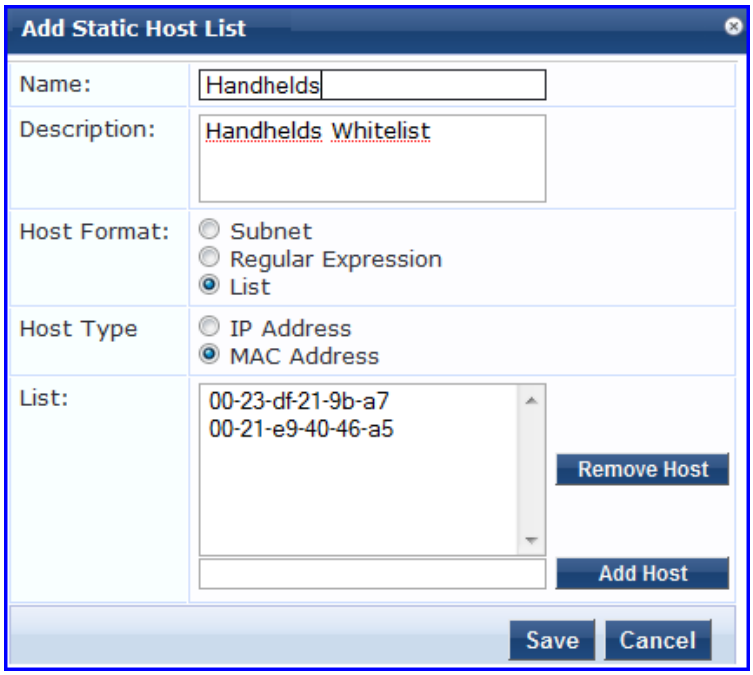


Table 74: *Add Static Host List*

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

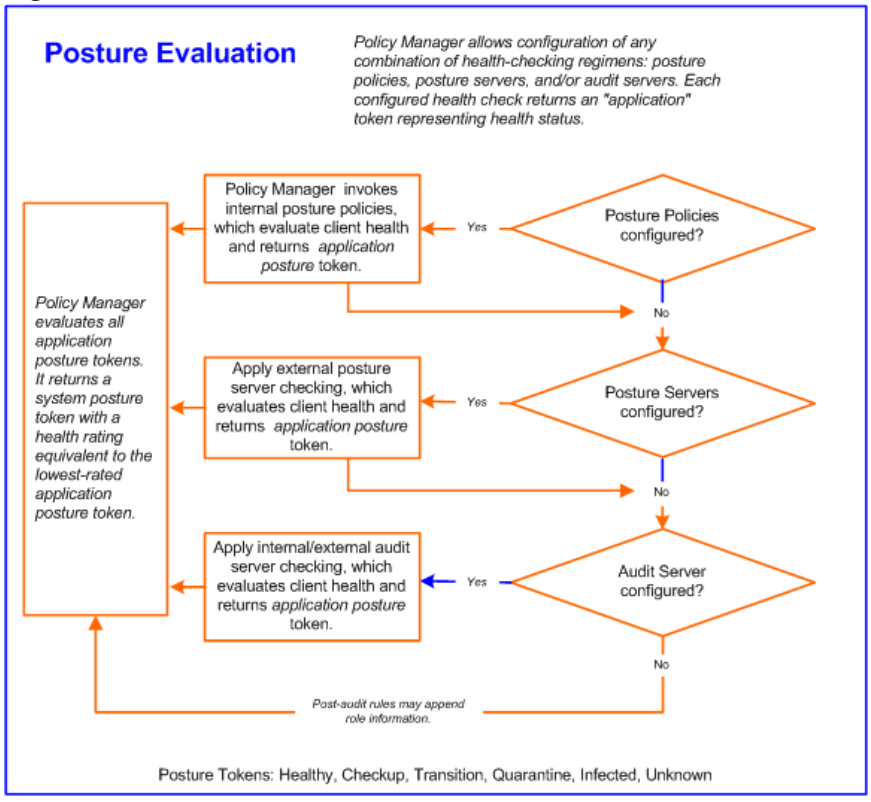
Policy Manager provides several *posture* methods for health evaluation of clients requesting access. These methods all return *Posture Tokens* (E.g., Healthy, Quarantine) for use by Policy Manager for input into *Enforcement Policy*. One or more of these posture methods may be associated with a *Service*.

Posture Architecture and Flow

Policy Manager supports three different 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 (i.e., 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: NMAP audit server, primarily to derive roles from post-audit rules; NESSUS audit server, primarily used for vulnerability scans (and, optionally, post-audit rules).

Figure 116 *Posture Evaluation Process*



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

- Operating system version/type

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

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

- **Healthy.** Client is compliant: there are no restrictions on network access.
- **Checkup.** Client is compliant; however, there is an update available. This can be used to proactively remediate to healthy state.
- **Transient.** Client evaluation is in progress; typically associated with auditing a client. The network access granted is interim.
- **Quarantine.** Client is out of compliance; restrict network access, so the client only has access to the remediation servers.
- **Infected.** Client is infected and is a threat to other systems in the network; network access should be denied or severely restricted.
- **Unknown.** The posture token of the client is unknown.

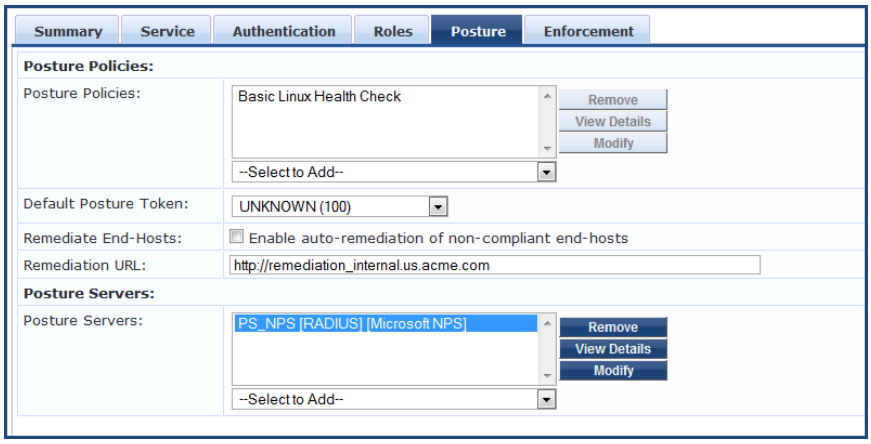
Upon completion of all configured posture checks, Policy Manager evaluates all *application tokens* and calculates a *system token,* equivalent to the most restrictive rating for all returned application tokens. The *system token* provides the health posture component for input to the Enforcement Policy.

A Service can also be configured without any Posture policy.

Configuring Posture

The following image displays how to configure Posture at the Service level. Note that the Posture Compliance check box must be selected on the Service tab in order for Posture to be enabled.

Figure 117 *Posture Features at the Service Level*



You can configure the following features of posture:

Table 75: *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 and Modifying Posture Policies " on page 152. • To edit the selected posture policy, click **Modify** and refer to "Adding and Modifying Posture Policies " on page 152.
Default Posture Token	The default posture token is UNKNOWN (100)
Remediation End-Hosts	Select this check box to enable auto-remediation action on non-compliant endpoints.
Remediation URL	This URL defines where to send additional remediation information to endpoints.
Sequence of Posture Servers	Select a Posture Server, then select **Move Up**, **Move Down**, **Remove**, or **View Details**. • To add a previously configured Posture Server, select from the **Select** drop-down list, then click **Add.** • To configure a new Posture Server, click **Add New Posture Server** (link) and refer to "Adding and Modifying Posture Servers " on page 177. • To edit the selected posture server, click **Modify** and refer to "Adding and Modifying Posture Servers " on page 177.
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 and Modifying Posture Policies

Policy Manager supports pre-configured posture plugins, against which administrators can configure rules that test for specific attributes of client health and correlate the results to posture tokens:

- *If you have NAP Agent (USHA) running on a NAP-compatible client (Windows 8, Windows 7, Windows Vista, Windows XP SP3, Windows Server 2008), use:*

  ClearPass Windows Universal System Health Validator. Configurable checking for present/absent Registry Keys, Services and processes, and product-/version-/update- specific checking for Antivirus, Antispyware, and Firewall applications. Checks for peer-to-peer applications or networks, patch management applications, hotfixes, USB devices, virtual machines, and network devices.

- *If you have ClearPass Linux NAP Agent running on a Linux client (CentOS, Fedora, Red Hat Enterprise Linux, SUSE Linux Enterprise Desktop), use:*

  ClearPass Linux Universal System Health Validator. Configurable checking for present/absent Services, and product-/version-/update- specific checking for Antivirus application, and Firewall configuration.

- *If you have a Microsoft NAP Agent running on the client, use:*
  - **Windows System Health Validator.** Configurable checking for required operating system versions and service packs.

- **Windows Security Health Validator.** Configurable checking for Antivirus/Antispyware/Firewall applications, as well as automatic updates and security updates.

- *If you have ClearPass OnGuard Agent (dissolvable or persistent) running on the client (Windows 8, Windows 7, Windows XP SP3, Windows Vista, Windows Server 2008, Windows Server 2003, SUSE Linux, Redhat Enterprise Linux, Fedora Linux, CentOS Linux, MAC OS X), use:*
  - **ClearPass Windows Universal System Health Validator.** Configurable checking for present/absent Registry Keys and Services, and product-/version-/update- specific checking for Antivirus, Antispyware, and Firewall applications. Checks for peer-to-peer applications or networks, patch management applications, hotfixes, USB devices, virtual machines, and network devices.
  - **Windows System Health Validator.** Configurable checking for required operating system versions and service packs.
  - **ClearPass Linux Universal System Health Validator.** Configurable checking for present/absent services.
  - **ClearPass Mac OS X Universal System Health Validator.** Configurable checking for product-/version-/update-specific checking for Antivirus/Antispyware application, and Firewall configuration.

Note that ClearPass OnGuard Agent - both persistent and dissolvable forms - can be used in the following scenarios:

- An environment that does not support 802.1X based authentication (legacy Windows Operating Systems, or legacy devices in the network)
- An OS that supports 802.1X natively, but does not have a built-in health agent. For example, MAC OS X.

Refer to "Configuring Posture Policy Plugins " on page 153 for additional information.

Configuring Posture Policy Plugins

From the **Services** page (**Configuration > Service**) or using the Add Posture Policy button (**Configuration > Posture > Posture Policies**), you can configure posture for a new service (as part of the flow of the **Add Service** wizard), or modify an existing posture policy or server directly (**Configuration > Posture > Posture Policies**, then click on its name in the **Posture Policies** listing page).

When you click **Add Posture Policy** from any of these locations, Policy Manager displays the **Add Posture Policy** page, which contains three configurable tabs:

- The **Policy** tab labels the policy and defines operating system and the type of deployed agent.

Figure 118 *Add Posture Policy (Policy Tab)*

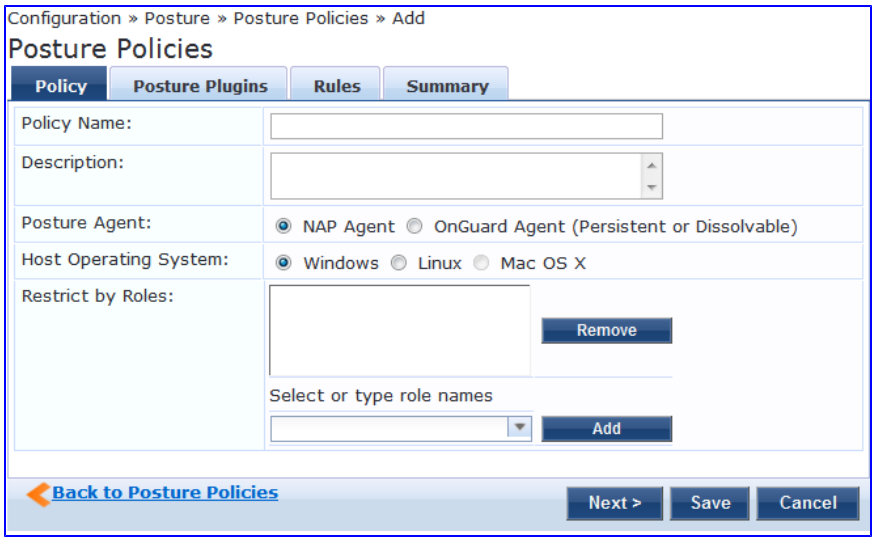


Table 76: *Add Posture Policy*

Parameter	Description
Policy Name/Description	Freeform label and description.
Posture Agent	• **NAP Agent** - Use this to configure posture policies for host operating systems with an embedded NAP-compliant agent (Microsoft Windows NAP Agent or ClearPass Linux NAP Agent). Currently, the following OSes are supported: Windows 8, Windows 7, Windows Vista, Windows XP SP3, Windows Server 2008, Windows Server 2008 R2, and Linux OSes supported by ClearPass Linux NAP Agent. • **OnGuard Agent** - Use this to configure posture policies for guest or web portal based use cases (via a dissolvable Java-applet based agent), or for use cases where ClearPass (persistent) OnGuard Agent is installed on the endpoint. Currently, the following OSes are supported by the OnGuard Agent: Windows 8, Windows 7, Windows Vista, Windows XP SP3, Windows Server 2008, Windows Server 2008 R2, Windows Server 2003, Mac OS X 10.5 or above, and Linux OSes supported by ClearPass Linux NAP Agent.
Host Operating System	Select **Linux**, **Windows** or **Mac OS X**. Note that Mac OS X is not available if the Posture Agent is NAP.
Restrict by Roles	Select role(s) that the Posture policy will apply to. Leave empty for the Posture policy to apply to all riles. • To add a role, select a role from the drop-down list, and then click **Add**. • To remove a role, select a role in the list, and then click **Remove**.

- The **Posture Plugins** tab provides a selector for posture policy plugins. Select a plugin (by enabling its check box), then click **Configure**.

Figure 119 *Add Posture Policy (Posture Plugins Tab) - Windows NAP Agent*

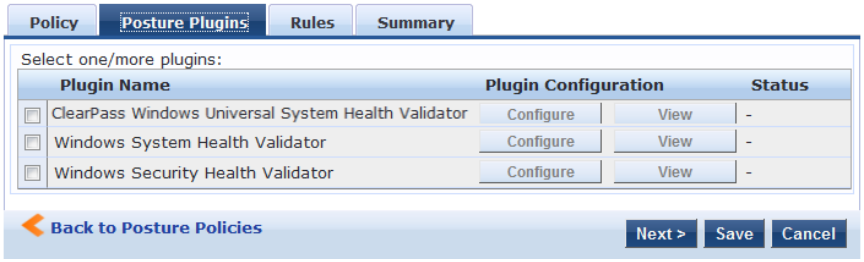


Figure 120 *Add Posture Policy (Posture Plugins Tab) - Linux NAP Agent*

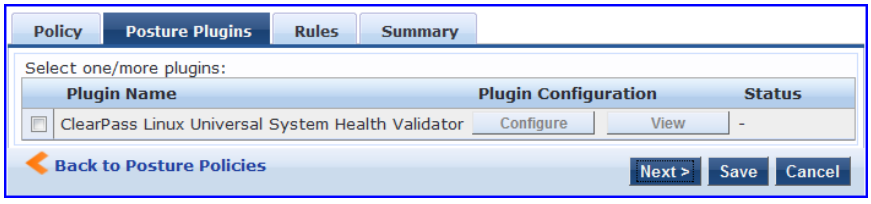


Figure 121 *Add Posture Policy (Posture Plugins Tab) - Windows OnGuard Agent*

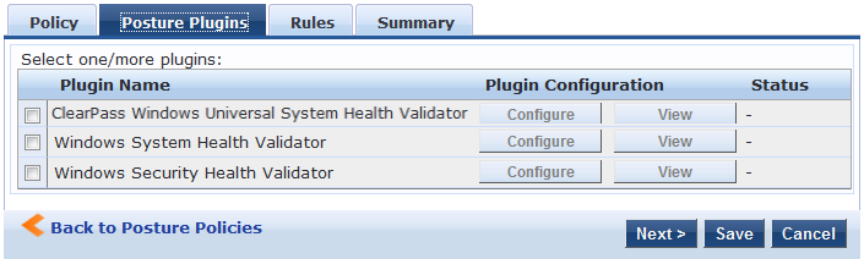


Figure 122 *Add Posture Policy (Posture Plugins Tab) - Linux OnGuard Agent*

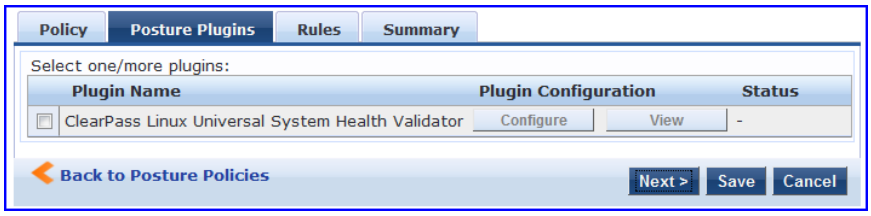
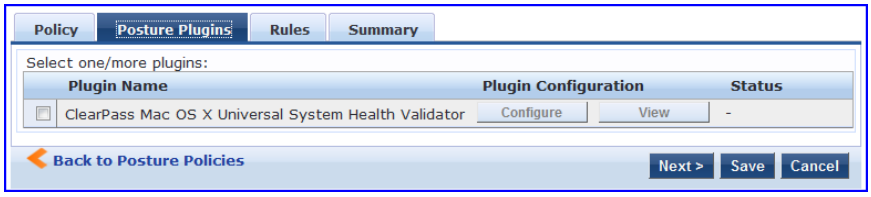


Figure 123 *Add Posture Policy (Posture Plugins Tab) - Mac OS X OnGuard Agent*



Refer to the following sections for plugin-specific configuration instructions:

- "ClearPass Windows Universal System Health Validator - NAP Agent " on page 156
- "Windows System Health Validator - NAP Agent " on page 176
- "Windows Security Health Validator - NAP Agent " on page 176
- "ClearPass Windows Universal System Health Validator - OnGuard Agent " on page 172
- "ClearPass Linux Universal System Health Validator - NAP Agent" on page 172
- "ClearPass Linux Universal System Health Validator - OnGuard Agent " on page 174
- "Windows System Health Validator - OnGuard Agent " on page 177
- "Windows Security Health Validator - OnGuard Agent " on page 176
- "ClearPass Mac OS X Universal System Health Validator - OnGuard Agent " on page 174

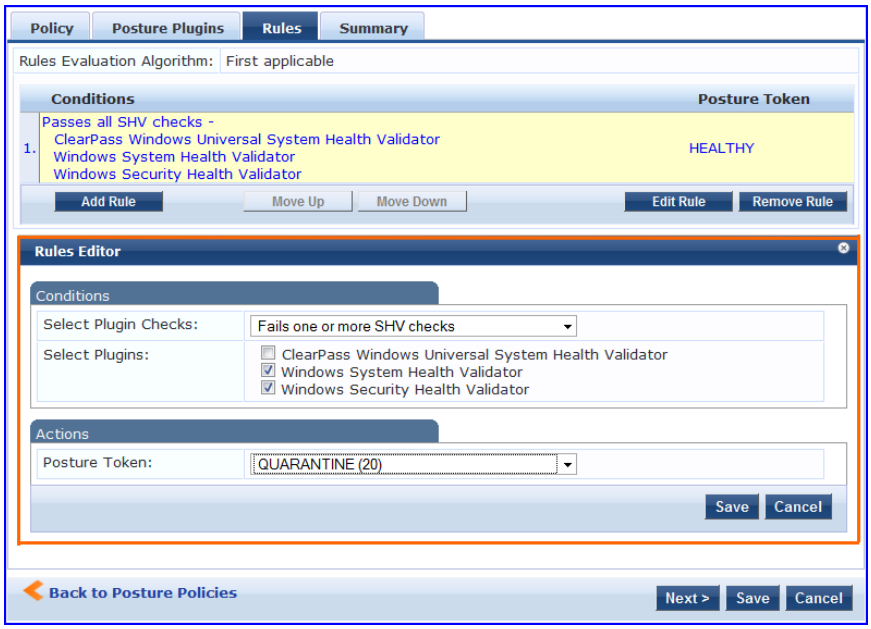
The **Rules** tab matches posture checking outcomes.

1. Select one of the following plugin checks.
   - Passes all System Health Validator (SHV) checks
   - Passes one or more SHV checks
   - Fails all SHV checks
   - Fails one or more SHV checks
2. Select the plugin.
3. Specify one of the following posture tokens:
   - **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.

- **Transition**. 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.

4. Click **Save** when you are finished.

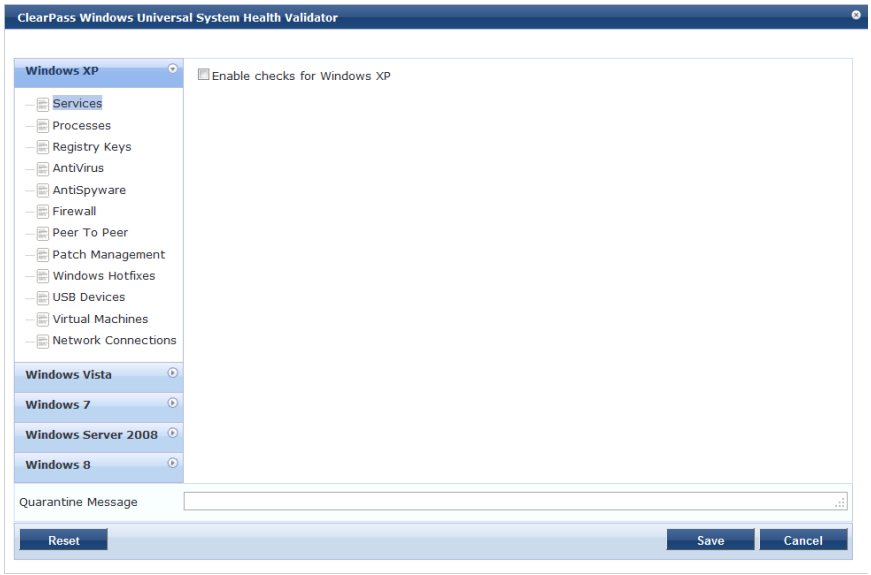
Figure 124 *Fig: Add Posture Policy (Rules Tab)*



ClearPass Windows Universal System Health Validator - NAP Agent

The **ClearPass Windows Universal System Health Validator** page popup appears in response to actions in the **Posture Plugins** tab of the **Posture** configuration.

Figure 125 *ClearPass Windows Universal System Health Validator - NAP Agent*



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 sections that follow.

Services

The **Services** page provides a set of widgets for specifying specific services to be explicitly running or stopped.

Figure 126 *Services Page*

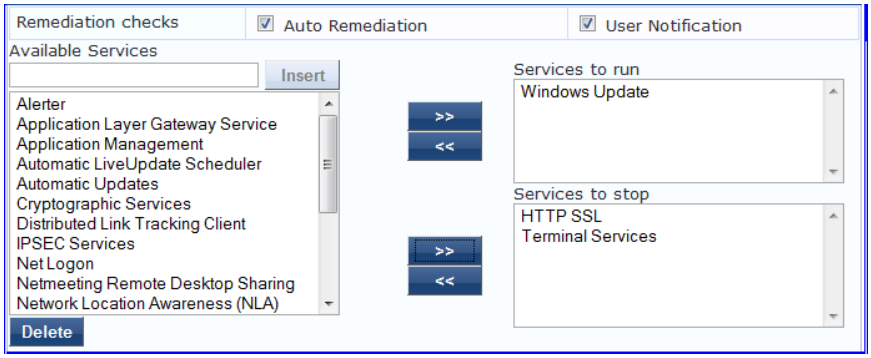


Table 77: *Services Page*

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 is different for the different 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 widgets for specifying specific processes to be explicitly present or absent on the system.

Figure 127 *Processes Page (Overview)*

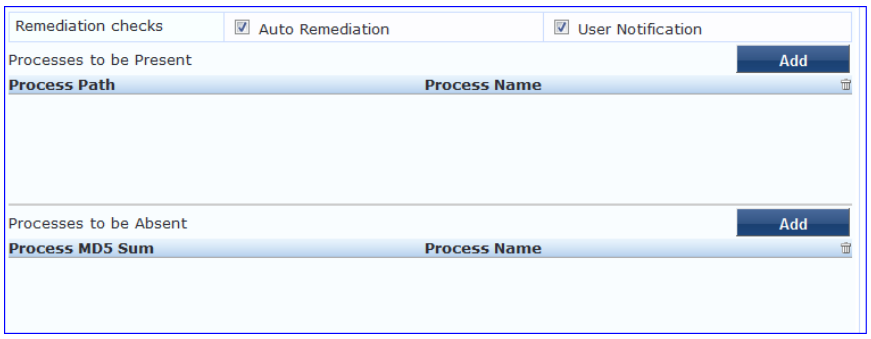


Table 78: *Process Page (Overview - Pre-Add)*

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 128 *Process to be Present Page (Detail)*

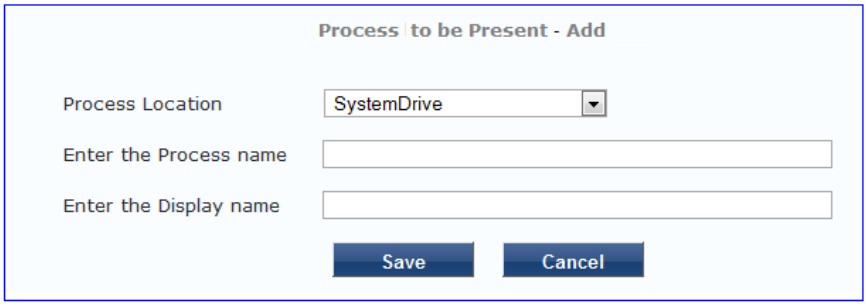


Table 79: *Process to be Present Page (Detail)*

Parameter	Description
Process Location	Choose from one of the pre-defined paths, or choose None. • SystemDrive - For example, C: • SystemRoot - For example, C:\Windows • ProgramFiles - For example, “C:\Program Files” • HOMEDRIVE - For example, C: • HOMEPATH - For example, \Users\JohnDoe • None - By selecting None, you can enter a custom path name in the Process Name field.
Enter the Process name	A pathname containing the process executable name. Some valid examples are listed below: • If SystemRoot is specified in the Process Location field, then entering notepad.exe in this field specifies that the following full pathname for the process should be checked: %SystemRoot%\notepad.exe. Typically, this expands to: C:\Windows\notepad.exe • If ProgramFiles is specified in the Process Location field, then entering “Mozilla Firefox\firefox.exe” in this field specifies that the following full pathname for the process should be checked: “%ProgramFiles%\Mozilla Firefox\firefox.exe”. Typically, this expands to: “C:\Program Files\Mozilla Firefox\firefox.exe” • If None is specified in the Process Location field, then entering “\temp\usurf.exe” in this field specifies that the following full pathname for the process should be checked: “c:\temp\foo.exe” Note that when the agent looks for running processes on the system, it looks for a process started from the specified location. For example, if the process to be running is specified to be C:\Windows\notepad.exe, the agent checks to see if there is a process running on the system that was started from the location C:\Windows. Even if the agent finds another process with the same name (notepad.exe) but started from a different location (C:\Temp), it will not match with what it is looking for. In this case, it will still start the process C:\Windows\notepad.exe.
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

When you save your Process details, the key information appears in the **Processes to be present** page list.

Processes to be Absent

Figure 129 *Process to be Absent Page (Detail)*

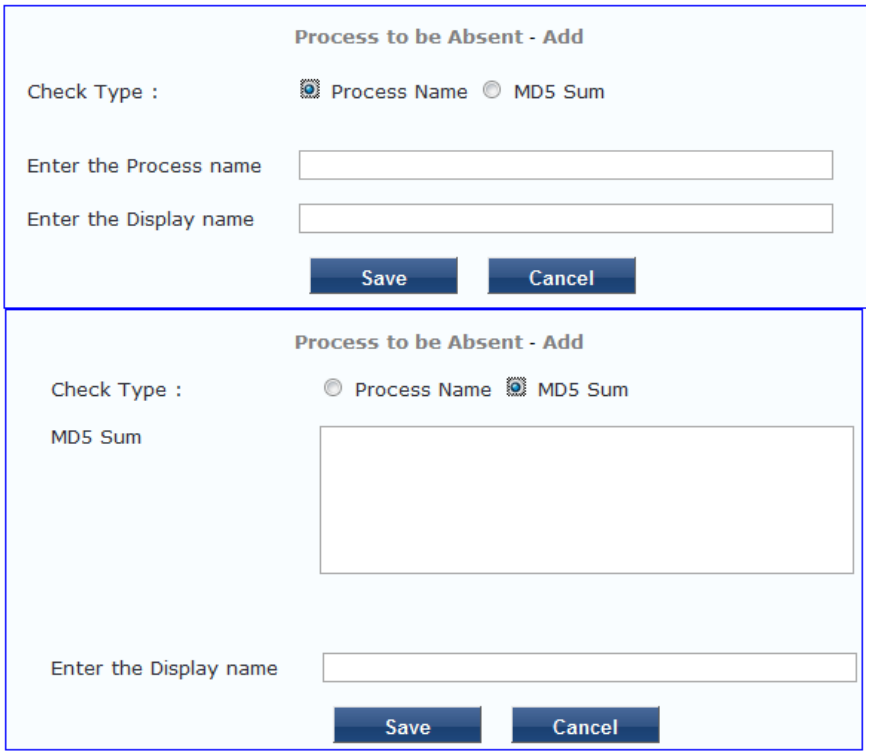
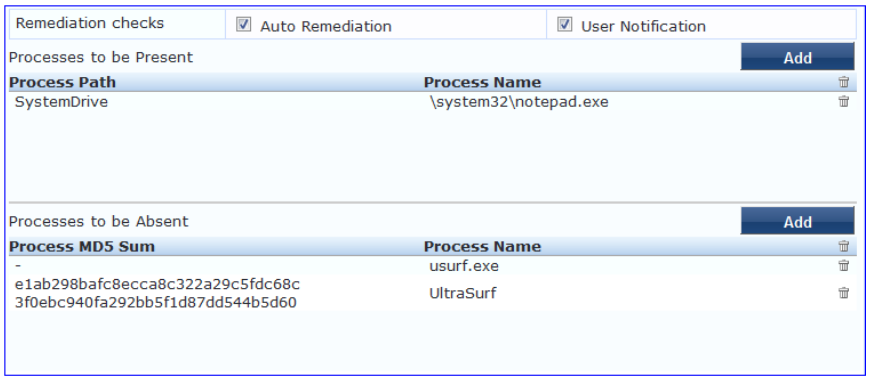


Table 80: *Process to be Absent Page (Detail)*

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 speicfied, 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 130 *Process Page (Overview - Post Add)*



Registry Keys

The **Registry Keys** page provides a set of widgets for specifying specific registry keys to be explicitly present or absent.

Figure 131 *Registry Keys Page (Overview)*

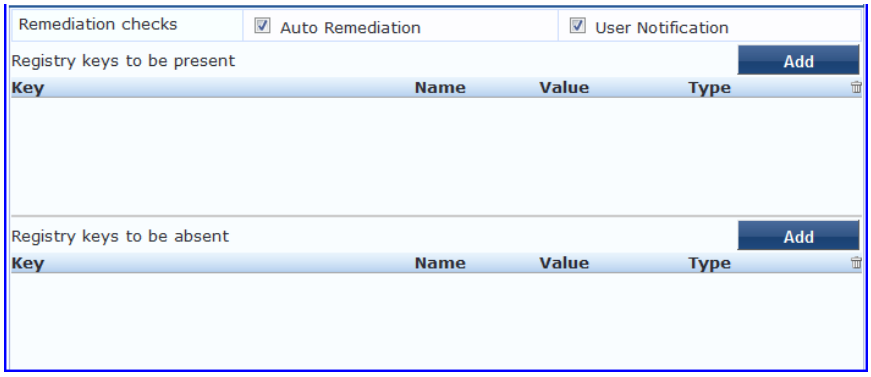


Table 81: *Registry Keys Page (Overview - Pre-Add)*

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.
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 132 *Registry Keys Page (Detail)*

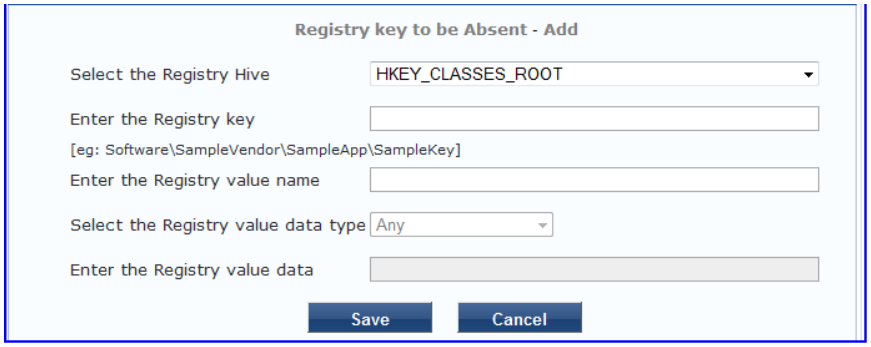
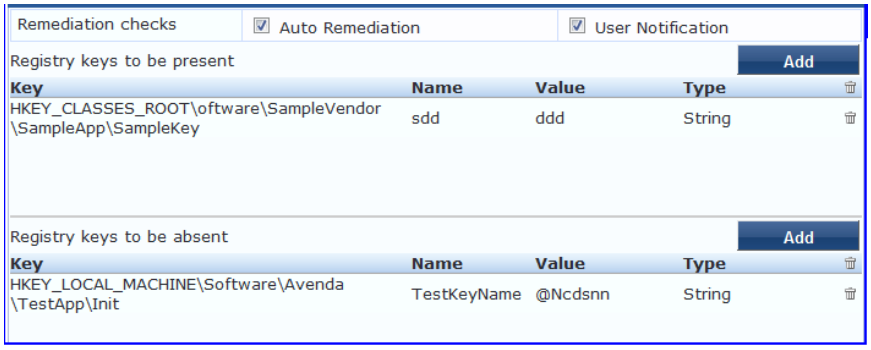


Table 82: *Registry Keys Page (Detail)*

Parameter	Description
Hive/Key/value (name, type, data)	Identifying information for a specific setting for a specific registry key.

When you save your Registry details, the key information appears in the **Registry** page list.

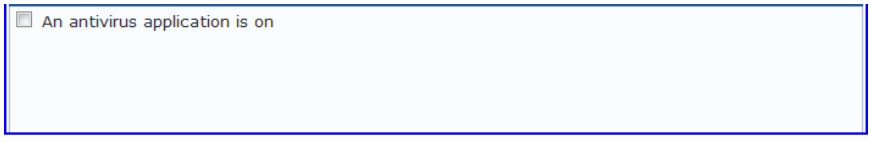
Figure 133 *Registry Keys Page (Overview - Post Add)*



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 **An Antivirus Application is On** to configure the Antivirus application information.

Figure 134 *Antivirus Page (Overview - Before)*

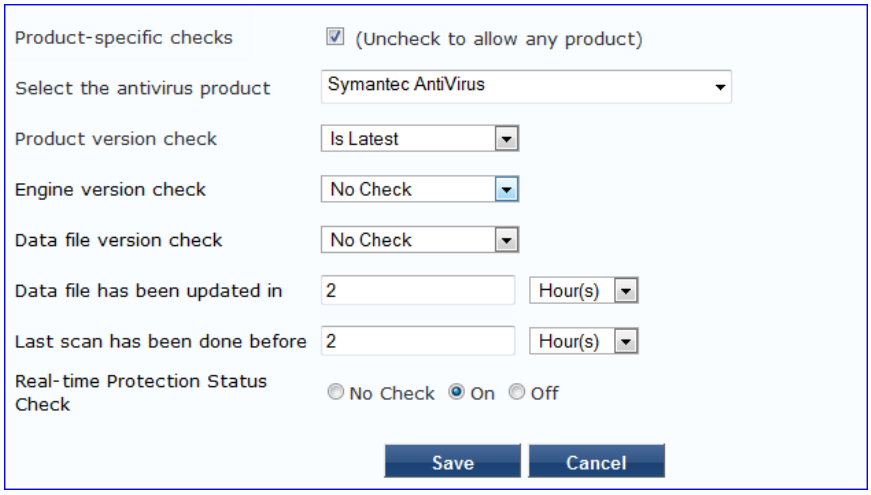


When enabled, the **Antivirus** detail page appears.

Figure 135 *Antivirus Page (Detail 1)*

Click **Add** to specify product, and version check information.

Figure 136 *Antivirus Page (Detail 2)*



After you save your Antivirus configuration, it appears in the **Antivirus** page list.

Figure 137 *Antivirus Page (Overview - After)*

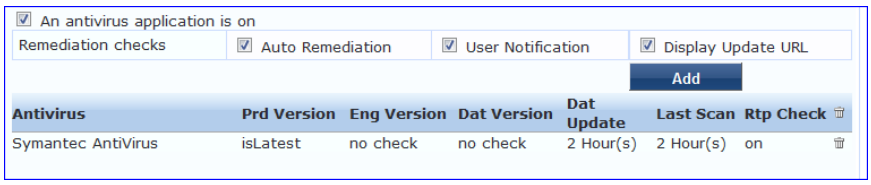


Table 83: *Antivirus Page*

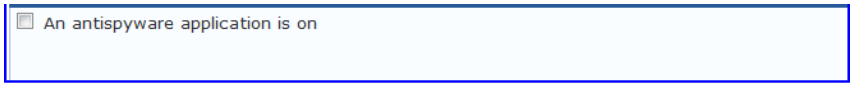
Interface	Parameter	Description
Antivirus Page	• An Antivirus Application is On • Auto Remediation • User Notification • Display Update URL	• Check the **Antivirus Application is On** check box to enable testing of health data for configured Antivirus application(s). • Check the **Auto Remediation** 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 • Trashcan icon	• To configure Antivirus application attributes for testing against health data, click **Add**. • To remove configured Antivirus application attributes from the list, click the **trashcan icon** in that row.

Interface	Parameter	Description
Antivirus Page (Detail 2)	Product/Version/Last 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

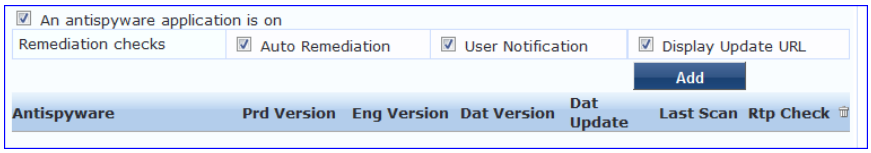
In the **AntiSpyware** page, an administrator can specify that an AntiSpyware application must be on and allows drill-down to specify information about the AntiSpyware application. Click **An Antipyware Application is On** to configure the AntiSpyware application information.

Figure 138 *AntiSpyware Page (Overview Before)*



When enabled, the **AntiSpyware** detail page appears.

Figure 139 *AntiSpyware Page (Detail 1)*



Click **Add** to specify product, and version check information.

Figure 140 *AntiSpyware Page (Detail 2)*

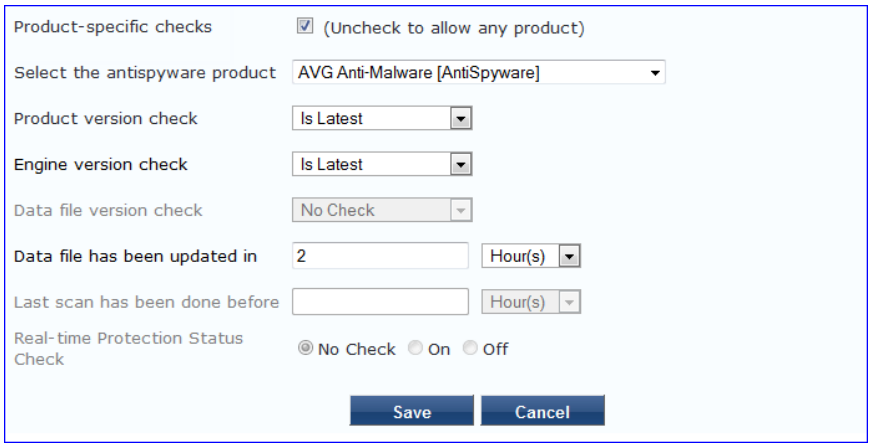


Figure 141 *AntiSpyware Page (Overview After)*

When you save your AntiSpyware configuration, it appears in the **AntiSpyware** page list.

The configuration elements are the same for antivirus and antispyware products. Refer to the previous AntiVirus configuration instructions

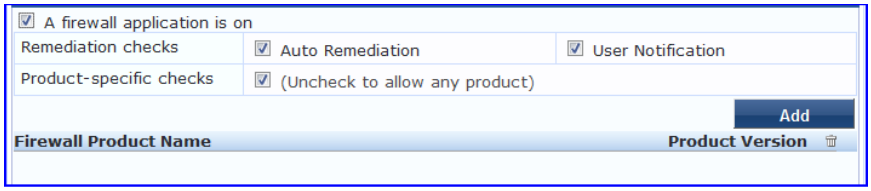
Firewall

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.

Figure 142 *Firewall Page (Overview Before)*

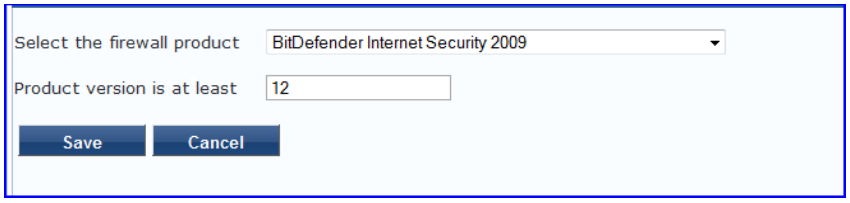
In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

Figure 143 *Firewall Page (Detail 1)*



When enabled, the **Firewall** detail page appears.

Figure 144 *Firewall Page (Detail 2)*



When you save your Firewall configuration, it appears in the **Firewall** page list.

Figure 145 *Firewall Page (Overview After)*

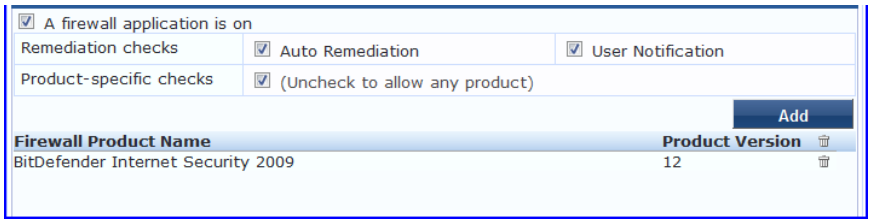


Table 84: *Firewall Page*

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 146 *Peer to Peer Page*

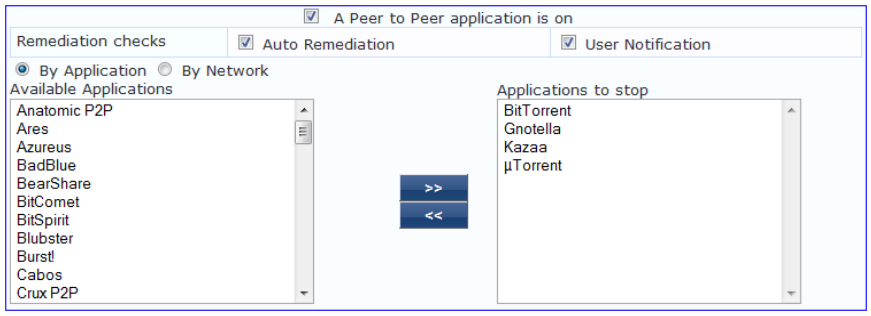


Table 85: *Peer to Peer Page*

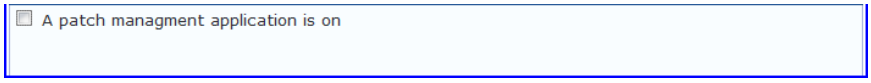
Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop peer to peer applications based on the entries in **Applications to stop** configuration).
User Notification	Enable to allow user notifications for peer to peer application/network check policy 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.

Parameter	Description
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

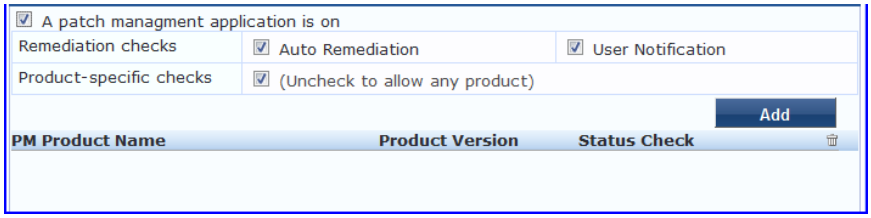
In the **Patch Management** page, you can specify that a patch management application must be on and allows drill-down to specify information about the patch management application. Click **An patch management application is On** to configure the patch management application information.

Figure 147 *Patch Management Page (Overview - Before)*



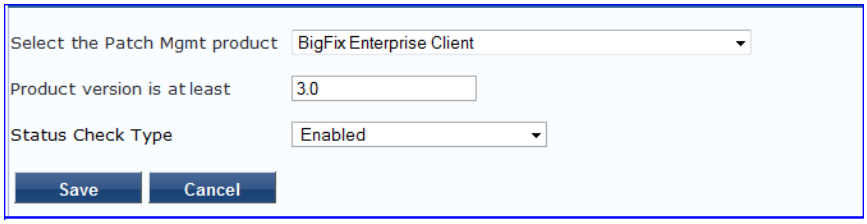
When enabled, the **Patch Management** detail page appears.

Figure 148 *Patch Management Page (Detail 1)*



Click **Add** to specify product, and version check information.

Figure 149 *Patch Management Page (Detail 2)*



When you save your patches configuration, it appears in the **Patch Management** page list.

Figure 150 *Patch Management Page (Overview - After)*

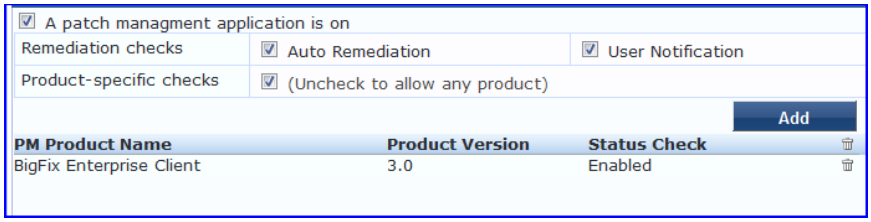


Table 86: *Patch Management Page*

Interface	Parameter	Description
Patch Management Page	• A patch management application is on • Auto Remediation • User Notification • Uncheck to allow any product	• Check the **Patches / Hot fixes Application is On** check box 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. • Uncheck the **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 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 Patch Mgmt product - Select a vendor from the list • Product version is at least - Enter version number • Status check type - No check, Enabled, Disabled

Windows Hotfixes

The **Windows Hotfixes** page provides a set of widgets for checking if specific Windows hotfixes are installed on the endpoint.

Figure 151 *Windows Hotfixes Page*

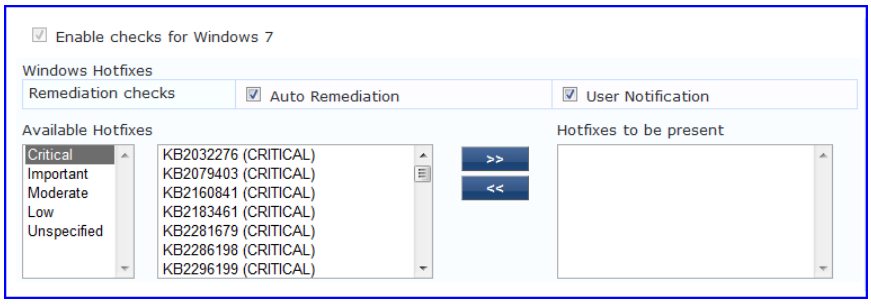


Table 87: *Windows Hotfixes*

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.

Parameter	Description
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 152 *USB Devices*

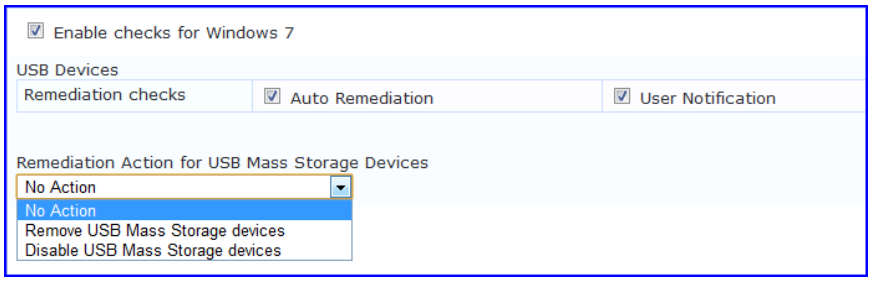


Table 88: *USB Devices*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for USB mass storage devices attached to the endpoint (Automatically stop or eject the drive).
User Notification	Enable to allow user notifications for USB devices policy violations.
Remediation Action for USB Mass Storage Devices	• No Action - Take no action; do not eject or disable the attached devices. • Remove USB Mass Storage Devices - Eject the attached devices. • Remove USB Mass Storage Devices - Stop the attached devices.

Virtual Machines

The **Virtual Machines** page provides configuration to Virtual Machines utilized by your network.

Figure 153 *Virtual Machines*

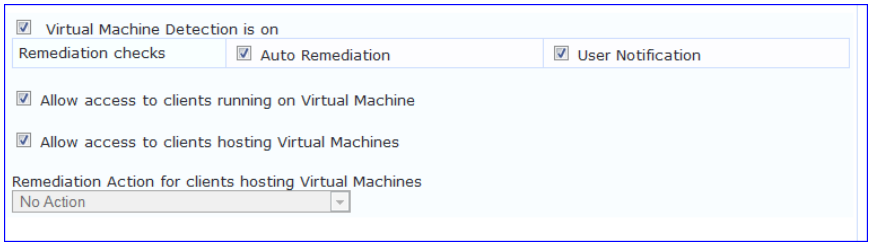


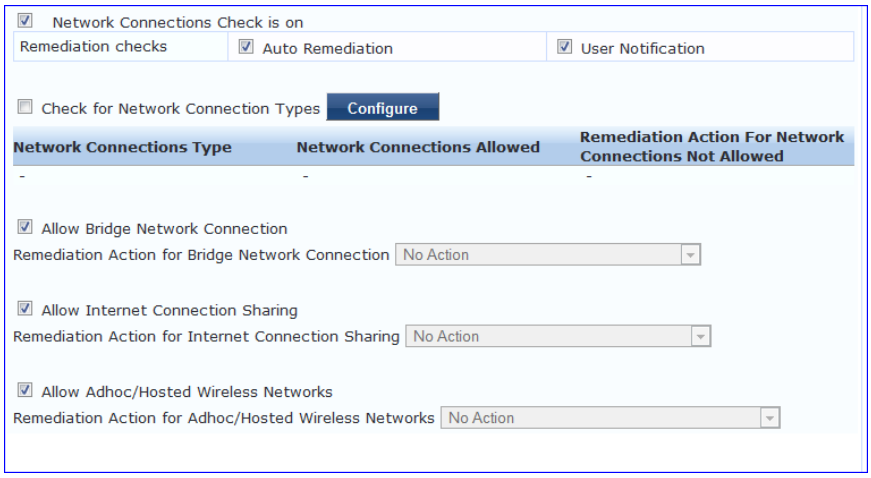
Table 89: *Virtual Machines*

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 154 *Network Connections*



Select the **Check for Network Connection Types** check box, and then click **Configure** to specify type of connection that you want to include.

Configure Network Connection Type

Figure 155 *Network Connection Type Configuration*

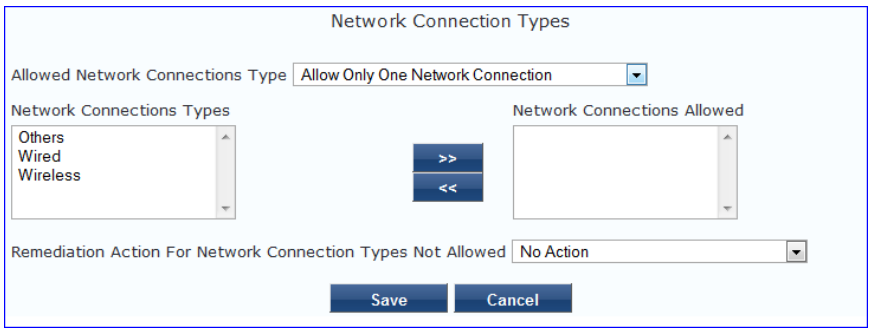


Table 90: *Network Connection Type Configuration Page*

Parameter	Description
Allow Network Connections Type	• Allow Only One Network Connection • Allow One Network Connection with VPN • Allow Multiple Network Connections
User Notification	Enable to allow user notifications for hotfixes check policy violations.
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** when you are finished. This returns you to the Network Connections Configuration page. The remaining fields on this page are described below.

Table 91: *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 a adhoc wireless networks exists or to disable all adhoc/hosted wireless networks.

ClearPass Windows Universal System Health Validator - OnGuard Agent

The **ClearPass Windows Universal System Health Validator - OnGuard Agent** page popup appears in response to actions in the **Posture Plugins** p of the **Posture** configuration. (When you select **Windows** and **OnGuard Agent** from the posture policy page)

The OnGuard Agent version of the ClearPass Windows Universal System Health Validator supports all the features supported by the NAP Agent validator. In addiiton, it also supports Windows Server 2003.

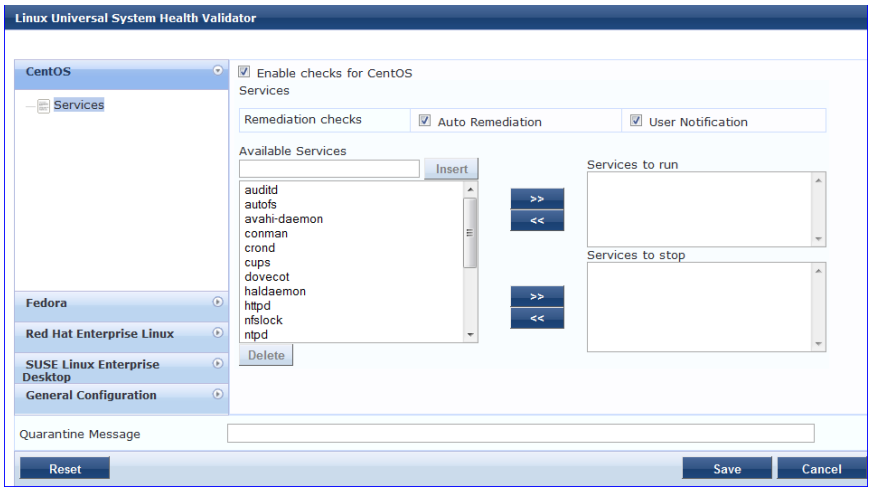
The configuration options and steps described under the ClearPass Windows Universal System Health Validator - NAP Agent section also apply to the OnGuard Agent.

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 156 *Fig: ClearPass Linux Universal system Health Validator - NAP Agent*



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 92: *Services View*

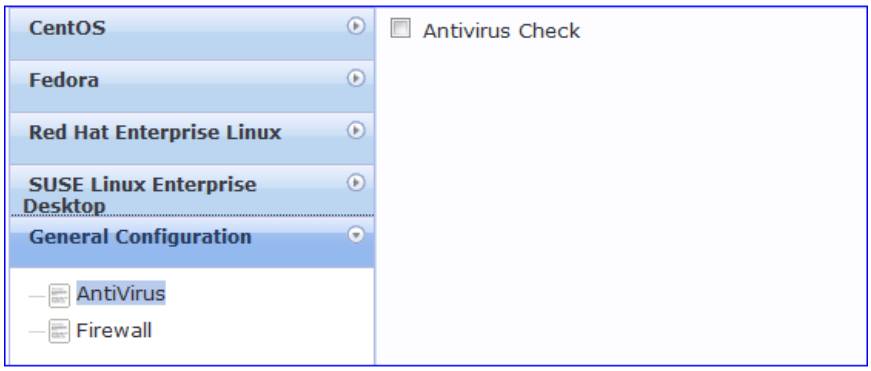
Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically start or stop services based on the entries in **Service to run** and **Service to stop** configuration).
User Notification	Enable to allow user notifications for service status policy violations.
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).

Parameter	Description
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:

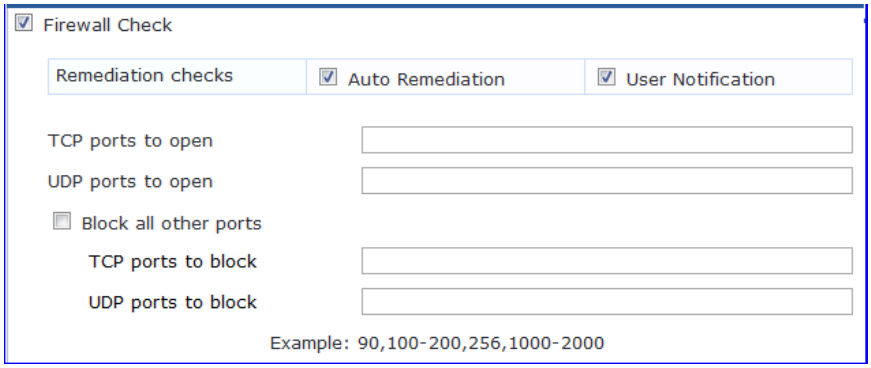
The configurations done in the General Configuration section apply to all operating systems whose checks have been turned on.

Figure 157 *General Configuration Section*



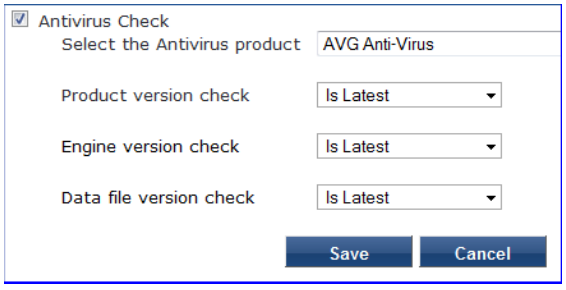
Select **Firewall Check** to display a view where you can specify Firewall parameters, specifically with respect to which ports may be open or blocked.

Figure 158 *Firewall view*



Select **Antivirus Check**, then click **Add** in the view that appears to specify Antivirus details.

Figure 159 *Antivirus Check view*



When you save your Antivirus configuration, it appears in the Antivirus page list.

Figure 160 *Antivirus Check*

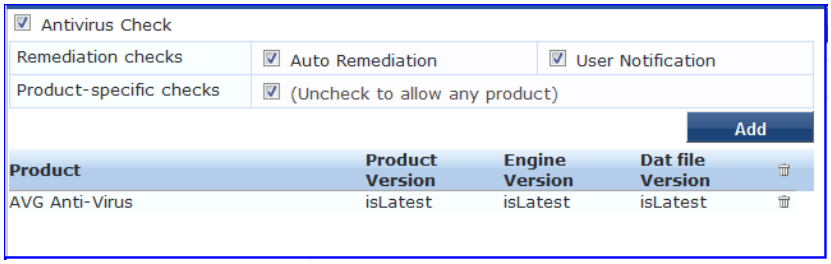


Table 93: *Antivirus Check*

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).

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).

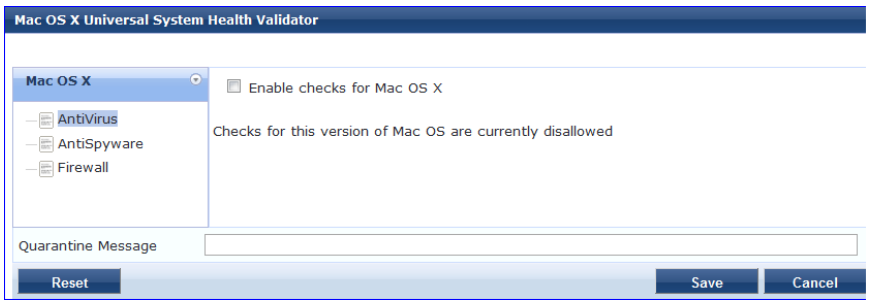
The dissolvable agent version of the ClearPass Linux Universal System Health Validator supports all the features supported by the "ClearPass Linux Universal System Health Validator - NAP Agent" on page 172 except for the following:

- 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 in response to actions in the **Posture Plugins** tab of the **Posture** configuration.

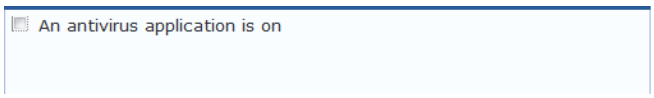
Figure 161 *ClearPass Mac OS X Universal System Health Validator - OnGuard Agent*



Select a check box to enable checks for Mac OS X. Enabling these check boxes displays a corresponding set of configuration pages:

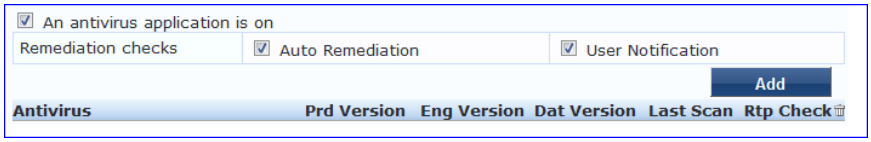
- In the Antivirus page, you can specify that an Antivirus application must be on and allows drill-down to specify information about the Antivirus application. Click on **An Antivirus Application is On** to configure the Antivirus application information.

Figure 162 *Antivirus Page (Overview - Before)*



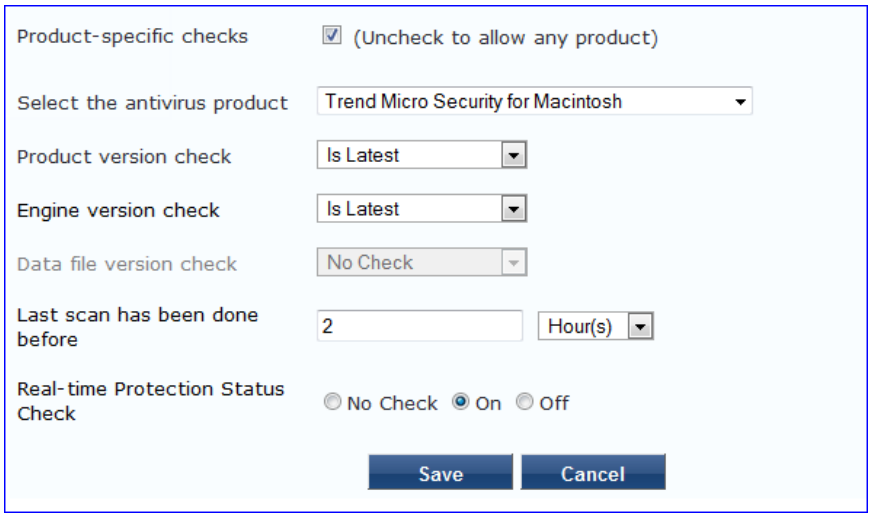
When enabled, the **Antivirus** detail page appears.

Figure 163 *Antivirus Page (Detail 1)*



Click **Add** to specify product and version check information.

Figure 164 *Antivirus Page (Detail 2)*



When you save your Antivirus configuration, it appears in the **Antivirus** page list. See "ClearPass Windows Universal System Health Validator - NAP Agent " on page 156 for antivirus page and field descriptions.

- 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.

  In the **Antispyware** page, click **An Antispyware Application is On** to configure the Antispyware application information. See Antivirus configuration details above for 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.

- 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.

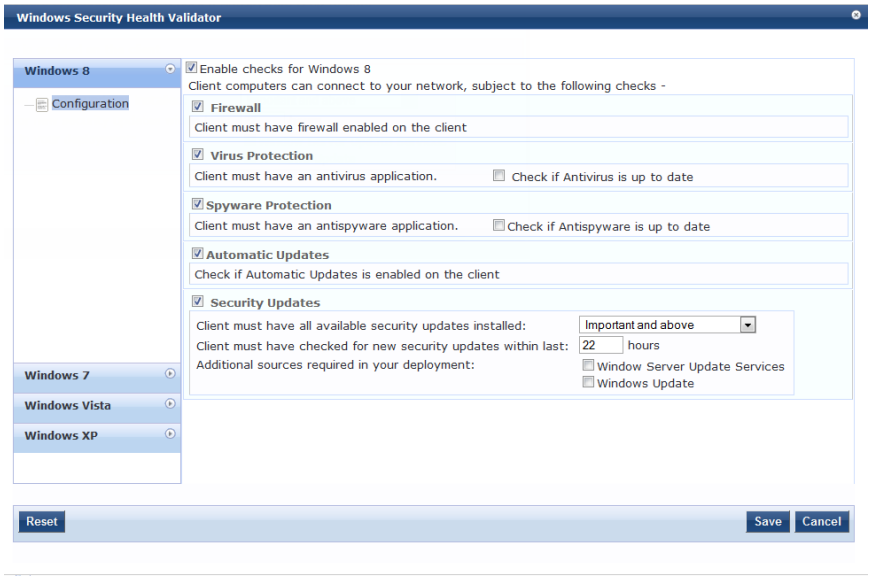
  In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

  When enabled, the **Firewall** detail page appears. See "ClearPass Windows Universal System Health Validator - NAP Agent " on page 156 for firewall page and field descriptions.

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.

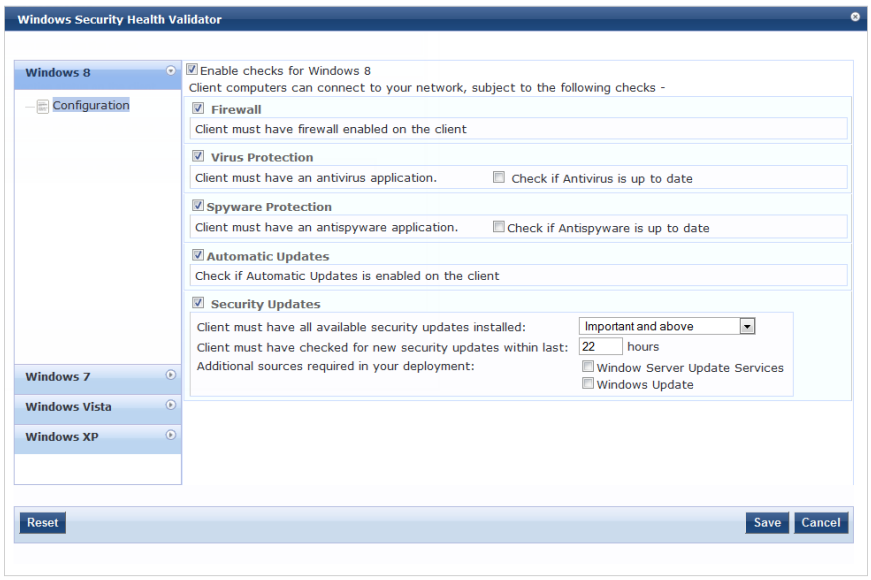
Figure 165 *Windows Security Health Validator*



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.

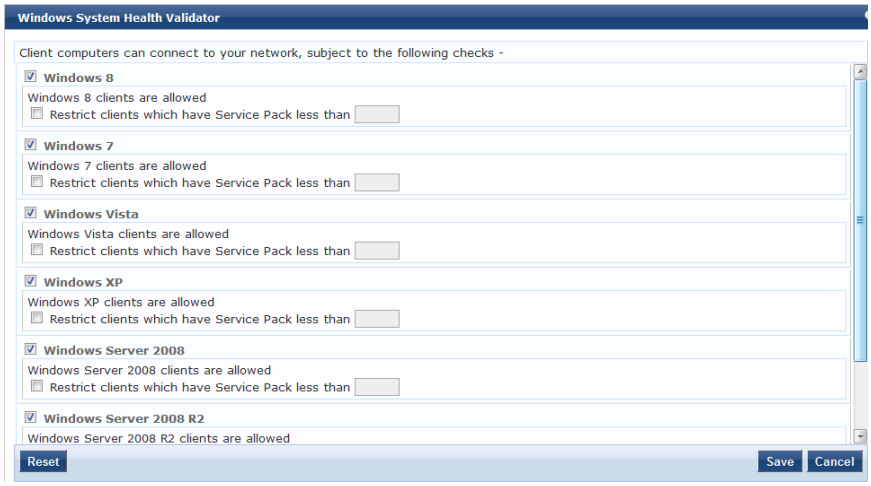
Figure 166 *Windows Security Health Validator*



Windows System Health Validator - NAP Agent

This validator checks for current Windows Service Packs. An administrator can use the check boxes to enable support of specific operating systems and to restrict access based on service pack level.

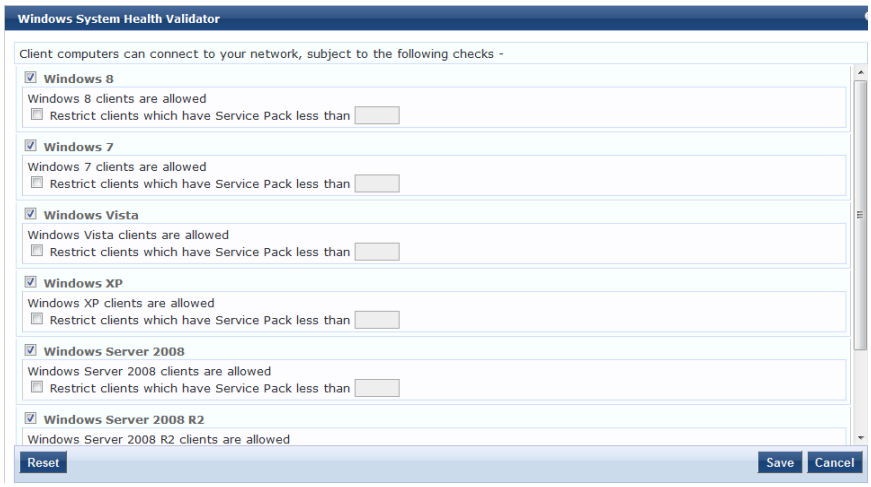
Figure 167 *Windows System Health Validator (Overview)*



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 168 *Windows System Health Validator - OnGuard Agent (Overview)*



Adding and Modifying Posture Servers

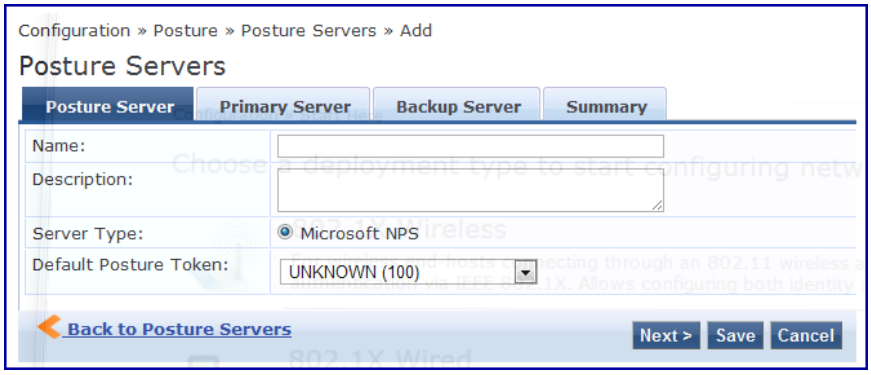
Policy Manager can forward all or part of the posture data received from the client to Posture Servers. The Posture Server evaluates the posture data and returns Application Posture Tokens.

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

Figure 169 *Posture Servers Listing Page*

When you click **Add Posture Server** from any of these locations, Policy Manager displays the **Posture Servers** configuration page.

Figure 170 *Add Posture Server Page*



Depending on the **Protocol** and **Requested Credentials**, different tabs and fields appear. Refer to "Microsoft NPS " on page 178.

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 94: *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 171 *Microsoft NPS Settings (Primary and Backup Server tabs)*

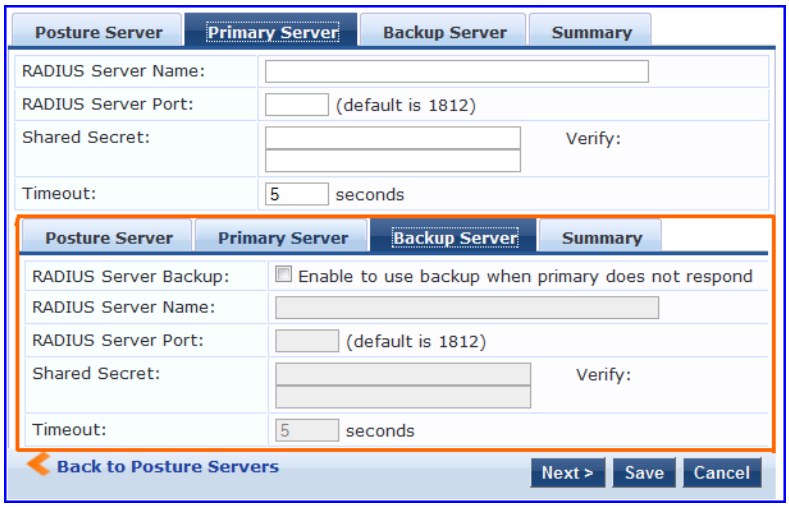


Table 95: *Microsoft NPS Settings (Primary and Backup Server tabs)*

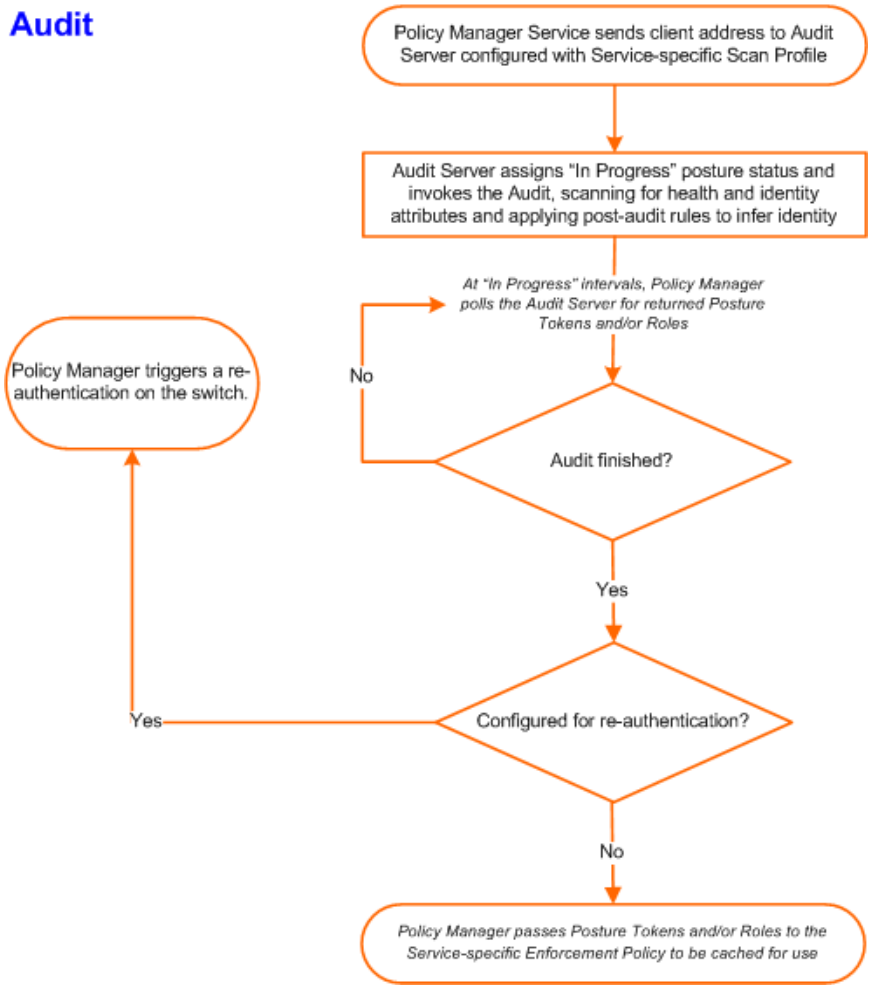
Parameter	Description
RADIUS Server Name/Port	Hostname or IP address and RADIUS server UDP port
Shared Secret	Enter the shared secret for RADIUS message exchange; the same secret has to be entered on the RADIUS server (Microsoft NPS) side
Timeout	How many seconds to wait before deeming the connection dead; if a backup is configured, Policy Manager will attempt to connect to the backup server after this timeout. For the backup server to be invoked on primary server failover, check the **Enable to use backup when primary does not respond** check box.

Audit Servers evaluate posture and/or role for unmanaged or unmanageable clients; that is, clients that lack an adequate posture agent or 802.1X supplicant (for example, printers, PDAs, or guest users may 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, which returns attributes for role mapping and posture evaluation.

Architecture and Flow

Audit servers are configured at a global level. Only one audit server may be associated with a Service. The flow-of-control of the audit process occurs as follows:

Figure 172 *Flow of Control of Policy Manager Auditing*



Refer to "Configuring Audit Servers" on page 180 for additional information.

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.

This section contains the following topics:

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.

Adding Auditing to a Policy Manager Service

1. Navigate to the **Audit** tab
   - To configure an audit server for a new service (as part of the flow of the Add Service wizard), navigate to **Configuration > Services**. Select the **Add Services** link. In the **Add Services** form, select the **Audit** tab.

You must select the **Audit End-hosts** check box on the **Services** tab in order for the **Audit** tab to display.

   - To modify an existing audit server, navigate to **Configuration > Posture > Audit Servers**, then select an audit server from the list.
2. Configure auditing

   Complete the fields in the **Audit** tab as follows:

Figure 173 *Audit Tab*

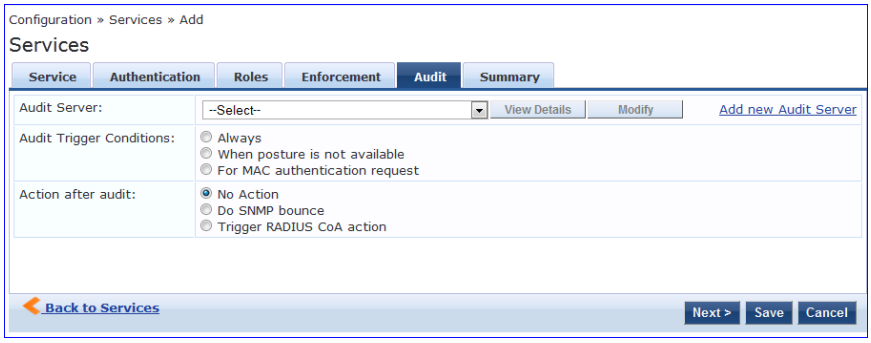


Table 96: *Audit Tab*

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 addresss 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 that Policy Manager does not issue 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.

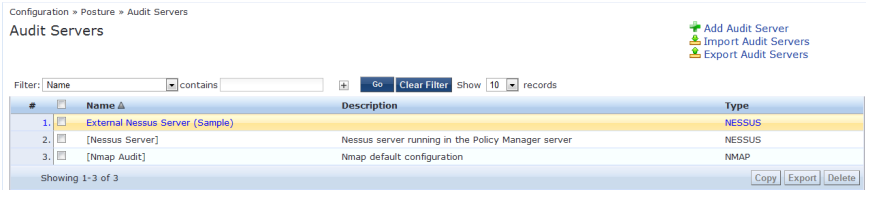
Modifying Built-In Audit Servers

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.

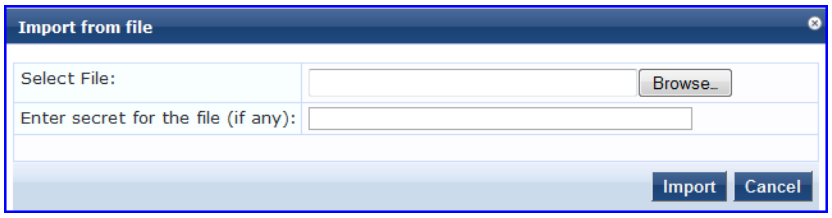
Figure 174 *Audit Servers Listing*



2. Modify the profile, plugins, and/or preferences.
   - In the **Audit** tab, you can modify the **In Progress Posture Status** and **Default Posture Status**.
   - If you selected a NESSUS Server, then the **Primary/Backup Server** tabs allow you to specify a scan profile. In addition, when you add a new scan profile, you can select plugins and preferences for the profile. Refer to "Nessus Scan Profiles" on page 186 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 175 *Upload Nessus Plugins Popup*



   - In the **Rules** tab, you can create post-audit rules for determining Role based on identity attributes discovered by the audit. Refer to Post-Audit Rules.

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 plugin 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 183
   - "NMAP Audit Server" on page 185

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 176 *NESSUS Audit Server (Audit Tab)*

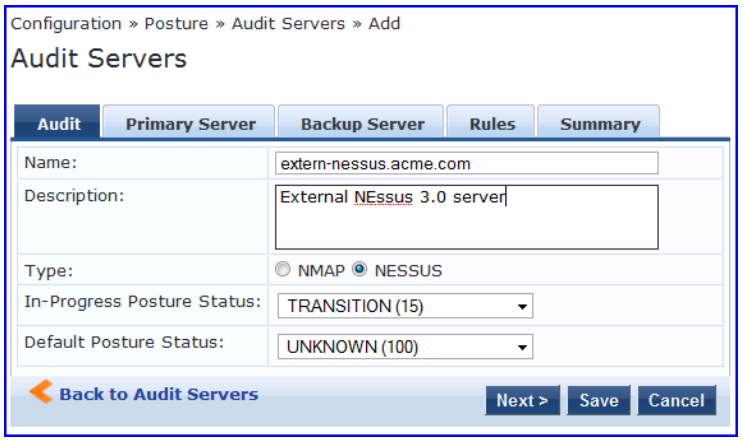


Table 97: *NESSUS Audit Server (Audit tab)*

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 177 *Fig: NESSUS Audit Server (Primary & Backup Tabs)*

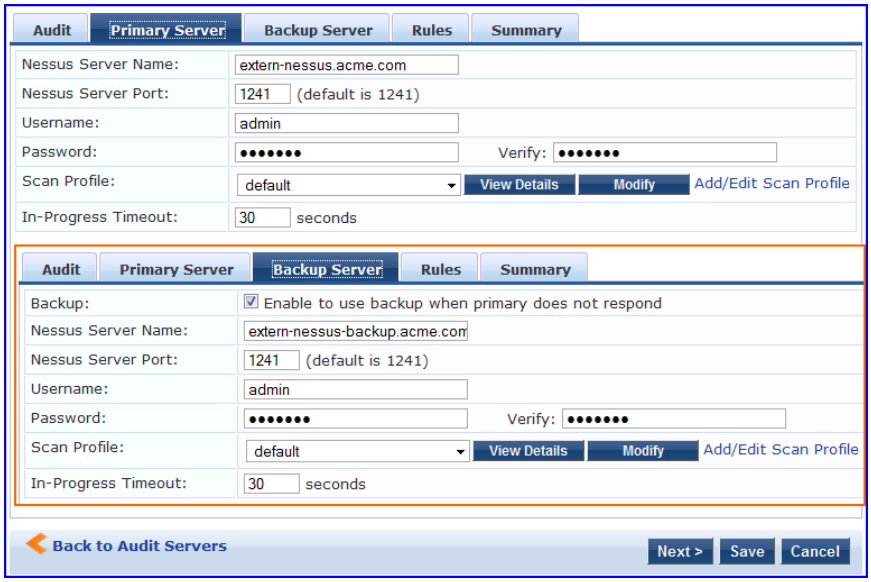


Table 98: *NESSUS Audit Server - Primary and Backup Server tabs*

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 186.

The **Rules** tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to "Post-Audit Rules" on page 189.

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 178 *Audit Tab (NMAP)*

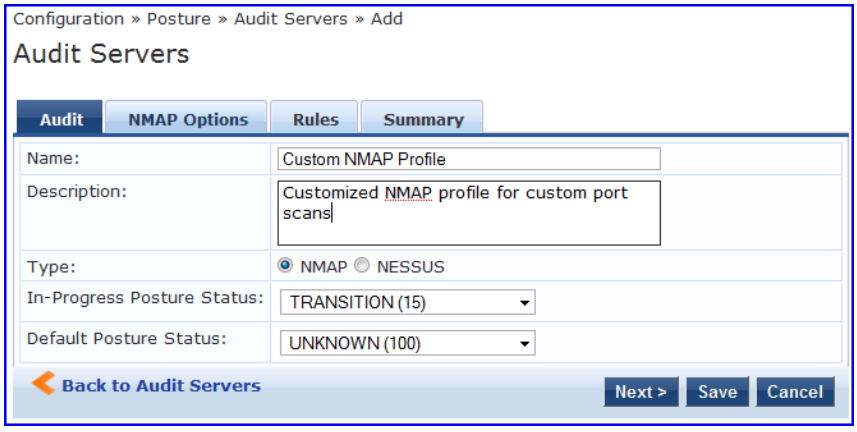


Table 99: *Audit Tab (NMAP)*

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 179 *Options Tab (NMAP)*

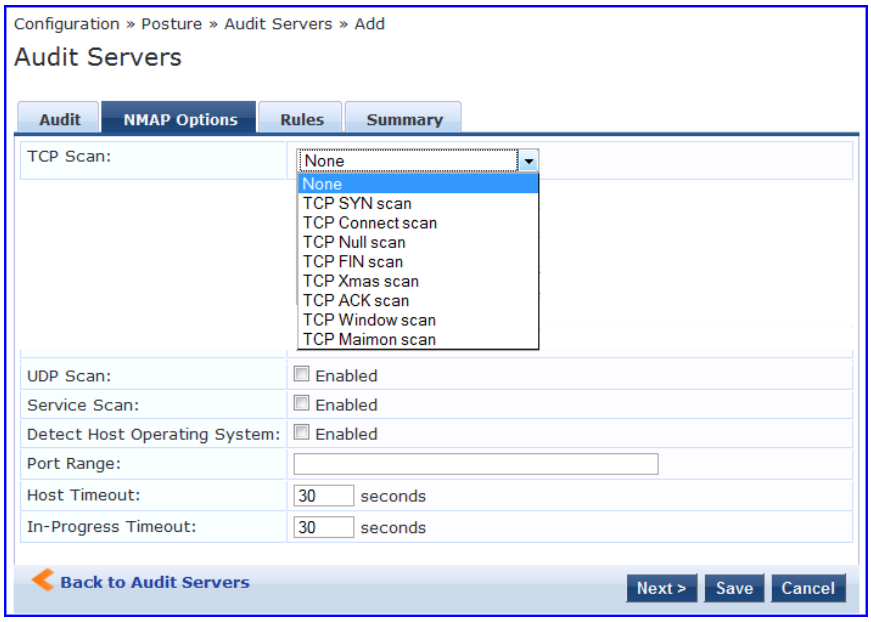


Table 100: *Options Tab (NMAP)*

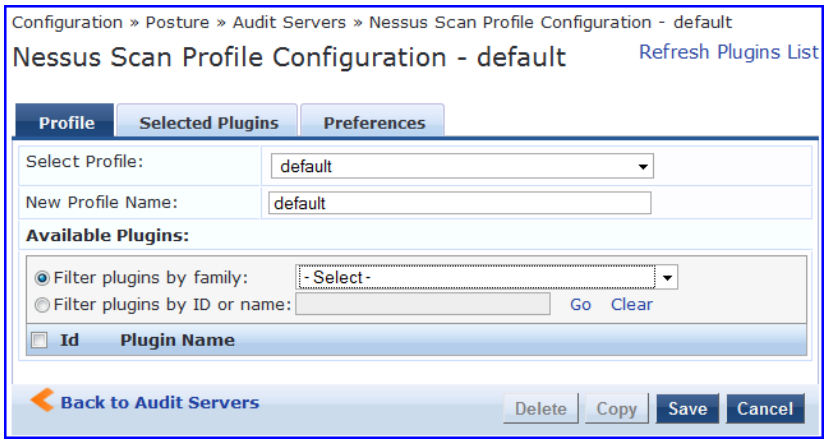
Parameter	Description
TCP Scan	To specify a TCP scan, select from the **TCP Scan** drop-down list. Refer to NMAP documentation for more information on these options. NMAP option --scanflags.
UDP Scan	To enable, check the **UDP Scan** check box. NMAP option -sU.
Service Scan	To enable, check the **Service 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 189.

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.

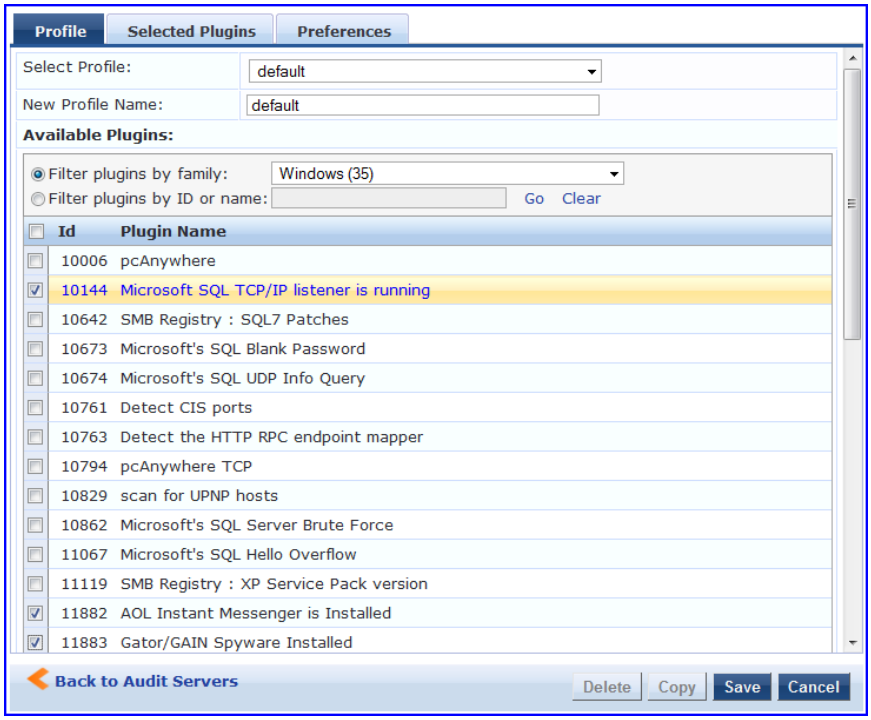
Figure 180 *Nessus Scan Profile Configuration Page*



You can refresh the plugins list (after uploading plugins into Policy Manager, or after refreshing the plugins on your external Nessus server) by clicking Refresh Plugins List. The Nessus Scan Profile Configuration page provides three views for scan profile configuration:

- The **Profile** tab identifies the profile and provides a mechanism for selection of plugins:
  - From the **Filter plugins by family** drop-down list, select a family to display all available member plugins in the list below. You may also enter the name of a plugin in **Filter plugins by ID** or name text box.
  - Select one or more plugins by enabling their corresponding check boxes (at left). Policy Manager will remember selections as you select other plugins from other plugin families.
  - When finished, click the **Selected Plugins** tab.

Figure 181 *Nessus Scan Profile Configuration (Profile Tab)*



- The **Selected Plugins** tab displays all selected plugins, plus any dependencies.

  To display a synopsis of any listed plugin, click on its row.

Figure 182 *Nessus Scan Profile Configuration (Profile Tab) - Plugin Synopsis*

Of special interest is the secton 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, INFO, NOTE. This tells Policy Manager the vulnerability level that is considered to be assigned QUARANTINE status.

Figure 183 *Nessus Scan Profile Configuration (Selected Plugins Tab)*

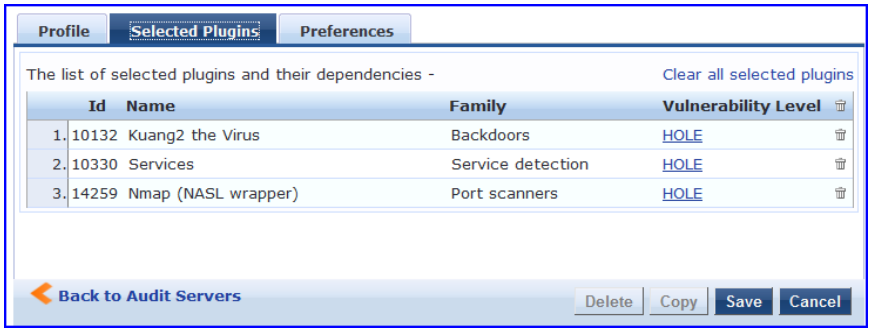


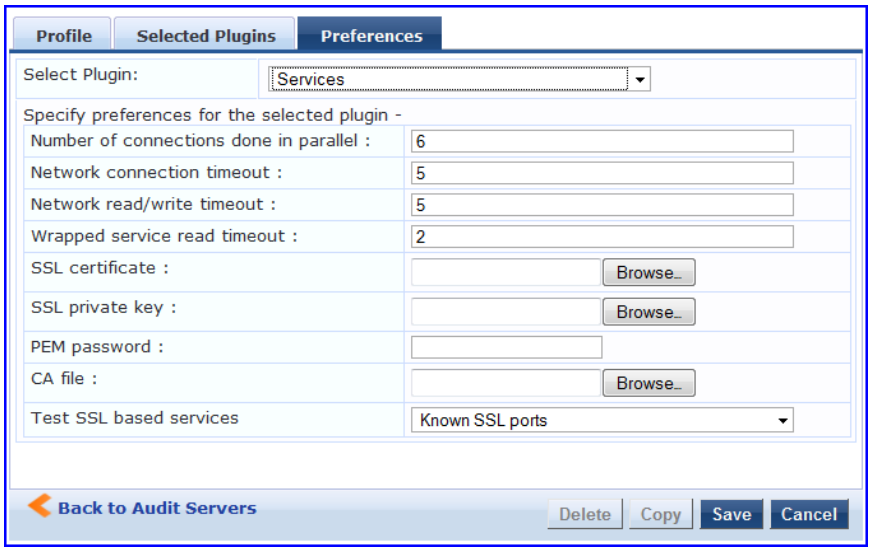
Figure 184 *Nessus Scan Profile Configuration (Selected Plugins Tab) - Vulnerability Level*

For each selected plugin, the Preferences tab contains a list of fields that require entries.

In many cases, these fields will be pre-populated. In other cases, you must provide information required for the operation of the plugin.

By way of example of how plugins use this information, consider a plugin that must access a particular service, in order to determine some aspect of the client's status; in such cases, login information might be among the preference fields.

Figure 185 *Nessus Scan Profile Configuration (Preferences Tab)*



Upon 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.

Post-Audit Rules

The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role.

Figure 186 *All Audit Server Configurations (Rules Tab)*

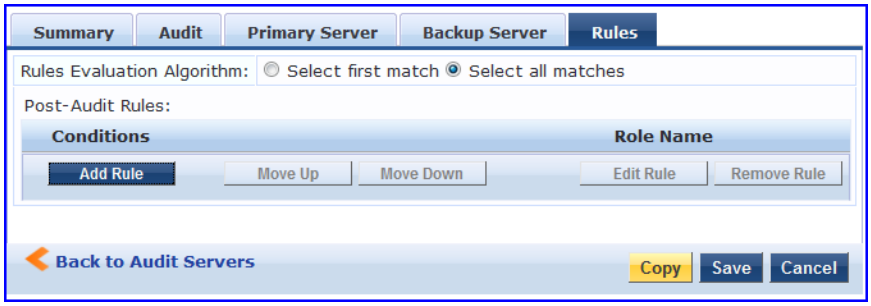


Table 101: *All Audit Server Configurations (Rules Tab)*

Parameter	Description
Rules Evaluation Algorithm	**Select first matched** rule and return the role or **Select all matched** rules and eturn 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 187 *All Audit Server Configurations (Rules Editor)*

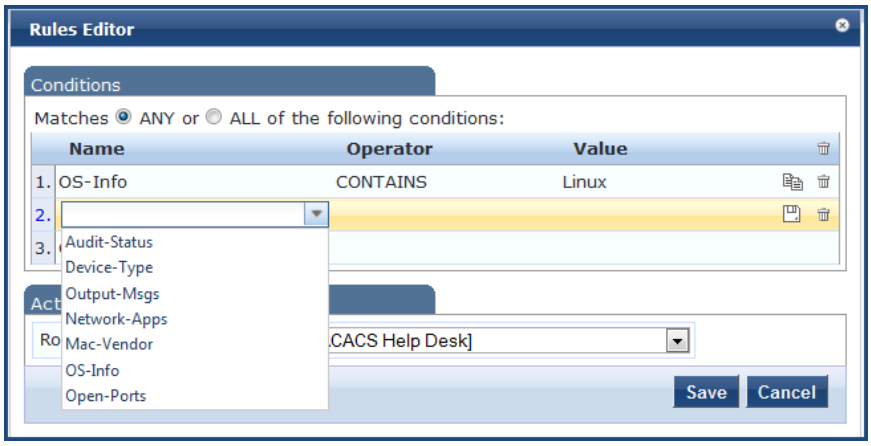


Table 102: *All Audit Server Configurations (Rules Editor)*

Parameter	Description
Conditions	The **Conditions** list includes five dictionaries: Audit-Status, Device-Type, Output-Msgs, Mac-Vendor, Network-Apps, Open-Ports, and OS-Info.. Refer to "Namespaces" on page 314.
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 *Enfocement 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.

Enforcement Architecture and Flow

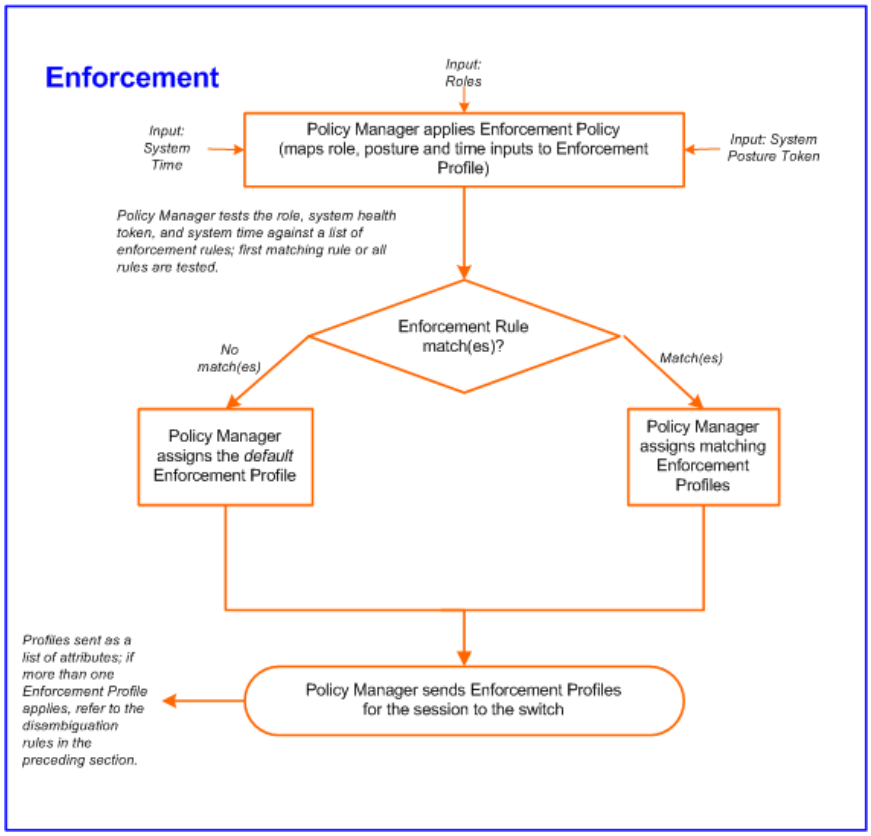
To evaluate a request, a Policy Manager Application assembles the request's client roles, client posture (system posture token), and system time. The calculation that matches these components to a pre-defined Enforcement Profile occurs inside of a black box called an Enforcement Policy.

Each Enforcement Policy contains a rule or set of rules for matching Conditions (role, posture and time) to Actions (Enforcement Profiles). For each request, it yields one or more matches, in the form of Enforcement Profiles, from which Policy Manager assembles access-control attributes for return to the originating NAD, subject to the following disambiguation rules:

- If an attribute occurs only once within an Enforcement Profile, transmit as is.
- If an attribute occurs multiple times within the same Enforcement Profile, transmit as a multi-valued attribute.
- If an attribute occurs in more than one Enforcement Profile, only transmit the value from the first Enforcement Profile in priority order.

Optionally, each Enforcement Profile can have an associated group of NADs; when this occurs, Enforcement Profiles are only sent if the request is received from one of the NADs in the group. For example, you can have the same rule for VPN, LAN and WLAN access, with enforcement profiles associated with device groups for each type of access. If a device group is not associated with the enforcement profile, attributes in that profile are sent regardless of where the request originated.

Figure 188 *Flow of Control of Policy Manager Enforcement*

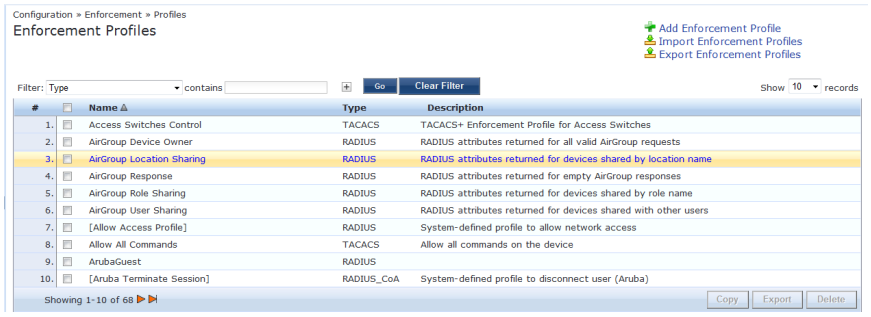


Configuring Enforcement Profiles

You configure Policy Manager Enforcement Profiles globally, but they must be referenced in an enforcement policy that is associated with a Service to be evaluate,

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).

Figure 189 *Enforcement Profiles Page*

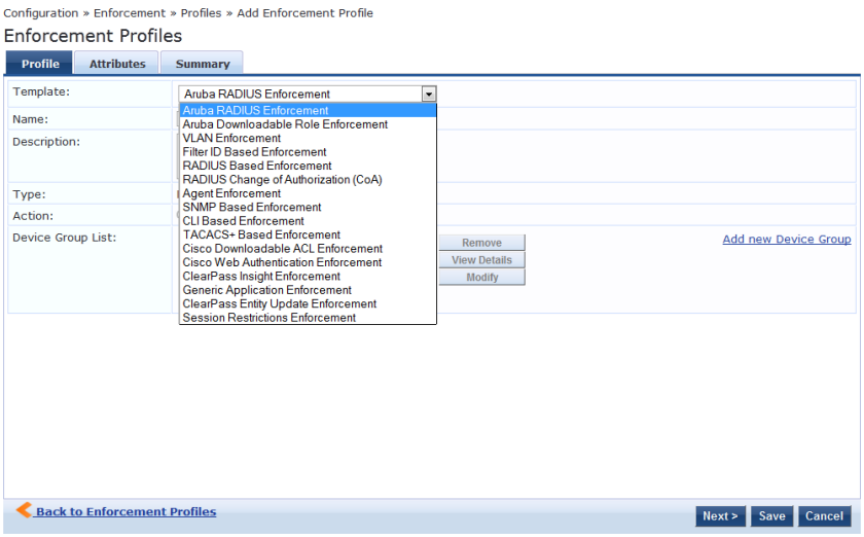


Policy Manager comes pre-packaged with the following system-defined enforcement profiles:

- **[Allow Access Profile].** System-defined RADIUS profile to allow network access; Policy Manager sends a RADIUS *AccessAccept* message with no attributes.
- **[Deny Access Profile].** System-defined RADIUS profile to deny network access; Policy Manager sends a RADIUS *AccessReject* message with no attributes.
- **[Drop Access Profile].** System-defined profile to drop the network access request; Policy Manager silently drops the RADIUS *AccessRequest* message.
- **[TACACS Deny Profile].** System-defined TACACS+ profile to deny network device access through the TACACS+ protocol.
- There are several system-defined profiles associated with different vendors' RADIUS CoA actions.
  - **[Cisco - Terminate Session]** - Terminate a session on a Cisco device.
  - **[Cisco - Disable-Host-Port]** - Disable a port on a Cisco Ethernet switching device.
  - **[Cisco - Bounce-Host-Port]** - Perform link-up/link-down action on a Cisco Ethernet switching device.
  - **[Cisco - Reuthenticate-Session]** - Trigger a session reauthentication on a Cisco device.
  - **[HP - Terminate Session]** - Terminate a session on an HP device.
  - **[Dell - Terminate Session]** - Terminate a session on a Dell Wireless Controller.
- There are four built-in TACACS+ profiles that are mapped to the different administrator roles available in Policy Manager. These profiles can be used to give permissions to log into the Policy Manager UI.
  - **[TACACS Help Desk].** System-defined profile to allow administrative access to Policy Manager using the **Helpdesk** role.
  - **[TACACS Network Admin].** System-defined profile to allow administrative access to Policy Manager using the **Network Administrator** role.
  - **[TACACS Receptionist].** System-defined profile to allow administrative access to Policy Manager using the **Receptionist** role.
  - **[TACACS Super Admin].** System-defined profile to allow administrative access to Policy Manager using the **Super Administrator** role.

From the **Enforcement Profile** page, when you click **Add Enforcement Profile,** Policy Manager displays the **Add Enforcement Profile** page:

Figure 190 *Add Enforcement Profile Page*



Policy Manager comes pre-packaged with several enforcement profile templates:

- VLAN Enforcement - All RADIUS attributes for VLAN enforcement are pre-filled in this template.

- Dell RADIUS Enforcement - RADIUS tempate that can be filled with attributes from the Dell RADIUS dictionaries loaded into Policy Manager.
- Dell Downloadable Role Enforcement - RADIUS template that can be filled with role attributes to create roles that can be assigned to users after successful authentication.
- Filter ID Based Enforcement - All RADIUS attributes for filter-id based enforcement are pre-filled in this template.
- RADIUS Based Enforcement - Generic RADIUS tempate that can be filled with any attribute from the RADIUS vendor dictionaries loaded into Policy Manager.
- RADIUS Change of Authorization (CoA) - Enforcement profile that encapsulates CoA actions sent to the network device. Note that the system comes pre-packaged with default Enforcement Profiles for “Disconnect” (Terminate Session) actions for the different supported vendor devices; there is no need to create profiles for these actions.
- TACACS+ Based Enforcement - TACACS+ based enforcement profile with UI customized for TACACS+ service & command authorization.
- SNMP Based Enforcement - Generic SNMP based enforcement profile with SNMP dictionaries for VLAN steering and Reset Connection.
- Cisco Downloadable ACL Enforcement - RADIUS based enforcement profile with UI customized for Cisco Downloadable ACL Enforcement.
- Cisco Web Authentication Enforcement - RADIUS based enforcement profile with pre-loaded attributes for enforcement for Cisco switch-hosted web authentication.
- Dell Guest Enforcement - Application specific enforcement profile with pre-loaded attributes for authorization of Guest users.
- Dell W-Insight Enforcement - Application specific enforcement profile with pre-loaded attributes for authorization of Insight users.
- Generic Application Enforcement - Application specific enforcement profile with customization attribute-value pairs for authorization of generic applications.
- CLI Based Enforcement - Enforcement profile that encapsulates CLI commands to be issued to the network device. The “Target Device” attribute specifies the device on which the “Command” attribute is executed.
- Agent Enforcement - Enforcement profile that encapsulates attributes sent to Dell W-OnGuard agent. Attributes can be specified to bounce the client or to send a custom message to the client.
- ClearPass Entity Update Enforcement - Post-authentication enforcement profile that can be filled with attributes to update the tag entries in endpoints and guest users.
- Session Restrictions Enforcement - Post-authentication enforcement profile that can be filled with attributes to restrict users based on various factors such as bandwidth usage, active session count, and also terminate sessions when the limits are reached.

Table 103: *Add Enforcement Profile page*

Parameter	Description
Name/ Description	Freeform label for enforcement profile.
Type	Auto-filled based on the selected template: RADIUS, TACACS, SNMP, Application, RADIUS_CoA
Action	Relevant only for RADIUS type enforcement profiles. Accept, Deny or Drop the request.

Parameter	Description
Device Group List	Associate the profile with pre-configured Device Groups. • **Add New Device Group** to add a new device group. • **Add** to add a device group from this drop-down list. • **Remove**, **View Details**, **Modify** to remove, view the details of, or modify the selected enforcement profile, respectively **NOTE:** This feature does not work with RADIUS CoA type Enforcement Profiles.

The remaining **Enforcement Profile** tabs vary in content, depending on the *Template Type* (auto-specified in the **Type** field when a **Template** has been selected):

- "RADIUS Enforcement Profiles " on page 196
- "RADIUS CoA Enforcement Profiles" on page 198
- "SNMP Enforcement Profiles " on page 198
- "TACACS+ Enforcement Profiles " on page 199
- "Application Enforcement Profiles " on page 201
- "CLI Enforcement Profile " on page 202
- "Agent Enforcement Profiles " on page 202
- Post Authentication Enforcement Profiles

RADIUS Enforcement Profiles

RADIUS Enforcement Profiles contain name/value pairings of attributes from the RADIUS dictionaries; in this editing context, Policy Manager displays only those attributes marked in the dictionary with the *OUT* or *INOUT* qualifier.

The following figures illustrate rules for several sample profiles:

A - VLAN Enforcement; **B** - Filter ID Based Enforcement; **C** - Cisco Downloadable ACL Enforcement; **D** - Cisco We Authentication Enforcement; **E** - Generic RADIUS Enforcement; **F** -

Figure 191 *RADIUS Enforcement Profile (Attributes Tab)*

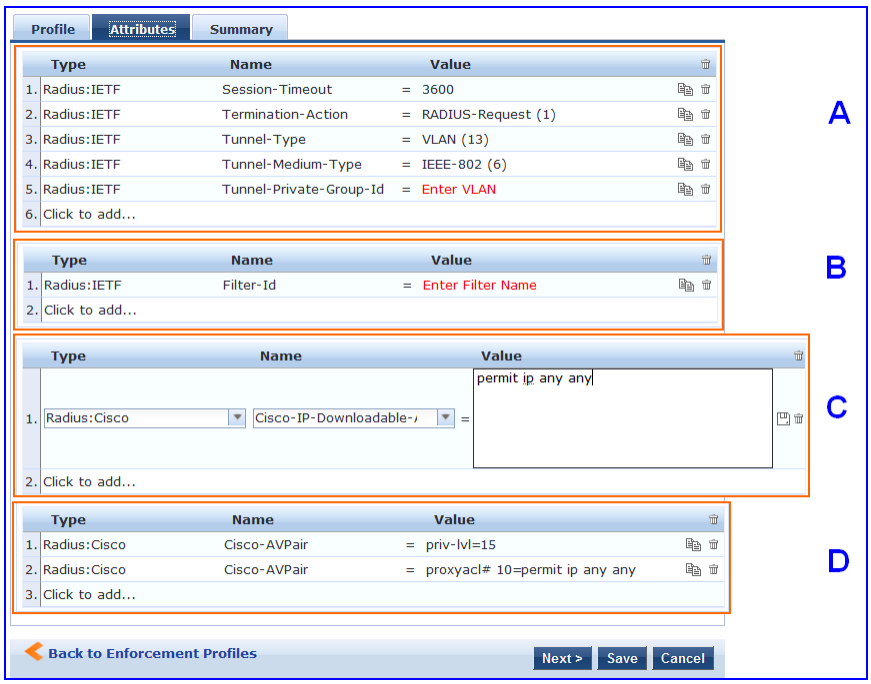


Figure 192 *RADIUS Enforcement Profile (Attributes Tab) - Generic RADIUS Enforcement Profile*

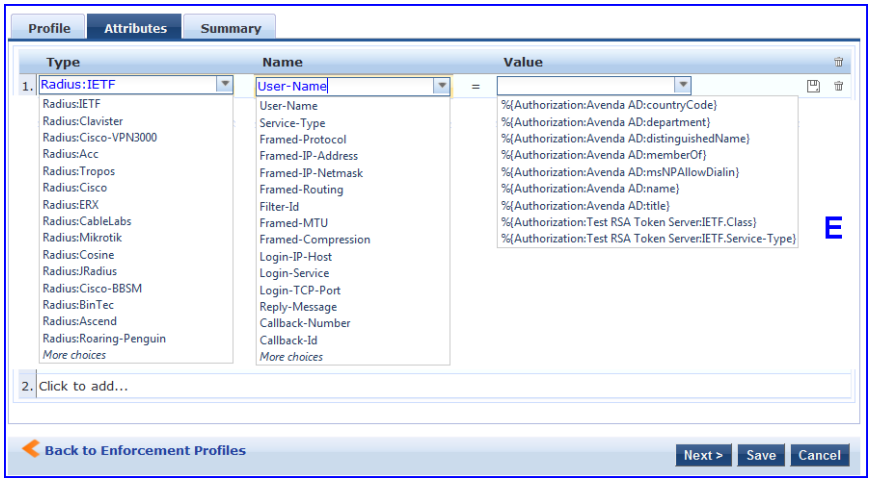


Table 104: *RADIUS Enforcement Profile (Attributes tab)*

Enforcement Profile Template	Description
A– VLAN Enforcement	Enforcement profile template to set IETF RADIUS standard VLAN attributes.
B–Filter ID Based Enforcement	Enforcement profile template to set IETF RADIUS standard filter ID attribute.

Enforcement Profile Template	Description
C–Cisco Downloadable ACL Enforcement	Enforcement profile template for Cisco IOS downloadable ACLs.
D–Cisco Web Authentication Enforcement	Enforcement profile template to set Cisco Web Authentication ACLs.
E–(Generic) RADIUS-Based Authentication	**Type** is any RADIUS vendor dictionary that is pre-packaged with Policy Manager, or imported by the Administrator. This field is prepopulated with the dictionary names. **Name** is the name of the attribute from the dictionary selected in the Type field. The attribute names are prepopulated from the dictionary. **Value** is the value of the attribute. If the value has prepopulated values is the dictionary, these appear in a drop-down list. Otherwise, you can enter freeform text. An Enforcement Profile can also contain dynamic values (as received in the request or authentication handshake, or as derived by the Policy Manager policy system). For example, to set the name of the VLAN to the name of the role, enter `%{Tips:Role}` as the value for `RADIUS:IETF:Tunnel-Private-Group-Id`. These dynamic values must be entered in the following format, without any spaces: `%{namespace:attribute-name}`. For convenience, the value field also has a drop down that contains all the authorization attributes. You can use these directly to assign dynamic values in the profile. Refer to figure above.

RADIUS CoA Enforcement Profiles

The **RADIUS CoA** tab contains a template type and the actions associated with that template type.

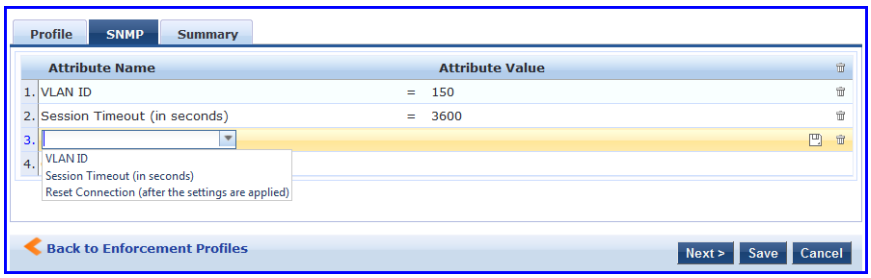
The RADIUS CoA Enforcement **Profile** tab loads the CoA template attributes supported a specific template.

Interface	Description
Select RADIUS CoA Template	The supported template types are: • Cisco - Disable-Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate-Session • HP - Change-VLAN • HP - Generic-CoA
Attributes	The RADIUS (standard and vendor-specific) shown here are base on the CoA Template selected from the drop down. Fill in values for all entries marked “Enter value here”. The other pre-filled attributes must not be deleted, since the device requires these to be present.

SNMP Enforcement Profiles

The **SNMP** tab contains a VLAN identifier and timeout.

Figure 193 *Fig: SNMP Enforcement Profile (SNMP Tab)*



The SNMP Enforcement Profile **SNMP** tab loads the SNMP dictionary attributes supported by Policy Manager.

Table 105: *SNMP Enforcement Profile (SNMP tab)*

Interface	Description
VLAN Id	VLAN ID to be sent to the device
Session Timeout	Session timeout in seconds.
Reset Connection (after the settings are applied)	Reset Connection is a primitive that does different actions based on the capabilities of the network device. For devices that support the 802.1X re-authentication, Policy Manager triggers a re-authentication; in other cases, it bounces the port.

TACACS+ Enforcement Profiles

TACACS+ Enforcement Profiles contain attribute-value pairs and other permissions related to administrative access to a network device. The built-in TACACS+ enforcement profiles can also be used to log into the Policy Manager UI. TACACS+ enforcement profiles use ARAP, Policy Manager:HTTP, PIX Shell, PPP:IP, PPP:IPX, PPP:LCP, Wireless-WCS:HTTP, CiscoWLC:Common and Shell namespaces to define service attributes.

Figure 194 *TACACS+ Enforcement Profiles (Services Tab)*

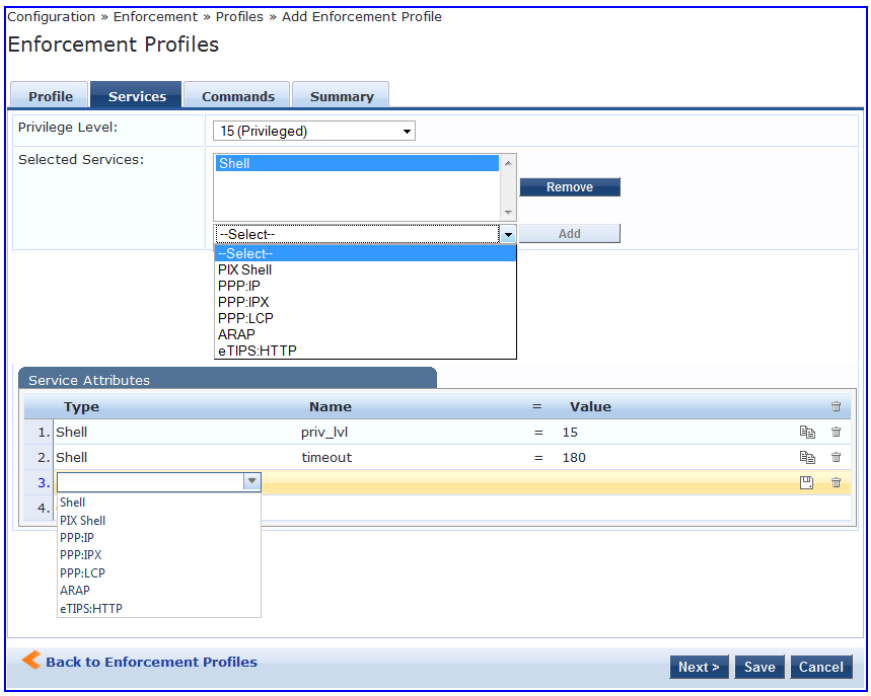


Table 106: *TACACS+ Enforcement Profile (Services tab)*

Container	Description
Privilege Level	Enter a value, from 0 to 15. **NOTE:** Refer to your network device documentation for definitions of the different privilege levels.
Selected Services	To add supported services, click **Add.** To remove a service, select it and click **Remove.** Policy Manager supports ARAP,eTIPS:HTTP (Policy Manager administrative interface login), PIX shell, Shell, PPP:IP, PPP:IPX, Wireless-WCS:HTTP, CiscoWLC:Common and PPP:LCP.
Service Attributes	Once the services have been selected, you can select the attributes to send for those services. Some services have pre-defined attributtes (which are automatically populated by Policy Manager in a drop down list in the **Name** field). You can also add custom attributes in the Name field. Add service attributes corresponding to the services selected in **Selected Services.** Policy Manager ships configured with attributes for some of the listed services.

Selections in the **Commands** tab configure commands and arguments allowed/disallowed for the selected Service Type.

Figure 195 *TACACS+ Enforcement Profiles (Commands tab)*

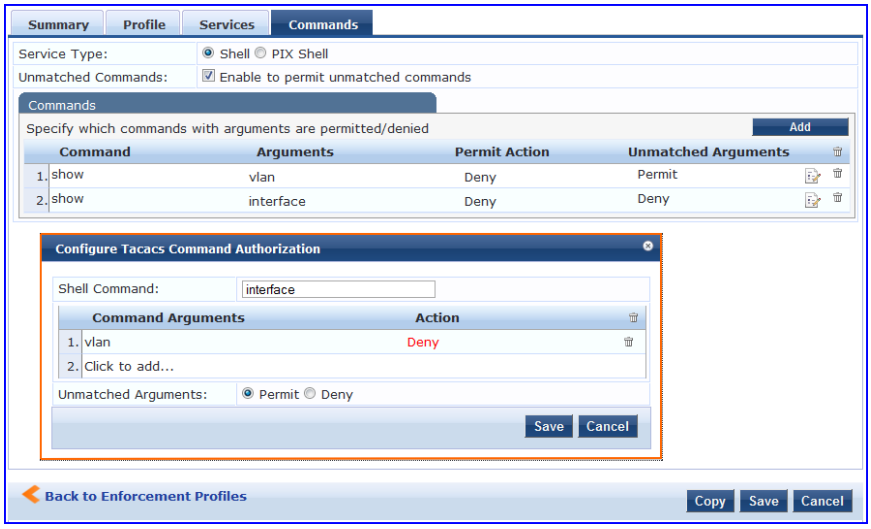


Table 107: *Commands tab (TACACS+ Enforcement Profiles)*

Container	Description
Service Type	Select **Shell** or **PIX shell** radio button. Subsequent selections in this tab configure commands and arguments allowed/disallowed for this selection.
Unmatched Commands	Enable to permit commands that are not explicitly entered in the **Commands** field.
Commands	Contains a list of the commands recognized for the specified **Service Type**: To add a command, click **Add**. In the **Configure Tacacs Command Authorization** popup, enter values for: • **Command.** A string for the command. This is followed by one or more command argument rows. • **Command Arguments.** The arguments for the command. • **Action.** Click on **Enable to permit** check box to permit use of this command argument. If this box is unchecked the column shows **Deny** and the command argument is not allowed. • Click **Trashcan** to delete the command argument. • **Unmatched Arguments.** Select **Permit** radio button to permit this command even if Policy Manager receives arguments for the command that it does not recognize. Select **Deny** radio button to deny the command if Policy Manager receives unrecognized arguments. To save and exit, click outside the row you are editing. To delete a command, click the **Trashcan** icon for that row.

Application Enforcement Profiles

Application Enforcement Profiles contain attribute-value pairs and other permissions related to authorization of users of Dell Applications - Guest and Insight. There are three different types of application enforcement profile templates that can be selected:

- ClearPass Insight Enforcement - Attributes for users of Insight application.
- Generic Application Enforcement - Attributes for users of any generic application.

Figure 196 *Application Enforcement Profiles (Attributes Tab)*

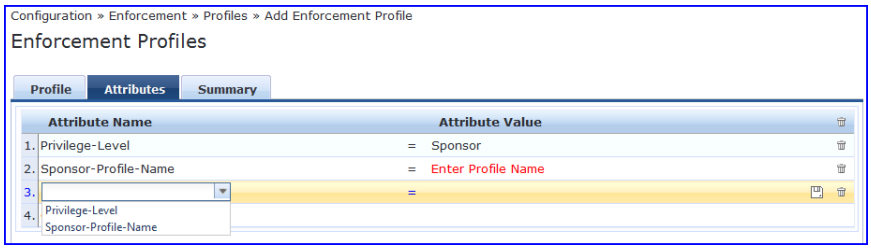


Table 108: *Application Enforcement Profiles (Attributes tab)*

Container	Description
Privilege-Level	Enter a predefined value: **Admin**, **Sponsor**, **Helpdesk**; or enter an application-specific custom value. **NOTE:** Sponsor is only valid for the Guest application
Sponsor-Profile-Name	Valid only for Guest application. This is the (case-sensitive) name of the sponsor profile defined in the Guest application.
Sponsor-Email	Enter the email address of the sponsor.

CLI Enforcement Profile

CLI Enforcement Profiles contain attribute-value pairs related to authorization of users/devices via CLI commands executed on a target network device.

Figure 197 *CLI Enforcement Profile (Attributes Tab)*

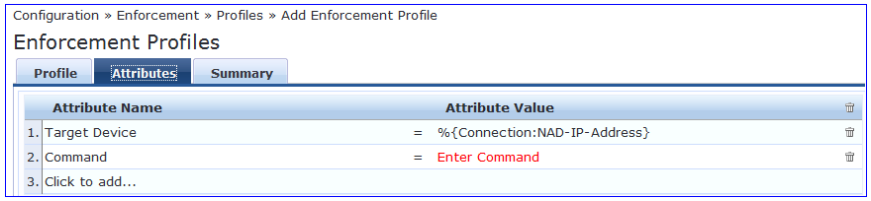


Table 109: *CLI Enforcement Profiles (Attributes tab)*

Container	Description
Target Device	Enter the device on which the CLI commands are executed. Typically, this is the edge device on which the user/endpoint connected (%{Connection:NAD-IP-Address}).
Command	Multiple commands (separated by a new line) that are executed on the target device.

Agent Enforcement Profiles

Agent Enforcement Profiles contain attribute-value pairs related to enforcement actions sent to Dell W-OnGuard Agent.

Figure 198 *Agent Enforcement Profile (Attributes Tab)*

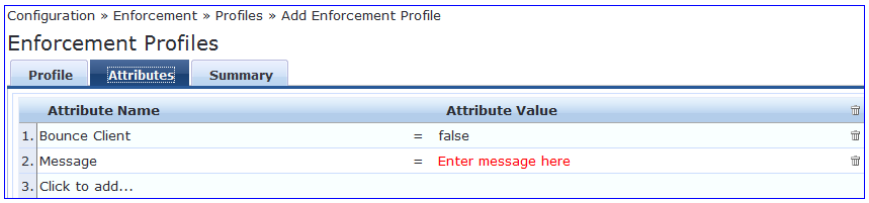


Table 110: *Agent Enforcement Profiles (Attributes tab)*

Container	Description
Bounce Client	If checked, the endpoint is bounced by the OnGuard agent (this feature is only available with the persistent agent)
Message	A custom message to send to the endpoint.
Session Timeout (in seconds)	Timeout after which the OnGuard agent forces a re authentication on the endpoint.

Post Authentication Enforcement Profiles

Post Authentication Enforcement Profiles contain combinations of type, attribute names, and values related to post authentication. You can add more context to a user who is authenticated earlier and this information is used for subsequent requests. Two post authentication profiles are provided:

- Entity Update Enforcement
- Session Restrictions Enforcement

Figure 199 *Post Authentication Enforcement Profiles*

This figure illustrates rules for the two sample profiles:

A— ClearPass Entity Update Enforcement, **B**—Session Restrictions Enforcement

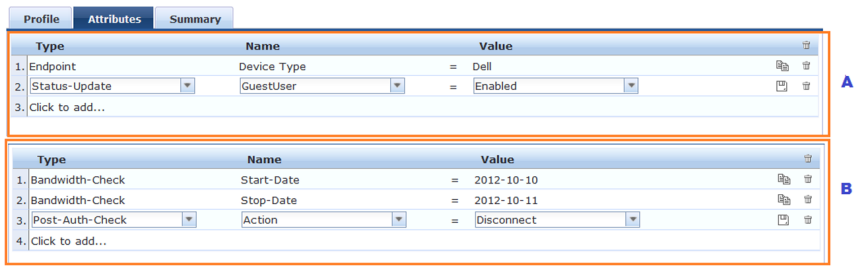


Table 111: *Post Authentication Enforcement Profiles*

Enforcement Profile Template	Description
A– ClearPassEntity Update Enforcement	Enforcement profile template used to update tags in endpoints and guest users. **Type** is any endpoint, guest user, or a session update. **Name** is the name of an attribute associated with an endpoint, guest user, or a session update. If the type is session update, the tags are updated for either an endpoint or a guest user. **Value** is the value of the attribute.
B–Session Restrictions Enforcement	Enforcement profile template used to restrict users based on bandwidth usage and also disconnect users when the specified limits are crossed. **Type** is any post authentication check or session check that is applicable to the user. **Name** is the name of any specific check related the selected **Type**. **Value** is the value of the attribute. For example, if **Bandwidth-Check** is selected as the **Type**, you can select **Start-Date** from the **Name** drop-down list, and specify the start date in the **Value** field.

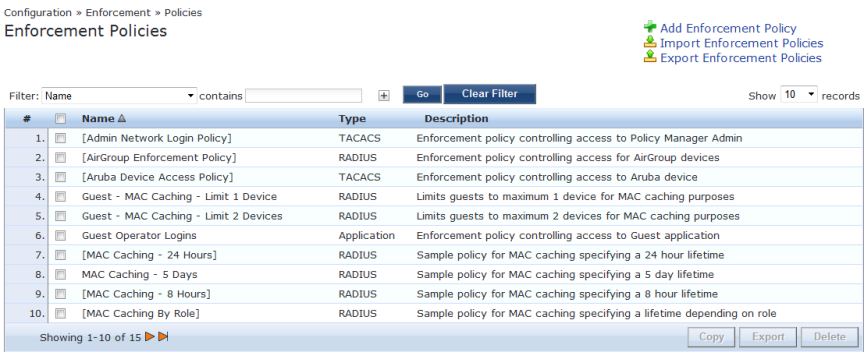
If you have configured to disconnect users or devices that exceed bandwidth or session related limits, then the users or devices that exceed the specified limit get added to the blacklist user repository. You must add the **Blacklist User Repository** as an authentication source so that such users are denied access. For information on configuring Authentication Sources, refer to Adding and Modifying Authentication Sources

Configuring Enforcement Policies

One and only one Enforcement Policy can be associated with each Service.

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

Figure 200 *Enforcement Policies Listing Page*



When you click **Add Enforcement Policy**, Policy Manager displays the **Add Enforcement Policy** wizard page:

Figure 201 *Add Enforcement Policy (Enforcement tab)*

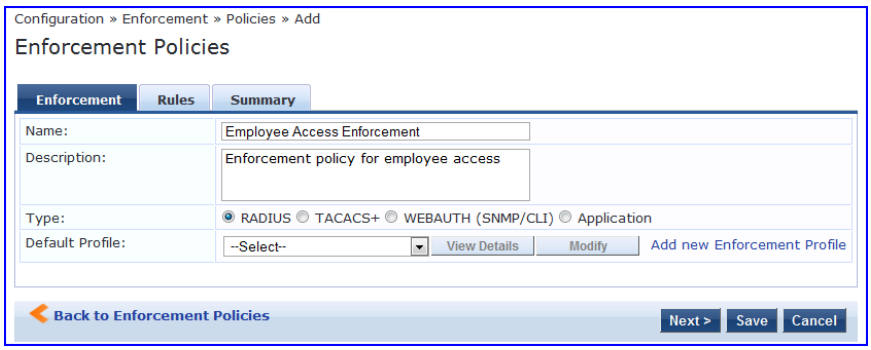


Table 112: *Add Enforcement Policy (Enforcement tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	Select: **RADIUS, TACACS+, WebAuth (SNMP/CLI)** or **Application**. Based on this selection, the Default Profile list shows the right type of enforcement profiles in the dropdown 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. Once 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 202 *Add Enforcement Policy (Rules Tab)*

Figure 203 *Add Enforcement Policy (Rules Editor)*

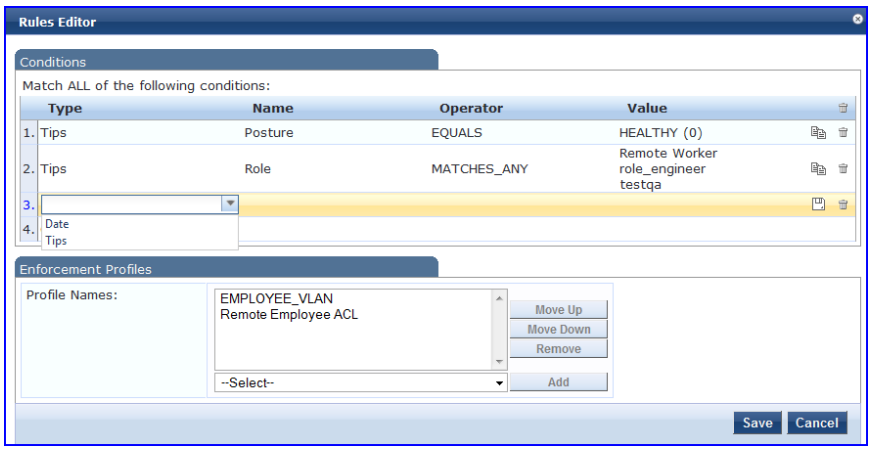


Table 113: *Add Enforcement Policy (Rules tab)*

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 114: *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 to see how Enable as Role can be turned on for a fetched attribute). Role names fetched from the authorization source can be entered freeform in value field. To commit the rule, click **Save**.
Enforcement Profiles	If the rule conditions match, attributes from the selected enforcement profiles are sent to Network Access Device. If a rule matches and there are multiple enforcement profiles, the enforcement profile disambiguation rules apply.

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.

Refer to the following sections:

- "Adding and Modifying Devices " on page 208
- "Adding and Modifying Device Groups " on page 212
- "Adding and Modifying Proxy Targets " on page 214

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 204 *Network Devices page*

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 205 *Device tab*

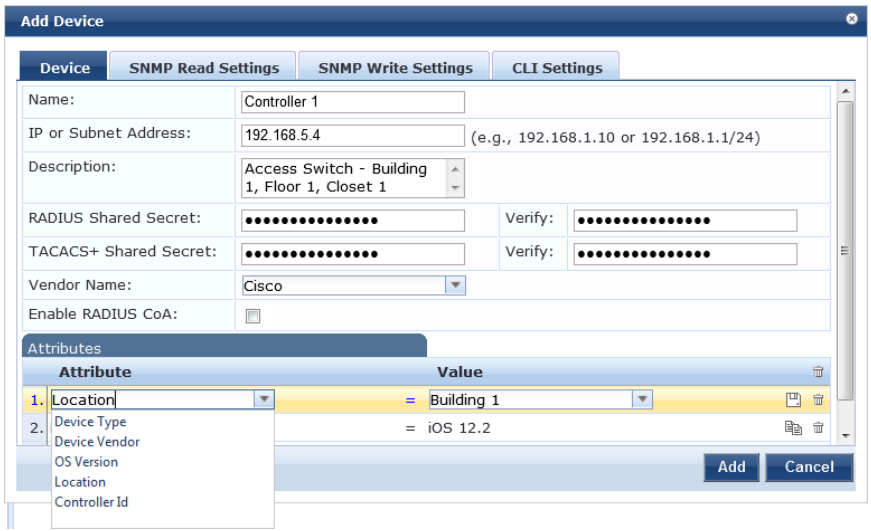


Table 115: *Device tab*

Container	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 standard the 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, 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 206 *SNMP Read/Write Settings tabs*

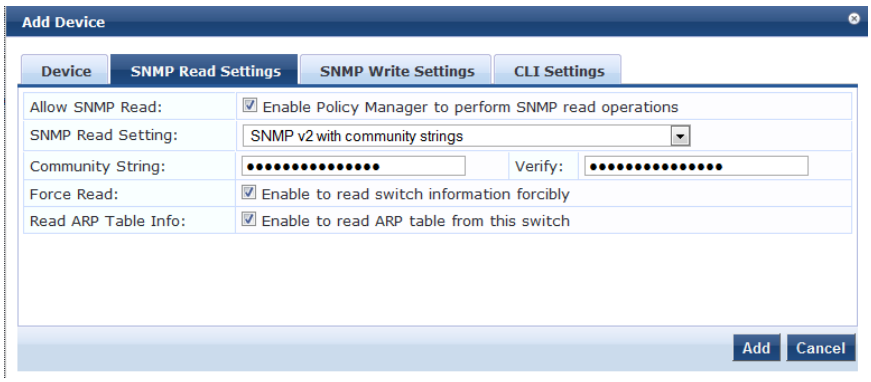


Figure 207 *SNMP Read/Write Settings tabs - SNMP v3 Details*

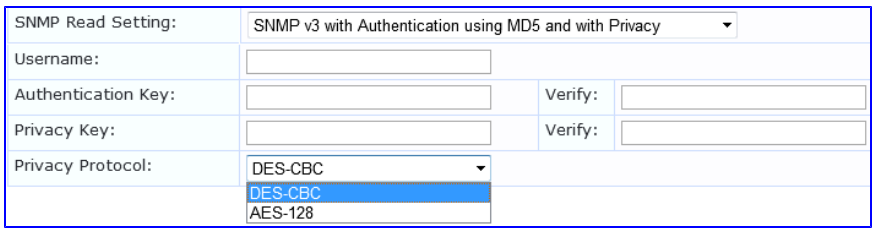


Table 116: *SNMP Read/Write Settings tabs*

Container	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.
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.

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 208 *CLI Settings tab*

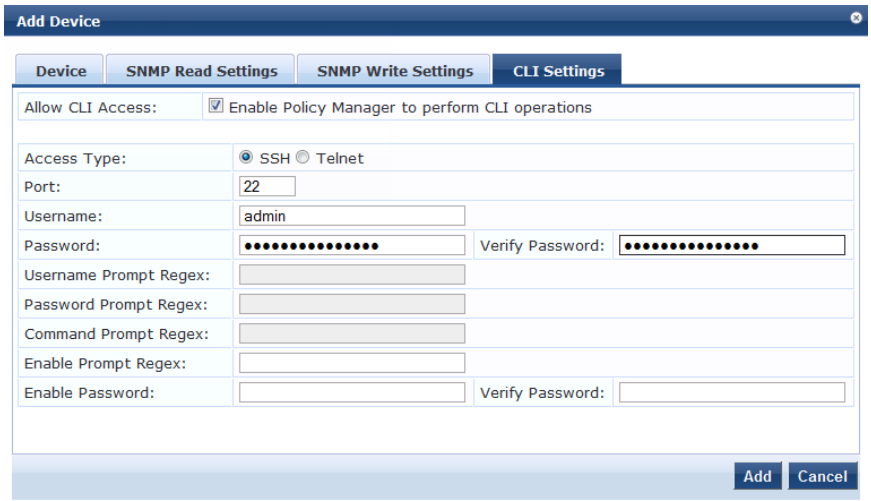


Table 117: *CLI Settings tab*

Container	Description
Allow CLI Access	Toggle to enable/disable CLI access.
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 that you exported with.
- 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.**

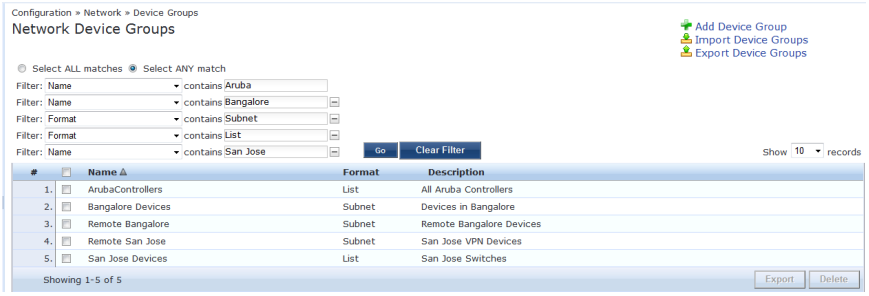
Adding and Modifying Device Groups

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 209 *Device Groups Page*



To add a Device Group, click **Add Device Group**. Complete the fields in the **Add New Device Group** popup:

Figure 210 *Add New Device Group Popup*

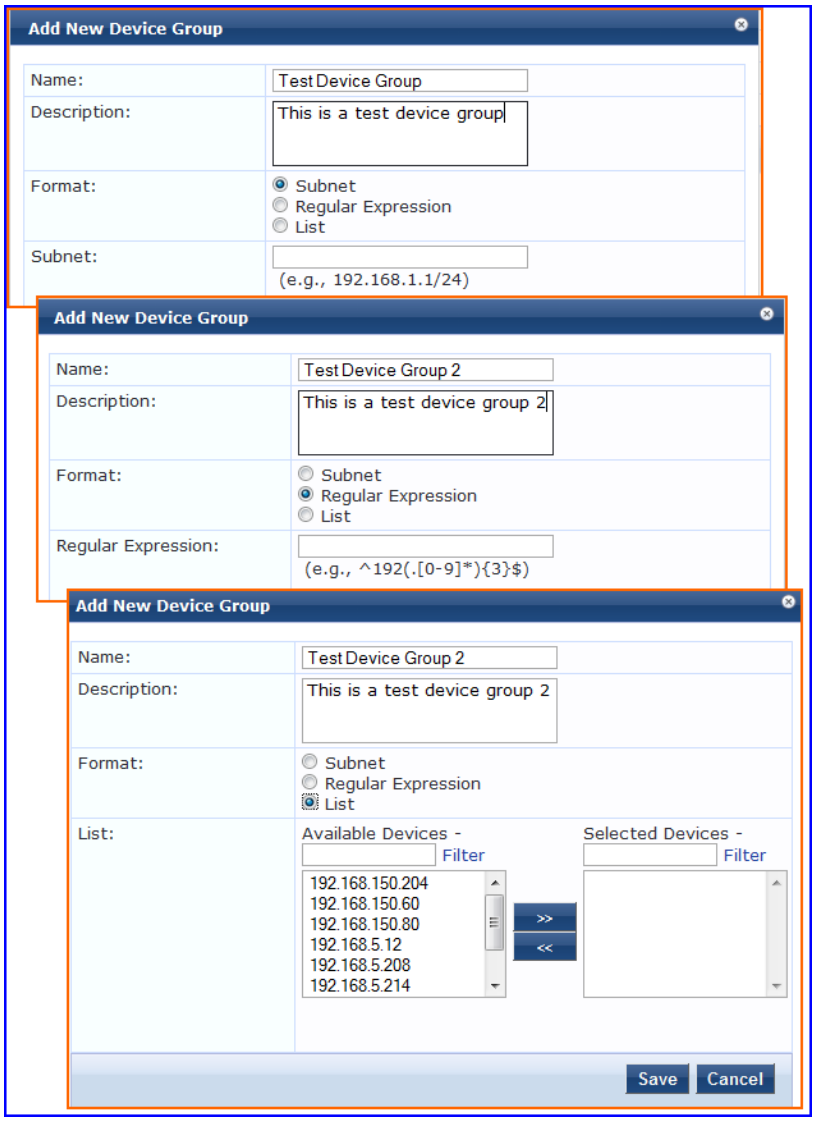


Table 118: *Add New Device Group popup*

Container	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 used in configuring RADIUS proxy Services. (Refer to Policy Manager Service Types.)

Policy Manager lists all configured proxy servers in the **Proxy Servers** page: **Configuration > Network > Proxy Servers**.

Figure 211 *Proxy Targets Page*

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 212 *Add Proxy Target Popup*

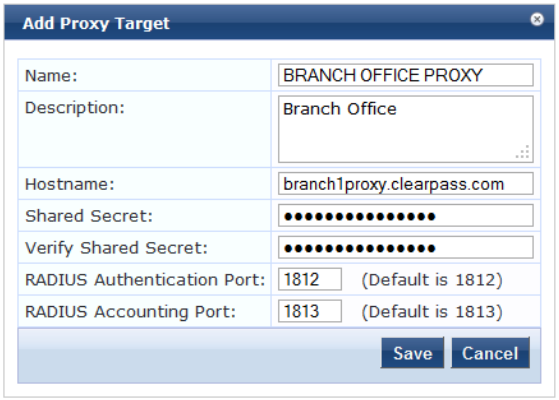


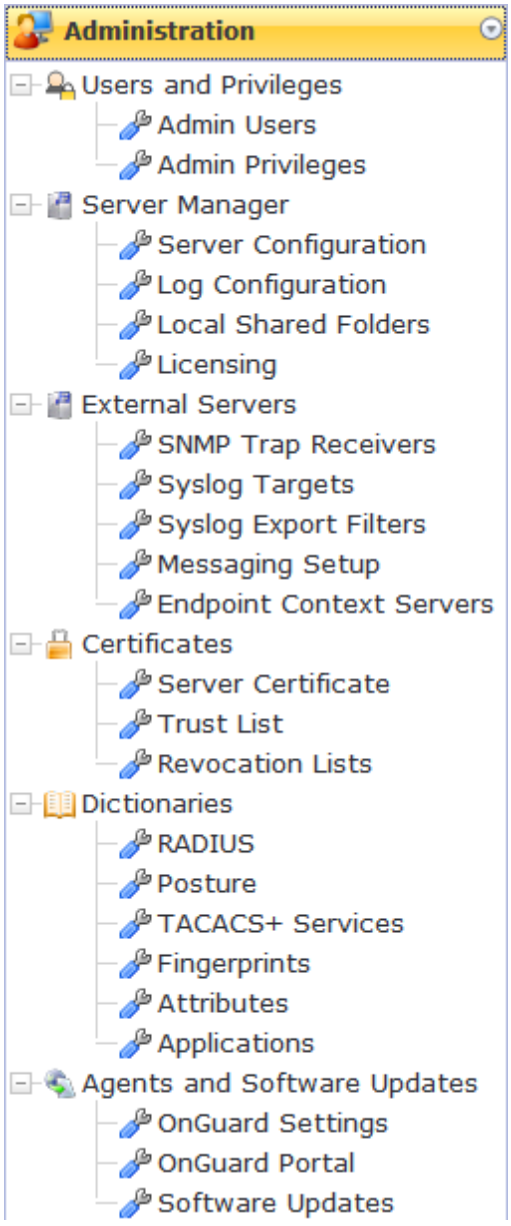
Table 119: *Add Proxy Target popup*

Container	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

- To import a Proxy Target, click **Import Proxy Targets**. In the **Import from File** popup, browse to select a file, then click **Import**.
- To export all Proxy Targets from the configuration, click **Export Proxy Targets**. In the **Export to File** popup, specify a file path, and then click **Export**.
- To export a single Proxy Target from the configuration, select it (check box on left), then click **Export**. In the **Save As** popup, specify a file path, and then click **Export**.
- To delete a single Proxy Target 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**.

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:



Admin Users

The Policy Manager Admin Users menu **Administration > Users and Privileges > Admin Users** provides the following interfaces for configuration:

- "Import Users " on page 218
- "Export Users " on page 218
- "Export " on page 218

Figure 213 *Admin Users*

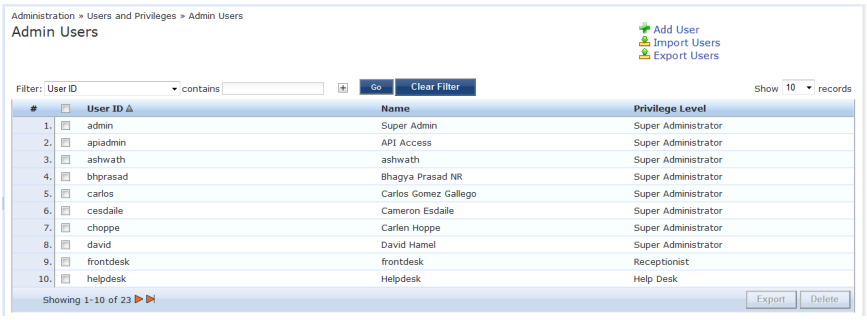


Table 120: *Admin Users*

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 214 *Add Admin User*

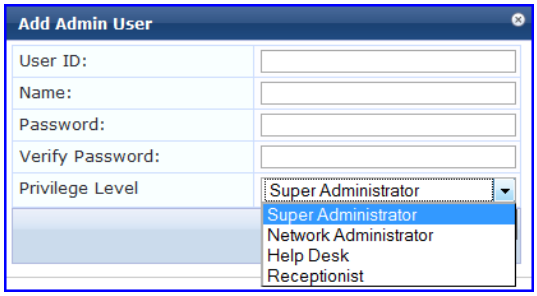


Table 121: *Add Admin User*

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 215 *Import (Admin) Users*

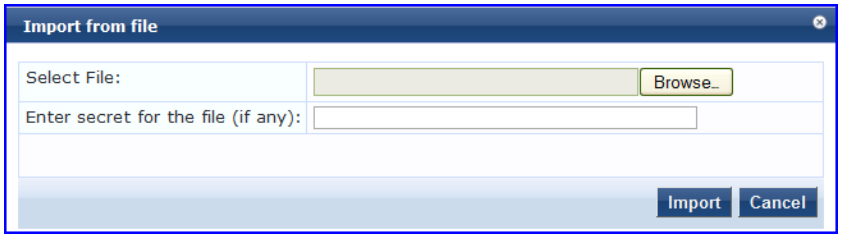


Table 122: *Import (Admin) Users*

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 will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Export

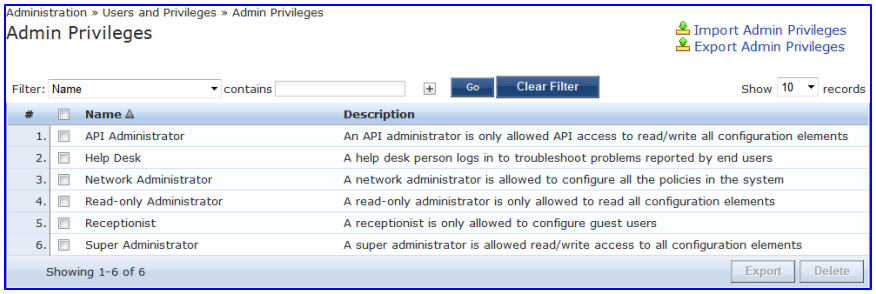
Select the **Export** button on the lower right portion of the page.

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 216 *Admin Privileges*



See Custom Admin Privileges to create additional admin privileges and Exporting to export the definition of one or more admin privileges.

Custom Admin Privileges

While Dell Networking W-ClearPass Policy Manager doesn't let you change the definition of the built-in admin privileges, you can create and import custom ones. Customer admin privileges are defined in a specifically formatted XML file and then imported into Policy Manager on the Admin Privileges page.

Create a Custom Admin Privilege

You will need a plain text or XML editor, not a word processor such as Microsoft Word, to create a custom admin privilege.

To create a custom admin privilege

1. Using a plain text or XML editor (not a word processor such as Microsoft Word), create an XML file that defines a privilege and its definition. (See the following sections for information on the XML structure, and privilege definitions.)
2. Go to **Administration > Users and Privileges > Admin Privileges**.
3. Import the admin privilege file you created in step 1. See Importing for details.

The admin privilege is added to the list.

Admin Privilege XML 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>
```

Admin Privileges and IDs

The following section lists the areas and sub-areas of the Policy Manager application and the associated taskid of each one.

- 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 TrendingL `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.

Sample Admin Privilege XML

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
```

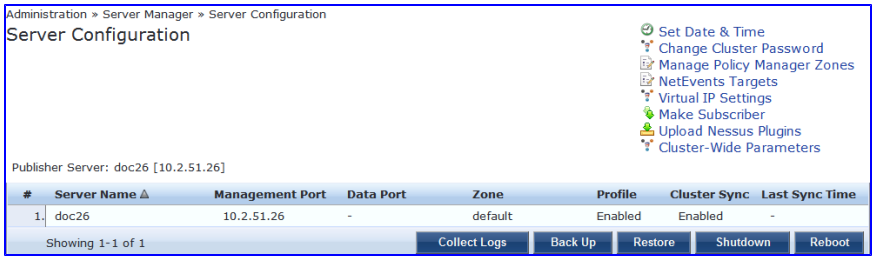
```
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="mon"> //Refers to Monitoring
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="adm.mg.sc"> //Refers to Server Configuration
        <AdminTaskAction type="RO"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

Server Configuration

The Policy Manager Server Configuration menu (**Administration > Server Manager > Server Configuration**) provides the following interfaces for configuration:

- "Set Date/Time " on page 224
- "Change Cluster Password " on page 225
- "Manage Policy Manager Zones " on page 226
- "NetEvents Targets" on page 227
- "Virtual IP Settings" on page 227
- "Make Subscriber " on page 228
- "Upload Nessus Plugins " on page 229
- "Cluster-Wide Parameters " on page 229
- "Collect Logs " on page 233
- "Backup " on page 235
- "Restore" on page 236
- "Shutdown/Reboot " on page 237
- "Drop Subscriber " on page 237

Figure 217 *Server Configuration*



Clicking on the server row provides the following interfaces for configuration:

- "System Tab " on page 237
- "Services Control Tab " on page 240
- "Service Parameters Tab " on page 240
- "System Monitoring Tab " on page 248
- "Network Tab" on page 249

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 218 *Change Date and Time - Date & Time tab*

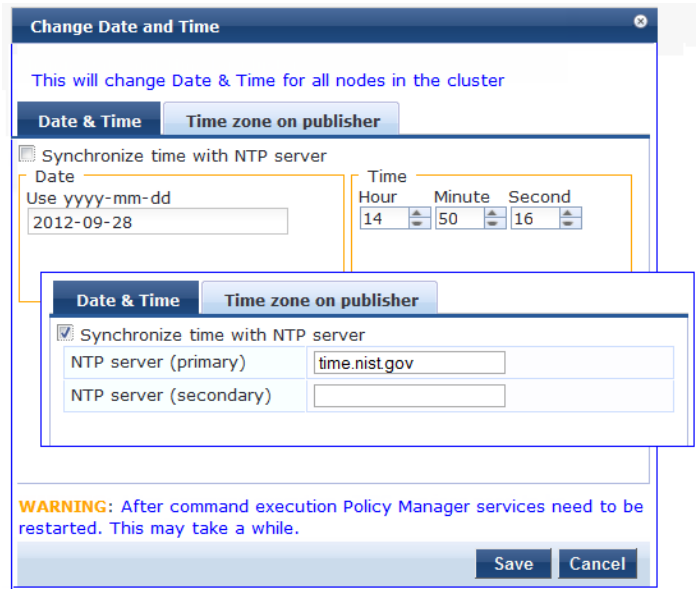


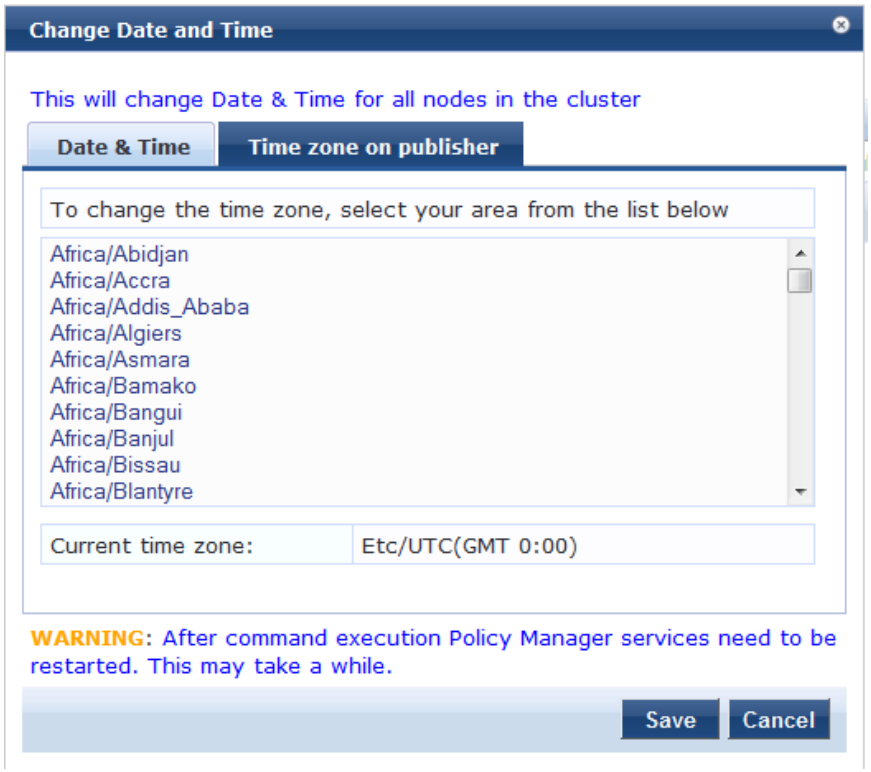
Table 123: *Change Date and Time - Date & Time tab*

Container	Description
Date in yyyy-mm-dd format	To specify date and time, use the indicated syntax. This is available only when Synchronize time with NTP server is unchecked.
Time in hh:mm:ss format	
Synchronize Time With NTP Server	To synchronize with a Network Time Protocol Server, enable this check box and specify the NTP servers. Only two servers may be specified.
NTP Servers	

After configuring the date and time, select the time zone on the Time zone on publisher tab. This displays a time zone list alphabetical order. Select a time zone and click **Save**.

This option is only available on the publisher. To set time zone on the subscriber, select the specific server and set time zone from the server-specific page.

Figure 219 *Time zone on publisher*



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.

Changing this password also changes the password for the CLI user - 'appadmin'.

Figure 220 *Change Cluster Password*

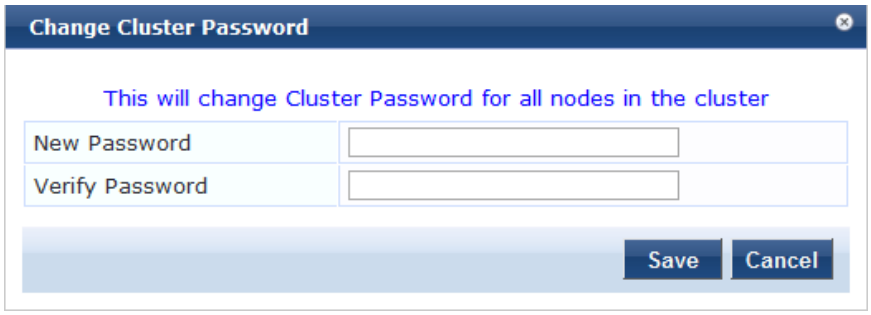


Table 124: *Change Cluster Password*

Container	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 CPPM to match with the geographical areas in your deployment. There can be multiple Zones per cluster, and each Zone has a number of CPPM nodes that share runtime state.

Figure 221 *Policy Manager Zones*

Table 125: *Policy Manager Zones*

Container	Description
Name	Enter the name of the configured Policy Manager Zone.
Delete	Select the delete (trashcan) icon to delete a zone.

NetEvents Targets

Netevents is 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 222 *NetEvents Targets*

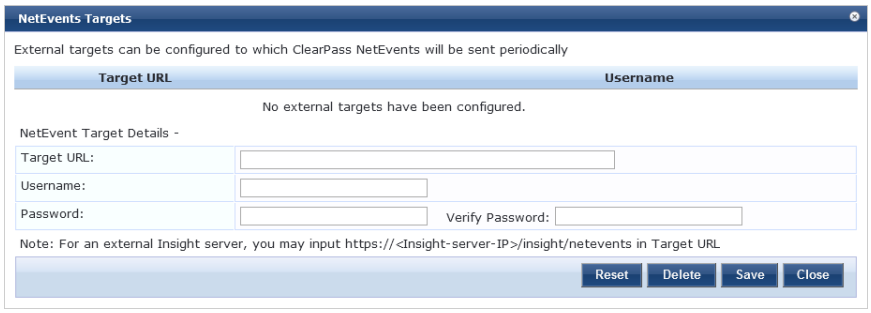


Table 126: *NetEvents targets*

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 may input https://<Insight-server-IP>/insight/netevents in 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.

Figure 223 *Virtual IP Settings*

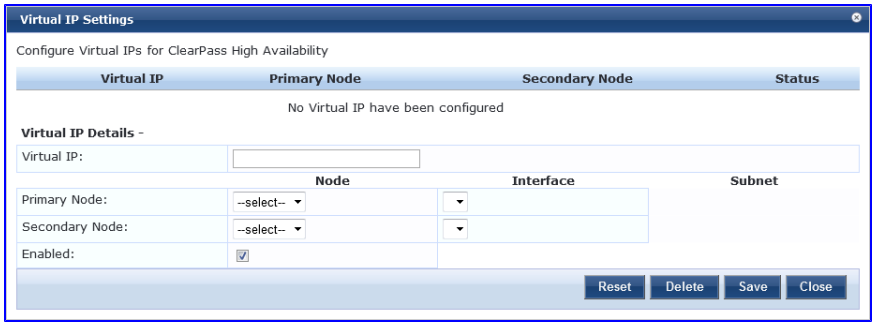


Table 127: *Virtual IP Settings Parameters*

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. An 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 224 *Add Subscriber Node*

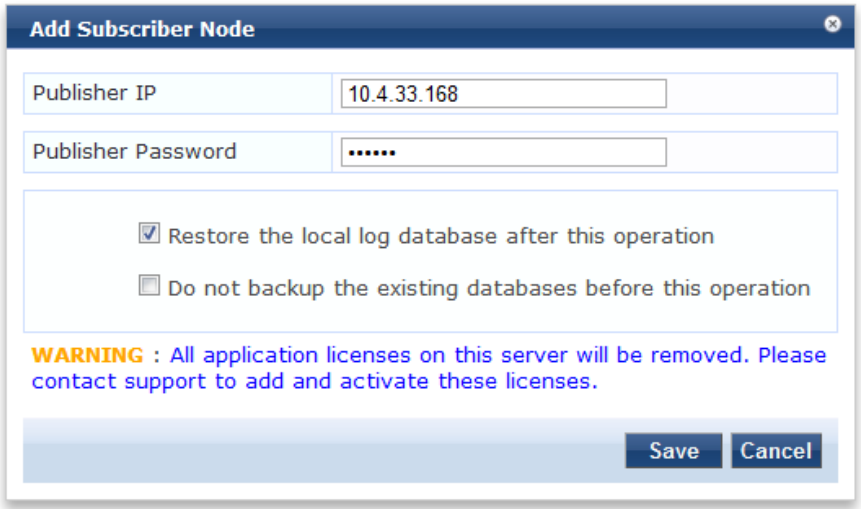


Table 128: *Add Subscriber Node*

Container	Description
Publisher IP	Specify publisher address and password. Note that 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.

Container	Description
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 225 *Upload Nessus Plugins*

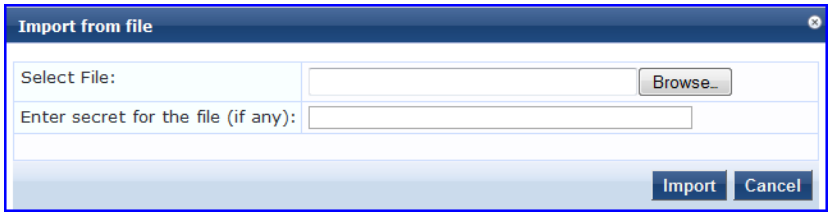


Table 129: *Upload Nessus Plugins*

Container	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 226 *Cluster-Wide Parameters dialog box, General tab*

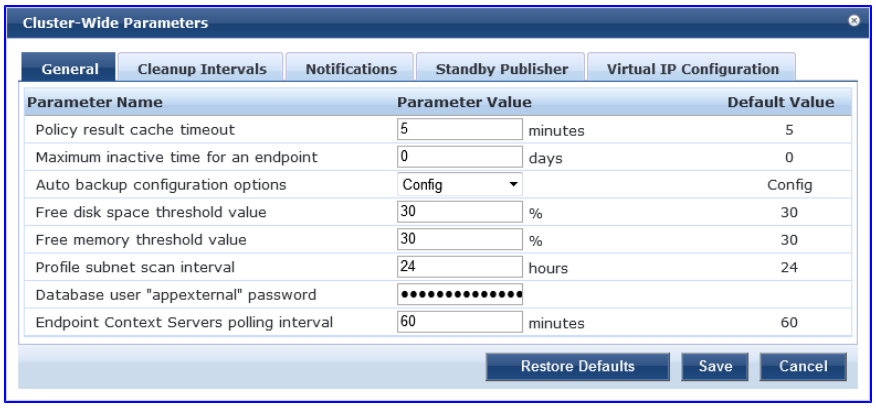


Figure 227 *Cluster-Wide Parameters dialog box, Cleanup Interval tab*

Figure 228 *Cluster-Wide Parameters dialog box, Notification tab*

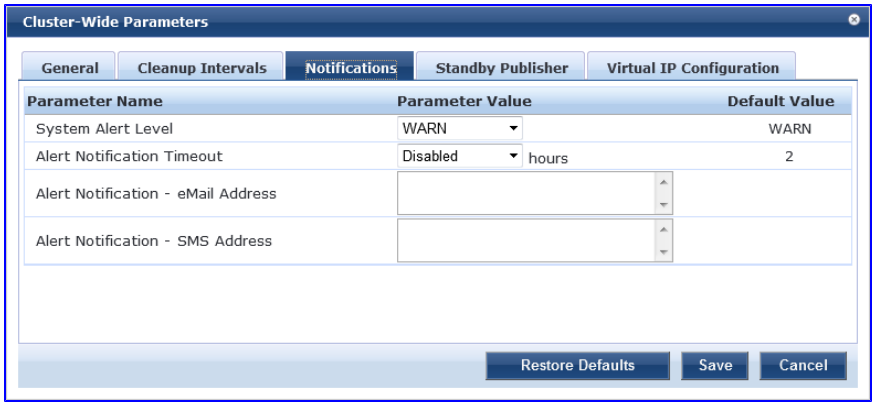


Figure 229 *Cluster-Wide Parameters dialog box, Standby Publisher tab*

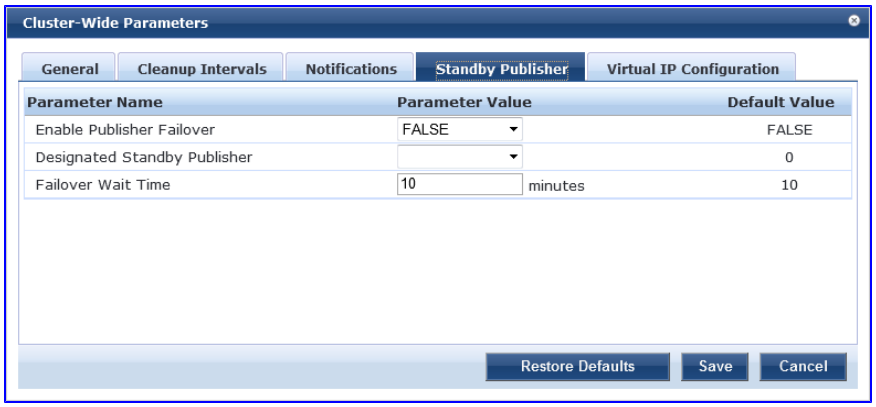


Figure 230 *Cluster-Wide Parameters dialog box, Virtual IP Configuration tab*

Table 130: *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.

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 disk.
Known or disabled endpoints cleanup interval	This controls how often (in days) endpoints with a status of Known or Disabled are cleaned up from the endpoints table.
Unknown endpoints cleanup interval	This controls how often (in days) endpoints with a status of Unknown are cleaned up from the endpoints table.
Expired guest accounts cleanup interval	This controls the cleanup interval of expired guest accounts; this is number of days after expiry that the cleanup happens. No cleanup is performed if the value is 0.
Profiled endpoints cleanup interval	Enter a value in days.
Notifications	
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.

Parameter	Description
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.
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	
Fallover 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.

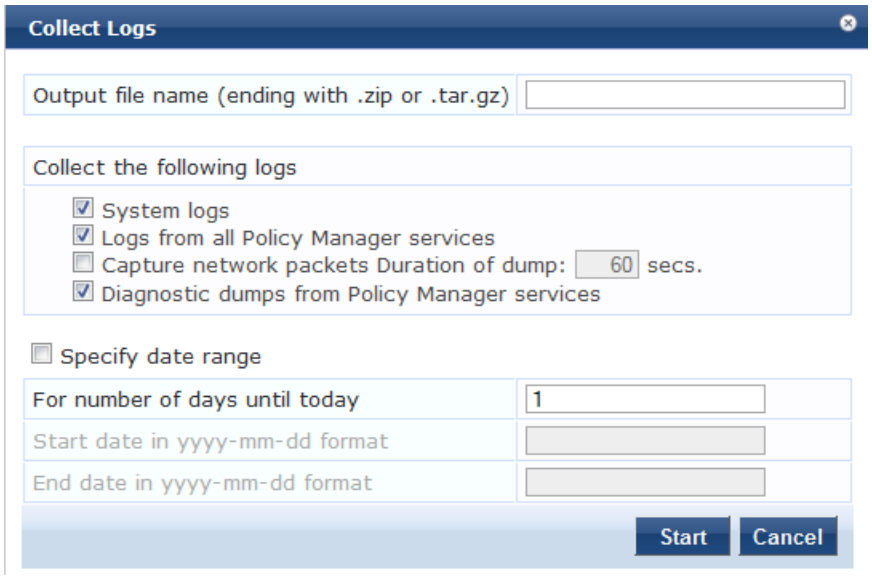
Collect Logs

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 231 *Collect Logs*



3. Enter a filename and add the .tar.gz extension to the filename.
4. Select which 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
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. When finished:
7. Click **Close** to finish or click **Download File** to save the log file to your computer.

The following information is useful if you are attempting to open a capture file (.cap or .pcap) using WireShark. First, untar or unzip the file (based on the file extension). When the entire file is extracted, navigate to the PacketCapture folder. Within this folder, you will see a file with a .cap extension. WireShark can be used to open this file and study the network traffic.

Viewing Log Files

Log files contain transactional and diagnostic data separated by information type into separate files. They are collected into a single file using the .tar file format, then compressed into a .gz file using the GZip compression utility. You will need an application that can read and unpack a GZip file to view the files in a log file.

Dell cannot recommend specific software for viewing the contents of files compressed with GZip.

To view log files

1. Open the file in software that can read and extract from GZip files.

2. Extract the file in the .tar.gz file. The result will be a file with the .tar extension.
3. Open the .tar file and extract the files within it. The result will be a folder named the same as the .tar file.

Inside that folder, you will find another folder with a randomly generated name that begins with "tmp." Inside that folder, you will find one folder for each of the 4 types of information you wanted to save. For example, if you selected System logs and Diagnostic dumps, you will have folders with the name SystemLogs and DiagnosticDumps. Inside each of those folders will be files containing various types of information. Some of those files are in additional sub-folders.

Backup

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Back Up** button. Note that this action can also be performed using the "`backup`" CLI command

Figure 232 *Backup Popup*

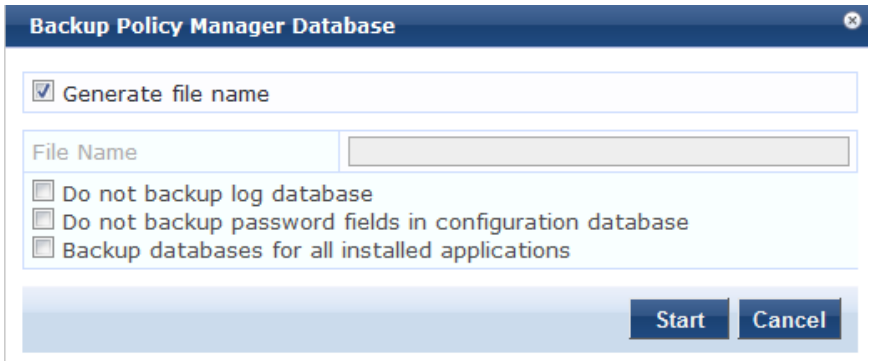


Figure 233 *Post-Backup Popup*

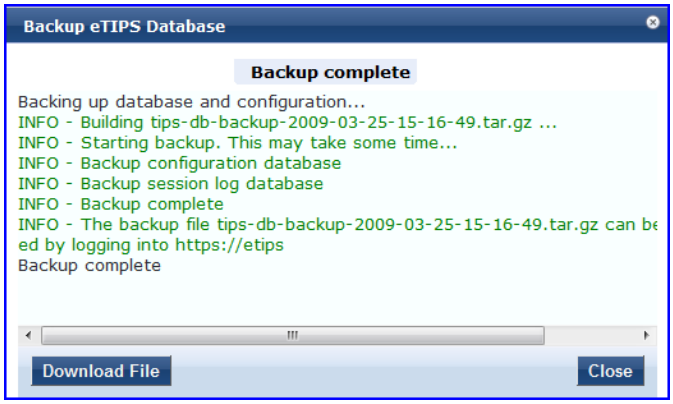


Table 131: *Back Up*

Container	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.

Container	Description
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. Note that this action can also be performed using the "`restore`" CLI command.

Figure 234 *Restore*

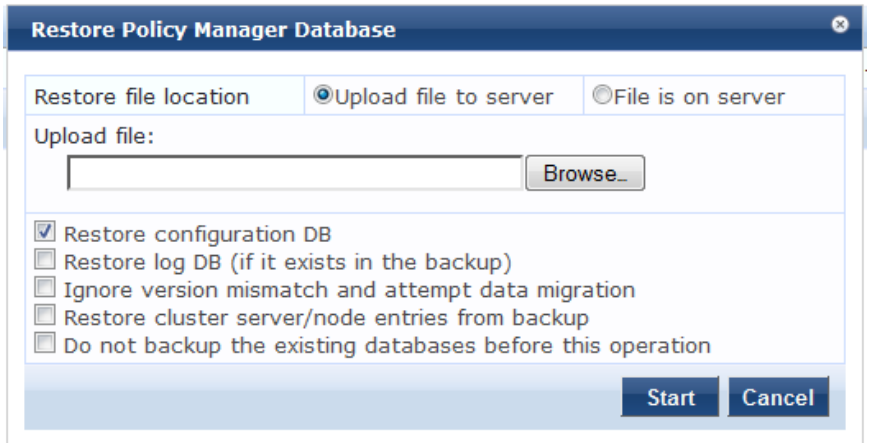


Table 132: *Restore*

Container	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 (shown only when Upload file to server radio button is selected).
Shared backup files present on the server	Select a file from the files in the local shared folders (See Local Shared Folders). This is shown only when **File on server** radio button is selected.
Restore configuration DB	Enable to include the configuration database in the restore.
Restore log DB (if it exists in the backup).	Enable to include the log database 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.

Container	Description
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 from the UI.

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 that this button is not seen in a single node deployment.

System Tab

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.

Figure 235 *System Tab*

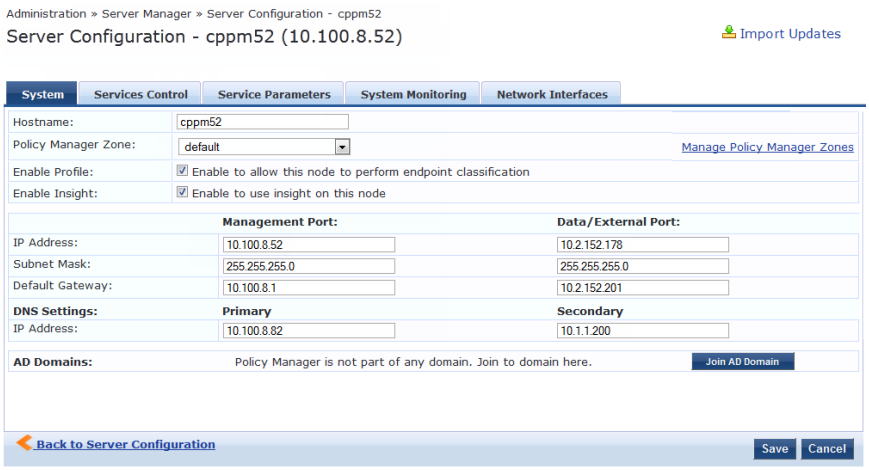


Table 133: *Server Configuration System tab*

Container	Description
Hostname	Hostname of Policy Manager appliance. It is not necessary to enter the fully qualified domain name here.
Policy Manager Timezone	Select a previously configured timezone from the drop down menu. 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.

Container	Description
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.
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
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. See below.

Multiple Active Directory Domains

You can join CPPM to an Active Directory domain to authenticate users and computers that are members of an Active Directory domain.

Users can then authenticate into the network using 802.1X and EAP methods, such as PEAP-MSCHAPv2, with their own their own AD credentials.

Joining CPPM to an Active Directory domain creates a computer account for the CPPM node in the AD database.

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 belong to the same AD forest because a one-way trust relationship exists between these domains. In thsi 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.

Leave Domain - 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 236 *Join Active Directory Domain*

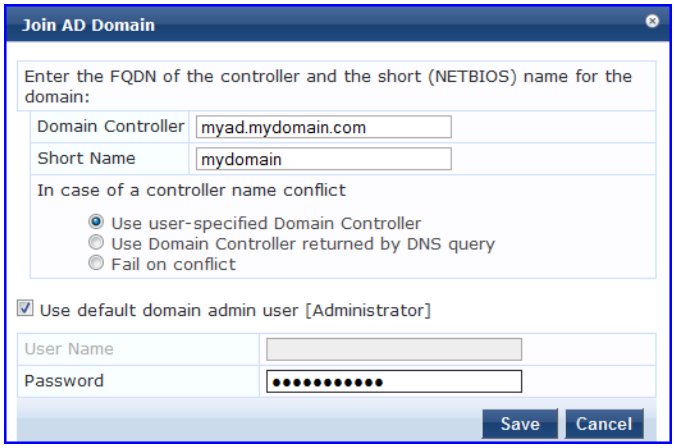


Table 134: *Join AD Domain*

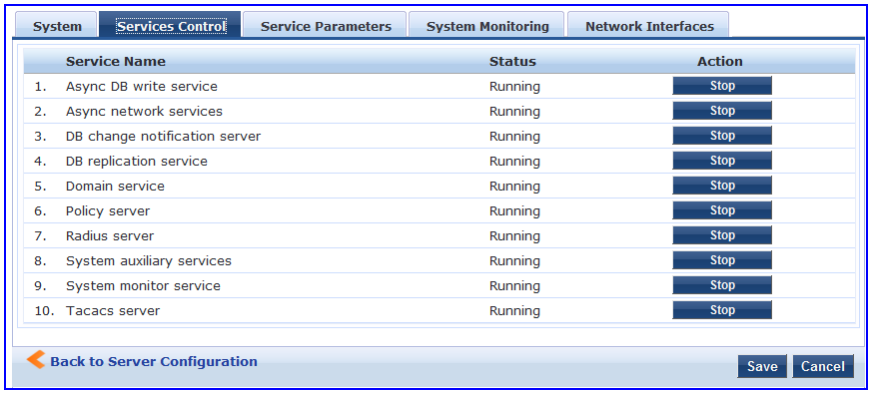
Container	Description
Domain Controller	*Fully qualified* name of the Active Directory domain controller
Short Name - NETBIOS name (optional)	The short name or NETBIOS name of the domain. Enter this value only if this is different from your regular Active Directory domain name. If this is different from your domain name (usually a shorter name), enter that name here. Contact your AD administrator about the NETBIOS name. Note that 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: • Continue to use the domain controller name that you entered • Use the domain controller name returned by the DNS query • Abort the Join Domain operation.
Use default domain admin user	Check this box to use the *Administrator* user name to join the domain

Container	Description
User Name	User ID of the domain administrator account
Password	Password of the domain administrator account

Services Control Tab

From the **Services Control** tab, you can view a service status and control (stop or start) Policy Manager services.

Figure 237 *Services Control Tab*



Service Parameters Tab

Navigate to the **Service Parameters** tab to change system parameters of the services.

Figure 238 *Policy Server Service Parameters*

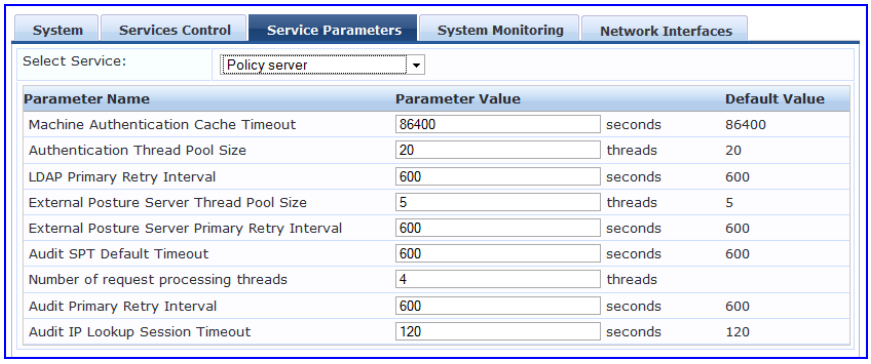


Table 135: *Service Parameters tab - Policy Server*

Service Parameter	Description
Machine Authentication Cache Timeout	This specifies the time (in seconds) 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.

Service Parameter	Description
LDAP Primary Retry Interval	Once 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.
External Posture Server Thread Pool Size	This specifies the number of threads to use for posture servers.
External Posture Server Primary Retry Interval	Once 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.
Audit Primary Retry Interval	Once a primary audit 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 IP Lookup Session Timeout	Temporary session timeout returned for a request that triggers an audit, and Policy Manager needs to lookup IP address for the MAC address of the host before proceeding with audit

Figure 239 *RADIUS Server Service Parameters*

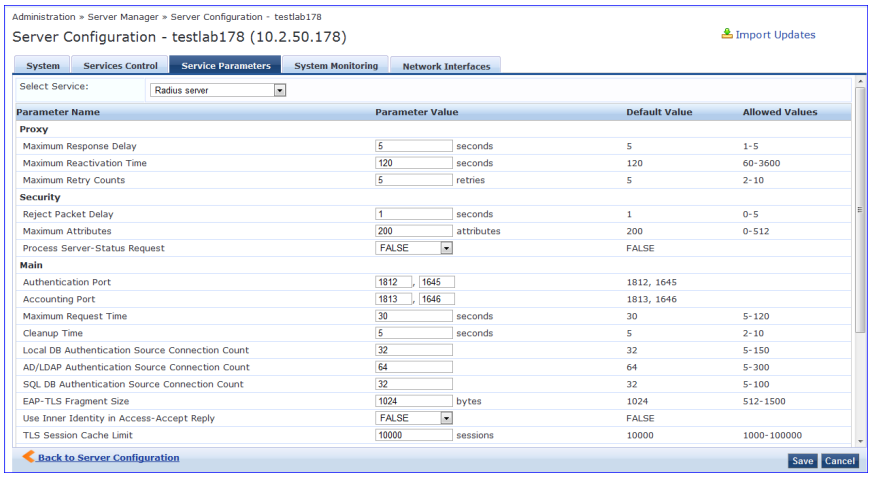


Table 136: *Service Parameters tab - Radius server*

Service Parameter	Description
Proxy	

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 a 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 DB connections opened
AD/LDAP Authentication Source Connection Count	Maximum number of AD/LDAP connections opened

Service Parameter	Description
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 • Stop Domain Service - To restart the Winbind service
Thread Pool	
Maximum Number of Threads	Maximum number of threads in the RADIUS server thread pool to process requests
Number of Initial Threads	Initial number of thread in the RADIUS server thread pool to process requests
EAP-FAST	
Master Key Expire Time	Lifetime of a generated EAP-FAST master key
Master Key Grace Time	Grace period for a 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

Service Parameter	Description
PACs are valid across cluster	Whether PACs generated by this server are valid across the cluster or not
Accounting	
Log Accounting Interim-Update Packets	Store the Interim-Update packets in session logs.

Figure 240 *TACACS+ Service Parameters*

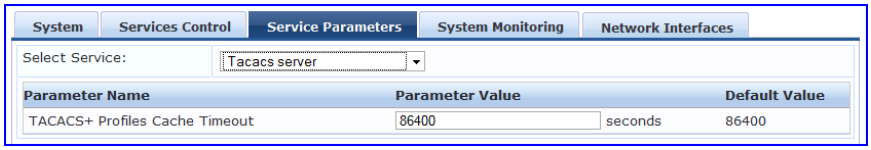


Table 137: *Service Paramters tab - TACACS server*

Service Parameter	Description
TACACS+ Profiles Cache Timeout	This specifies the time (in seconds) for which TACACS+ profile result entries are cached by Policy Manager

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 241 *ClearPass System Services Parameters*

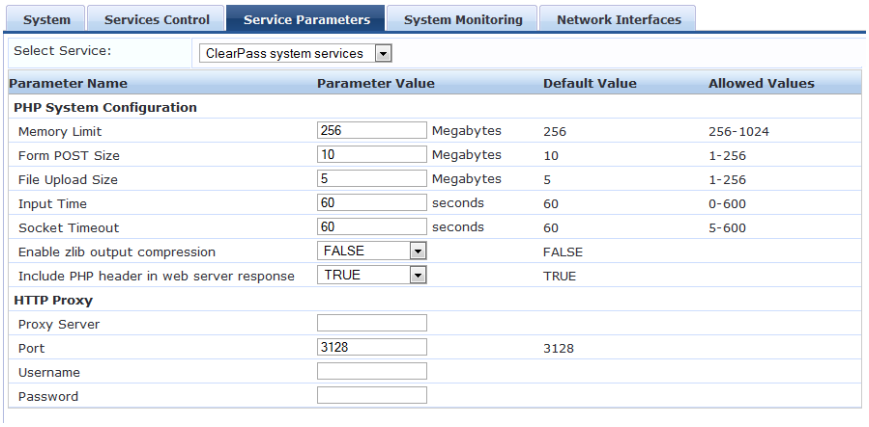


Table 138: *Service Parameters - ClearPass system services*

Service Parameter	Description
PHP System Configuration	
Memory Limit	Maximum memory that can be used by the PHP applications.

Service Parameter	Description
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

The ClearPass Network Services parameters aggregate service parameters from the following services:

- DhcpSnooper Service
- Snmp Service
- WebAuth Service
- Posture Service

Figure 242 *ClearPass Network Services Parameters*

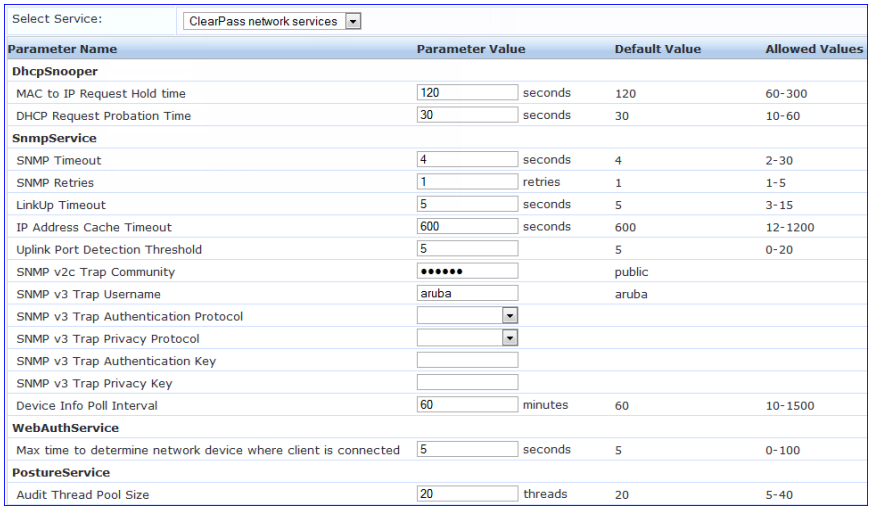


Table 139: *Service Parameters - ClearPass network services*

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)

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.
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.
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 connect 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.

Figure 243 *System Monitor Service Parameters*

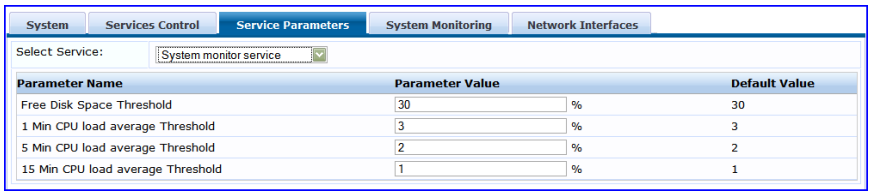


Table 140: *Services Parameters tab - System monitor service*

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.

Service Parameter	Description
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	

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.

Figure 244 *System Monitoring Tab*

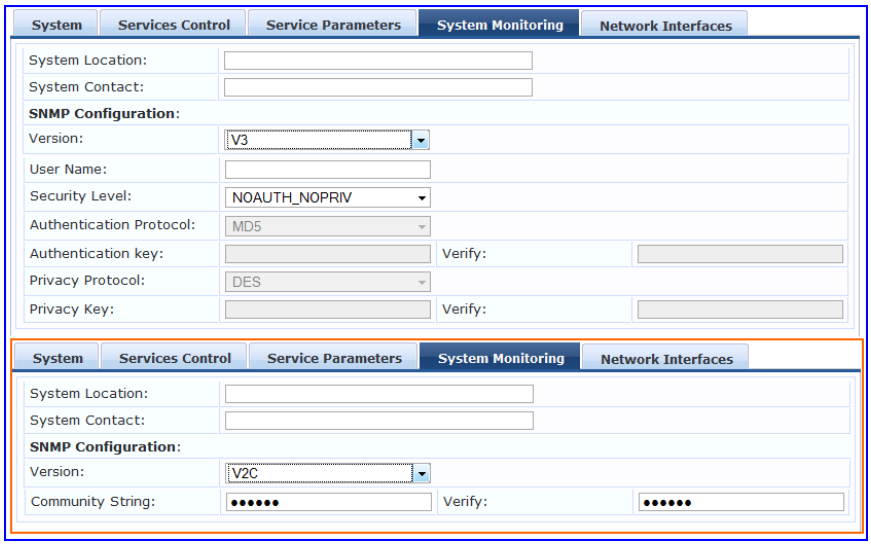


Table 141: *System Monitoring tab details*

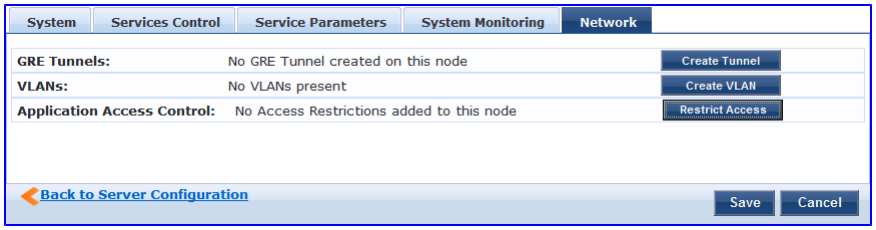
Service Parameter	Description
System Location/System Contact	Policy Manager appliance location and contact information
SNMP Configuration: Version	V1, V2C or V3
SNMP Configuration: Community String	Read community string.

Service Parameter	Description
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), 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 245 *Network Interfaces Tab*



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 246 *Creating GRE Tunnel*

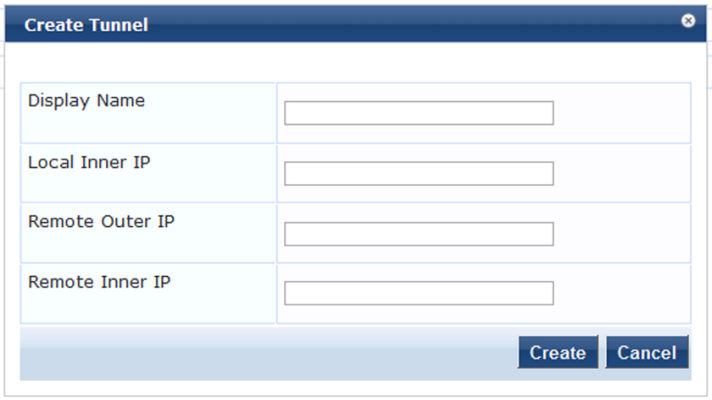


Table 142: *Creating GRE Tunnel*

Container	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 VLAN

Navigate to the **Network** tab and click **Create VLAN**.

Figure 247 *Creating VLAN*

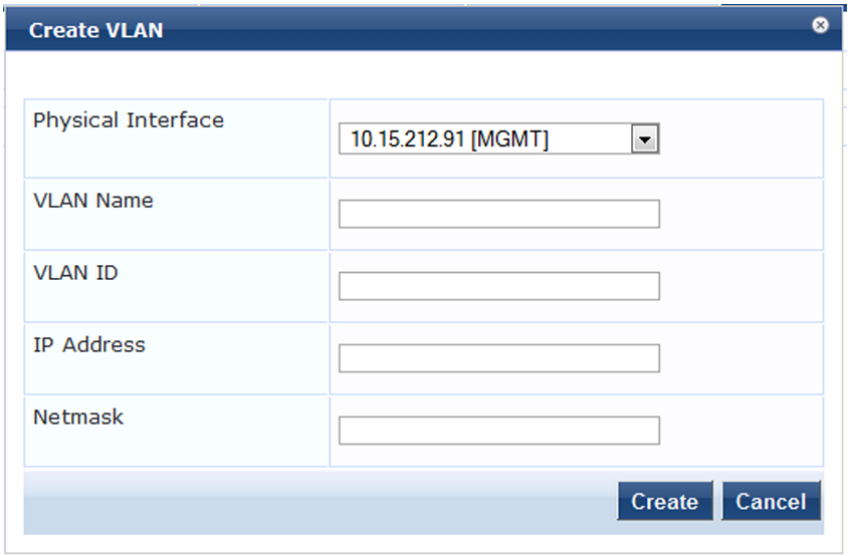


Table 143: *Creating VLAN Parameters*

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 248 *Restrict Access dialog box*

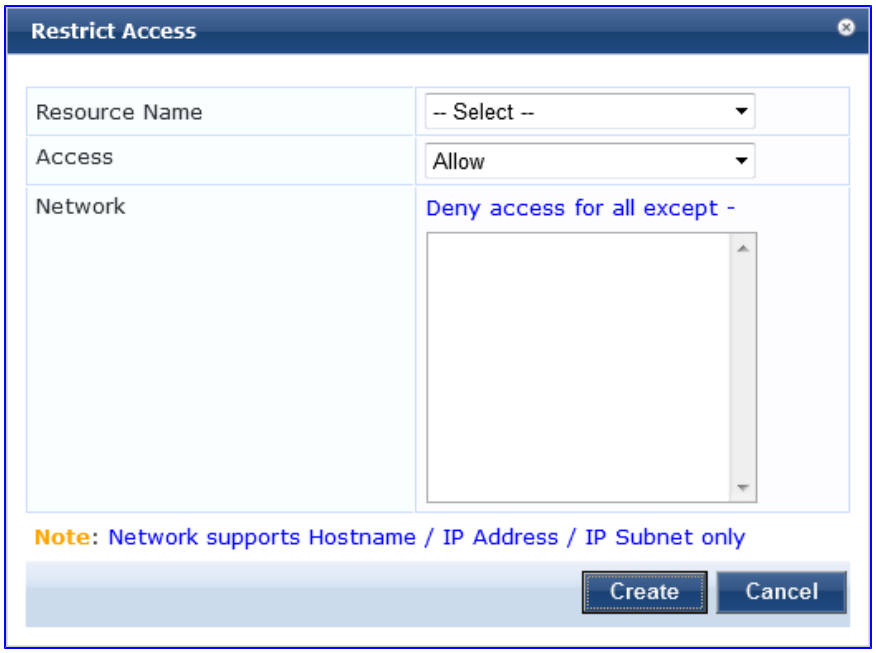


Table 144: *Restrict Access Parameters*

Parameter	Description
Resource Name	Select the applicvation you want to allow or deny access to.
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.

Log Configuration

The Policy Manager Log Configuration menu at **Administration > Server Manager > Log Configuration** provides the following interface for configuration:

Figure 249 *Log Configuration (Services Level tab)*

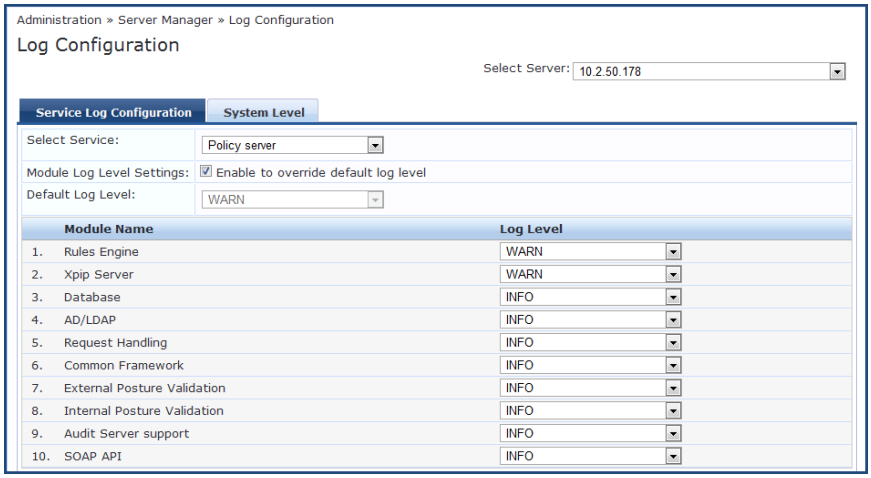


Table 145: *Log Configuration (Services Level tab)*

Container	Description
Select Server	Specify the server for which to configure logs. All nodes in the cluster appear in the drop down list.
Select Service	Specify the service for which to configure logs.
Module Log Level Settings	**Enable** this options 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.

Container	Description
Default Log Level	This drop down 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 250 *Log Configuration (System Level tab)*

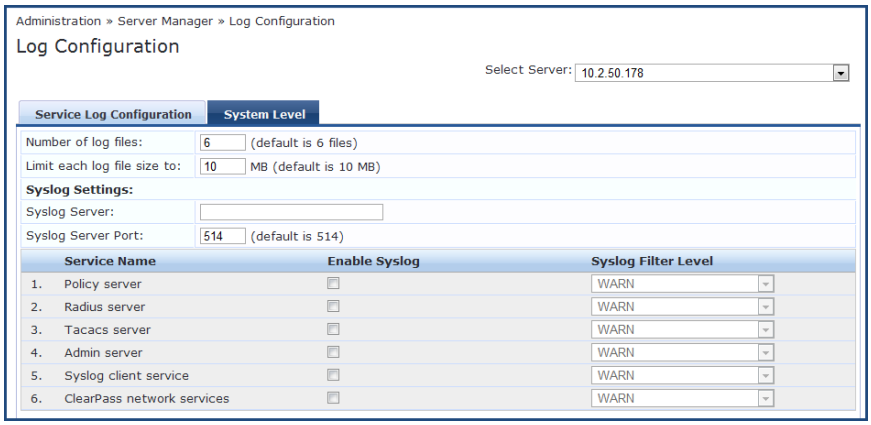


Table 146: *Log Configuration (System Level tab)*

Container	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 this 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.

Container	Description
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.

Local Shared Folders

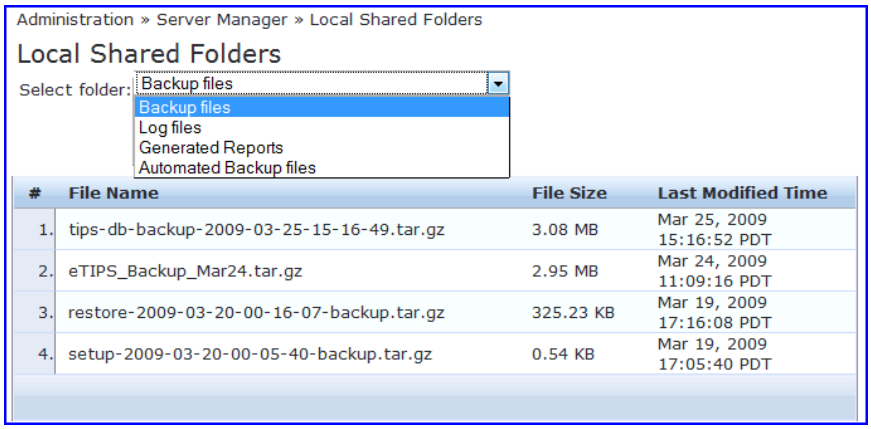
To view backup files, log files, and generated reports, navigate to **Administration > Server Manager > Local Shared Folders**.

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.

Figure 251 *Local Shared Folders*



Server and Application Licensing

The **Administration > Server Manager > Licensing** page shows all the licenses that have been activated for the entire CPPM cluster. You mist have a Dell Networking W-ClearPass Policy Manager base license for every instance of the product. You can:

- Activate a Server License
- Add an Application License
- Activate an Application License
- Update an Application License

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 252 *Licensing Page - License Summary tab*

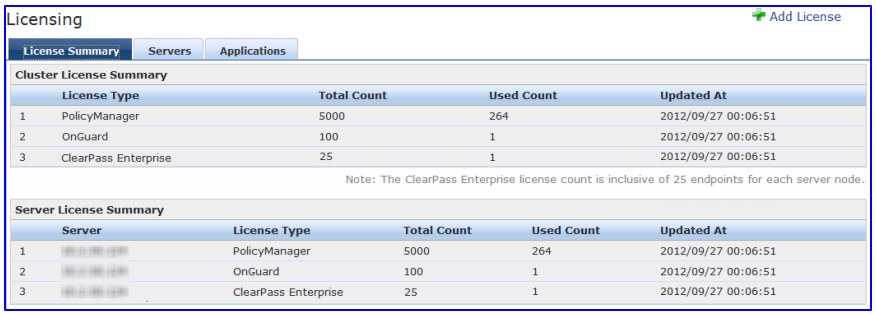
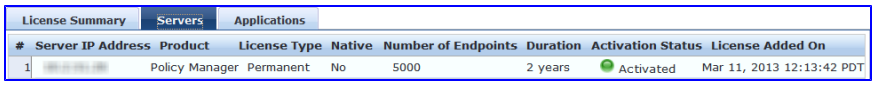


Figure 253 *Licensing Page - Servers tab*



NOTE

If the number of licenses used exceeds the number purchased, you will see a warning four months after the number is exceeded. The licenses used number is based on the daily moving average.

Activate a Server License

You need to activate a server license only once, when you first install Policy Manager on a server.

To activate a server license

1. Go to **Administration > Server Manager > Licensing**.
2. Click the **Servers** tab.

   Servers that are not activated will have a red dot in the Activation Status column.
3. Click **Activate** next to the red dot in the Activation Status column.

4. 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.

Add an Application License

You can add a license by clicking the **Add License** button on the top right portion of this page.

Figure 254 *Add License dialog box*

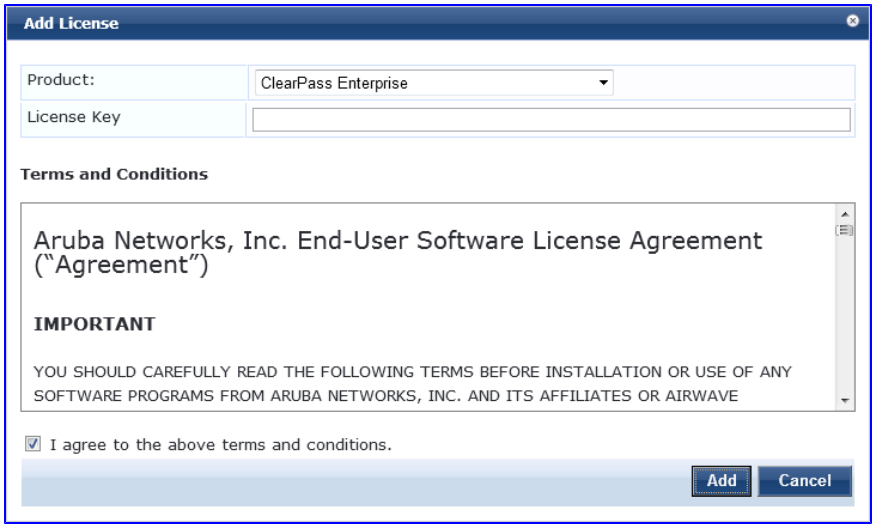


Table 147: *Add a License*

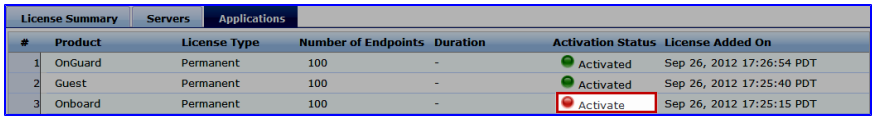
Container	Description
Product	Select a product from the drop down menu. **NOTE:** WorkSpace licenses require a valid Onboard or ClearPass Enterprise license. The default 25 endpoint ClearPass Enterprise license does not qualify.
License Key	Enter the license key for the new license.
Terms and Conditions	Read the Terms and Conditions before adding a license. You must select the I agree to the above terms and conditions check box to enable the Add button.

Activate an Application License

Adding an application license adds an Application tab on the Licensing page. Once you add or update an application license, it must be activated.

To activate a license

1. Go to **Administration > Server Manager > Licensing**.
2. Click the **Applications** tab.



3. Click **Activate** in the Activation Status column for the application yu want to activate.

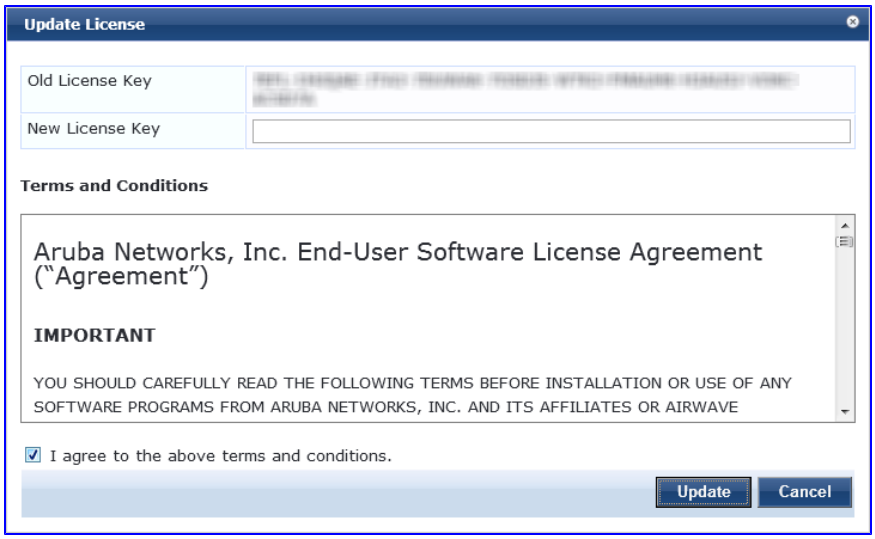
4. Click **OK**.

Update an Application License

Licenses typically require updating when they expire (for example, in the case of an evaluation license) or when capacity exceeds its licensed amount. You update an application's license by entering a new license key.

To update a license

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 dialog box appears.



4. Enter the **New License Key**.
5. Read the Terms and Conditions, then select the **I agree to the above terms and conditions** check box.
6. Click **Update**.

SNMP Trap Receivers

Policy Manager sends SNMP traps that expose the following server information:

- **System uptime.** Conveys information about how long the system is running
- **Network interface statistics [up/down].** Provides information if the network interface is up or down.
- **Process monitoring information.** Check for the processes that should be running. Maximum and minimum number of allowed instances. Sends traps if there is a change in value of maximum and minimum numbers.
- **Disk usage.**Check for disk space usage of a partition. The agent can check the amount of available disk space, and make sure it is above a set limit. The value can be in % as well. Sends traps if there is a change in the value.
- **CPU load information.** Check for unreasonable load average values. For example if 1 minute CPU load average exceeds the configured value [in percentage] then system would send the trap to the configured destination.
- **Memory usage.** Report the memory usage of the system.

The Policy Manager SNMP Trap Configuration page at Administration > External Servers > SNMP Trap Receivers provides the following interfaces for configuration:

- "Add SNMP Trap Server " on page 258
- "Import SNMP Trap Server " on page 259
- "Export all SNMP Trap Servers " on page 259

- "Export a Single SNMP Trap Server " on page 259

Figure 255 *SNMP Trap Receivers Listing Page*

Table 148: *SNMP Trap Receivers*

Container	Description
Add Trap Server	Opens the **Add Trap Server** popup.
Import Trap Server	Opens the **Import Trap Server** popup.
Export Trap Server	Opens the **Export Trap Server** popup.
Export	Opens the **Export** popup.
Delete	To delete an SNMP Trap Configuration, select it (using the check box at the left), and then click **Delete**.

Add 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 256 *Add SNMP Trap Server*

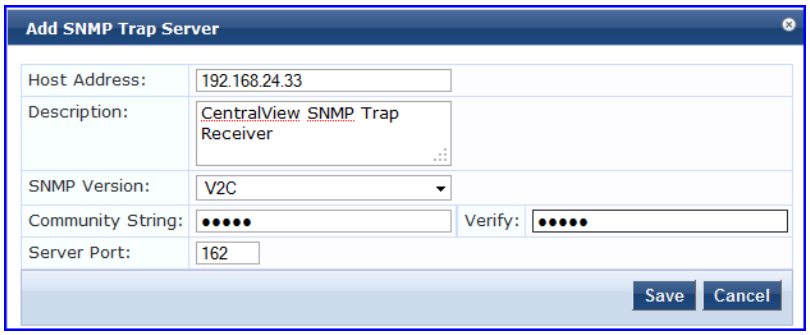


Table 149: *Add SNMP Trap Server fields*

Container	Description
Host Address	Trap destination hostname or ip address. **NOTE:** This server must have an SNMP trap receiver or trap viewer installed.

Container	Description
Description	Freeform description.
SNMP Version	V1 or V2C.
Community String /Verify Community String	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.
Save/Cancel	Click **Save** to commit the configuration or **Cancel** to dismiss.

Import 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 257 *Fig: Import SNMP Trap Server*

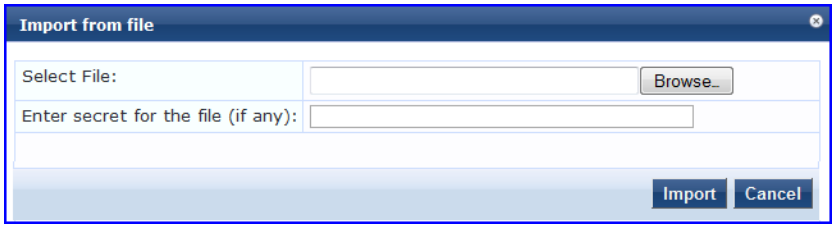


Table 150: *Import SNMP Trap Server*

Container	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.
Import/Cancel	Click **Import** to commit, or **Cancel** to dismiss the popup.

Export 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**. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the SNMP trap server configuration.

Export a Single SNMP Trap Server

To export a single SNMP trap servers, navigate to **Administration > External Servers > SNMP Trap Receivers**. Select the SNMP Trap server that you want to export (using the check box at the left) and click the **Export** button in the lower-right corner of the page. Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Syslog Targets

Policy Manager can export session data (seen in the Access Tracker), audit records (seen in the Audit Viewer) and event records (seen in the Event Viewer). 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 260
- "Import Syslog Target " on page 261
- "Export Syslog Target " on page 262
- "Export " on page 262

Figure 258 *Syslog Target Listing Page*

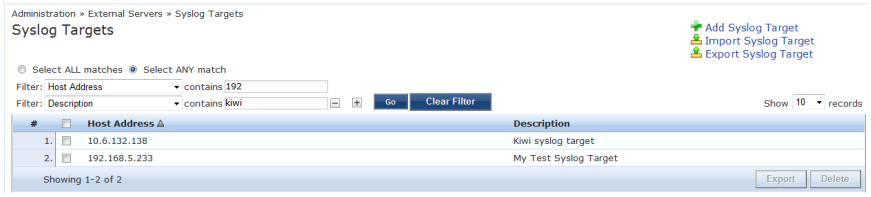


Table 151: *Syslog Target Configuration*

Container	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.
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 259 *Add Syslog Target*

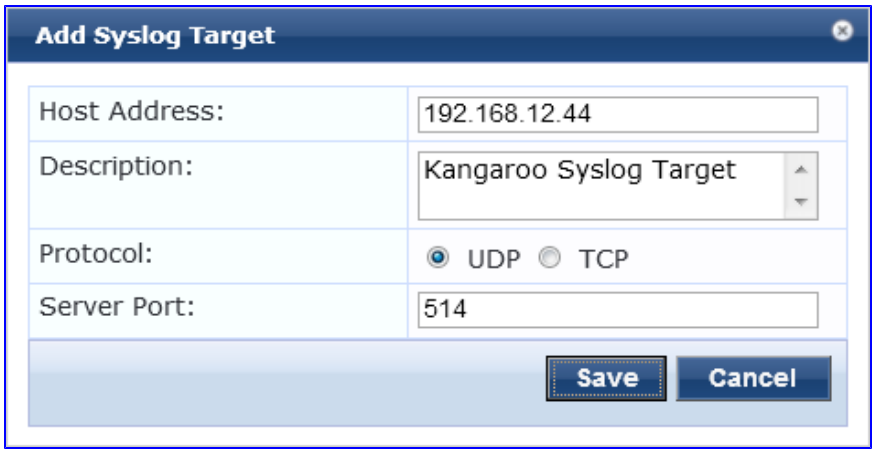


Table 152: *Add Syslog Target*

Container	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 260 *Import Syslog Target*

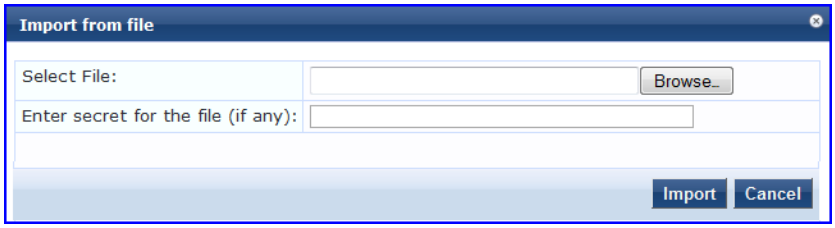


Table 153: *Import from file*

Container	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 (seen in the Access Tracker), audit records (seen in the Audit Viewer) and event records (seen in the Event Viewer). 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).

The Policy Manager Syslog Targets page at **Administration > External Servers > Syslog Targets** provides the following interfaces for configuration:

- "Add Syslog Filter " on page 263
- "Import Syslog Filter " on page 264
- "Export Syslog Filter " on page 265
- "Export " on page 265

Figure 261 *Syslog Filters Listing page*

Table 154: *Syslog Export Filters Configuration*

Container	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.

Container	Description
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.**

Add Syslog Filter

To add a Syslog Filter, navigate to **Administration > External Servers > Syslog Filters > Add Syslog Filter**. Refer to the following image.

Figure 262 *Add Syslog Filters (General tab)*

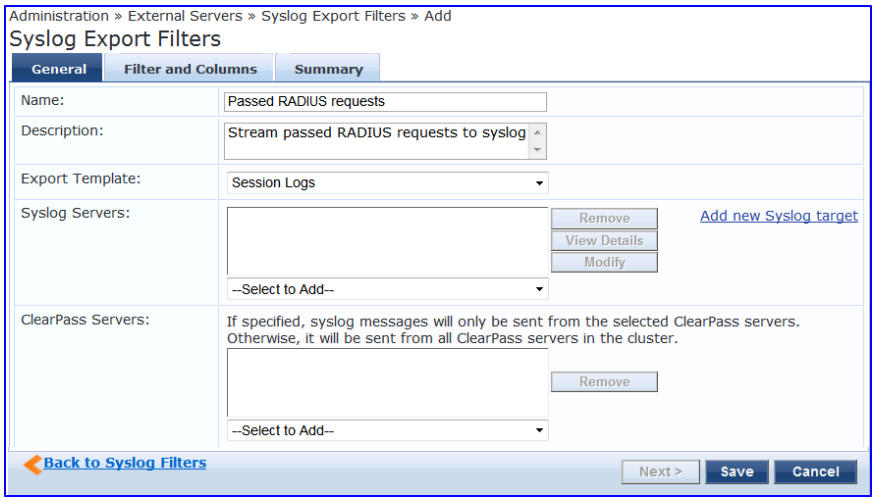


Table 155: *Syslog Export Filters Configuration*

Container	Description
Name/Description	Freeform label.
Export Template	Session Logs, Audit Records or System Events
Syslog Servers	Syslog servers define the recievers 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 recsinving 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.

If you selected Session Logs as the export termplate in the General tab, a new tab Filter and Columns appears. In this tab you specify the Data Filter (See Adding Data Filters) you want to use. 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.

This form provides two methods for configuring data filters. 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 the Custom SQL method contact Support. Support can assist you with entering the correct information in this template.

Figure 263 *Add Syslog Filters (Filter and Columns tab)*

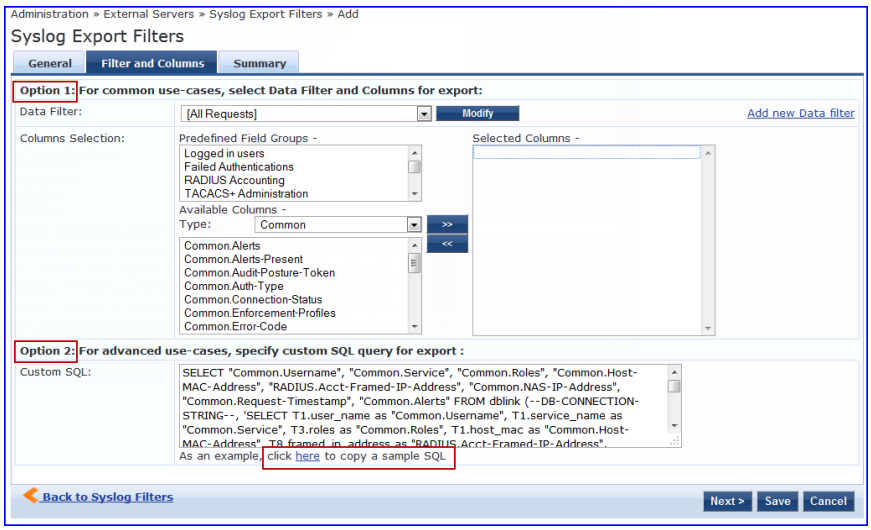


Table 156: *Add Syslog Filters (Filter and Columns tab)*

Container	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.
Columns Selection	This provides a way to limit the type of columns sent to syslog. There are Predfined 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.

Import Syslog Filter

Navigate to **Administration > External Servers > Syslog Filters > Import Syslog Filter**.

Figure 264 *Import Syslog Filter*

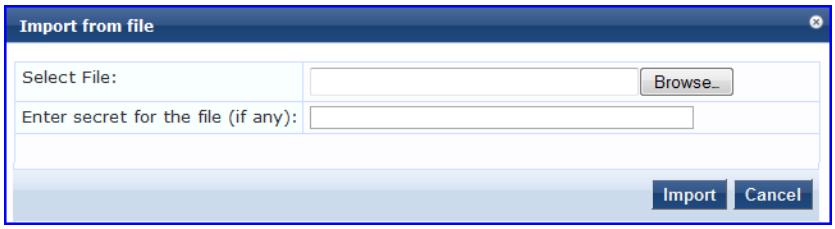


Table 157: *Import from File*

Container	Description
Select File	Browse to the Syslog Filter configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.
Import/Cancel	Click **Import** to commit, or **Cancel** to dismiss the popup.

Export Syslog Filter

Navigate to **Administration > External Servers > Syslog Filters** and select the **Export Syslog Filter** link.

The **Export Syslog Filter** link exports all configured syslog filters. Click **Export Syslog Filter**. Your browser will display its normal Save As dialog, in which to 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.

Messaging Setup

The Policy Manager Messaging Setup menu at **Administration > Server Manager > Messaging Setup** provides the following interface for configuration:

Figure 265 *Messaging Setup (SMTP Servers)*

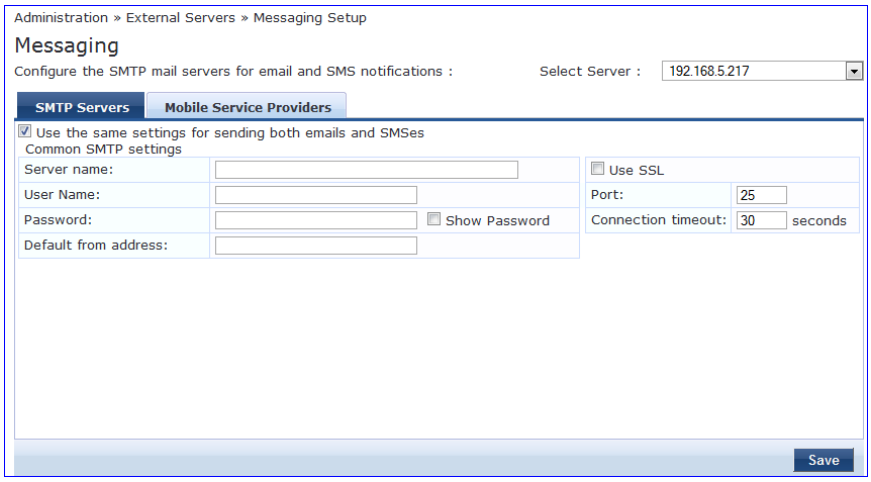


Table 158: *Messaging Setup (SMTP Servers tab)*

Container	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 266 *Messaging Setup (Mobile Service Providers tab)*

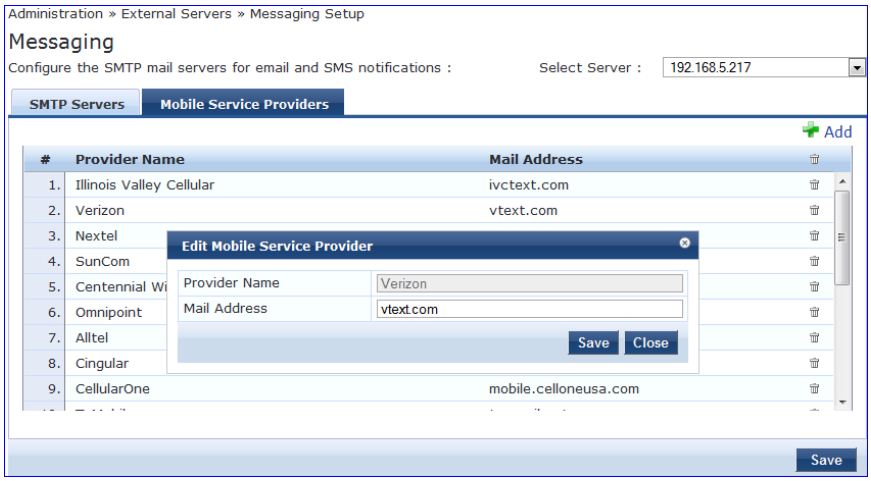


Table 159: *Messaging Setup (Mobile Service Providers tab)*

Container	Description
Add	Add a mobile service provider
Provider Name	Name of the provider
Mail Address	Domain name of the provider

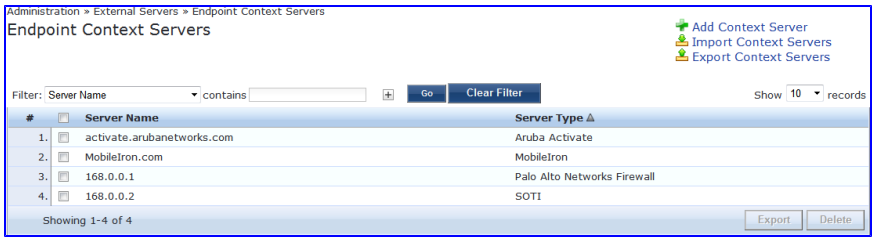
Endpoint Context Servers

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 Aurwatch, JAMF, Maas360, MobileIron, and SOTI.

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 267 *Endpoint Context Servers*



You can

- Add an endpoint context server
- Modify an endpoint context server
- Importing
- Exporting
- Delete an endpoint context server

Add an endpoint context server

- To add 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 will determine what other configuration options you will enter.
4. Enter the rest of the server configuration information. See Endpoint Context Server Configuration Details for more information.
5. Click **Save**.

Modify an endpoint context server

To modify an endpoint server

1. Go to **Administration > External Servers > Endpoint Context Servers**.
2. Click the server name .
3. Make any desired changes. See Endpoint Context Server Configuration Details 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.

To delete an endpoint context server

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**.

Endpoint Context Server Configuration Details

The following table explains each field used for configuring endpoint context servers.

Table 160: *Endpoint Context Server Configuration Fields*

Item	Description
Select Server Type	Select the type of server Several configuration options are specific to a server type.
Server Name	Enter a valid server name. This can be either a human-readable name, such as yourserver.yourcompany.com, or an IP address.
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/password	Enter the username and password (twice)for the server.
Device Filter (Aruba Activate)	This field is populated with a default regex to retrieve only the information of RAP and IAP information.
Folder Filter (Aruba Activate)	This field is set to "*" by default.
API Key (airwatch) Customer ID (JAMF) Group ID (SOTI)	Enter the values (provided by the vendor.
Application Access Key Application ID Application Version Platform ID Billing ID	If you selected MaaS360 as the server type, then enter the access key, application ID, version, platform ID, and billing ID associated with this MDM server. These values are provided by the vendor.
Palo Alto Firewall Names (Palo Alto Networks)	Enter a valid Palo Alto firewall IP address or hostname.
UserID Post URL (Palo Alto Networks)	This URL is automatically generated and used internally to post information to Palo Alto firewall. It should not need to be changed.

Server Certificate

The Policy Manager Server Certificate menu at **Administration > Certificates > Server Certificates** provides the following interfaces for configuration:

- "Create Self-Signed Certificate " on page 270
- "Create Certificate Signing Request " on page 272
- "Export Server Certificate " on page 273

- "Import Server Certificate " on page 273

Figure 268 *Server Certificates*

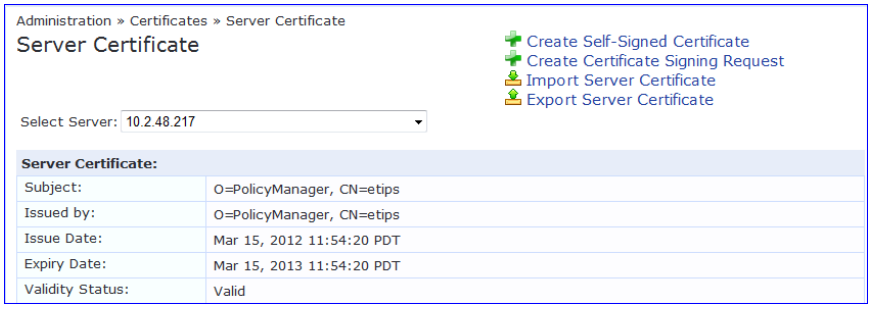


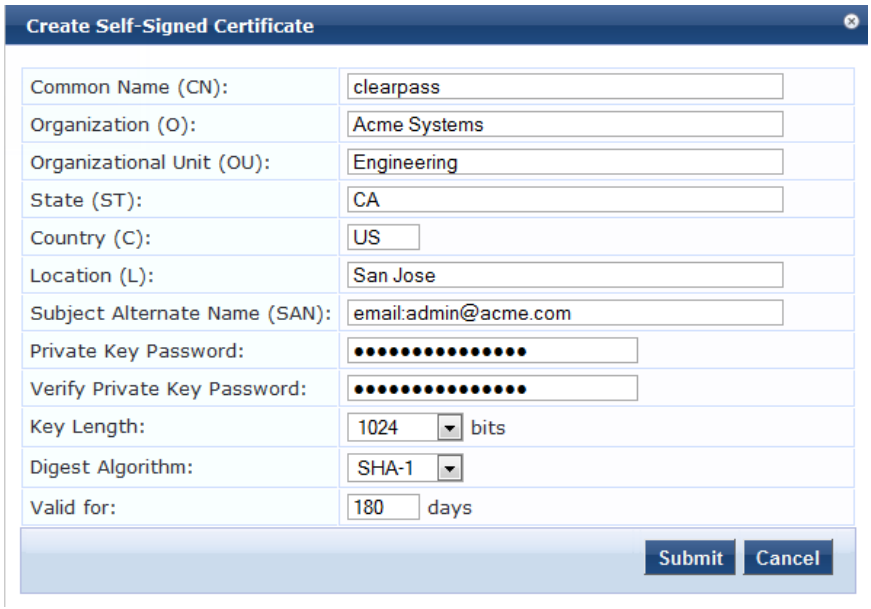
Table 161: *Server Certificate*

Container	Description
Create Self-Signed Certificate	Opens the **Create Self-Signed Certificate** popup.
Create Certificate Signing Request	Opens the **Create Certificate Signing Request** popup.
Select Server	Select a server in the cluster for server certificate operations.
Export	Opens the **Export** popup.
Import	Opens the **Import** popup.

Create Self-Signed Certificate

Navigate to **Administration > Certificates > Server Certificate** and click the **Create Self-Signed Certificate** link. This opens the **Create Self-Signed Certificate** form.

Figure 269 *Create Self-Signed Certificate*



After you click **Submit**, you will be prompted to install the self-signed certificate

Figure 270 *Generated Self Signed Certificate*

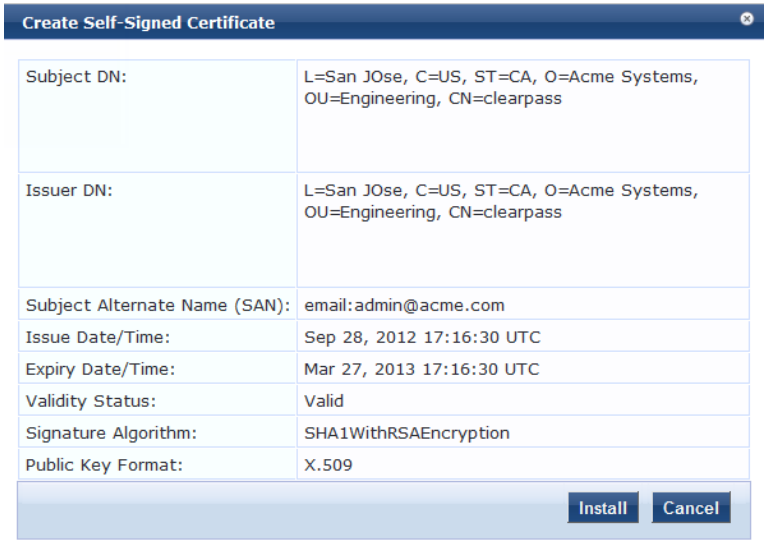


Table 162: *Create Self-Signed Certificate*

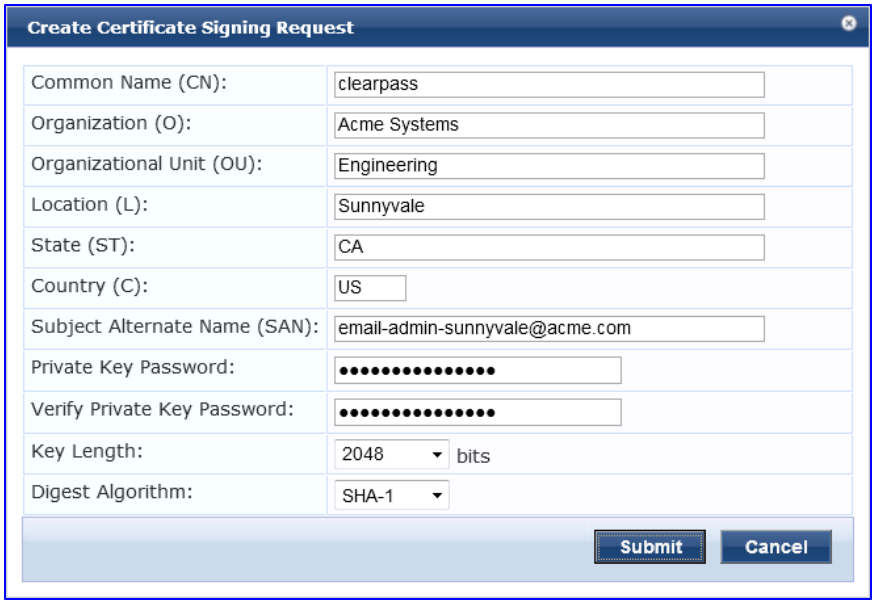
Container	Description
Common Name (CN)	Name associated with this entity. This can be a host name, IP address or other meaningful name. This field is required.
Organization (O)	Name of the organization. This field is optional.
Organizational Unit (OU)	Name of a department, division, section, or other 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 that 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	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**.
Digest Algorithm	Select message digest algorithm to use: **SHA-1**, **MD5**, and **MD2**.

Container	Description
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.

Create Certificate Signing Request

Navigate to **Administration > Certificates > Server Certificates** and click on the **Create Certificate Signing Request** link. This task creates a self-signed certificate to be signed by a CA.

Figure 271 *Create Certificate Signing Request*



A generated certificate signing request displays after you click **Submit**. Copy the certificate and paste it into the Web form as part of the enrollment process.

Figure 272 *Generated Certificate Signing Request*

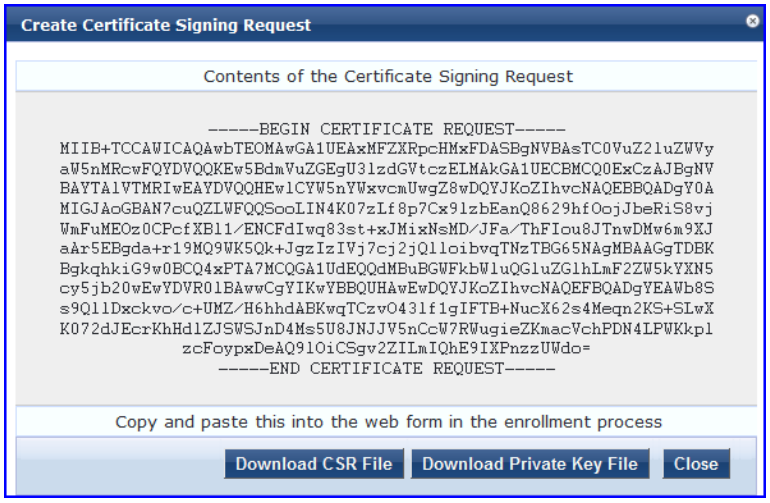


Table 163: *Create Certificate Signing Request*

Container	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 that 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	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/Cancel	On submit, Policy Manager generates a popup containing the certificate signing request for copying/pasting into the web form that you typically use to get the certificate signed by a CA. • To create a file containing the certificate signing request, click **Download CSR File**. A .csr file is downloaded to your local computer. • To download the generated private key file, click **Download Private Key File**. **NOTE:** Make sure that you save the downloaded private key in a secure place.

Export 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).

Import Server Certificate

Navigate to **Administration > Certificates > Server Certificates**, and select the **Import Server Certificate** link.

Figure 273 *Import Server Certificate*

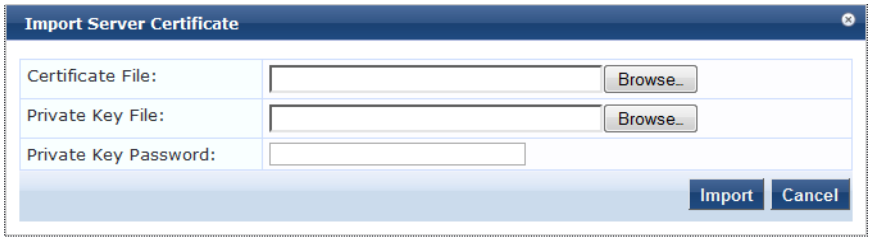


Table 164: *Import Server Certificate*

Container	Description
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.
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 274 *Certificate Trust List*

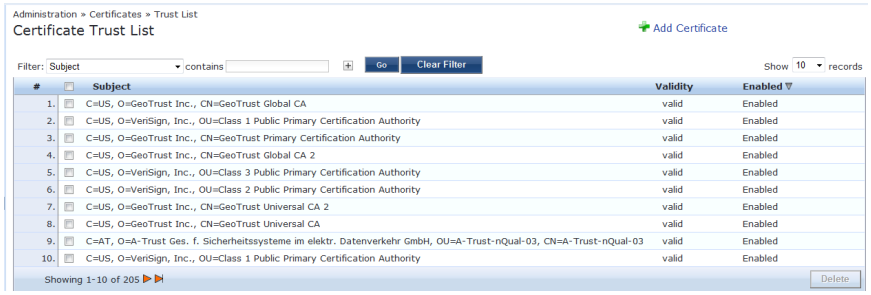


Table 165: *Certificate Trust List*

Container	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 275 *Add Certificate*

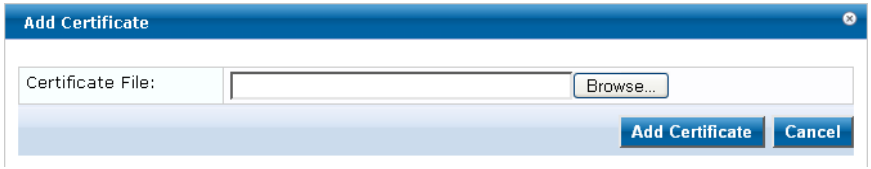


Table 166: *Add Certificate*

Container	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 276 *Revocation Lists*

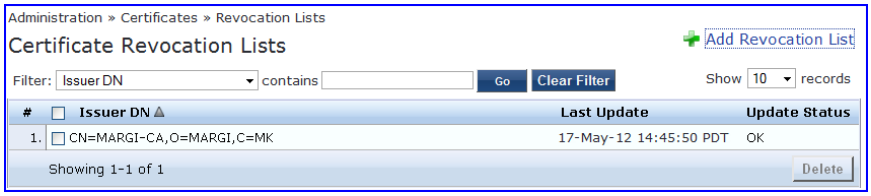


Table 167: *Revocation Lists*

Container	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.**

Add Revocation List

Navigate to **Administration > Certificates > Revocation Lists** and select the **Add Revocation List** link.

Figure 277 *Add Certificate Revocation List*

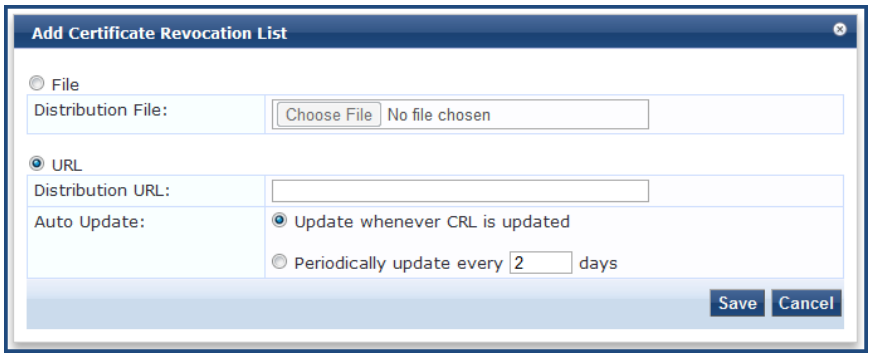


Table 168: *Add Revocation List*

Container	Description
File	File enables the Distribution File option.
Distribution File	Specify the distribution file (e.g., **C:/distribution/crl.verisign.com/Class3InternationalServer.crl**) to fetch the certificate revocation list.
URL	URL enables the Distribution URL option.
Distribution URL	Specify the distribution URL (e.g., **http://crl.verisign.com/Class3InternationalServer.crl**) to fetch the certificate revocation list.
Auto Update	Select **Update whenever CRL is updated** to update the CRL at intervals specified in the list. Or select **Periodically update** to check periodically and at the specified frequency (in days).

RADIUS Dictionaries

RADIUS dictionaries are available on the **Administration > Dictionaries > RADIUS**. This page includes the list of available vendor dictionaries.

Figure 278 *RADIUS*

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 279 *RADIUS IETF Dictionary Attributes*

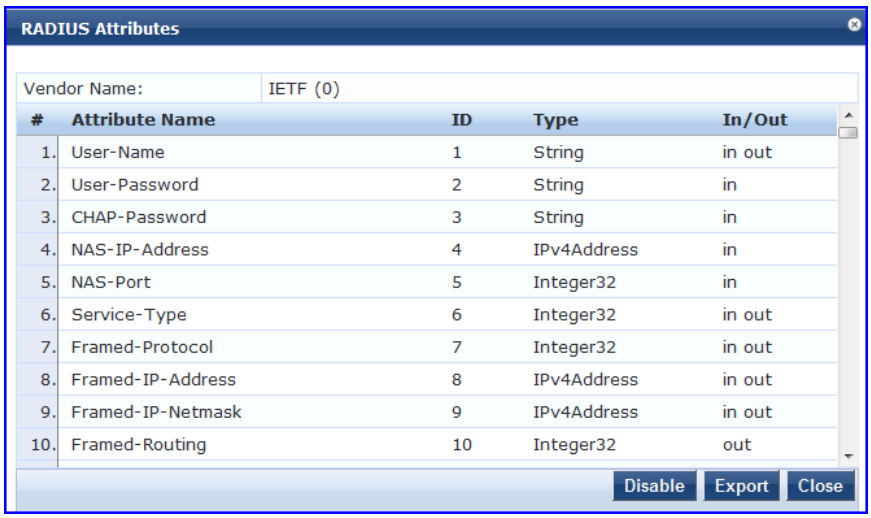


Table 169: *RADIUS Dictionary Attributes*

Container	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 280 *Import RADIUS Dictionary*

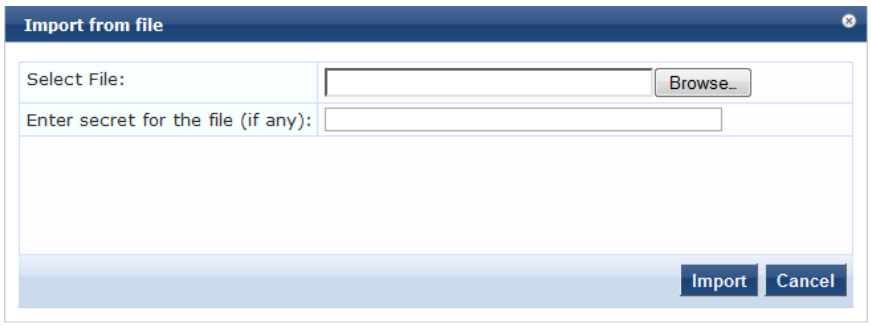


Table 170: *Import RADIUS Dictionary*

Container	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 Dictionaries

To add a new 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**.

Fig: Posture

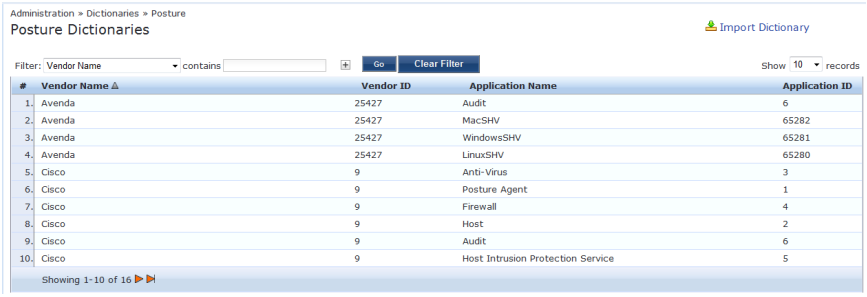


Table 171: *Posture*

Container	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 281 *Fig: Posture Dictionary*

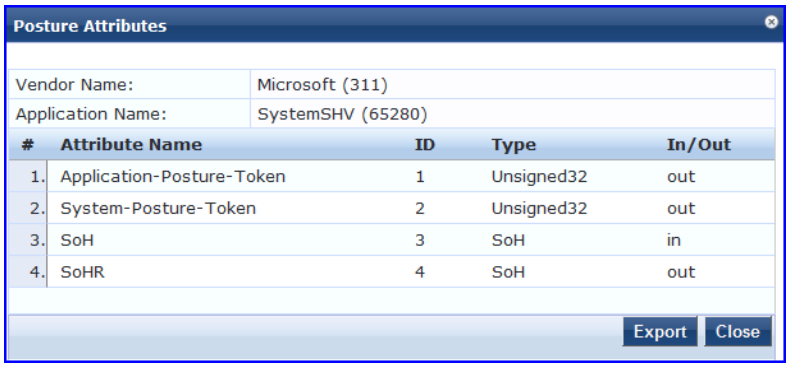


Table 172: *Posture Dictionary Attributes*

Container	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

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 282 *TACACS+ Services*

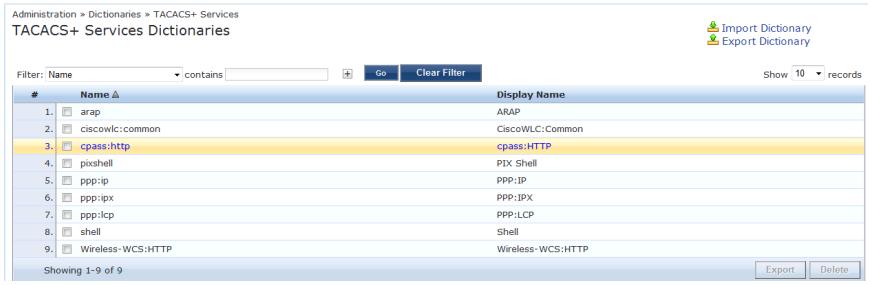


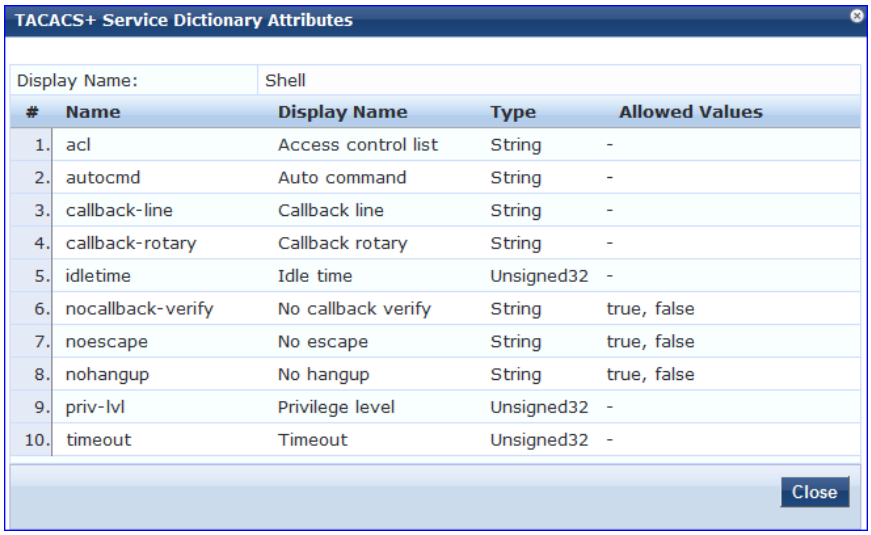
Table 173: *TACACS+ Services Dictionary*

Container	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.

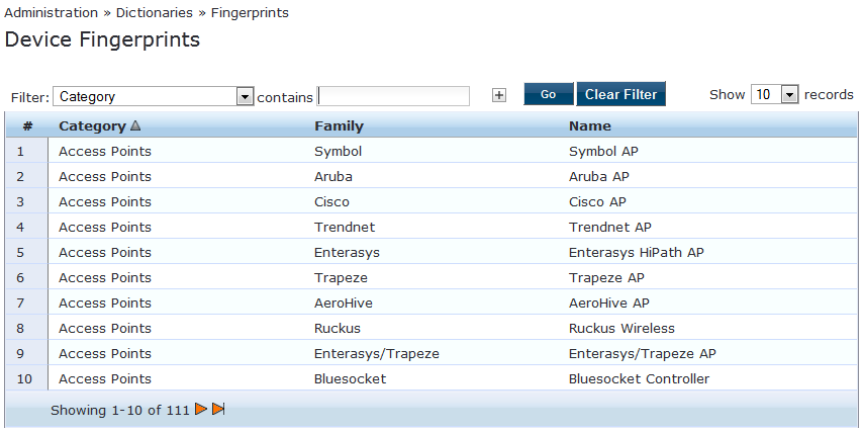
Figure 283 *Fig: Shell Service Dictionary Attributes*



Fingerprints

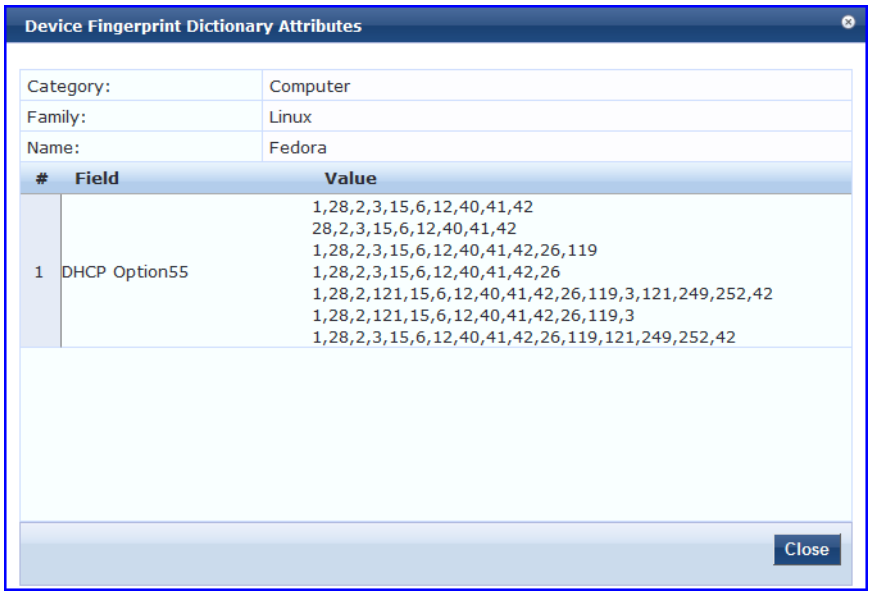
The **Device Fingerprints** table shows a listing of all the device fingerprints recognized by the Profile module. These fingerprints are updated from the Dell W-ClearPass Update Portal (See "Update Portal " on page 288 for more information.)

Figure 284 *Device Fingerprints*



You can click on a line in the Device Fingerprints list to drill down and view additional details about the category.

Figure 285 *Fig: Device Fingerprints*



Attributes

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:

- "Add Attribute " on page 281
- "Import Attributes" on page 282
- "Export Attributes" on page 282
- "Export " on page 282

Figure 286 *Attributes page*

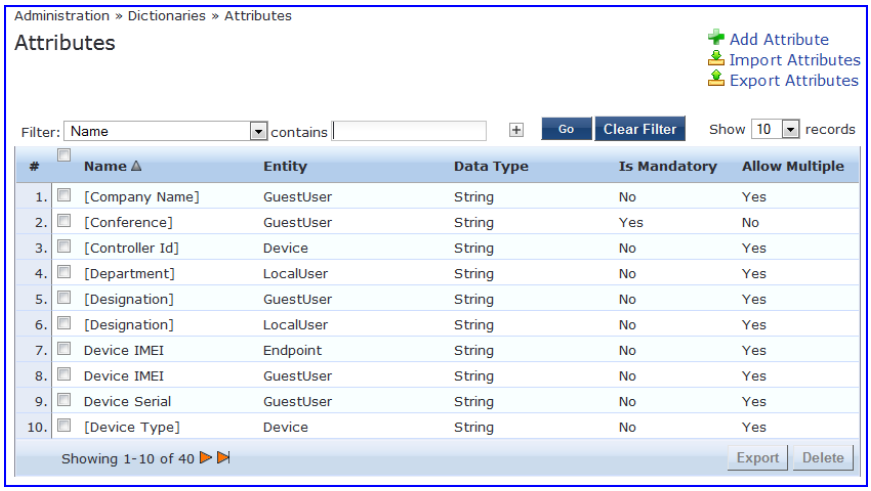


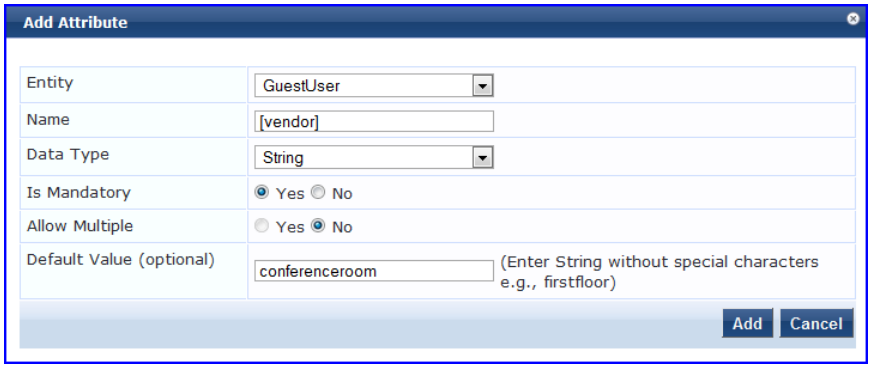
Table 174: *Attribute settings*

Container	Description
Filter	Use the drop down menu 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.

Add Attribute

To add a new Attribute dictionary, select Add Attribute in the upper right portion of the page.

Figure 287 *Add Attributes*



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 175: *Add Attribute settings*

Container	Description
Entity	Specify whether the attribute applies to a LocalUser, GuestUser, Device, or Endpoint.
Name	Enter a unique ID for this attribute.
Data Type	Specify whether the data type is string, integer, boolean, list, text, date, MAC address, or IPv4 address.
Is Mandatory	Specify whether the attribute is required for a specific entity.
Allow Multiple	Specify whether multiple attributes are allowed for an entity. Note that 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.

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 288 *Import from file*

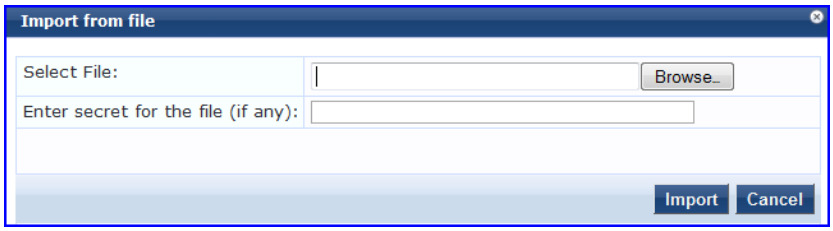


Table 176: *Import from File settings*

Container	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 exports all attributes.

The **Export Attributes** button saves the file **Attributes.zip.** The zip file has 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.

Application Dictionaries

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.

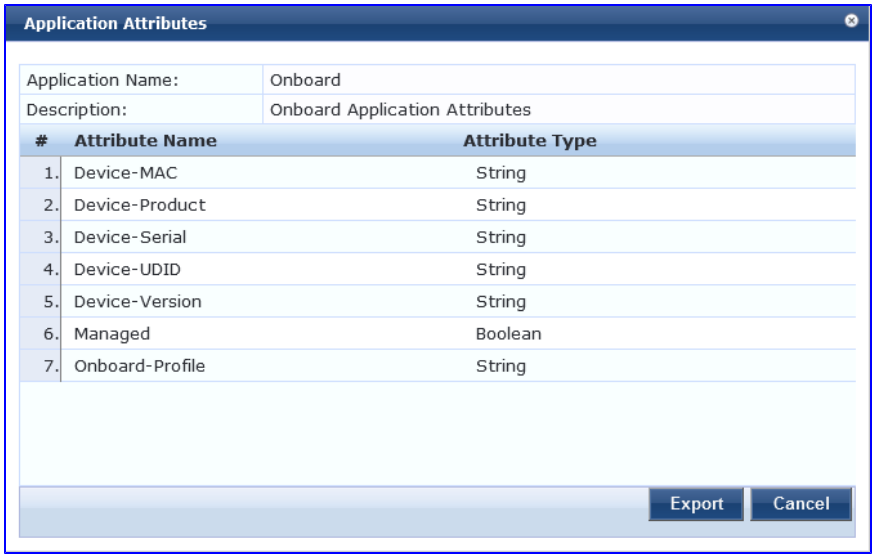
You can

- View an application dictionary
- Delete an application dictionary
- Importing
- Exporting.

View an application dictionary

To view an application dictionary

1. Go to **Administration > Dictionaries > Applications**.
2. Click the name of an application. The Application Attributes dialog box appears.



Delete an application dictionary

In general, you should have no need to delete an application dictionary. They have no effect on Policy Manager performance.

To delete an application dictionary

1. Go to **Administration > Dictionaries > Applications**.
2. Click the check box next to an application name.
3. Click **Delete**.

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 289 *OnGuard Settings*

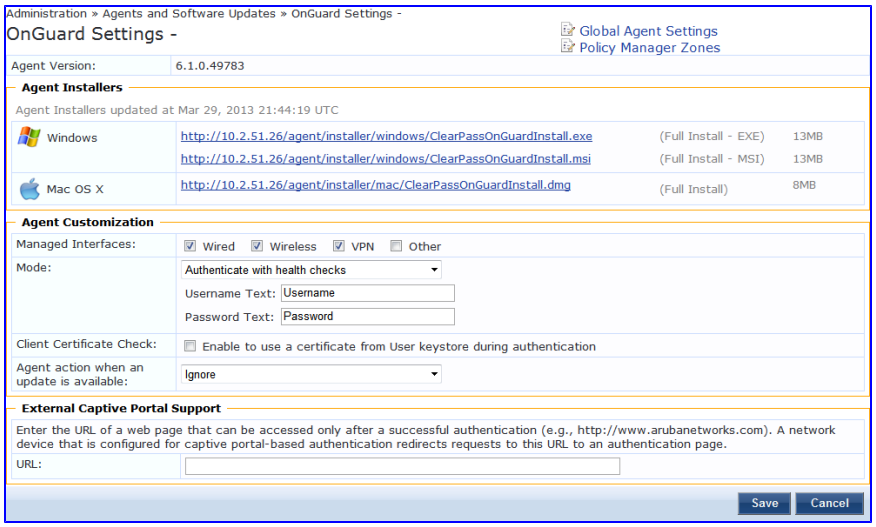


Table 177: *OnGuard Settings*

Container	Description
Global Agent Settings	Configure global parameters for OnGuard agents. Parameters include the following: • CacheCredentialsForDays : Select the number of days the user credentials should be cached on OnGuard agents. • WiredAllowedSubnets : Add a comma-separated list of IP or subnet addresses. • WirelessAllowedSubnets : Add a comma-separated list of IP or subnet addresses • KeepAliveIntervalSeconds : Add a keep alive interval for OnGuard agents • EnableClientLoadBalance : Enable this option to load balance OnGuard authentication requests across ClearPass Policy Servers in a cluster • AllowRemoteDesktopSession : Enable this option to allow OnGuard access via a Remote Desktop session. • HideLogoutButton : Enable this option to hide the Logout button. • InstallVPNComponent: Enable this option to install the OnGuard VPN component. • UseWindowsCredentials: Enable this option to allow a user's Windows credentials for authentication. • SupportEmailAddress: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	The URLs for the different agent deployment packages for Windows and Mac OS.
Managed Interfaces	Select the type of interfaces that OnGuard will manage on the endpoint.

Container	Description
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, Download Installer, Notify User.
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.

OnGuard Portal

Navigate to the **Administration > Agents and Software Updates> OnGuard Portal** page.

Click on any of the four editable sections of this page to customize the content for your enterprise:

Figure 290 *OnGuard Portal*

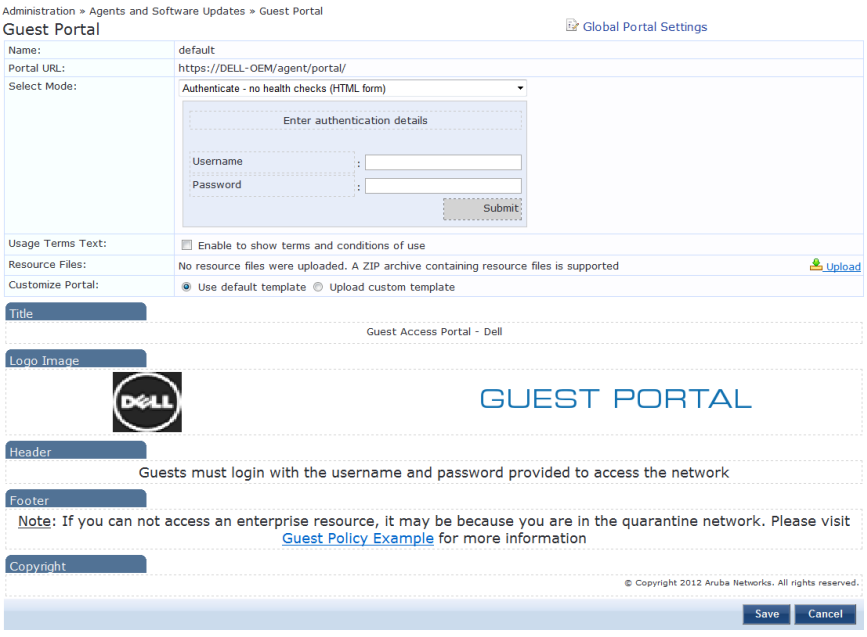


Figure 291 *OnGuard Portal parameters*

Parameter	Description
Global Portal Settings	Attribute names and value configuration for the portal. • *UsernameFormat*: Format of username sent in authentication requests. This can be used in service rules (Authentication:Full-Username attribute) to write different service rules for different portals. • *SharedSecret*: Secret shared with a Wireless Controller (for example, Xirrus Wireless Controller) when Policy Manager is configured as an external captive portal on the network device. • *ShowOriginalPageRedirectLink*: Show a link that will take the user to the original page (prior to being redirected to the captive portal).
Name	Name is 'default'.
Portal URL	This is the URL that presents the OnGuard portal page. (Note that this is automatically generated by Policy Manager).
Select Mode	Select from the following for different modes of the portal: • **Authenticate - no health validation (HTML Form)** - Policy Manager presents a simple HTML form with the username and password. Health credentials are not collected from the client. • **Authenticate - no health validation (Java Applet)** - Policy Manager presents an applet based form with the username and password. Health credentials are not collected from the client. Note that, the Java applet collects the MAC address of all interfaces on the client. In the case of a simple HTML form, Policy Manager would have to perform the extra step of DHCP snooping to collect the MAC address of the client. • **Check Health - no authentication (Java applet)** - Username/password are not collected. Health is evaluated via a Java applet. • **Authenticate with health checks (Java Applet)** - Policy Manager prompts the user for username and password, and also collects client health credentials by means of a Java applet downloaded to the page. • **Authenticate with optional health checks (Dual mode)** - User is presented with a simple HTML form. User can choose to load the Java applet by clicking on a link on this page; the java applet (dissolvable agent) also collects health information. • **No Authentication and no health checks (HTML form)** - User is presented with a simple HTML form for the username, which is hidden.
Authentication Details	Click within the Enter Authentication Details field to enter credential details. **NOTE:** This section only appears for modes that require authentication.
Username/Password label	Click on the Username/Password labels (D) to change the respective label strings.
Usage Terms Text	Select this check box to display the terms and conditions of use.

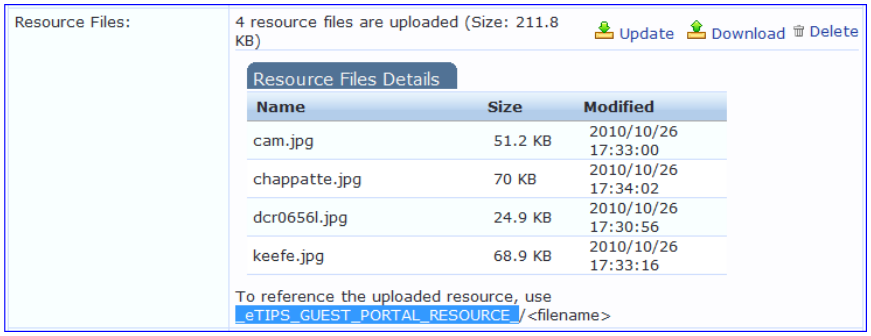
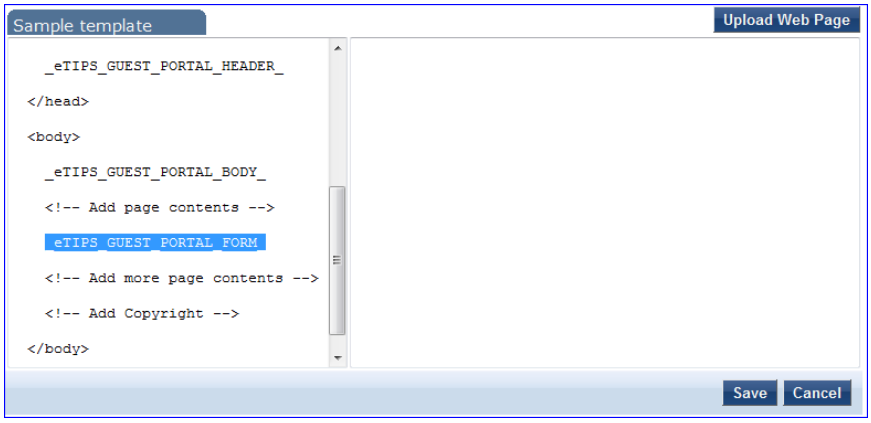
Parameter	Description
Resource Files	Click on Upload link to upload a zipped archive of resource files consisting of images, style sheets, scripts, etc. These are hosted on the Policy Manager appliance and can be referenced by prefixing the _eTIPS_GUEST_PORTAL_RESOURCE_ to the patch component. For example, if there is a file named logo.jpg in the zipped archive, refer to this resource as "_eTIPS_GUEST_PORTAL_RESOURCE_/logo.jpg" on the OnGuard portal page. After the zipped archive is successfully uploaded, a screen showing the contained files is shown: 
Customize Portal	**Use default template** to edit the different fields as described above. To import a custom HTML file to be used as the OnGuard portal, select **Upload custom template**. Note that the following macros must be present in the custom HTML template: • _eTIPS_GUEST_PORTAL_HEADER_ • _eTIPS_GUEST_PORTAL_BODY_ • _eTIPS_GUEST_PORTAL_FORM_
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.
Header Message	Click to enter text that will display in the header.
Footer Message	Click to enter text that will display in the footer.
Copyright Message	Click to enter copyright text.

Figure 292 *Custom HTML Template Upload*



Update Portal

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 ClearPass's 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 293 *Software Updates*

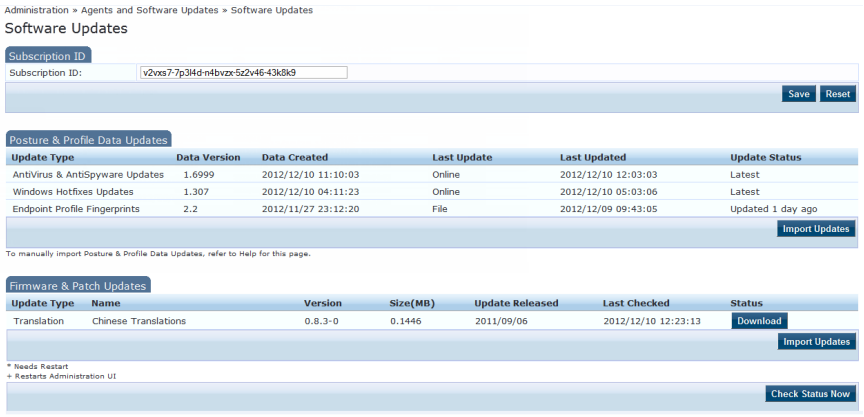


Table 178: *Software Updates*

Container	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 that this does not clear the text box.
Posture & Profile Data Updates	

Container	Description
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.arubanetworks.com/cppm/appupdate/cppm_apps_updates.zip. When prompted, enter the provided Subscription ID for the username and the password for authentication. **NOTE:** This button is enabled only on publisher node.
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 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 294 *Install Update*

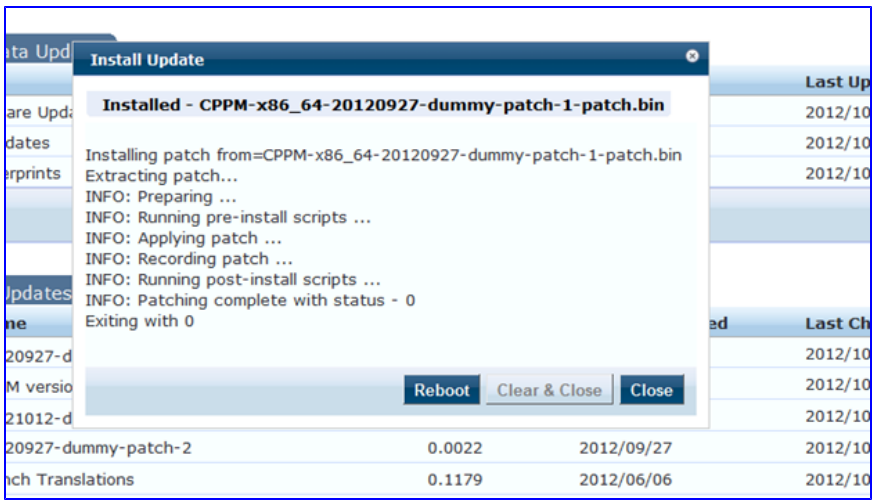


Table 179: *Install Update dialog box buttons and descriptions*

Container	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 webservice. 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 webservice, 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 an 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).

The Policy Manager command line provides commands of the following types:

Available Commands

Table 180: *Command Categories*

Command
ad auth See "Miscellaneous Commands" on page 308
ad netleave See "Miscellaneous Commands" on page 308
ad netjoin See "Miscellaneous Commands" on page 308
ad testjoin See "Miscellaneous Commands" on page 308
alias See "Miscellaneous Commands" on page 308
backup See "Miscellaneous Commands" on page 308
cluster drop-subscriber
cluster list
cluster make-publisher
cluster make-subscriber
cluster reset-database
cluster set-cluster-passwd
cluster set-local-passwd

Command
configure date
configure dns
configure hostname
configure ip
configure timezone
dump certchain See "Miscellaneous Commands" on page 308
dump logs See "Miscellaneous Commands" on page 308
dump servercert See "Miscellaneous Commands" on page 308
exit See "Miscellaneous Commands" on page 308
help See "Miscellaneous Commands" on page 308
krb auth See "Miscellaneous Commands" on page 308
krb list See "Miscellaneous Commands" on page 308
ldapsearch See "Miscellaneous Commands" on page 308
network ip
network nslookup
network ping
network traceroute
network reset
quit See "Miscellaneous Commands" on page 308
restore See "Miscellaneous Commands" on page 308
service activate
service deactivate
service list

Command
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

Removes specified subscriber node from the cluster.

Syntax

```
cluster drop-subscriber [-f] [-i <IP Address>] -s
```

Where:

Table 181: *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 182: *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 297
- "dns" on page 298
- "hostname" on page 298
- "ip" on page 298
- "timezone" on page 299

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 183: *Date Commands*

Flag/Parameter	Description
-s <ntpserver>	Optional. Synchronize time with specified NTP server.
-d <date>	Required. *Syntax:* yyyy-mm-dd
-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 184: *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

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 185: *Network IP Add 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 186: *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 187: *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 188: *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 189: *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 190: *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 191: *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 303
- "date" on page 303

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

Sets system boot image control options.

Syntax

```
system boot-image [-l] [-a <version>]
```

Where:

Table 192: *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 193: *Install-License Commands*

Flag/Parameter	Description
<license-key>	Mandatory. This is the newly issued license key.

Example

```
[appadmin]#  system install-license
```

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 194: *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.

Example

```
[appadmin]# system update
```

upgrade

Upgrades the system.

Syntax

```
system upgrade <filepath>
```

Where:

Table 195: *Upgrade Commands*

Flag/Parameter	Description
<filepath>	Required. Enter filepath, using either syntax provided in the two examples provided.

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

Authenticate the user against AD.

Syntax

```
ad auth --username=<username>
```

Where:

Table 196: *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 197: *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 198: *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 backups up the configuration to this file.

Syntax

```
backup [-f <filename>] [-L] [-P]
```

Where:

Table 199: *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 200: *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 201: *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 202: *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 203: *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 204: *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
```

restore

Restores Policy Manager configuration data from the backup file

Syntax

```
restore user@hostname:/<backup-filename> [-l] [-i] [-c|-C] [-p] [-s]
```

Where:

Table 205: *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
```

quit

Exits shell.

Syntax

```
quit
```

Example

```
[appadmin]#  quit
```

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 menu 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 menu 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 and operators in more detail.

Namespaces

There are multiple namespaces exposed in the rules editing interface. The namespaces exposed depend upon what you are editing. For example, 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.

Enumerated below are the namespaces you will find in the different rules editing contexts:

- *RADIUS Namespace* - Dictionaries in the RADIUS namespace come pre-packaged with the product. The administration interface does provide a way to add new dictionaries into the system (See "RADIUS Dictionaries " on page 276 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:IETF, RADIUS:Cisco, RADIUS:Juniper.

RADIUS namespace appears in the following editing contexts:

- Service rules: All RADIUS namespace attributes that can appear in a request (the ones marked with the IN or INOUT qualifier)
- RADIUS Enforcement profiles: All RADIUS namespace attributes that can be send back to a RADIUS client (the ones marked with the OUT or INOUT qualifier)
- Role mapping policies
- Policy simulation attributes
- Post-proxy attribute pruning rules
- Filter rules for Access Tracker and Activity Reports

- *Posture Namespace* - Dictionaries in the posture namespace come pre-packaged with the product. The administration interface does provide a way to add new dictionaries into the system (See "Posture Dictionaries " on page 278 for more information.) 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 appears in the following editing contexts:

  - Internal posture policies conditions - Attributes marked with the IN qualifier
  - Internal posture policies actions - Attributes marked with the OUT qualifier
  - Policy simulation attributes
  - Filter rules for Access Tracker and Activity Reports

- *Authorization Namespaces* - Policy Manager supports a number of 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:). They are:

  - *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.
  - *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 in the UI for administrative convenience. 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 107 for more information).
  - *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 in the UI for administrative convenience. 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 107 for more information).
  - *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 that you have 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.

- *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 that you have 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 the following editing contexts:

- Role mapping policies

- *Date Namespace* - The date namespace has three pre-defined attributes defined: Time-of-Day, Day-of-Week and Date-of-Year. Depending on the attribute selected in the UI, the operator and value fields change. For Day-of-Week, the operators supported 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 widget in the value field. The Date-of-Year attribute shows a date, month and year widget 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 (See section for more details.

  Date namespace appears in the following editing contexts:

  - Service rules
  - Role mapping policies
  - Enforcement policies
  - Filter rules for Access Tracker and Activity Reports
- *Connection Namespace* - 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. The connection namespace has the following pre-defined attributes:

Table 206: *Connection Namespace Pre-defined Attributes*

Attribute	Description
Src-IP-Address	Src-IP-Address and Src-Port are the IP address and port from which the request (RADIUS, TACACS+, etc.) originated
Src-Port	
Dest-IP-Address	Dst-IP-Address and Dst-Port are the IP address and port at which Policy Manager received the request (RADIUS, TACACS+, etc.)
Dest-Port	
Protocol	Request protocol: RADIUS, TACACS+, WebAuth
NAD-IP-Address	IP address of the network device from which the request originated
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)

Connection namespace appears in the following editing contexts:

- Service rules
- Role mapping policies

- *Authentication Namespace* - The authentication namespace can be used in role mapping policies to define roles based on what kind of authentication method was used or what the status of the authentication is. The attribute names and possible values with descriptions are shown in the table below:

Table 207: *Authentication Namespace Attributes*

Attribute Name	Values
InnerMethod	PAP CHAP MSCHAP EAP-GTC EAP-MSCHAPv2 EAP-MD5 EAP-TLS
OuterMethod	PAP CHAP MSCHAP EAP-MD5 EAP-TLS EAP-TTLS EAP-FAST EAP-PEAP
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 90).
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

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

Authentication namespace appears in the following editing contexts:

- Role mapping policies

- *Certificate Namespace* - 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). The attribute names and possible values with descriptions are shown in the table below:

Table 208: *Certificate Namespace Attributes*

Attribute Name	Values
Version	Certificate version
Serial-Number	Certificate serial number
Subject-DN, Subject-DC, Subject-UID, Subject-CN, Subject-GN, Subject-SN, Subject-C, Subject-L, Subject-ST, Subject-O, Subject-OU, Subject-emailAddress	Attributes associated with the subject (user or machine, in this case). Not all of these fields are populated in a certificate.
Issuer-DN, Issuer-DC, Issuer-UID, Issuer-CN, Issuer-GN, Issuer-SN, Issuer-C, Issuer-L, Issuer-ST, Issuer-O, Issuer-OU, Issuer-emailAddress	Attributes associated with the issuer (Certificate Authorities or the enterprise CA). Not all of these fields are populated in a certificate.
Subject-AltName-Email, Subject-AltName-DNS, Subject-AltName-URI, Subject-AltName-DirName, Subject-AltName-IPAddress, Subject-AltName-RegisterdID, Subject-AltName-msUPN	Attributes associated with the subject (user or machine, in this case) alternate name. Not all of these fields are populated in a certificate.

Certificate namespace appears in the following editing contexts:

- Role mapping policies

- *Tips Namespace* - Tips namespace has two pre-defined attributes: Role and Posture. Values are assigned to these attributes at run-time after Policy Manager evaluates role mapping and posture related policies. The value for the Role attribute is a set of roles assigned by the 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 value for the Posture attribute is one of HEALTHY, CHECKUP, TRANSITION, QUARANTINE, INFECTED or UNKNOWN. The posture value is computed after Policy Manager evaluates internal posture policies, gets posture status from posture servers or audit servers.

Tips namespace appears in the following editing contexts:

- Enforcement policies

- *Host Namespace* - Host namespace has a number of pre-defined attributes: Name, OSType, FQDN, UserAgent, CheckType, UniqueID, AgentType and InstalledSHAs. Host:Name, Host:OSType, Host:FQDN, Host:AgentType, Host:InstalledSHAs are only populated when request is originated by a Microsoft NAP-compatible agent. UserAgent and CheckType are present when Policy Manager acts as a Web authentication portal.
- *Endpoint Namespace* - Endpoint namespace has the following attributes: Disabled By, Disabled Reason, Enabled By, Enabled Reason, Info URL. Use these attributes look for attributes of authenticating endpoints (present in the Policy Manager endpoints list).
- *Device Namespace* - Device namespace has the attributes associated with the network device that originated the request. Device namespace has four pre-defined attributes: Location, OS-Version, Device-Type and Device-Vendor. Custom attributes also appear in the attribute list if they are defined as custom tags for the device. Note that these attributes can be used only if you have pre-populated the values for these attributes when a network device is configured in Policy Manager.
- *LocalUser Namespace* - LocalUser namespace has the attributes associated with the local user (resident in the Policy Manager local user database) who authenticated in this session. As the name suggests, this namespace is only applicable if a local user authenticated. LocalUser namespace has four pre-defined attributes: Phone, Email, Sponsor and Designation. Custom attributes also appear in the attribute list if they are defined as custom tags for the local user. Note that 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.
- *GuestUser Namespace* - GuestUser namespace has the attributes associated with the guest user (resident in the Policy Manager guest user database) who authenticated in this session. As the name suggests, this namespace is only applicable if a guest user authenticated. GuestUser namespace has six pre-defined attributes: Company-Name, Location, Phone, Email, Sponsor and Designation. Custom attributes also appear in the attribute list if they are defined as custom tags for the guest user. Note that 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.
- *Audit Namespace* - Dictionaries in the audit namespace come pre-packaged with the product. Audit namespace has the notation Vendor:Audit, where Vendor is the name of the Company that has defined attributes in the dictionary. An example of a dictionary in the audit namespace is: Avenda Systems:Audit or Qualys:Audit.
  - Audit namespace appears when editing post-audit rules. (See " Audit Servers " on page 180for more information.)
  - Avenda Systems:Audit namespace appears when editing post-audit rules for NESSUS and NMAP audit servers. The attribute names and possible values with descriptions are shown in the table below:

Table 209: *Audit Namespace Attributes*

Attribute Name	Values
Audit-Status	AUDIT_SUCCESS, AUDIT_INPROGRESS or AUDIT_ERROR
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

Attribute Name	Values
OS-Info	OS information string returned by NMAP
Open-Ports	The port numbers of open applications on the host

- *Tacacs Namespace* - Tacacs namespace has the attributes associated with attributes available in a TACACS+ request. Available attributes are AvendaAVPair, UserName and AuthSource.
- *Application Namespace* - Application namespace has a name attribute. This attribute is an enumerated type currently containing the following string values: Guest, Insight.

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 210: *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 107.
%{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 that you can also use any other dictionary-based attributes (or namespace attributes defined in this chapter) 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 in the UI is based on the data type of the attribute for which the operator is being used. Wherever the data type of the attribute is not known, the UI treats that attribute as a string type. The following table lists the operators presented for common attribute data types:

Table 211: *Attribute Operators*

Attribute Type	Operators
String	EQUALS, NOT_EQUALS, CONTAINS, NOT_CONTAINS, BEGINS_WITH, NOT_BEGINS_WITH, ENDS_WITH, NOT_ENDS_WITH, BELONGS_TO, NOT_BELONGS_TO, EQUALS_IGNORE_CASE, NOT_EQUALS_IGNORE_CASE, MATCHES_REGEX, NOT_MATCHES_REGEX, EXISTS, NOT_EXISTS
Integer	EQUALS, NOT_EQUALS, GREATER_THAN, GREATER_THAN_OR_EQUALS, LESS_THAN, LESS_THAN_OR_EQUALS, EXISTS, NOT_EXISTS, BELONGS_TO, NOT_BELONGS_TO
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_ANY, NOT_MATCHES_ANY, MATCHES_ALL, NOT_MATCHES_ALL, 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 the operator types:

Table 212: *Operator Types*

Operator	Description
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"`
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"`
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-"`
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"`

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.
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"`
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*`
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`
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`
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`
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`
MATCHES_ANY	For list data types, true if any of the run-time values in the list matches one of the configured values. E.g., `Tips:Role MATCHES_ANY HR,ENG,FINANCE`

Operator	Description
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_ 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.
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`.

This appendix contains listings of Dell Networking W-ClearPass Policy Manager error codes, SNMP traps, and system events.

Error Codes

The following table shows the 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
211	Client certificate not valid	Authentication failure
212	Client certificate has expired	Authentication failure

Code	Description	Type
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
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

Code	Description	Type
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
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 'net-SNMP' package to send trap notifications for the following events:

1. SNMP daemon trap events

   Trap OIDs:

   .1.3.6.1.6.3.1.1.5.1

   .1.3.6.1.6.3.1.1.5.2

2. CPPM processes stop and start events

   Trap OIDs:

   .1.3.6.1.2.1.88.2.0.2 [mteTriggerRising]

   .1.3.6.1.2.1.88.2.0.3 [mteTriggerFalling]

3. Network interface up and down events

   Trap OIDs:

   .1.3.6.1.6.3.1.1.5.3:

   .1.3.6.1.6.3.1.1.5.4:

4. Disk utilization threshold exceed events

   Trap OIDs:

   .1.3.6.1.2.1.88.2.0.2 [mteTriggerRising]

   .1.3.6.1.2.1.88.2.0.3 [mteTriggerFalling]

5. CPU load average exceed events for 1, 5 and 15 mins thresholds

   Trap OIDs:

   .1.3.6.1.2.1.88.2.0.2 [mteTriggerRising]

   .1.3.6.1.2.1.88.2.0.3 [mteTriggerFalling]

The following are the OIDs for the various trap events that are sent from CPPM.

SNMP daemon traps:

.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

Process status traps:

.1.3.6.1.4.1.2021.2.1.100.X ==> Error flag on a process status. The value will be set to 1, if the process is stopped and set to 0 if the process is running.

.1.3.6.1.4.1.2021.2.1.101.X ==> Error message on the process status. The value will contain the error message when the process is stopped and will be empty when the process is running.

.1.3.6.1.4.1.2021.2.1.2.X ==> Name of the process for which the status is reported as indicated by above trap OIDs.

In all the above trap OIDs, the value of X varies from 1 through N depending on the number of process status being checked. Details of the specific OIDs associated with the processes are listed in the next section.

Example 1

The following example shows the OIDs and the values set when Policy Server process is stopped

```
OID: .1.3.6.1.4.1.2021.2.1.100.1:
Value: INTEGER: 1:
.1.3.6.1.4.1.2021.2.1.2.1: policy_server:
```

```
.1.3.6.1.4.1.2021.2.1.101.1: No policy_server process running.:
```

Example 2

The following example shows the trap OIDs and the values set when Policy Server process is running:

```
OID: .1.3.6.1.4.1.2021.2.1.100.1:
Value: INTEGER: 0:
.1.3.6.1.4.1.2021.2.1.2.1: policy_server:
.1.3.6.1.4.1.2021.2.1.101.1:
```

CPPM Processes and OIDs

The following is a list of monitored CPPM processes and the corresponding OID list associated with these processes:

.1.3.6.1.4.1.2021.2.1.2.1: policy_server: ==> Policy Server Module

.1.3.6.1.4.1.2021.2.1.2.2: TACACSServer: ==> TACACS Server module

.1.3.6.1.4.1.2021.2.1.2.3: londiste: ==> Cluster operation process

.1.3.6.1.4.1.2021.2.1.2.4: radiusd: ==> Radius server

.1.3.6.1.4.1.2021.2.1.2.5: launch-dbcn-dae: ==> Database change notification module

.1.3.6.1.4.1.2021.2.1.2.6: frontend-tomcat: ==> Administration UI instance

.1.3.6.1.4.1.2021.2.1.2.7: backend-tomcat: ==> System auxiliary service

.1.3.6.1.4.1.2021.2.1.2.8: snmpd: ==> net-SNMP daemon

.1.3.6.1.4.1.2021.2.1.2.9: launch-async-ne: ==> Asynchronous network services

.1.3.6.1.4.1.2021.2.1.2.10: winbindd: ==> Domain services

.1.3.6.1.4.1.2021.2.1.2.11: launch-battery: ==> Multi-master cache

CPU Load Average Traps

.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

.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

.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

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

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 both the cases, 'ifIndex' value is set to 2 for management interface and 3 for the data port interface.

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 333 section for the list of available service names.

Admin UI Events

Critical Events

“Admin UI”, “ERROR” “Email Failed”, “Sending email failed”

“Admin UI”, “ERROR” “SMS Failed”, “Sending SMS failed”

“Admin UI”, “WARN”, “Login Failed”, “User:<X>”

"Admin UI", "WARN", "Login Failed", description

Info Events

"Admin UI", "INFO", "Logged out"

"Admin UI", "INFO", "Session destroyed"

"Admin UI", "INFO", "Logged in", description

"Admin UI", "INFO", "Clear Authentication Cache", “Cache is cleared for authentication source <X>"

"Admin UI", "INFO", "Clear Blacklist User Cache", “Blacklist Users cache is cleared for authentication source <X>"

"Admin UI", "INFO", "Server Certificate", "Subject:<X>“, "Updated"

"Admin UI", "INFO", "Updated Nessus Plugins"

"Install Update", "INFO", "Installing Update", "File: <X>", "Success"

"Admin UI", “INFO” “Email Successful”, “Sending email succeeded”

"Admin UI", “INFO” “SMS Successful”, “Sending SMS succeeded”

Admin Server Events

Info Events

“Admin server”, “INFO”, “Performed action start on Admin server”

Async Service Events

Info Events

“Async DB write service”, “INFO”, “Performed action start on Async DB write service”

“Multi-master cache”, “INFO”, “Performed action start on Multi-master cache”

“Async netd service”, “INFO”, “Performed action start on Async netd service”

ClearPass/Domain Controller Events

Critical Events

“netleave”, “ERROR”, “Failed to remove <HOSTNAME> from the domain <DOMAIN_NAME>”

“netjoin”, “WARN”, “configuration”, “<HOSTNAME> failed to join the domain <DOMAIN NAME> with domain controller as <DOMAIN CONTROLLER>”

Info Events

“Netjoin”, “INFO”, "<HOSTNAME> joined the domain <REALM>"

“Netjoin”, “INFO”, “<HOSTNAME> removed from the domain <DOMAIN_NAME>“

ClearPass System Configuration Events

Critical Events

“DNS”, “ERROR”, “Failed configure DNS servers = <X>”

“datetime”, “ERROR”, “Failed to change system datetime.”

“hostname”, “ERROR”, “Setting hostname to <X> failed”

“ipaddress”, “ERROR”, “Testing cluster node connectivity failed”

“System TimeCheck “, “ WARN ,” , “Restarting CPPM services as the system detected time drift , Current system time= 2013-07-27 17:00:01, System time 5 mins back = 2013-01-25 16:55:01”

Info Events

“Cluster”, “INFO”, “Setup”, “Database initialized”

“hostname”, “INFO”, “configuration”, “Hostname set to <X>”

“ipaddress”, “INFO”, “configuration”, Management port information updated to - IpAddress = <X>, Netmask = <X>, Gateway = <X>”

“IpAddress”, “INFO”, "Data port information updated to - IpAddress = <X>, Netmask = <Y>, Gateway = <Z>"

“DNS”, “INFO”, “configuration”, “Successfully configured DNS servers - <X>”

“Time Config”, “INFO”, “Remote Time Server”, “Old List: <X>\nNew List: <Y>”

“timezone”, “INFO”, “configuration”, “”

“datetime”, “INFO”, “configuration”, “Successfully changed system datetime.\nOld time was <X>”

ClearPass Update Events

Critical Events

“Install Update”, “ERROR”, “Installing Update”, “File: <X>”, “Failed with exit status - <Y>”

“ClearPass Firmware Update Checker”, “ERROR”, “Firmware Update Checker”, “No subscription ID was supplied. To find new plugins, you must provide your subscription ID in the application configuration”

Info Events

“ClearPass Updater”, “INFO”, “Hotfixes Updates”, “Updated Hotfixes from File”

“ClearPass Updater”, “INFO”, “Fingerprints Updates”, “Updated fingerprints from File”

“ClearPass Updater”, “INFO”, “Updated AV/AS from ClearPass Portal (Online)”

“ClearPass Updater”, “INFO”,” Updated Hotfixes from ClearPass Portal (Online)”

Cluster Events

Critical Events

“Cluster”, “ERROR”, “SetupSubscriber”, “Failed to add subscriber node with management IP=<IP>“

Info Events

"AddNode", “INFO”, "Added subscriber node with management IP=<IP>"

"DropNode", “INFO”, "Dropping node with management IP=<IP>, hostname=<Hostname>"

Command Line Events

Info Events

"Command Line”, “INFO”, “User:appadmin"

DB Replication Services Events

Info Events

"DB replication service”, “INFO”, “Performed action start on DB replication service”

"DB replication service”, “INFO”, “Performed action stop on DB replication service”

“DB change notification server”, “INFO”, “Performed action start on DB change notification server”

“DB replication service”, “INFO”, “Performed action start on DB replication service”

Licensing Events

Critical Events

“Admin UI”, “WARN”, “Activation Failed”, “Action Status: This Activation Request Token is already in use by another instance\nProduct Name: Policy Manager\nLicense Type: <X>\nUser Count: <Y>”

Info Events

“Admin UI”, “INFO”, “Add License”, “Product Name: Policy Manager\nLicense Type: <X>\nUser Count: <Y>”

Policy Server Events

Info Events

“Policy Server”, “INFO”, “Performed action start on Policy server”

“Policy Server”, “INFO”, “Performed action stop on Policy server”

RADIUS/TACACS+ Server Events

Critical Events

“TACACSServer”, “ERROR”, “Request”, “Nad Ip=<X> not configured”

“RADIUS”, “WARN”, “Authentication”, “Ignoring request from unknown client <IP>:<PORT>”

“RADIUS”, “ERROR”, “Authentication”, “Received packet from <IP> with invalid Message-Authenticator! (Shared secret is incorrect.)”

“RADIUS”, “ERROR”, “Received Accounting-Response packet from client <IP Address> port 1813 with invalid signature (err=2)! (Shared secret is incorrect.)”

“RADIUS”, “ERROR”, “Received Access-Accept packet from client <IP Address> port 1812 with invalid signature (err=2)! (Shared secret is incorrect.)”

Info Events

“RADIUS”, “INFO”, “Performed action start on Radius server”

“RADIUS”, “INFO”, “Performed action restart on Radius server

“TACACS server”, “INFO”, “Performed action start on TACACS server”

“TACACS server”, “INFO”, “Performed action stop on TACACS server”

SNMP Events

Critical Events

“SNMPService”, “ERROR”, “ReadDeviceInfo”, “SNMP GET failed for device <X> with error=No response received\nReading sysObjectId failed for device=<X>\nReading switch initialization info failed for <X>”

"SNMPService","ERROR", "Error fetching table snmpTargetAddr. Request timed out. Error reading SNMP target table for NAD=10.1.1.1 Maybe SNMP target address table is not supported by device? Allow NAD update. SNMP GET failed for device 10.1.1.1 with error=No response received Reading sysObjectId failed for device=10.1.1.1 Reading switch initialization info failed for 10.1.1.1”

Info Events

“SNMPService”, “INFO”, “Device information not read for <Ip Address> since no traps are configured to this node”

Support Shell Events

Info Events

“Support Shell” , “INFO”, “User:arubasupport”

System Auxiliary Service Events

Info Events

“System auxiliary service”, “INFO”, “Performed action start on System auxiliary service”

System Monitor Events

Critical Events

“Sysmon”, “ERROR”, “System”, “System is running with low memory. Available memory = <X>%”

“Sysmon”, “ERROR”, “System”, “System is running with low disk space. Available disk space = <X>%”

“System TimeCheck”, “WARN”, “Restart Services”, “Restarting CPPM services as the system detected time drift. Current system time= <X>, System time 5 mins back = <Y>”

Info Events

“<Service Name>”, “INFO”, “restart”, “Performed action restart on <Service Name>”

“SYSTEM”, “INFO”, “<X> restarted”, “System monitor restarted <X>, as it seemed to have stopped abruptly”

"SYSTEM", "ERROR", "Updating CRLs failed", "Could not retrieve CRL from <URL>."

“System monitor service”, “INFO”, “Performed action start on System monitor service”

"Shutdown” “INFO” system "System is shutting down" Success

Service Names

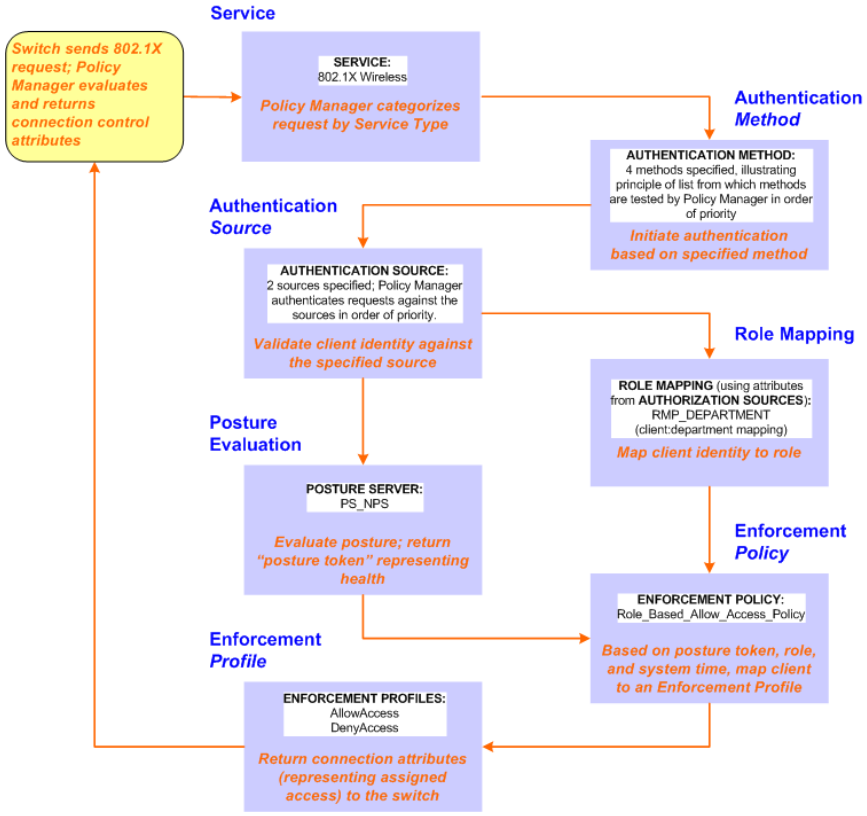
- AirGroup notification service
- Async DB write service
- Async network services
- DB change notification server
- DB replication service
- Micros Fidelio FIAS
- Multi-master cache
- Policy server
- RADIUS server
- System auxiliary services
- System monitor service
- TACACS server
- Virtual IP service
- [YOURSERVERNAME] Domain service

This appendix contains several specific Dell Networking W-ClearPass Policy Manager use cases. Each one explains what it is typically used for, and then describes how to configure Policy Manager for that use case.

802.1x Wireless Use Case

The basic Policy Manager Use Case configures a Policy Manager Service to identify and evaluate an 802.1X request from a user logging into a Wireless Access Device. The following image illustrates the flow of control for this Service.

Figure 295 *Flow of Control, Basic 802.1X Configuration Use Case*



Configuring the Service

Follow the steps below to configure this basic 802.1X service:

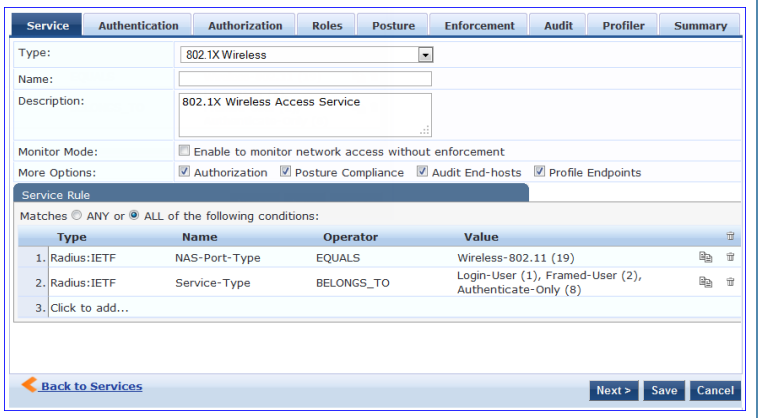
1. Create the Service

   The following table provides the model for information presented in Use Cases, which assume the reader's ability to extrapolate from a sequence of navigational instructions (left column) and settings (in summary form in the right column) at each step. Below the table, we call attention to any fields or functions that may not have an immediately obvious meaning.

   Policy Manager ships with fourteen preconfigured Services. In this Use Case, you select a Service that supports 802.1X wireless requests.

Table 213: *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

Navigation	Settings
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **802.1X Wireless** > • **Name/Description** (freeform) > • Upon completion, click **Next** (to Authentication)	

The following fields deserve special mention:

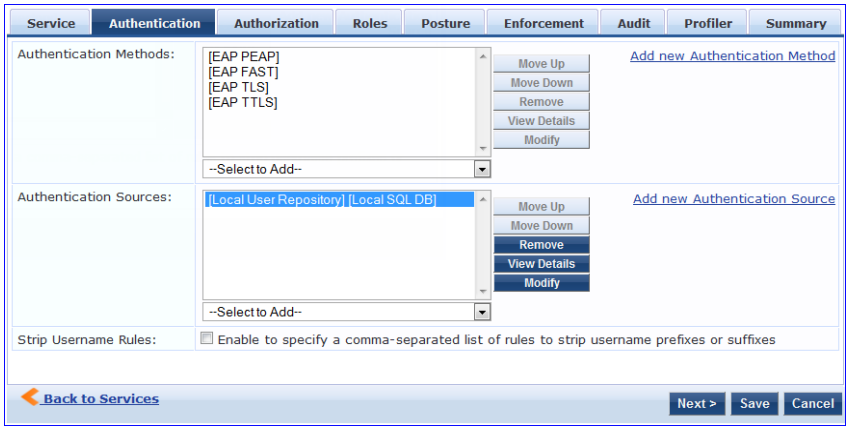
- **Monitor Mode:** Optionally, check here to allow handshakes to occur (for monitoring purposes), but without enforcement.
- **Service Categorization Rule:** For purposes of this Use Case, accept the preconfigured Service Categorization Rules for this Type.

2. Configure Authentication.

   Follow the instructions to select **[EAP FAST]**, one of the pre-configured Policy Manager Authentication Methods, and **Active Directory Authentication Source (AD)**, an external Authentication Source within your existing enterprise.

Policy Manager fetches attributes used for role mapping from the Authorization Sources (that are associated with the authentication source). In this example, the authentication and authorization source are one and the same.

Table 214: *Configure Authentication Navigation and Settings*

Navigation	Settings
Select an Authentication Method and an Active Directory server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (Select a method from the drop-down list) • **Add** > • **Sources** (**Select** drop-down list): [Local User Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB] [Guest Device Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] [Onboard Devices Repository] [Local SQL DB] > [Admin User Repository] [Local SQL DB] > AmigoPod AD [Active Directory> • **Add** > • Upon completion, **Next** (to configure Authorization)	

The following field deserves special mention:

- **Strip Username Rules:** Optionally, check here to pre-process the user name (to remove prefixes and suffixes) before sending it to the authentication source.

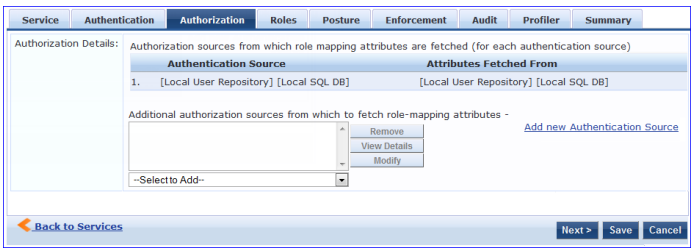
NOTE

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 215: *802.1X - Configure Authorization Navigation and Settings*

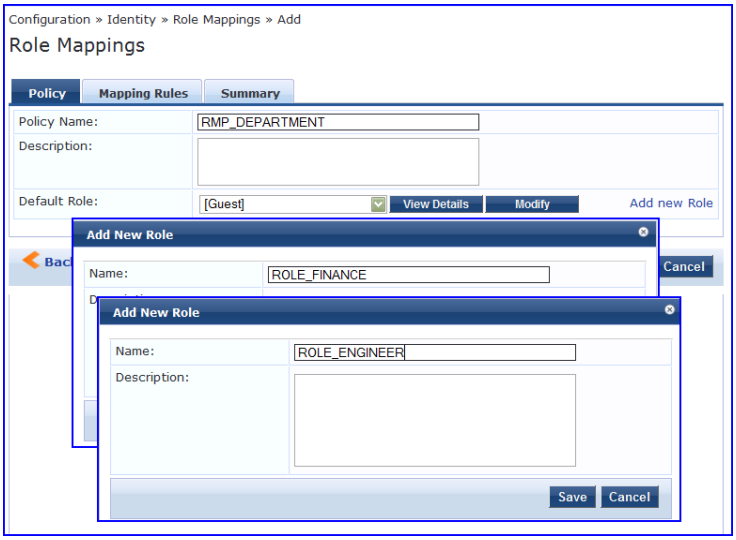
Navigation	Settings
• Configure Service level authorization source. In this use case there is nothing to configure. Click the **Next** button. • Upon completion, click **Next** (to Role Mapping).	

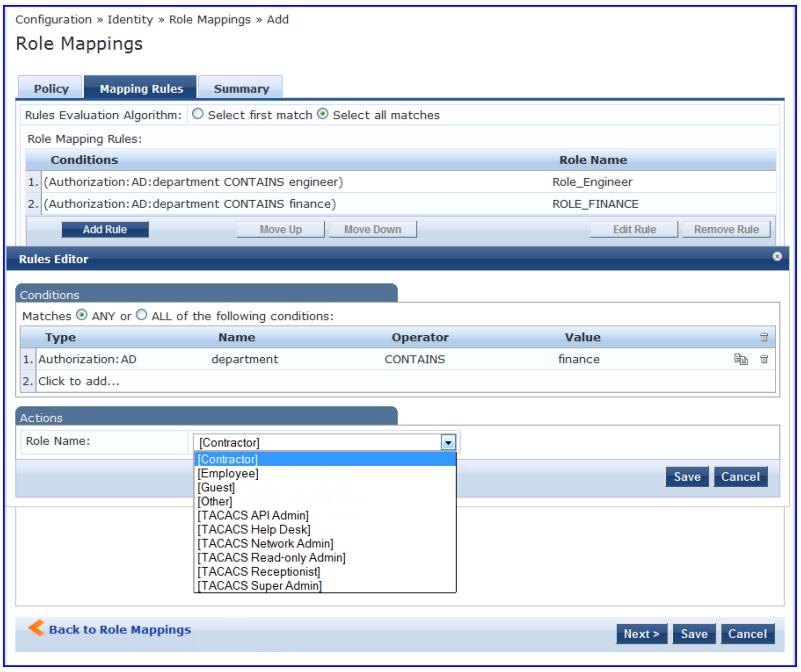
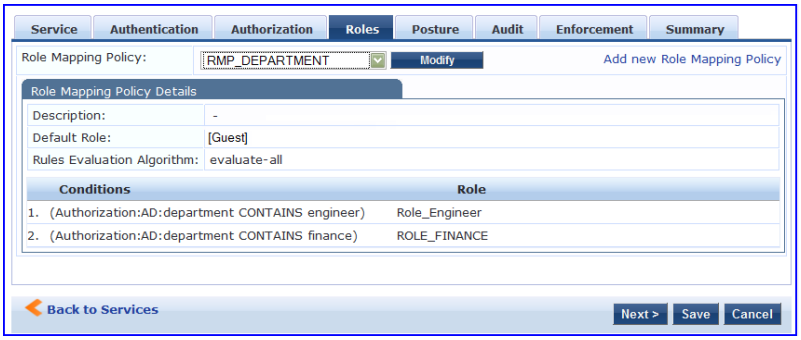
4. Apply a Role Mapping Policy

Policy Manager tests client identity against role-mapping rules, appending any match (multiple roles acceptable) to the request for use by the Enforcement Policy. In the event of role-mapping failure, Policy Manager assigns a default role.

In this Use Case, create the role mapping policy RMP_DEPARTMENT that distinguishes clients by department and the corresponding roles ROLE_ENGINEERING and ROLE_FINANCE, to which it maps:

Table 216: *Role Mapping Navigation and Settings*

Navigation	Settings
Create the new Role Mapping Policy: • Roles (tab) > • Add New Role Mapping Policy (link) >	
Add new Roles (names only): • **Policy** (tab) > • **Policy Name** (freeform): ROLE_ ENGINEER > • **Save** (button) > • Repeat for ROLE_FINANCE > • When you are finished working in the **Policy** tab, click the **Next** button (in the Rules Editor)	

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)	
Add the new Role Mapping Policy to the Service: • Back in **Roles** (tab) > • **Role Mapping Policy** (selector): *RMP_DEPARTMENT* > • Upon completion, click **Next** (to Posture)	

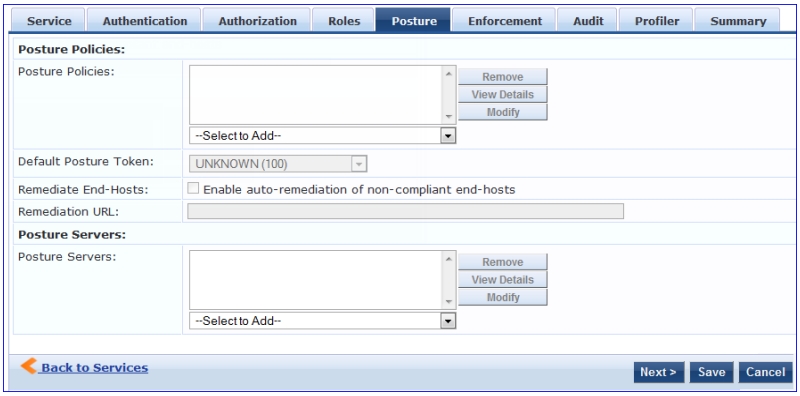
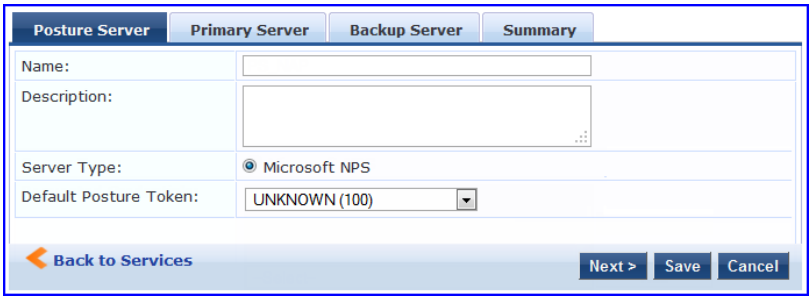
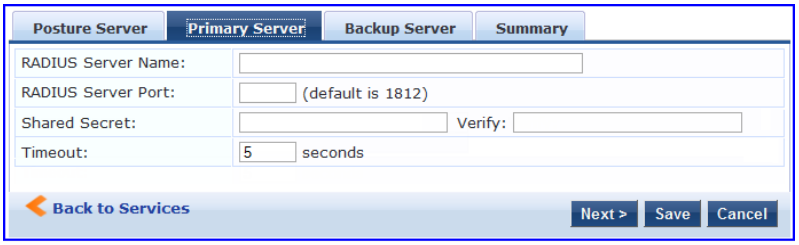
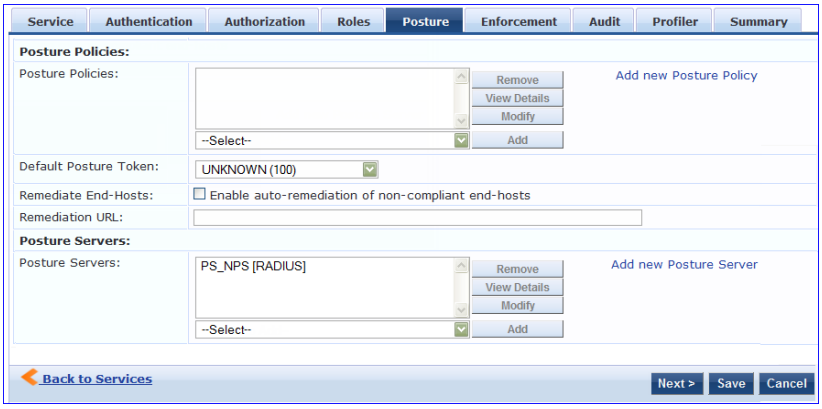
5. Configure a Posture Server

For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options; here, the Posture Server

Policy Manager can be configured for a third-party posture server, to evaluate client health based on vendor-specific credentials, typically credentials that cannot be evaluated internally by Policy Manager (that is, not in the form of internal posture policies). Currently, Policy Manager supports the following posture server interface: **Microsoft NPS (RADIUS)**.

Refer to the following table to add the external posture server of type **Micrsoft NPS** to the 802.1X service:

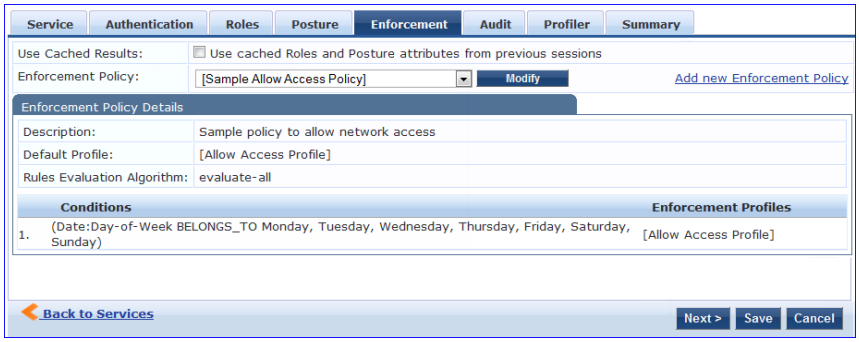
Table 217: *Posture Navigation and Settings*

Navigation	Setting
Add a new Posture Server: • **Posture** (tab) > • **Add new Posture Server** (button) >	
Configure Posture settings: • **Posture Server** (tab) > • **Name** (freeform): **PS_NPS** • **Server Type** (radio button): **Microsoft NPS** • **Default Posture Token** (selector): **UNKOWN** • **Next** (to Primary Server)	
Configure connection settings: • **Primary/ Backup Server** (tabs): Enter connection information for the RADIUS posture server. • **Next** (button): from Primary Server to Backup Server. • To complete your work in these tabs, click the **Save** button.	
Add the new Posture Server to the Service: • Back in the **Posture** (tab) > • **Posture Servers** (selector): **PS_NPS**, then click the **Add** button. • Click the **Next** button.	

6. Assign an Enforcement Policy

   Enforcement Policies contain dictionary-based rules for evaluation of Role, Posture Tokens, and System Time to Evaluation Profiles. Policy Manager applies all matching Enforcement Profiles to the Request. In the case of no match, Policy Manager assigns a default Enforcement Profile.

Table 218: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Configure the Enforcement Policy: • **Enforcement** (tab) > • **Enforcement Policy** (selector): **Role_Based_ Allow_Access_ Policy**	

For instructions about how to build such an Enforcement Policy, refer to "Configuring Enforcement Policies " on page 204.

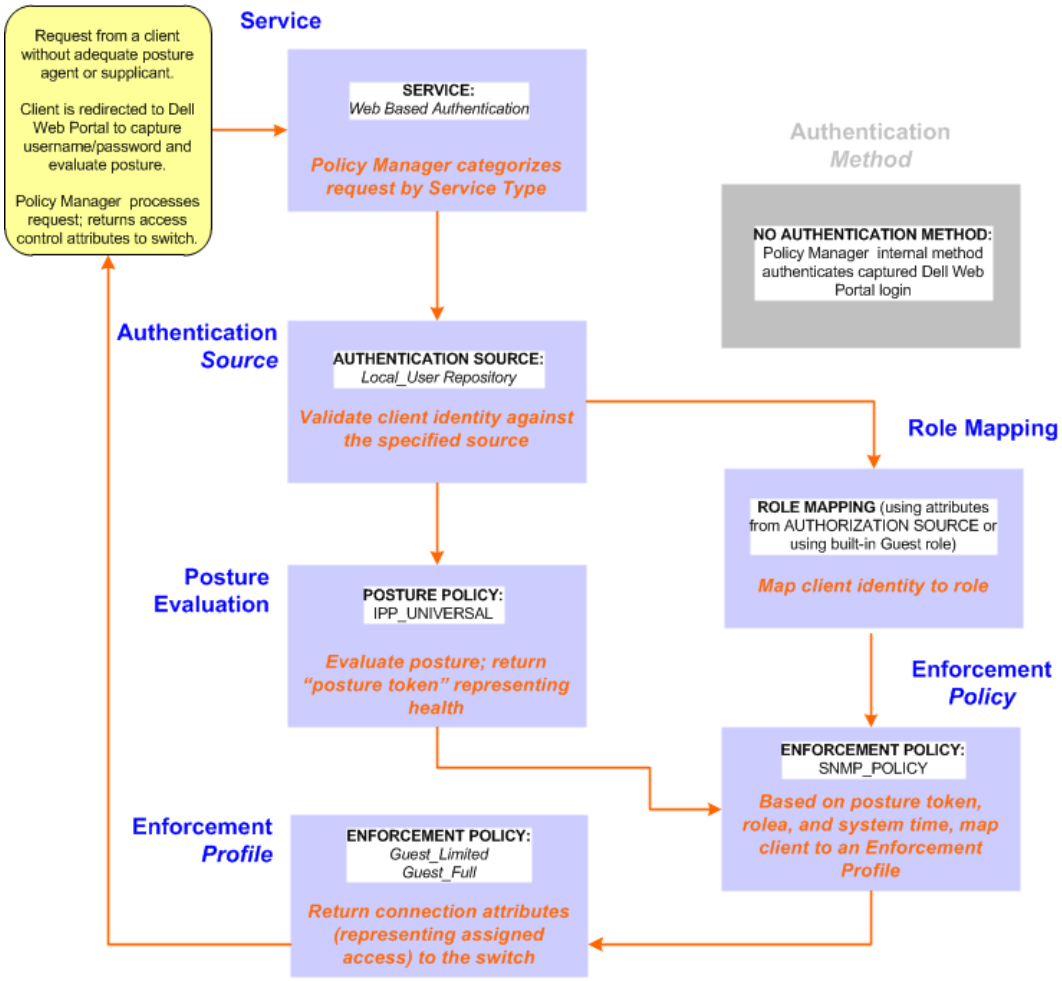
7. Save the Service.

   Click **Save**. The Service now appears at the bottom of the **Services** list.

Dell 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 296 *Flow-of-Control of Web-Based Authentication for Guests*



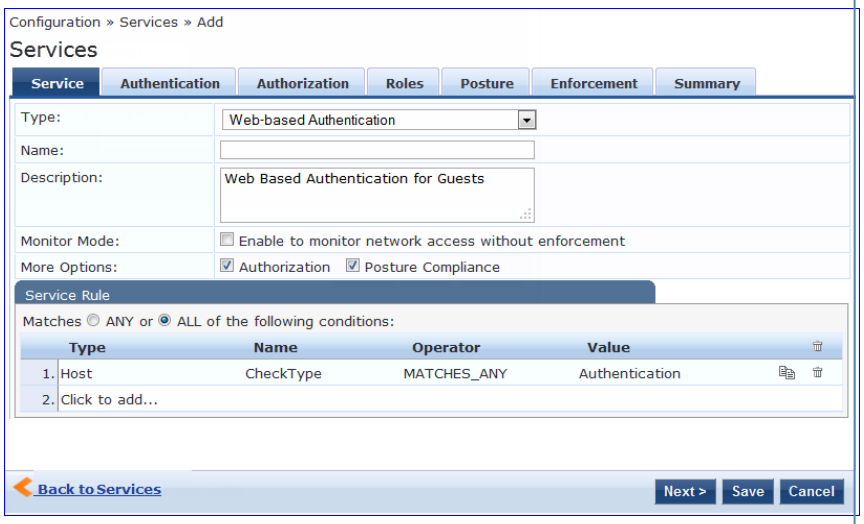
Configuring the Service

Perform the following steps to configure Policy Manager for WebAuth-based Guest access.

1. Prepare the switch to pre-process WebAuth requests for the Policy Manager *Dell WebAuth* service.

   Refer to your Network Access Device documentation to configure the switch such that it redirects HTTP requests to the *Dell Guest Portal* , which captures username and password and optionally launches an agent that returns posture data.
2. Create a WebAuth-based Service.

Table 219: *Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): Dell Web-Based Authentication > • **Name/Description** (freeform) > • Upon completion, click **Next**.	

3. Set up the Authentication.
   a. Method: The Policy Manager WebAuth service authenticates WebAuth clients internally.
   b. Source: Administrators typically configure Guest Users in the local Policy Manager database.
4. Configure a Posture Policy.

For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options. This use case demonstrates the Posture Policy.

As of the current version, Policy Manager ships with five pre-configured posture plugins that evaluate the health of the client and return a corresponding posture token.

To add the internal posture policy *IPP_UNIVERSAL_XP*, which (as you will configure it in this Use Case, checks any Windows® XP clients to verify the most current Service Pack).

Table 220: *Local Policy Manager Database Navigation and Settings*

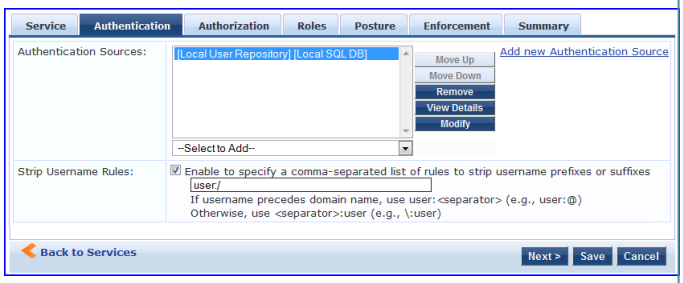
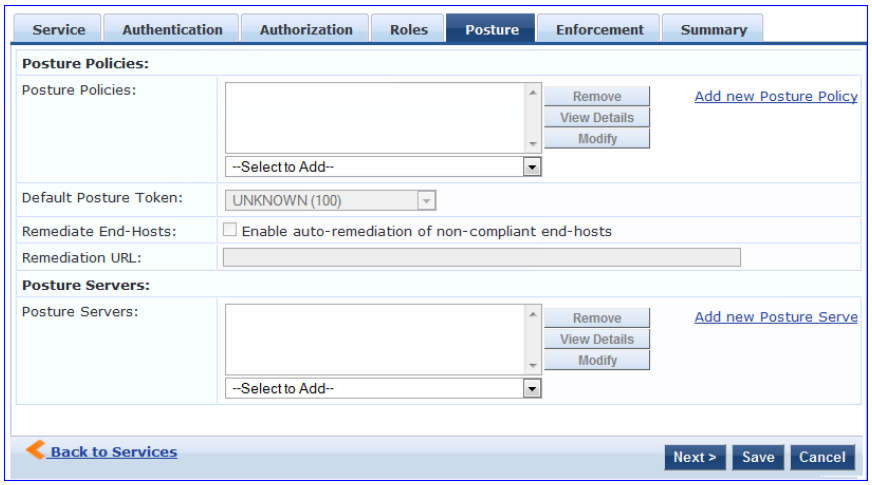
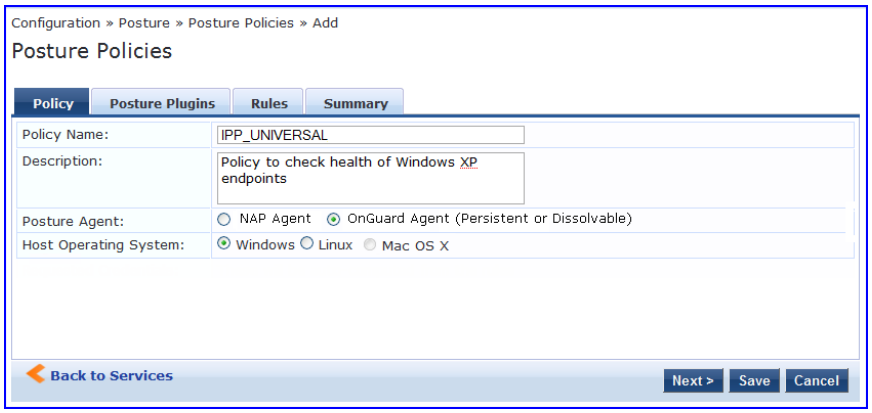
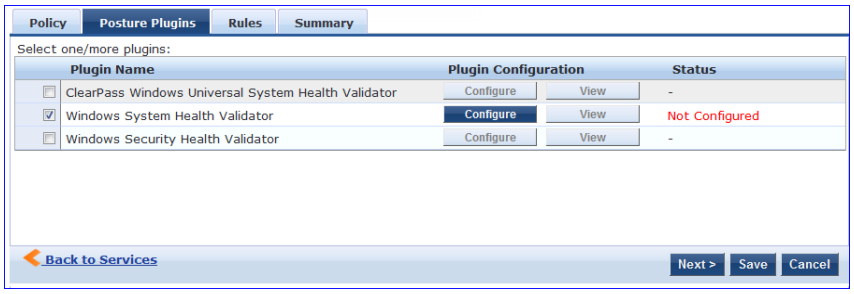
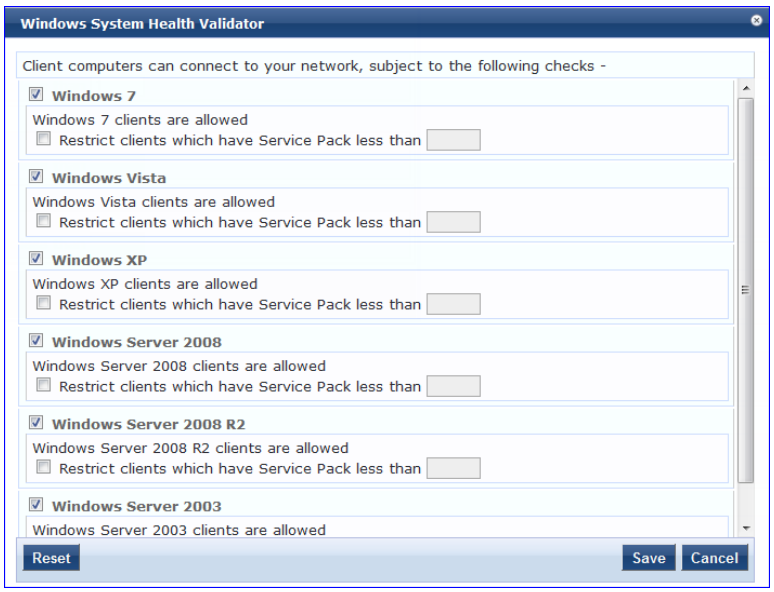
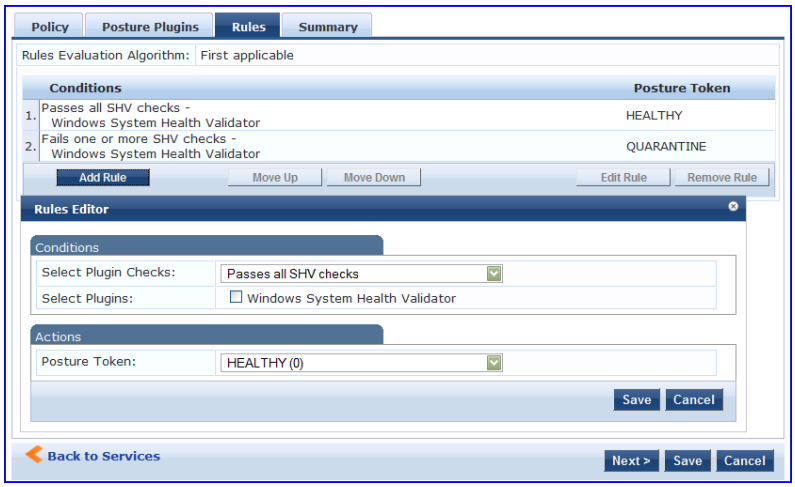
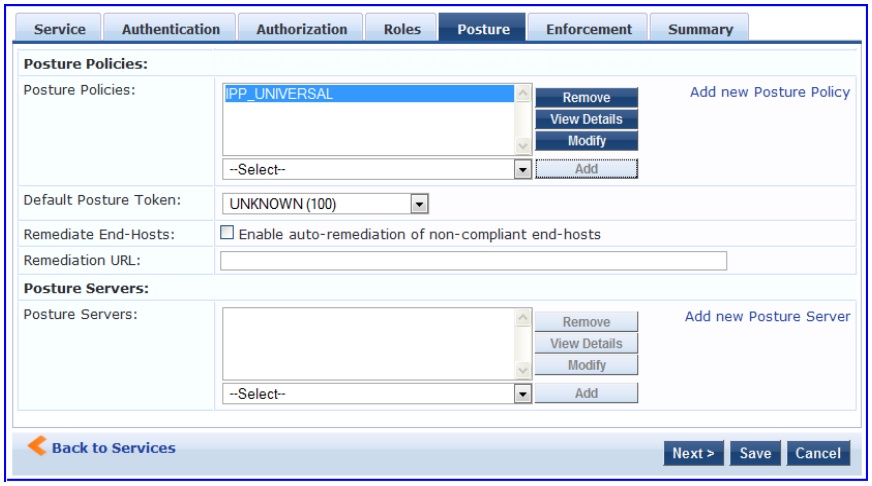
Navigation	Settings
Select the local Policy Manager database: • **Authentication** (tab) > • **Sources** (**Select** drop-down list): **[Local User Repository]** > • **Add** > • **Strip Username Rules** (check box) > • Enter an example of preceding or following separators (if any), with the phrase “user” representing the username to be returned. For authentication, Policy Manager strips the specified separators and any paths or domains beyond them. • Upon completion, click **Next** (until you reach Enforcement Policy).	

Table 221: *Posture Policy Navigation and Settings*

Navigation	Setting
Create a Posture Policy: • **Posture** (tab) > • Enable **Validation Check** (check box) > • **Add new Internal Policy** (link) >	

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	
Select a Validator: • **Posture Plugins** (tab) > • Enable **Windows Health System Validator** > • **Configure** (button) >	
Configure the Validator: • **Windows System Health Validator** (popup) > • **Enable all Windows operating systems** (check box) > • Enable Service Pack levels for Windows 7, Windows Vista®, Windows XP Windows Server® 2008, Windows Server 2008 R2, and Windows Server 2003 (check boxes) > • **Save** (button) > • When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)	

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.	
Add the new Posture Policy to the Service: Back in **Posture** (tab) > **Internal Policies** (selector): **IPP_ UNIVERSAL_XP**, then click the **Add** button	

The following fields deserve special mention:

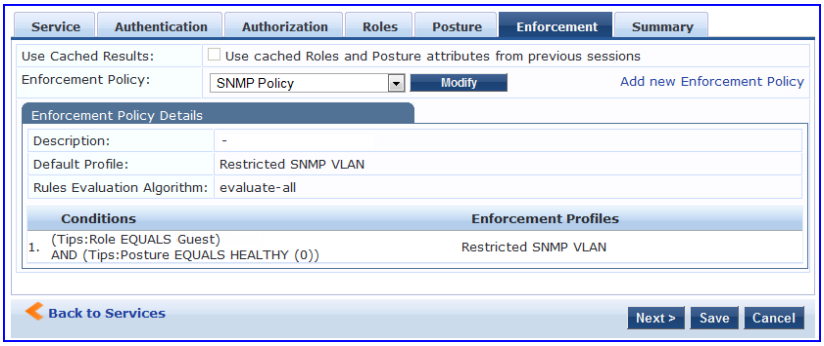
- **Default Posture Token.** Value of the posture token to use if health status is not available.
- **Remediate End-Hosts.** When a client does not pass posture evaluation, redirect to the indicated server for remediation.
- **Remediation URL.** URL of remediation server.

5. Create an Enforcement Policy.

   Because this Use Case assumes the *Guest* role, and the *Dell Web Portal* agent has returned a posture token, it does not require configuration of Role Mapping or Posture Evaluation.

The SNMP_POLICY selected in this step provides full guest access to a Role of [Guest] with a Posture of Healthy, and limited guest access.

Table 222: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Add a new Enforcement Policy: • **Enforcement** (tab) > • Enforcement Policy (selector): **SNMP_ POLICY** • Upon completion, click **Save**.	

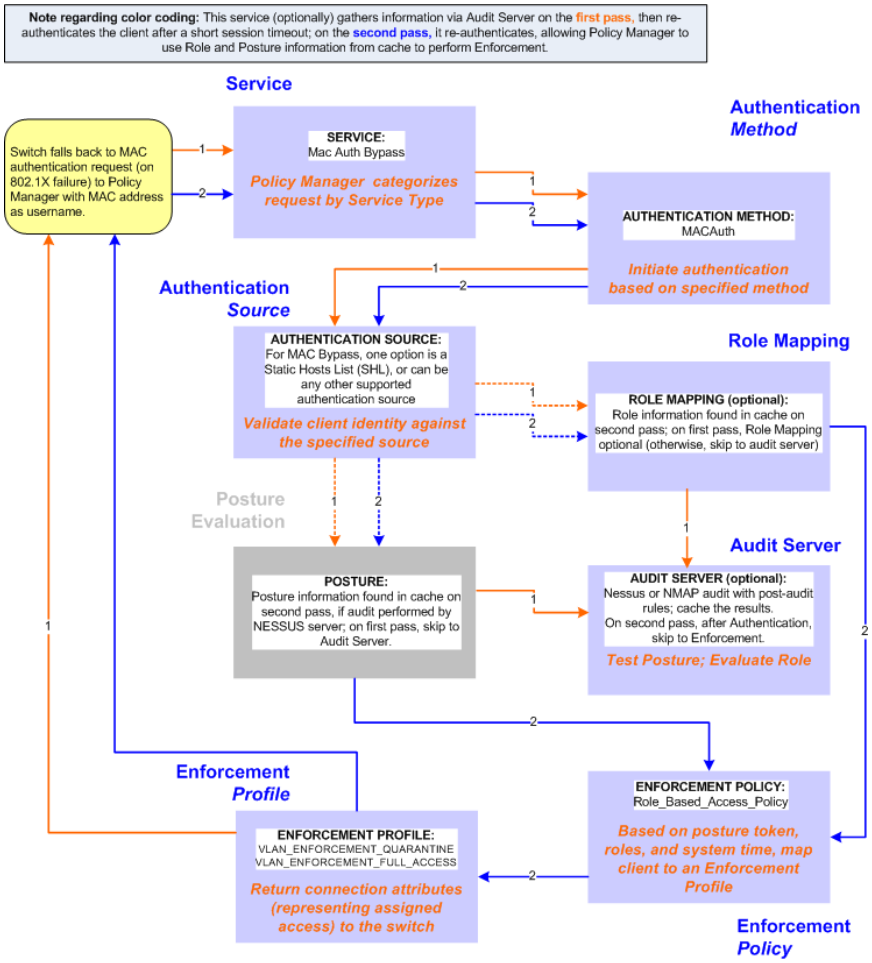
6. Save the Service.

   Click **Save**. The Service now appears at the bottom of the **Services** list.

MAC Authentication Use Case

This Service supports *Network Devices,* such as printers or handhelds. The following image illustrates the overall flow of control for this Policy Manager Service. In this service, an audit is initiated on receiving the first MAC Authentication request. A subsequent MAC Authentication request (forcefully triggered after the audit, or triggered after a short session timeout) uses the cached results from the audit to determine posture and role(s) for the device

Figure 297 *Flow-of-Control of MAC Authentication for Network Devices*

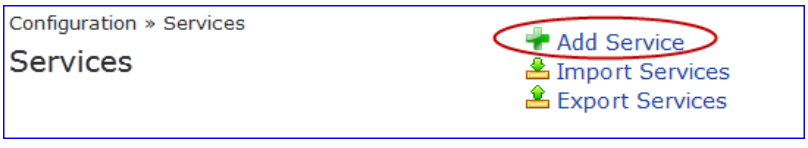


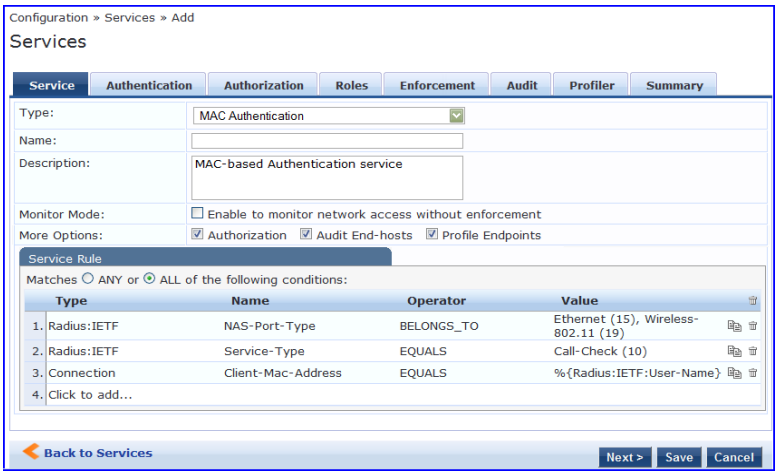
Configuring the Service

Follow these steps to configure Policy Manager for MAC-based Network Device access.

1. Create a MAC Authentication Service.

Table 223: *MAC Authentication Service Navigation and Settings*

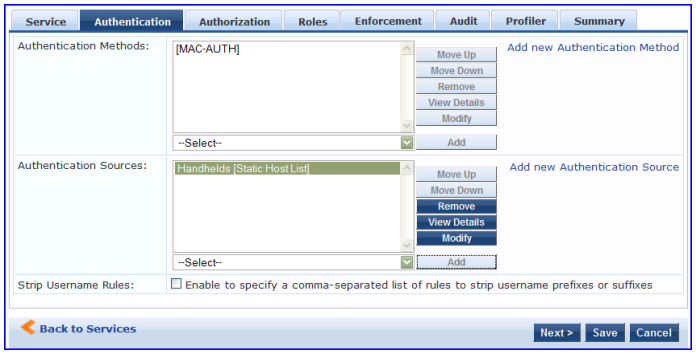
Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	

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	

2. Set up Authentication

   Note that 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 for more information. You can also select any other supported type of authentication source.

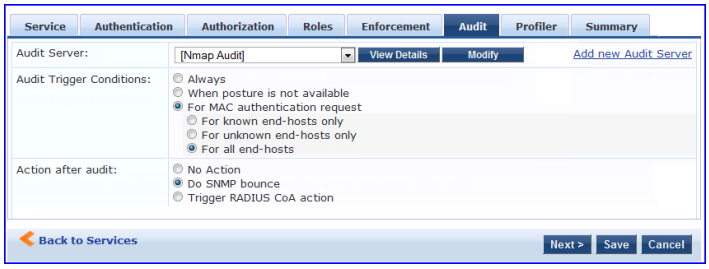
Table 224: *Authentication Method Navigation and Settings*

Navigation	Settings
Select an Authentication Method and two authentication sources - one of type Static Host List and the other of type Generic LDAP server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (This method is automatically selected for this type of service): **[MAC AUTH]** > • **Add** > • **Sources** (**Select** drop-down list): **Handhelds [Static Host List]** and Policy Manager Clients White List [Generic LDAP] > • **Add** > • Upon completion, **Next** (to Audit)	

3. Configure an Audit Server.

   This step is optional if no Role Mapping Policy is provided, or if you want to establish health or roles using an audit. An audit server determines health by performing a detailed system and health vulnerability analysis (NESSUS). You can also configure the audit server (NMAP or NESSUS) with post-audit rules that enable Policy Manager to determine client identity.

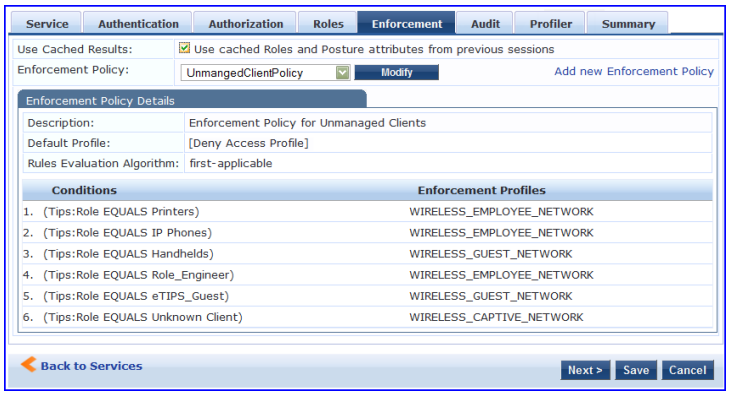
Table 225: *Audit Server Navigation and Settings*

Navigation	Settings
Configure the Audit Server: • **Audit** (tab) > • **Audit End Hosts** (enable) > • **Audit Server** (selector): **NMAP** • **Trigger Conditions** (radio button): **For MAC authentication requests** • **Reauthenticate client** (check box): **Enable**	

Upon completion of the audit, Policy Manager caches Role (NMAP and NESSUS) and Posture (NESSUS), then resets the connection (or the switch reauthenticates after a short session timeout), triggering a new request, which follows the same path until it reaches Role Mapping/Posture/Audit; this appends cached information for this client to the request for passing to Enforcement. Select an Enforcement Policy.

4. Select the Enforcement Policy *Sample_Allow_Access_Policy*:

Table 226: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: • **Enforcement** (tab) > • **Use Cached Results** (check box): Select **Use cached Roles and Posture attributes from previous sessions** > • **Enforcement Policy** (selector): UnmanagedClientPolicy • When you are finished with your work in this tab, click **Save**.	

Unlike the 802.1X Service, which uses the same Enforcement Policy (but uses an explicit Role Mapping Policy to assess Role), in this use case Policy Manager applies post-audit rules against attributes captured by the Audit Server to infer Role(s).

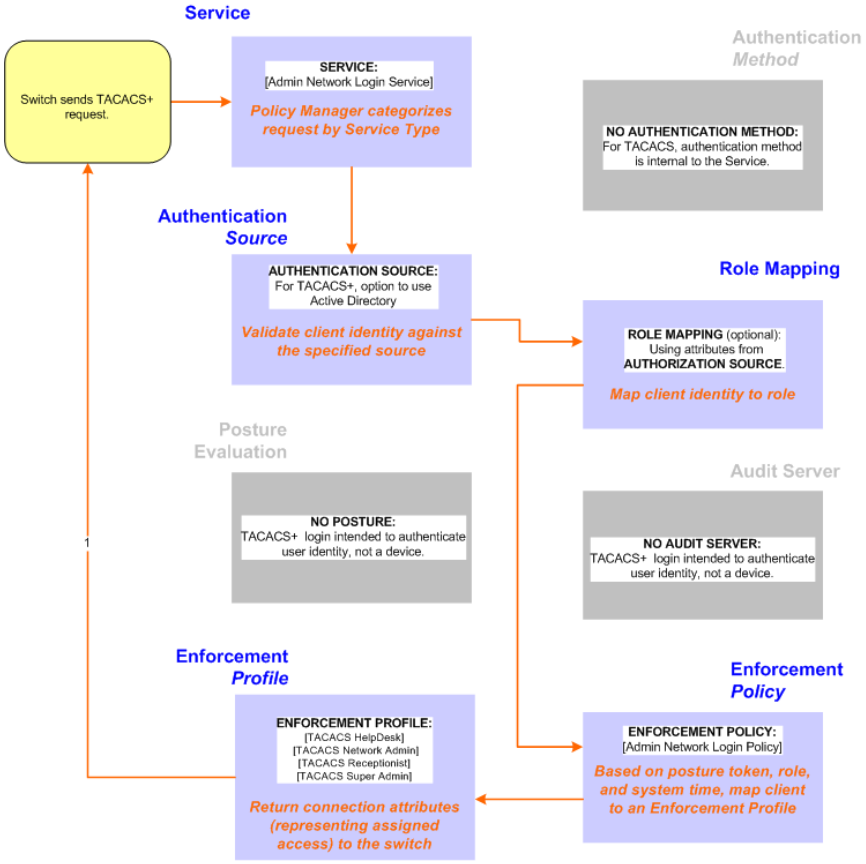
5. Save the Service.

   Click **Save.** The Service now appears at the bottom of the **Services** list.

TACACS+ Use Case

This Service supports Administrator connections to Network Access Devices via TACACS+. The following image illustrates the overall flow of control for this Policy Manager Service.

Figure 298 *Administrator connections to Network Access Devices via TACACS+*



Configuring the Service

Perform the following steps to configure Policy Manager for TACACS+-based access:

1. Create a TACACS+ Service.

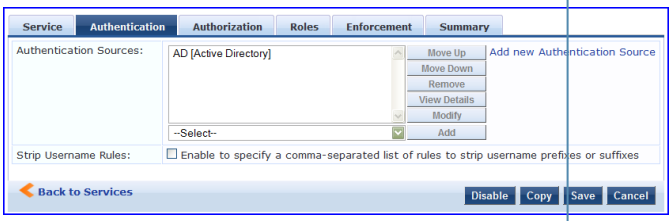
Table 227: *TACACS+ Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	Configuration » Services Services Add Service Import Services Export Services

Navigation	Settings
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **[Policy Manager Admin Network Login Service]** > • **Name/Description** (freeform) > • Upon completion, click **Next** (to Authentication)	

2. Set up the Authentication
   a. Method: The Policy Manager TACACS+ service authenticates TACACS+ requests internally.
   b. Source: For purposes of this use case, Network Access Devices authentication data will be stored in the Active Directory.

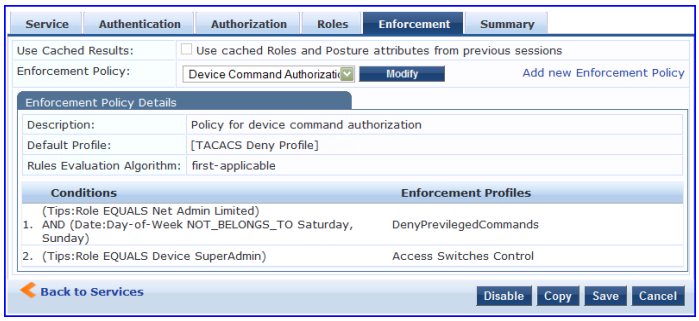
Table 228: *Active Directory Navigation and Settings*

Navigation	Settings
Select an Active Directory server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Add** > • **Sources** (**Select** drop-down list): AD (Active Directory) > • **Add** > • Upon completion, click **Next** (to Enforcement Policy)	

3. Select an Enforcement Policy.

   Select the Enforcement Policy **[Admin Network Login Policy]** that distinguishes the two allowed roles (**Net Admin Limited** and **Device SuperAdmin**.

Table 229: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: • **Enforcement** (tab) > • **Enforcement Policy** (selector): **Device Command Authorization Policy** • When you are finished with your work in this tab, click **Save**.	

4. Save the Service.

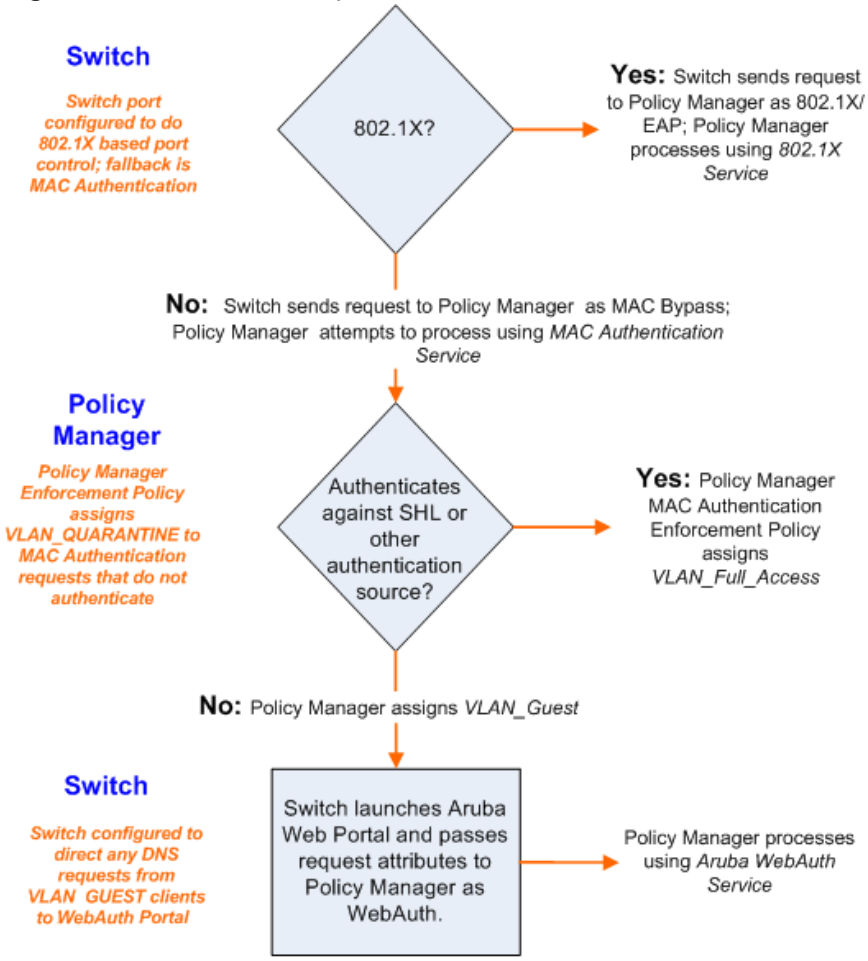
   Click **Save.** The Service now appears at the bottom of the **Services** list.

Single Port Use Case

This Service supports all three types of connections on a single port.

The following figure illustrates both the overall flow of control for this hybrid service, in which complementary switch and Policy Manager configurations allow all three types of connections on a single port:

Figure 299 *Flow of the Multiple Protocol Per Port Case*



This appendix lists the copyright notices for the binary distribution from Aruba Networks. A copy of the source code is available for portions of the software whose copyright statement requires Aruba Networks to publish any modified source code. To cover the costs of duplication and shipping, there is a nominal cost to obtain the source code material. To obtain a copy of the source code, contact info@arubanetworks.com.

Copyright statements for portions of software are listed below.

PostgreSQL Copyright

PostgreSQL is Copyright © 2004-2010 by the PostgreSQL Global Development Group and is distributed under the terms of the license of the University of California below.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS-IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GNU LGPL

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide

range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU GPL

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate

your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN

WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Lighthttpd License

Copyright (c) 2004, Jan Kneschke, incremental

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

1. You must give any other recipients of the Work or Derivative Works a copy of this License; and

2. You must cause any modified files to carry prominent notices stating that You changed the files; and

3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

OpenSSL License

/* ==

* Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are adhered to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgment:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the routines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgment:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The license and distribution terms for any publicly available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution license
* [including the GNU Public License.] */

OpenLDAP License

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document. The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT,INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation. Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

gSOAP Public License

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."