

# ClearPass Policy Manager 6.1



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, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFPProtect®, Green Island®. All rights reserved. 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](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.

### Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

The ClearPass Policy Manager platform provides role- and device-based network access control across any wired, wireless and VPN. Software modules for the 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, 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 3](#)
- ["Exporting" on page 4.](#)

## Importing

On most pages with lists in 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**.

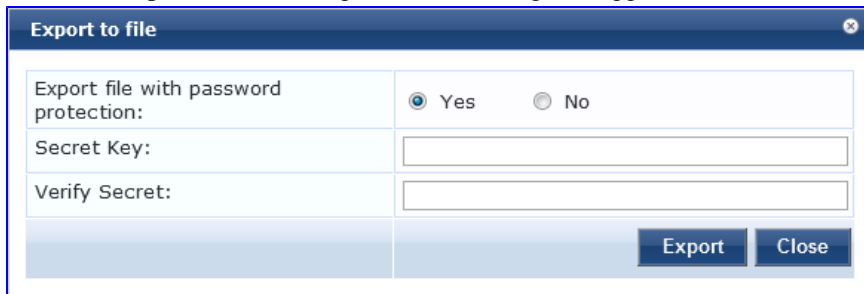
## Exporting

On most pages with lists in 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.

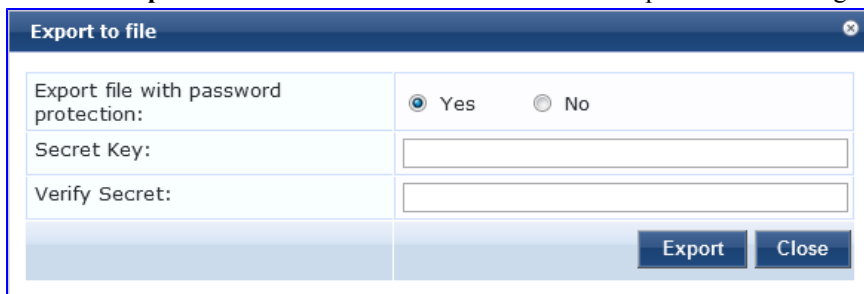


2. If you want the file password protected, select **Yes** and enter a password twice (in the Secret Key and Verify Secret fields). If you do not want the file password protected, select **No**.
3. Click **Export**.

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 password 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 backpanel 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 305](#) 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 6](#) 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 Aruba 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, Aruba 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 6](#) 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:


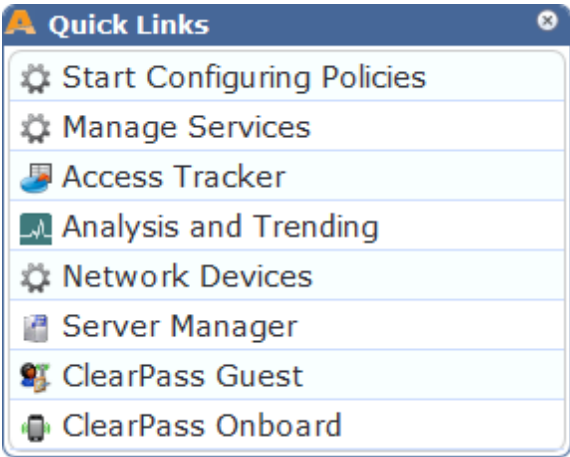


5. To generate the support key, select option 2 (or 3, if you want to generate a password recovery key, as well).
6. Once the password recovery key is generated, email the key to Aruba technical support. A unique password can now be generated by Aruba technical support to log into the support shell.



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:

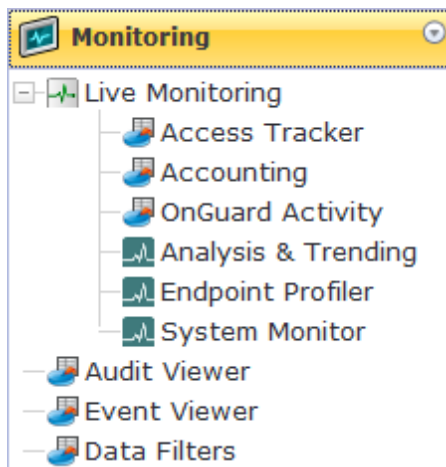
 <b>All Requests</b> <i>Trend all eTIPS requests</i>	<p>This shows a graph of all requests processed by Policy Manager over the past week. This includes RADIUS, TACACS+ and WebAuth requests. The default data filter “All Requests” is used to plot this graph. Clicking on each bar in the graph drills down into the Access Tracker and shows the requests for that day.</p>
 <b>Health Status</b> <i>Trend Healthy and Unhealthy requests</i>	<p>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.</p>
 <b>Authentication Status</b> <i>Trend Successful and Failed authentications</i>	<p>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.</p>
 <b>Latest Authentications</b> <i>Latest Authentications</i>	<p>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.</p>

 <b>Device Category</b> <i>Device Categories</i>	<p>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.</p> <p>Unknown devices are devices that the profiler was not able to profile.</p> <p>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.</p>
 <b>Device Family</b> <i>Device Family</i>	<p>The Device Family widget allows you to drill down further into each of the built-in device categories. For example, selecting <b>SmartDevice</b> shows the different kinds of smartdevices identified by Profile.</p>
 <b>Successful Authentications</b> <i>Track the latest successful authentications</i>	<p>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.</p>
 <b>Failed Authentications</b> <i>Track the latest failed authentications</i>	<p>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.</p>
 <b>Service Categorization</b> <i>Monitor Service Categorization of authentications</i>	<p>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.</p>
 <b>Alerts</b> <i>Latest Alerts</i>	<p>This shows a table of last few system level events. Clicking on a row drills down into the Event Viewer</p>

<div data-bbox="240 142 493 222">  <b>Quick Links</b>  Launch configuration interfaces with a single click </div> <div data-bbox="237 247 803 701">  <p>The screenshot shows a 'Quick Links' window with a blue header and a list of links, each with an icon:</p> <ul style="list-style-type: none"> <li>Start Configuring Policies (gear icon)</li> <li>Manage Services (gear icon)</li> <li>Access Tracker (laptop icon)</li> <li>Analysis and Trending (line graph icon)</li> <li>Network Devices (gear icon)</li> <li>Server Manager (server rack icon)</li> <li>ClearPass Guest (person icon)</li> <li>ClearPass Onboard (phone icon)</li> </ul> </div>	<p>Quick Links shows links to common configuration tasks:</p> <ul style="list-style-type: none"> <li>• <b>Start Configuring Policies</b> links to the Start Here Page under Configuration menu. Start configuring Policy Manager Services from here.</li> <li>• <b>Manage Services</b> links to the Services page under Configuration menu. Shows a list of configured services.</li> <li>• <b>Access Tracker</b> links to the Access Tracker screen under Reporting &amp; Monitoring menu.</li> <li>• <b>Analysis &amp; Trending</b> links to the Analysis &amp; Trending screen under Reporting &amp; Monitoring menu.</li> <li>• <b>Network Devices</b> links to the Network Devices screen under Configuration menu. Configure network devices from here.</li> <li>• <b>Server Manager</b> links to the Server Configuration screen under Administration menu.</li> <li>• <b>ClearPass Guest</b> links to the ClearPass Guest application. This application opens in a new tab.</li> <li>• <b>ClearPass Onboard</b> links to the ClearPass Onboard screen within the ClearPass Guest application. This application opens in a new tab.</li> </ul>
<div data-bbox="240 953 518 1033">  <b>Applications</b>  Launch other ClearPass Applications </div>	<p>This shows links to the Aruba applications that are integrated with Policy Manager. E.g., GuestConnect, Insight.</p>
<div data-bbox="240 1087 493 1167">  <b>Cluster Status</b>  Monitor the status of the entire cluster </div>	<p>This shows the status of all nodes in the cluster. The following fields are shown for each node:</p> <ul style="list-style-type: none"> <li>• <b>Status</b> 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.</li> <li>• <b>Host Name</b> Host name and IP address of the node</li> <li>• <b>CPU Util</b> Snapshot of the CPU utilization in percentage</li> <li>• <b>Mem Util</b> Snapshot of the memory utilization in percentage</li> <li>• <b>Server Role</b> Publisher or subscriber</li> </ul>



The Policy Manager **Monitoring** menu provides the following interfaces:

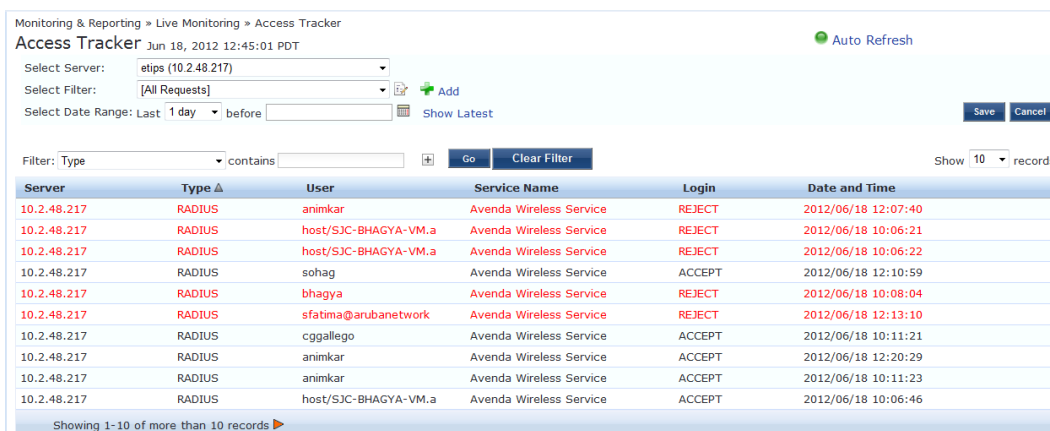


- Live Monitoring
  - "Access Tracker " on page 15
  - "Accounting" on page 17
  - "OnGuard Activity " on page 24
  - "Analysis and Trending" on page 26
  - "Endpoint Profiler " on page 27
  - "System Monitor" on page 28
- "Audit Viewer" on page 30
- "Event Viewer " on page 32
- "Data Filters " on page 33

## 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** *Fig: Access Tracker (Edit Mode)*



**Table 3:** *Access Tracker Display Parameters*

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

Container	Description
<b>Select Filter</b>	Select filter to constrain data display.
	Modify the currently displayed data filter
 <b>Add</b>	Go to <b>Data Filters</b> page to create a new data filter.
<b>Select Date Range</b>	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.
<b>Show Latest</b>	Sets the date to Today in the previous step to Today.
<b>Save/Cancel</b>	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 dropdown 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 Aruba application authentications (Insight, GuestConnect, EdgeManager)

## 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 reauthentication 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	<p>This button allows you to change the access control status of a session. This function is only available for RADIUS and WebAuth.</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• 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 Session) action is supported by all devices. Some devices support setting a session timeout, changing the VLAN for the session, applying an ACL, etc.</li></ul>
Export	<p>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.</p>
Show Logs	<p>Show logs of this session. Error messages are color coded in red. Warning messages are color coded in orange.</p>
Close	<p>RADIUS response attributes sent to the device</p>

## 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)**

Monitoring » Live Monitoring » Accounting

### Accounting

Select Server:

Select Filter:  **Add**

Select Date Range: Last  before  **Show Latest** **Save** **Cancel**

☐ Select ALL matches ☒ Select ANY match

Filter:  contains

Filter:  contains  **Go** **Clear Filter** Show  records

Server	Protocol	User	Access Device	Start Time ▾
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:17:27 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:12:39 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:12:39 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:12:01 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:11:44 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:11:17 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:11:12 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 17:11:03 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 16:58:37 PDT
10.2.50.178	RADIUS	[redacted]	10.2.50.197:10	May 16, 2012 16:56:47 PDT

Showing 1-10 of more than 10 records

**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)

**Accounting Record Details**

Summary Auth Sessions Utilization Details

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

Network Details -

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

Close

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

**Accounting Record Details**

Summary Auth Sessions Utilization Details

Number of Authentication Sessions: 3

Authentication Sessions Details

SessionId	Type	Time Stamp
R00000033-01-49b5571f	initial	Mar 09, 2009 10:51:30 PDT
R00000037-01-49b56533	re-auth	Mar 09, 2009 11:51:35 PDT
R0000003e-01-49b57348	re-auth	Mar 09, 2009 12:51:38 PDT

Close

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

Accounting Record Details

SummaryAuth SessionsUtilizationDetails

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

Close

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

Accounting Record Details

Summary	Auth Sessions	Utilization	Details
Tunnel-Private-Group-Id5			Mar 06, 2009 14:26:49 PST
For Session Id R0000000d-01-49b1b0a5			at Mar 06, 2009 15:24:21 PST
NAS-Identifier	avenda-wapcontroller	Mar 06, 2009 15:24:21 PST	
Airespace-Wlan-Id	1	Mar 06, 2009 15:24:21 PST	
Tunnel-Type	VLAN	Mar 06, 2009 15:24:21 PST	
Tunnel-Medium-Type	IEEE-802	Mar 06, 2009 15:24:21 PST	
Tunnel-Private-Group-Id5		Mar 06, 2009 15:24:21 PST	
For Session Id R00000011-01-49b1be22			at Mar 06, 2009 16:21:54 PST
NAS-Identifier	avenda-wapcontroller	Mar 06, 2009 16:21:54 PST	
Airespace-Wlan-Id	1	Mar 06, 2009 16:21:54 PST	
Tunnel-Type	VLAN	Mar 06, 2009 16:21:54 PST	
Tunnel-Medium-Type	IEEE-802	Mar 06, 2009 16:21:54 PST	
Tunnel-Private-Group-Id5		Mar 06, 2009 16:21:54 PST	
For Session Id R00000015-01-49b1cb9f			at Mar 06, 2009 17:19:27 PST
NAS-Identifier	avenda-wapcontroller	Mar 06, 2009 17:19:27 PST	

Close

**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)
	Account Input Octets	Octets sent and received from the device port over the course of the session
	Account Output Octets	

Tab	Container	Description
	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 reauthentications (each section in the details tab corresponds to a “session” in Policy Manager.

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

Accounting Record Details

Request

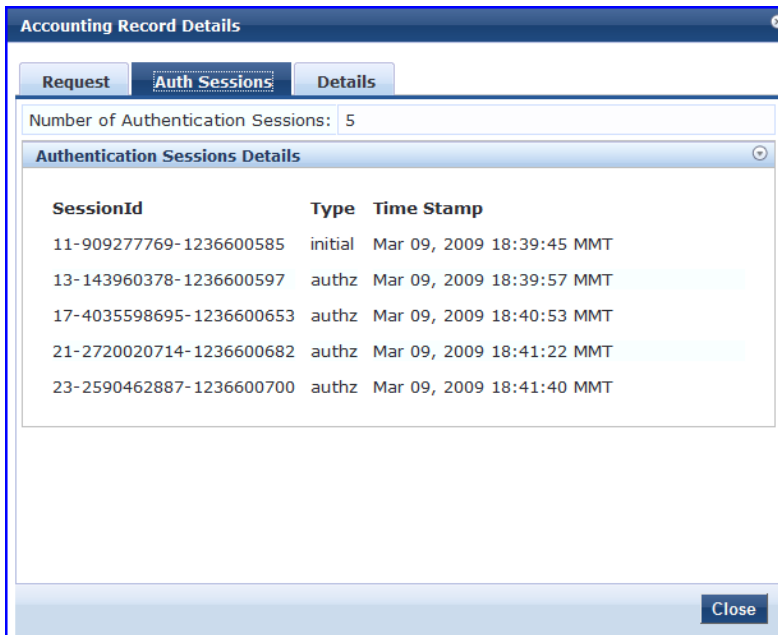
Auth Sessions

Details

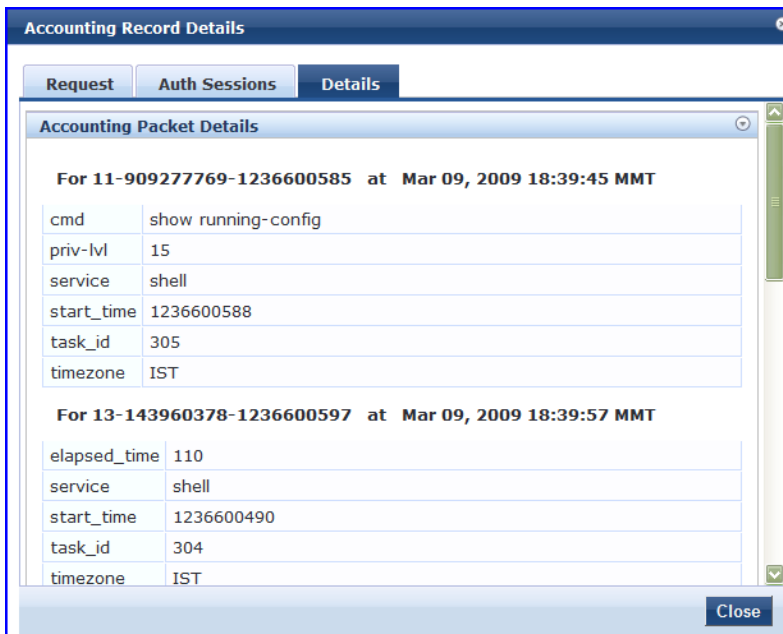
Session ID:	23-2590462887-1236600700
User Session ID:	T00000002-04-49b506f1
Start Timestamp:	Mar 09, 2009 18:39:45 MMT
End Timestamp:	Mar 09, 2009 18:41:40 MMT
User Name:	james
Client IP :	192.168.12.27:tty2
Remote IP:	192.168.12.101
Flags:	4
Privilege Level:	1
Authentication Method:	AUTHEN_METH_TACACSPLUS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

Close

**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	
	Authentication Type	
	Authentication Service	
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.

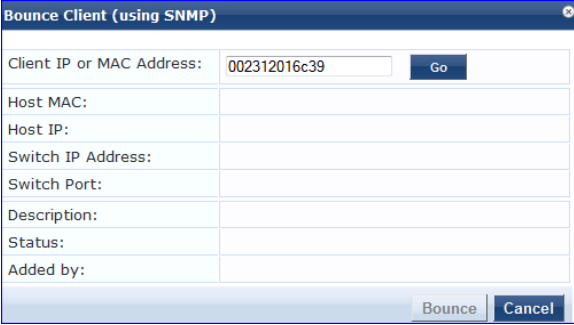
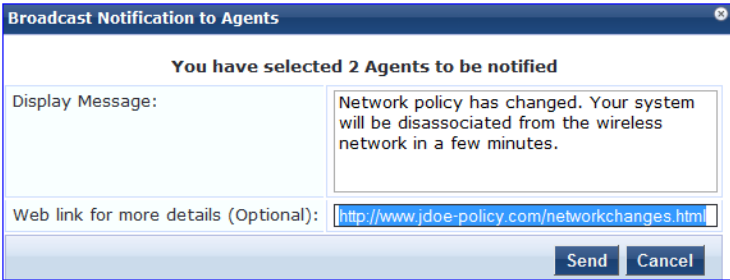
## OnGuard Activity

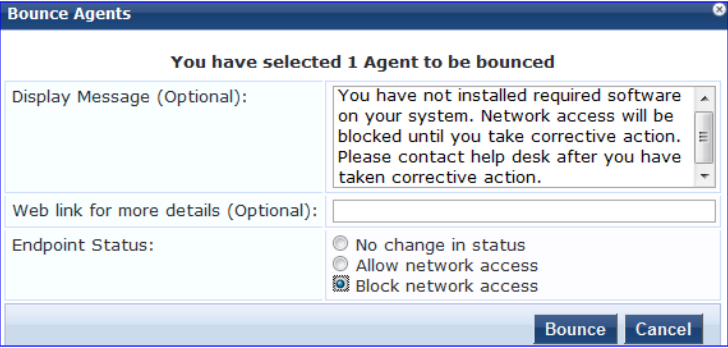
The OnGuard Activity screen shows the realtime status of all endpoints that have Aruba OnGuard persistent or dissolvable agent, at: **Monitoring > Live Monitoring > OnGuard Activity**. This screen also presents configuration tools to bounce an endpoint and to send unicast or broadcast messages to all endpoints running the OnGuard agent. Note that bouncing of endpoints will only work with endpoints running the persistent agent.

**Figure 11** *Fig: OnGuard Activity*

Monitoring & Reporting » Live Monitoring » OnGuard Activity						
OnGuard Activity May 16, 2012 17:16:26 PDT						
<div> <span>Auto Refresh</span>  <span>Bounce Client (using SNMP)</span>  <span>Broadcast Message</span> </div>						
Filter: <input type="text" value="User"/> contains <input type="text"/> <input type="button" value="Go"/> <input type="button" value="Clear Filter"/> Show <input type="text" value="10"/> records						
#	User	Host MAC	Host IP	Host OS	Status	Date and Time
1.	jbond	3C-07-54-3D-C9-9F	10.2.50.66	Mac OS X 10.7.4	<span style="color: green;">●</span>	2012/05/16 17:13:36
2.	mahesh	68-AB-6D-19-A9-9C	10.2.50.70	Mac OS X 10.7.4	<span style="color: red;">●</span>	2012/05/16 14:43:40
3.	vivek	24-77-03-47-85-18	10.11.8.23	Microsoft Windows 7	<span style="color: red;">●</span>	2012/05/16 16:32:00
4.	vivek	F0-DE-F1-C1-85-7B	10.2.50.63	Microsoft Windows 7	<span style="color: red;">●</span>	2012/05/16 15:29:28
Showing 1-4 of 4 <input type="button" value="Send Message"/> <input type="button" value="Bounce"/>						

**Table 10: OnGuard Activity**

Container	Description
Auto Refresh	Toggle auto-refresh. If this is turned on, all endpoint activities are refreshed automatically.
<p>Bounce Client (using SNMP)</p> 	<p>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:</p> <ul style="list-style-type: none"> <li>• The network device must be added to Policy Manager, and SNMP read and write parameters must be configured.</li> <li>• SNMP traps (link up and/or MAC notification) have to be enabled on the switch port.</li> <li>• 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.</li> </ul>
<p>Broadcast Message</p> 	Send a message to all active endpoints
Send Message	Send a message to the selected endpoints.
Bounce	<p>Initiate a bounce on the managed interface on the endpoint.</p> <ul style="list-style-type: none"> <li>• Display Message - An optional message to display on the endpoint (via the OnGuard interface).</li> <li>• Web link - An optional clickable URL that is displayed along with the Display Message.</li> <li>• Endpoint Status -</li> </ul>

Container	Description
	<p>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.</p> <p>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.</p> <p>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.</p> <p>This action results in tags being created for the specified endpoint in the Endpoints table (<b>Configuration &gt; Identity &gt; Endpoints</b>). One or more of the following tags are created: Disabled by, Disabled Reason, Enabled by, Enabled Reason, Info URL.</p>

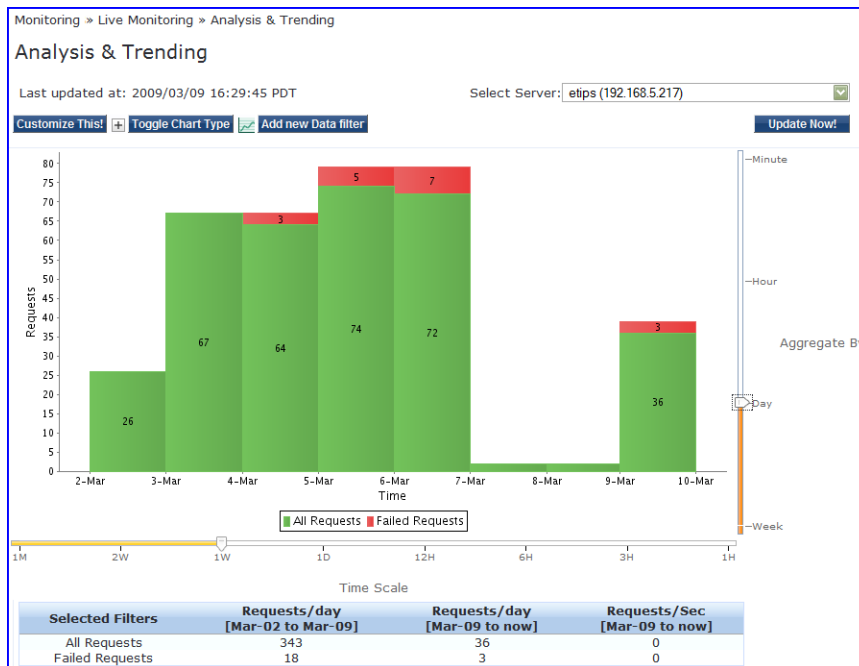
## Analysis and Trending

### 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 15, 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*



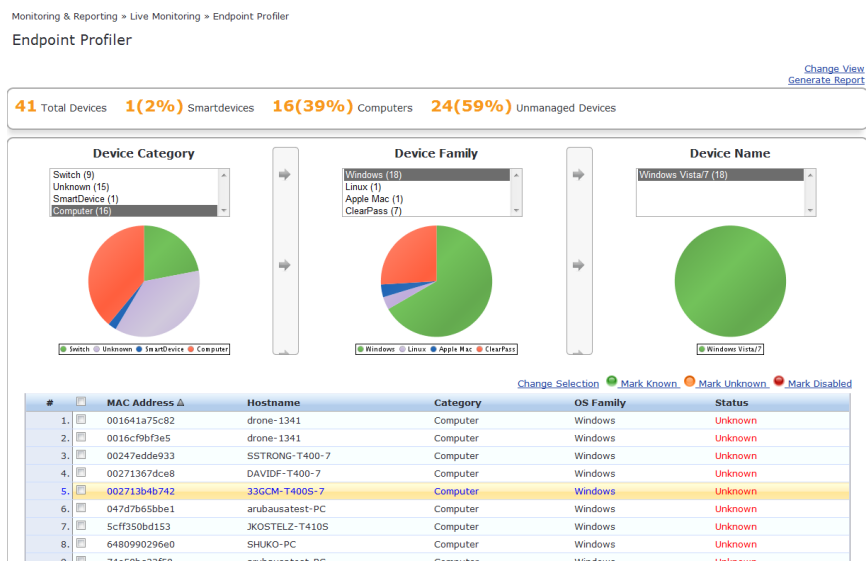
To add additional filters, refer to "Data Filters " on page 33.

- **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*



The screenshot shows a 'View Endpoint' dialog box with a table of device details. The table has two columns and multiple rows. The first column contains labels like 'MAC Address', 'Description', 'Status', 'Added by', 'IP Address', 'Hostname', 'MAC Vendor', 'Category', 'OS Family', 'Device Name', 'Updated At', and 'Show Fingerprint'. The second column contains the corresponding values: '000c2903c9bf', an empty field, 'Unknown', 'Policy Manager', '10.2.50.42', '-', 'VMware, Inc.', 'Unknown', 'Unknown', 'Unknown', 'Apr 19, 2012 15:01:26 PDT', and a checkbox. A 'Cancel' button is located at the bottom right of the dialog box.

MAC Address	000c2903c9bf	IP Address	10.2.50.42
Description		Hostname	-
Status	Unknown	MAC Vendor	VMware, Inc.
Added by	Policy Manager	Category	Unknown
		OS Family	Unknown
		Device Name	Unknown
		Updated At	Apr 19, 2012 15:01:26 PDT
		Show Fingerprint	<input type="checkbox"/>

Cancel

## 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:

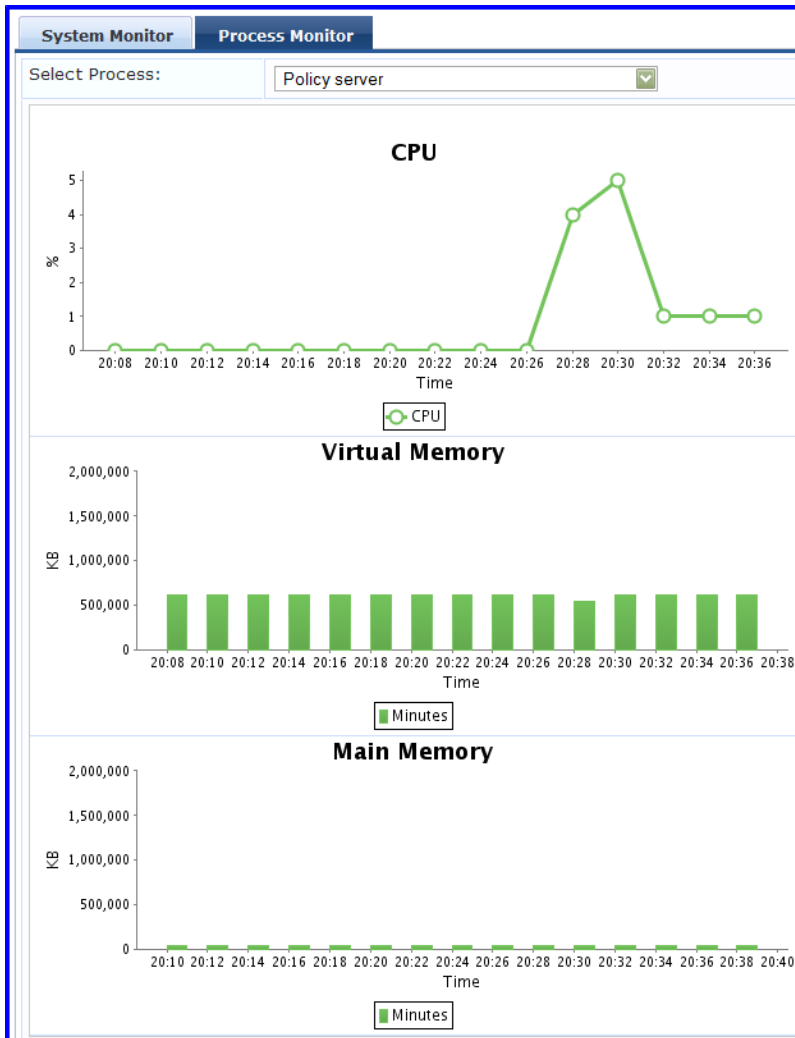
- **System Monitor**. For the selected server, provides load statistics, including CPU, memory, swap memory, physical disk space, and swap disk space:

**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*

Monitoring & Reporting > Audit Viewer

Audit Viewer

Filter: Category contains Go Clear Filter Show 10 records

#	Action	Name	Category	User	Timestamp
1.	MODIFY	ashwath	Local User	admin	Jun 15, 2012 11:53:14 PDT
2.	MODIFY	ashwath	Local User	admin	Jun 15, 2012 11:52:33 PDT
3.	ADD	AirGroup Service	Radius Enforcement Service	santhosh	Jun 14, 2012 10:45:18 PDT
4.	MODIFY	AirGroup Enforcement ..	Enforcement Policy	santhosh	Jun 14, 2012 10:45:18 PDT
5.	MODIFY	AirGroup Response	RADIUS Enforcement Profile	santhosh	Jun 14, 2012 10:45:17 PDT
6.	MODIFY	AirGroup Role Sharing	RADIUS Enforcement Profile	santhosh	Jun 14, 2012 10:45:17 PDT
7.	MODIFY	AirGroup Device Owner	RADIUS Enforcement Profile	santhosh	Jun 14, 2012 10:45:17 PDT
8.	MODIFY	AirGroup User Sharing	RADIUS Enforcement Profile	santhosh	Jun 14, 2012 10:45:17 PDT
9.	MODIFY	AirGroup Location Sha..	RADIUS Enforcement Profile	santhosh	Jun 14, 2012 10:45:17 PDT
10.	ADD	AirGroup Role Mapping	Role Mapping Policy	santhosh	Jun 14, 2012 10:45:17 PDT

Showing 1-10 of 2111 records

**Table 11:** *Audit Viewer*

Container	Description
Select Filter	Select the filter by which to constrain the display of audit data.

Container	Description
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)

**Audit Row Details**

Enforcement Policy - **Test\_enf\_Pol**

**Enforcement Details**

Name	Test_enf_Pol
Description	-
Type	RADIUS
Default Profile	-

**Rules**

Rules Evaluation Algorithm: evaluate-all

Conditions	Enforcement Profiles
1. (Tips:Role EQUALS Role_Engineer) AND (Tips:Posture EQUALS HEALTHY (0))	EMPLOYEE_VLAN
2. (Tips:Role EQUALS Senior_Mgmt) AND (Tips:Posture GREATER_THAN QUARANTINE (20))	EMPLOYEE_VLAN
3. (Tips:Role EQUALS eTIPS_Guest) AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday,	WIRELESS_GUEST_NETWORK

Close

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

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

**Audit Row Details**

Old Data | New Data | Inline Difference

Service Log Configuration - **Radius server**

**Log Configuration**

Node IP	192.168.5.96
Service	Radius server
Can override default log level	true
Syslog support	false

**Modules**

Module Name	Log Level
1. Radius Server	INFO

Close

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

**Audit Row Details**

Old Data **New Data** Inline Difference

Service Log Configuration - Radius server

**Log Configuration**

Node IP	192.168.5.96
Service	Radius server
Can override default log level	true
Syslog support	false

**Modules**

Module Name	Log Level
1. Radius Server	DEBUG

Close

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

**Audit Row Details**

Old Data New Data **Inline Difference**

**Modules**

Module Name	Log Level
1. Radius Server	INFO DEBUG

Modified Added Deleted Moved up Moved down

Close

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*

Monitoring & Reporting > Event Viewer

Event Viewer

Select Server: etips (10.2.48.217)

Filter: Source contains Go Clear Filter Show 10 records

#	Source	Level	Category	Action	Timestamp
1.	Admin UI	INFO	Logged in	None	Jun 18, 2012 11:37:38 PDT
2.	Admin UI	INFO	Logged in	None	Jun 18, 2012 11:33:03 PDT
3.	Admin UI	INFO	Logged out	None	Jun 18, 2012 11:33:03 PDT
4.	Admin UI	INFO	Logged in	None	Jun 18, 2012 11:05:28 PDT
5.	ClearPass Updater	INFO	AV/AS Updates	Success	Jun 18, 2012 11:03:01 PDT
6.	Admin UI	INFO	Logged in	None	Jun 18, 2012 10:58:39 PDT
7.	Admin UI	INFO	Logged in	None	Jun 18, 2012 10:32:51 PDT
8.	ClearPass Updater	INFO	AV/AS Updates	Success	Jun 18, 2012 10:03:02 PDT
9.	Admin UI	INFO	Logged in	None	Jun 18, 2012 09:49:39 PDT
10.	ClearPass Updater	INFO	AV/AS Updates	Success	Jun 18, 2012 09:03:02 PDT

Showing 1-10 of 1191

**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**

The dialog box titled "System Event Details" contains the following information:

Source	RADIUS
Level	INFO
Category	Authentication
Action	None
Timestamp	Mar 10, 2009 02:24:48 PDT
Description	Created EAP-FAST master keys for this server.

A "Close" button is located at the bottom right of the dialog.

## 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 15, "Syslog Export Filters " on page 277, "Analysis and Trending" on page 26, and "Accounting" on page 17 components in Policy Manager. It is available at: **Monitoring> Data Filters**.

**Figure 24 Data Filters**

The screenshot shows the "Data Filters" interface. At the top, there is a breadcrumb "Monitoring » Data Filters" and a title "Data Filters". On the right, there are three icons with labels: "Add Filter", "Import Filters", and "Export Filters". Below this, there is a filter input area with a dropdown menu set to "Name", a text box containing "contains", and a "Go" button. To the right of this is a "Clear Filter" button and a "Show 10 records" dropdown. The main area is a table with 10 rows, each representing a filter. The table has columns for "#", "Name", and "Description".

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

At the bottom of the table, it says "Showing 1-10 of 10". To the right of the table are buttons for "Copy", "Export", and "Delete".

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 Aruba Guest Portal).

**Table 13: Data Filters**

Container	Description
Add Filter	Click to open the Add Filter wizard.
Import Filters	Click to open the <b>Import Filters</b> popup.
Export Filters	Click to open the <b>Export Filters</b> popup. This exports all configured filters.
Copy	Copy the selected filters.
Export	Click to open the <b>Export</b> 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)**

Monitoring » Data Filters » Add

**Data Filters**

**Filter** Rules Summary

Name: All RADIUS Requests

Description: Filter for all RADIUS requests

Configuration Type: ☐ Specify Custom SQL ☒ Select Attributes

Custom SQL:

[Back to Data Filters](#) **Next >** **Save** **Cancel**

**Table 14:** Add Filter (Filter tab)

Container	Description
Name	Name and description of the filter (freeform).
Description	
Configuration Type	<p>Choose one of the following configuration types:</p> <ul style="list-style-type: none"> <li><b>Specify Custom SQL</b> - 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. <i>Note that selecting this option is not recommended. For users who need to utilize this, however, we recommend contacting Support.</i></li> <li><b>Select Attributes</b> - 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.</li> </ul>
Custom SQL	<p>If <b>Specify Custom SQL</b> 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.</p> <p><b>NOTE:</b> We recommend that users who choose this method contact Support. Support can assist you with entering the correct information in this template.</p>

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	<b>Select first match</b> is a logical OR operation of all the rules. <b>Select all matches</b> 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

Dashboard Filters

Conditions

Matches ☒ ANY or ☐ ALL of the following conditions:

	Type	Name	Operator	Value
1.	<div>Common RADIUS TACACS WEBAUTH</div>			
2.				

Save Cancel

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

Container	Description
Matches	<b>ANY</b> matches one of the configured conditions. <b>ALL</b> indicates to match all of the configured conditions.
Type	This indicates the namespace for the attribute. <ul style="list-style-type: none"> <li>Common - These are attributes common to RADIUS, TACACS, and WebAuth requests and responses</li> <li>RADIUS - Attributes associated with RADIUS authentication and accounting requests and responses</li> <li>TACACS - Attributes associated with TACACS authentication, accounting, and policy requests and responses</li> <li>Web Authentication Policy - Policy Manager policy objects assigned after evaluation of policies associated with Web Authentication requests. Example: Auth Method, Auth Source, Enforcement Profiles</li> </ul>
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" on page 37
  - "Viewing Existing Services " on page 39
  - "Adding and Removing Services " on page 40
  - "Links to Use Cases and Configuration Instructions " on page 41
- "Policy Simulation" on page 42
  - "Add Simulation Test" on page 43
  - "Import and Exporting Simulations " on page 48

## 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.



---

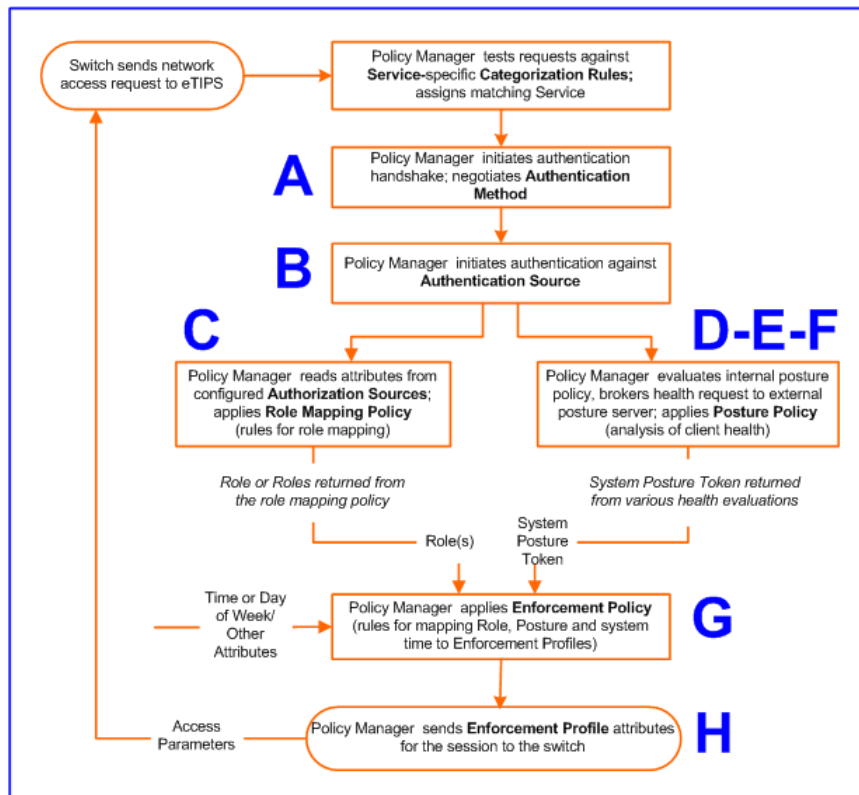
Policy Manager ships configured with a number of basic Service types. You can flesh out these Service types, copy them for use as templates, import other Service types from another implementation (from which you have previously exported them), or develop new Services from scratch

---

- 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
<b>A - Authentication Method</b>	Zero or more per service	<p>EAP or non-EAP method for client authentication. Policy Manager supports four broad classes of authentication methods:</p> <ul style="list-style-type: none"> <li>• <b>EAP, tunneled:</b> PEAP, EAP-FAST, or EAP-TTLS.</li> <li>• <b>EAP, non-tunneled:</b> EAP-TLS or EAP-MD5.</li> <li>• <b>Non-EAP, non-tunneled:</b> 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 <i>MAC Authentication</i> request (and not a spoofed request) and (2) makes sure that the MAC address of the device is present in the authentication source.</li> </ul> <p>Some Services (for example, <i>TACACS+</i>) contain internal authentication methods; in such cases, Policy Manager does not make this tab available.</p>
<b>B - Authentication Source</b>	Zero or more per service	<p>An Authentication Source is the identity repository against which Policy Manager verifies identity. It supports these Authentication Source types:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory</li> <li>• any LDAP compliant directory</li> <li>• RSA or other RADIUS-based token servers</li> <li>• SQL database, including the local user store.</li> <li>• Static Host Lists, in the case of MAC-based Authentication of</li> </ul>

Component	Service: component ratio	Description
		managed devices.
<b>C - Authorization Source</b>	One or more per Authentication Source and zero or more per service	<p>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:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory</li> <li>• any LDAP compliant directory</li> <li>• RSA or other RADIUS-based token servers</li> <li>• SQL database, including the local user store.</li> </ul>
<b>C - Role Mapping Policy</b>	Zero or one per service	<p>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.</p> <p>Some Services (for example, <i>MAC-based Authentication</i>) may handle role mapping differently:</p> <ul style="list-style-type: none"> <li>• For <i>MAC-based Authentication</i> 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.</li> </ul>
<b>D - Internal Posture Policies</b>	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.
<b>E - Posture Servers</b>	Zero or more per service	<p>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).</p> <p>Currently, Policy Manager supports two forms of posture server interfaces: <i>RADIUS</i>, and <i>GAMEv2</i> posture servers.</p>
<b>F - Audit Servers</b>	Zero or more per service	<p>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.</p> <p>In addition to returning posture tokens, Audit Servers can contain post-audit rules that map results from the audit into Roles.</p>
<b>G - Enforcement Policy</b>	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).
<b>H - Enforcement Profile</b>	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*

The screenshot shows the 'Service' tab in the configuration interface. The 'Name' field is 'WIRELESS\_SERVICE' and the 'Description' is '802.1x Wireless service'. The 'Monitor Mode' is checked, with a note 'Enable to monitor network access control without enforcement'. The 'Type' is '802.1x Wireless' and the 'Status' is 'Enabled'. Below this is a 'Service Categorization Rule' section with a table of conditions.

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

- 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*

The screenshot shows the 'Service' tab for 'DOT1X\_WIRED\_SERVICE'. The 'Name' is 'DOT1X\_WIRED\_SERVICE' and the 'Description' is '802.1x Wired service'. The 'Monitor Mode' is 'Disabled', 'Type' is '802.1x Wired', and 'Status' is 'Enabled'. Below is a 'Service Categorization Rule' section with a table of conditions.

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

Below the table is an 'Authentication' section with 'Methods' set to 'eTIPS\_MSCHAP[MSCHAP]' and 'Sources' set to 'eTIPS\_Local\_User\_Repository[Local]'. At the bottom, there is a 'Strip Username Rules' field and buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'.

## 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	<ul style="list-style-type: none"> <li>"802.1x Wireless Use Case" on page 55</li> <li>"Aruba Web Based Authentication Use Case " on page 63.</li> <li>" MAC Authentication Use Case " on page 69.</li> <li>"TACACS+ Use Case" on page 73.</li> </ul>	"Adding Services " on page 103
Authentication Method	<p>"802.1x Wireless Use Case" on page 55 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.</p> <p>"Aruba Web Based Authentication Use Case " on page 63 has only a single authentication method, which is specifically designed for authentication of the request attributes received from the Aruba Web Portal.</p>	"Adding and Modifying Authentication Methods" on page 111
Authentication Source	<ul style="list-style-type: none"> <li>"802.1x Wireless Use Case" on page 55 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.</li> <li>"Aruba Web Based Authentication Use Case " on page 63 uses the local Policy Manager repository, as this is common practice among administrators configuring Guest Users.</li> <li>" MAC Authentication Use Case " on page 69 uses a Static Host List for authentication of the MAC address sent by the switch as the device's username.</li> <li>"TACACS+ Use Case" on page 73 uses the local Policy Manager repository. Other authentication sources would also be fine.</li> </ul>	"Adding and Modifying Authentication Sources " on page 128
Role Mapping	<p>"802.1x Wireless Use Case" on page 55 has an explicit <b>Role Mapping Policy</b> that tests request attributes against a set of rules to assign a role.</p>	<ul style="list-style-type: none"> <li>"Adding and Modifying Role Mapping Policies " on page 157</li> <li>"Adding and</li> </ul>

Policy Component	Illustrative Use Cases	Configuration Instructions
		Modifying Roles " on page 160 <ul style="list-style-type: none"> <li>• "Adding and Modifying Local Users " on page 161</li> <li>• "Adding and Modifying Guest Users " on page 162</li> <li>• "Adding and Modifying Static Host Lists " on page 167</li> </ul>
Posture Policy	"Aruba Web Based Authentication Use Case " on page 63 uses an internal posture policy that evaluates the health of the originating client, based on attributes submitted with the request by the Aruba Web Portal, and returns a corresponding posture token.	"Adding and Modifying Posture Policies " on page 171
Posture Server	"802.1x Wireless Use Case" on page 55 appends a third-party posture server to evaluate health policies based on vendor-specific posture credentials.	"Adding and Modifying Posture Servers " on page 197
Audit Server	" MAC Authentication Use Case " on page 69, uses an Audit Server to provide port scanning for health.	"Configuring Audit Servers" on page 199
Enforcement Policy and Profiles	All Use Cases have an assigned Enforcement Policy and corresponding Enforcement Rules.	<ul style="list-style-type: none"> <li>• "Configuring Enforcement Profiles " on page 210</li> <li>• "Configuring Enforcement Policies " on page 221</li> </ul>

## Policy Simulation

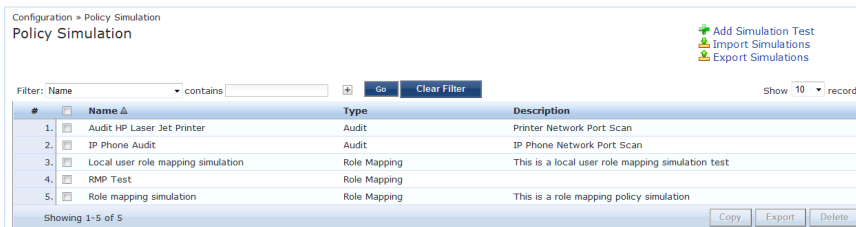
Once the policies have been set up, the Policy Simulation utility can be used to evaluate these policies - before deployment. The Policy Simulation utility applies a set of request parameters as input against a given policy component and displays the outcome, at: **Configuration > Policy Simulation**.

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

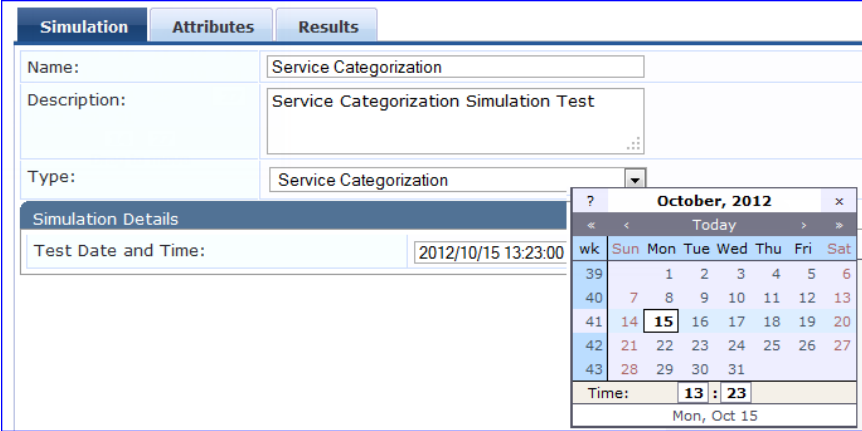
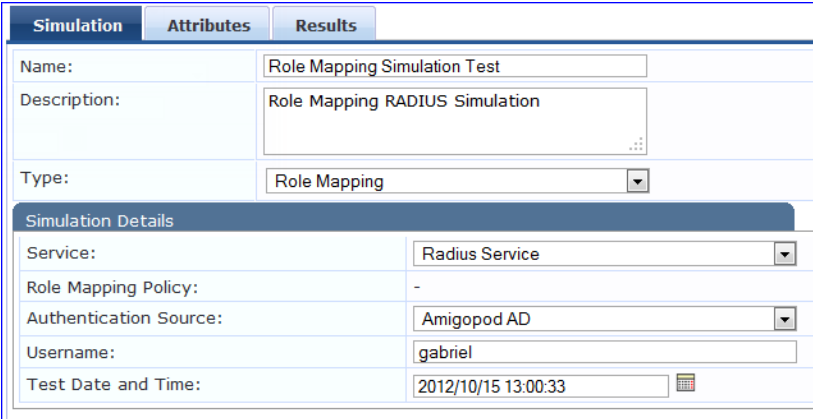
Container	Description
Add Simulation Test	Opens the <b>Add Simulation Test</b> page.
Import Simulations	Opens the <b>Import Simulations</b> popup.
Export Simulations	Opens the <b>Export Simulations</b> popup.
Filter	Select the filter by which to constrain the display of simulation data.
Copy	Make a copy the selected policy simulation. The copied simulation is renamed with a prefix of <b>Copy_Of_</b> .
Export	Opens the <b>Export</b> 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).

Container	Description
Type <b>Service Categorization.</b>	<ul style="list-style-type: none"> <li>Input (<b>Simulation</b> tab): Select <b>Date</b> and <b>Time</b>. (optional - use if you have time based service rules)</li> </ul>  <ul style="list-style-type: none"> <li>Input (<b>Attributes</b> tab): Use the <b>Rules Editor</b> to create a request with the attributes you want to test. All namespaces relevant to service rules creation are loaded in the Attributes editor.</li> <li>Returns (<b>Results</b> tab): <i>Service Name</i> (or status message in case of no match)</li> </ul>
Type <b>Role Mapping.</b>	<ul style="list-style-type: none"> <li>Input (<b>Simulation</b> tab): Select <b>Service</b> (<b>Role Mapping Policy</b> is implicitly selected, because there is only one such policy associated with a service), <b>Authentication Source</b>, <b>User Name</b>, and <b>Date/Time</b>.</li> </ul>  <ul style="list-style-type: none"> <li>Input (<b>Attributes</b> tab): Use the <b>Rules Editor</b> to create a request with the attributes you want to test. All namespaces relevant for role mapping policies are loaded in the attributes editor.</li> <li>Returns (<b>Results</b> tab): <i>Role(s)</i> - including authorization source attributes fetched as roles.</li> </ul>
Type <b>Posture Validation.</b>	<ul style="list-style-type: none"> <li>Input (<b>Simulation</b> tab): Select <b>Service</b> (Posture policies are implicitly selected by their association with the service).</li> </ul>

Container	Description
	<div> <div> <div>Simulation</div> <div>Attributes</div> <div>Results</div> </div> <div> <div>Name:</div> <div>Role Mapping Simulation Test</div> </div> <div> <div>Description:</div> <div>Role Mapping Posture Validation Simulation</div> </div> <div> <div>Type:</div> <div>Posture Validation</div> </div> <div> <div>Simulation Details</div> <div> <div>Service:</div> <div>[Policy Manager Admin Network Login Service]</div> </div> </div> </div> <ul style="list-style-type: none"> <li>Input (<b>Attributes</b> tab): Use the <b>Rules Editor</b> 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.</li> <li>Returns (<b>Results</b> tab): <i>System Posture Status</i> and <i>Status Messages</i>.</li> </ul>
Type <b>Audit.</b>	<ul style="list-style-type: none"> <li>Input (<b>Simulation</b> tab): Select the <b>Audit Server</b> and host to be Audited (IP address or hostname)</li> </ul> <div> <div> <div>Simulation</div> <div>Results</div> </div> <div> <div>Name:</div> <div>Test Audit Simulation</div> </div> <div> <div>Description:</div> <div>Audit Simulation</div> </div> <div> <div>Type:</div> <div>Audit</div> </div> <div> <div>Simulation Details</div> <div> <div>Audit Server:</div> <div>[Nmap Audit]</div> </div> <div> <div>Audit Host IP Address:</div> <div>192.168.34.32</div> </div> </div> </div> <ul style="list-style-type: none"> <li>Returns (<b>Results</b> tab): <i>Summary Posture Status</i>, <i>Audit Attributes</i> and <i>Status</i></li> </ul> <p><b>NOTE: Note:</b> Audit simulations can take a while; an AuditInProgress status is shown until the audit completes.</p>
Type <b>Enforcement Policy.</b>	<ul style="list-style-type: none"> <li>Input (<b>Simulation</b> tab): Select <b>Service</b> (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).</li> </ul>

Simulation	Attributes	Results
Name:	Test Enforcement Policy	
Description:	Enforcement Policy Simulation	
Type:	Enforcement Policy	
<b>Simulation Details</b>		
Service:	[Policy Manager Admin Network Login Service]	
Enforcement Policy:	[Admin Network Login Policy]	
Authentication Source:		
Username:	gabriel	
Roles:	<div> <div>[Contractor]</div> <div>[Employee]</div> <div>[Guest]</div> <div>[Machine Authenticated]</div> <div>[Other]</div> </div>	
Dynamic Roles:	<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> <div>Remove Role</div> <div>Add Role</div>	
System Posture Status:	HEALTHY (0)	
Test Date and Time:	2012/10/08 13:46:29	

- Input (**Attributes** tab): Use the **Rules Editor** to create a request with the attributes you want to test. Connection and RADIUS namespaces are loaded in the attributes editor.
- Returns (**Results** tab): *Enforcement Profile(s)* and the attributes sent to the device.

**NOTE:** Authentication Source and User Name inputs are used to derive dynamic values in the enforcement profile that are fetched from authorization source. These inputs are optional.

**NOTE:** Dynamic Roles are attributes (that are enabled as a role) fetched from the authorization source. For an example of enabling attributes as a role, refer to ["Generic LDAP or Active Directory"](#) on page 129 for more information.

#### Type Chained Simulations.

- Input (**Simulation** tab): Select **Service**, **Authentication Source**, **User Name**, and **Date/Time**.

Simulation	Attributes	Results
Name:	Test Chained Simulation	
Description:	Chained Simulation	
Type:	Chained Simulation	
<b>Simulation Details</b>		
Service:	[Guest Operator Logins]	
Authentication Source:	[Admin User Repository]	
Username:	gabriel	
Test Date and Time:	2012/10/08 13:57:08	

- Input (**Attributes** tab): Use the **Rules Editor** to create a request with the attributes you want to test. All namespaces that are relevant in the Role Mapping Policy context are loaded in the attributes editor.

Container	Description
	<ul style="list-style-type: none"> <li>Returns (<b>Results</b> tab): <i>Role(s)</i>, <i>Post Status</i>, <i>Enforcement Profiles</i> and <i>Status Messages</i>.</li> </ul>
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 <b>Attributes</b> tab.
Start Test	Run test. Outcome is displayed in the <b>Results</b> tab.
Save/Cancel	Click <b>Save</b> to commit or <b>Cancel</b> 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)

Type	Name	Value
1. Connection	Protocol	= RADIUS
2. Radius:IETF	NAS-IP-Address	= 192.168.5.233
3. <div>Device Host LocalUser GuestUser Certificate Authentication Connection Radius:IETF Radius:Clavister Radius:Cisco-VPN3000 Radius:Acc Radius:Tropos Radius:Cisco More choices</div>		

Back to Policy Simulation    Next >    Start Test    Save    Cancel

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)

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

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

[Back to Policy Simulation](#)
[Start Test](#)
[Copy](#)
[Save](#)
[Cancel](#)

## Import and Exporting Simulations

### Import Simulations

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

**Figure 35** Import Simulations

Import from file

Select File:  [Browse...](#)

Enter secret for the file (if any):

[Import](#) [Cancel](#)

**Table 21:** Import Simulations

Container	Description
Select file	Browse to select name of simulations import file.
Import/Cancel	<b>Import</b> to commit or <b>Cancel</b> 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; this is organized based on the type of OS or type of vendor. For example, Windows, Linux, and Mac OS X are some of the families when the category is Computer. Apple, Android are examples of DeviceFamily when category is SmartDevice.
- DeviceName - Devices in a family are further organized based on more granular details such as version. For example, Windows 7 and Windows 2008 server are device names under the Windows family.

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 Aruba 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 Apple 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
- Aruba 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 provided by Aruba 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*

The screenshot shows the 'Add Device' dialog box with the 'SNMP Read Settings' tab selected. The settings are as follows:

Setting	Value/Status
Allow SNMP Read:	<input checked="" type="checkbox"/> Enable Policy Manager to perform SNMP read operations
SNMP Read Setting:	SNMP v2 with community strings
Community String:	.....
Verify:	.....
Force Read:	<input checked="" type="checkbox"/> Enable to read switch information forcibly
Read ARP Table Info:	<input checked="" type="checkbox"/> Enable to read ARP table from this switch

In large or geographically spread cluster deployments you do not want all CPPM nodes to probe all SNMP configured devices. The default 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

Configuration » Profile Settings

### Profile Settings

The following additional Profile techniques may be configured, based on requirements.

**Subnet Scans**  
Specify the IP subnets to be scanned for discovering hosts and their capabilities -

Policy Manager Zone	IP Subnet to Scan	
1. default	= 10.15.0.0/16,10.13.0.0/16,10.12.0.0/16	
2. Click to add...		

## Profiling

The Profile module uses a two-stage approach to classify endpoints using input attributes.

### Stage 1

Stage 1 tries to derive device-profiles using static dictionary lookups. Based on the 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:

#### 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*

Service	Authentication	Roles	Enforcement	Audit	Profiler	Summary
<b>Endpoint Classification:</b> Select the classification(s) after which an action must be triggered-						
<div>SmartDevice Home Audio/Video Equipment Projectors -- Select --</div> <div>Remove</div>						
<b>RADIUS CoA Action:</b> [Aruba Terminate Session] <div>View Details</div> <div>Modify</div> <a href="#">Add new</a>						

## 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.

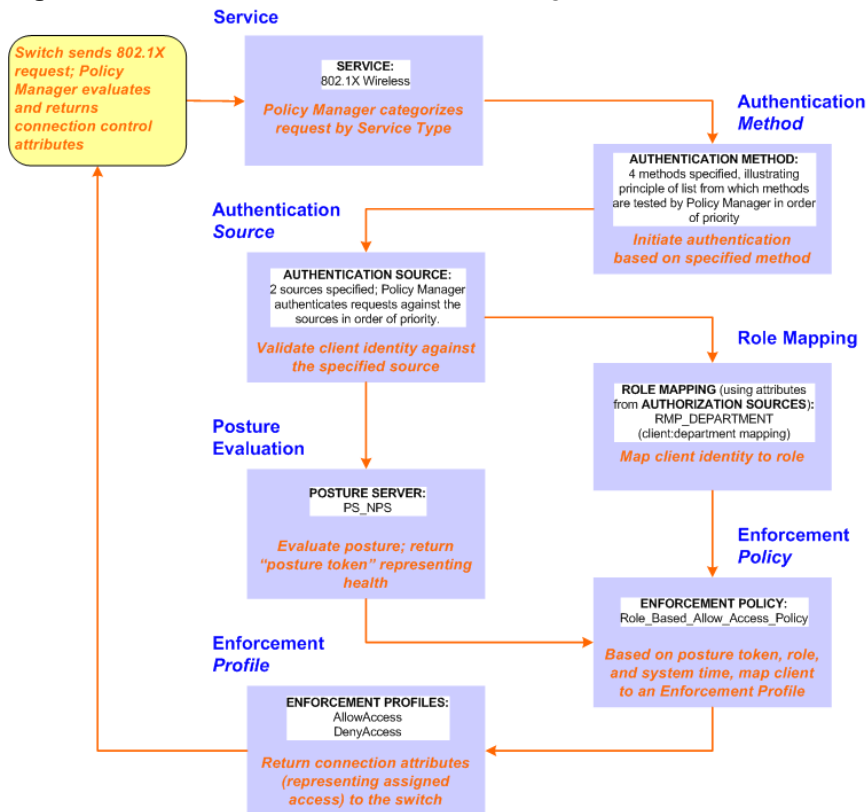
## The Profiler User Interface

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](#) for 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 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 39** *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 22: 802.1X - Create Service Navigation and Settings**

Navigation	Settings																
<p>Create a new Service:</p> <ul style="list-style-type: none"> <li>• <b>Services</b> &gt;</li> <li>• <b>Add Service</b> (link) &gt;</li> </ul>	<div> <p>Configuration » Services</p> <p><b>Services</b></p> <div>  Add Service            Import Services            Export Services         </div> </div>																
<p>Name the Service and select a pre-configured Service Type:</p> <ul style="list-style-type: none"> <li>• <b>Service</b> (tab) &gt;</li> <li>• <b>Type</b> (selector): <b>802.1X Wireless</b> &gt;</li> <li>• <b>Name/Description</b> (freeform) &gt;</li> <li>• Upon completion, click <b>Next</b> (to Authentication)</li> </ul>	<div> <p>Service Authentication Authorization Roles Posture Enforcement Audit Profiler Summary</p> <p>Type: 802.1X Wireless</p> <p>Name:</p> <p>Description: 802.1X Wireless Access Service</p> <p>Monitor Mode: <input type="checkbox"/> Enable to monitor network access without enforcement</p> <p>More Options: <input checked="" type="checkbox"/> Authorization <input checked="" type="checkbox"/> Posture Compliance <input checked="" type="checkbox"/> Audit End-hosts <input checked="" type="checkbox"/> Profile Endpoints</p> <p>Service Rule</p> <p>Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Name</th> <th>Operator</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>1. Radius:IETF</td> <td>NAS-Port-Type</td> <td>EQUALS</td> <td>Wireless-802.11 (19)</td> </tr> <tr> <td>2. Radius:IETF</td> <td>Service-Type</td> <td>BELONGS_TO</td> <td>Login-User (1), Framed-User (2), Authenticate-Only (8)</td> </tr> <tr> <td>3. Click to add...</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Back to Services</p> <p>Next &gt; Save Cancel</p> </div>	Type	Name	Operator	Value	1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	3. Click to add...			
Type	Name	Operator	Value														
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)														
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)														
3. Click to add...																	

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.

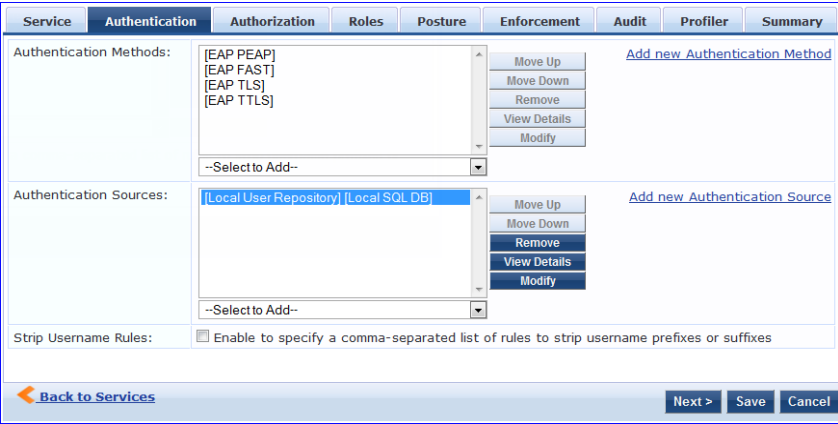
## 2. Configure Authentication.

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 23:** *Configure Authentication Navigation and Settings*

Navigation	Settings
<p>Select an Authentication Method and an Active Directory server (that you have already configured in Policy Manager):</p> <ul style="list-style-type: none"> <li>• <b>Authentication</b> (tab) &gt;</li> <li>• <b>Methods</b> (Select a method from the drop-down list)</li> <li>• <b>Add &gt;</b></li> <li>• <b>Sources</b> (Select drop-down list): <ul style="list-style-type: none"> <li>[Local User Repository] [Local SQL DB]</li> <li>[Guest User Repository] [Local SQL DB]</li> <li>[Guest Device Repository] [Local SQL DB]</li> <li>[Endpoints Repository] [Local SQL DB]</li> <li>[Onboard Devices Repository] [Local SQL DB] &gt;</li> <li>[Admin User Repository] [Local SQL DB] &gt;</li> <li>AmigoPod AD [Active Directory] &gt;</li> </ul> </li> <li>• <b>Add &gt;</b></li> <li>• Upon completion, <b>Next</b> (to configure Authorization)</li> </ul>	

The following field deserves special mention:

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

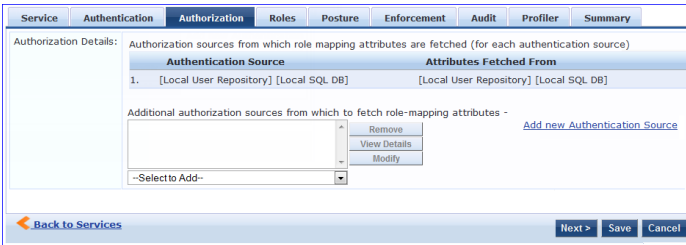


To view detailed setting information for any preconfigured policy component, select the item and click **View Details**.

### 3. Configure Authorization.

Policy Manager fetches attributes for role mapping policy evaluation from the Authorization Sources. In this use case, the Authentication Source and Authorization Source are one and the same.

**Table 24:** *802.1X - Configure Authorization Navigation and Settings*


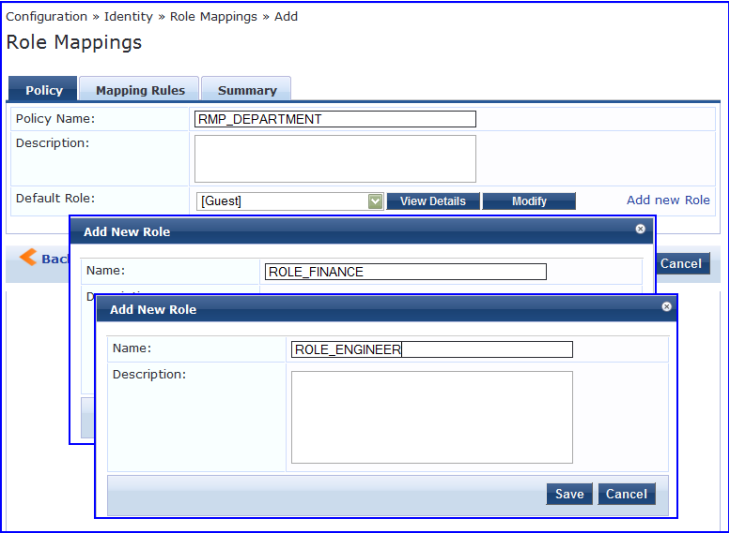
Navigation	Settings
<ul style="list-style-type: none"> <li>• Configure Service level authorization source. In this use case there is nothing to configure. Click the <b>Next</b> button.</li> <li>• Upon completion, click <b>Next</b> (to Role Mapping).</li> </ul>	

### 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 25: Role Mapping Navigation and Settings**

Navigation	Settings
<div>Create the new Role Mapping Policy:<ul style="list-style-type: none"><li>Roles (tab) &gt;</li><li>Add New Role Mapping Policy (link) &gt;</li></ul></div>	<div></div>
<div>Add new Roles (names only):<ul style="list-style-type: none"><li>Policy (tab) &gt;</li><li>Policy Name (freeform): ROLE_ENGINEER &gt;</li><li>Save (button) &gt;</li><li>Repeat for ROLE_FINANCE &gt;</li><li>When you are finished working in the Policy tab, click the Next button (in the Rules Editor)</li></ul></div>	<div></div>

## Navigation

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)

## Settings

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Mapping Rules Summary

Rules Evaluation Algorithm: ☐ Select first match ☒ Select all matches

Role Mapping Rules:

Conditions	Role Name
1. (Authorization:AD:department CONTAINS engineer)	Role_Engineer
2. (Authorization:AD:department CONTAINS finance)	ROLE_FINANCE

Add Rule Move Up Move Down Edit Rule Remove Rule

Rules Editor

Conditions

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator	Value
1. Authorization:AD	department	CONTAINS	finance
2. Click to add...			

Actions

Role Name: 

[Contractor]
[Employee]
[Guest]
[Other]
[TACACS API Admin]
[TACACS Help Desk]
[TACACS Network Admin]
[TACACS Read-only Admin]
[TACACS Receptionist]
[TACACS Super Admin]

Save Cancel

Back to Role Mappings Next > Save Cancel

Add the new Role Mapping Policy to the Service:

- Back in **Roles** (tab) >
- **Role Mapping Policy** (selector): *RMP\_DEPARTMENT* >
- Upon completion, click **Next** (to Posture)

Service Authentication Authorization Roles Posture Audit Enforcement Summary

Role Mapping Policy: RMP\_DEPARTMENT Modify Add new Role Mapping Policy

Role Mapping Policy Details

Description: -
Default Role: [Guest]
Rules Evaluation Algorithm: evaluate-all

Conditions	Role
1. (Authorization:AD:department CONTAINS engineer)	Role_Engineer
2. (Authorization:AD:department CONTAINS finance)	ROLE_FINANCE

Back to Services Next > Save Cancel

## 5. Configure a Posture Server

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

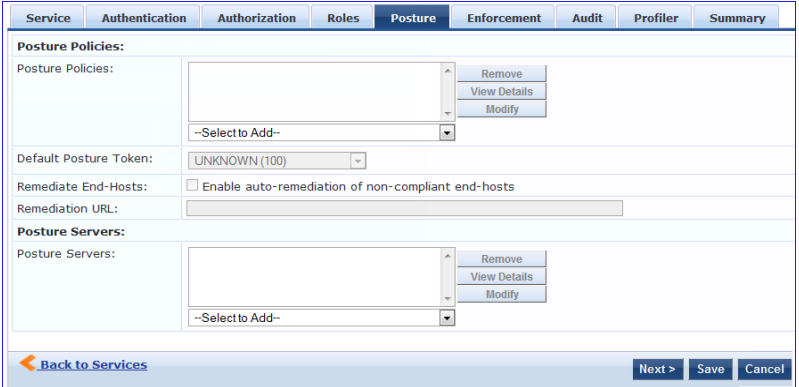
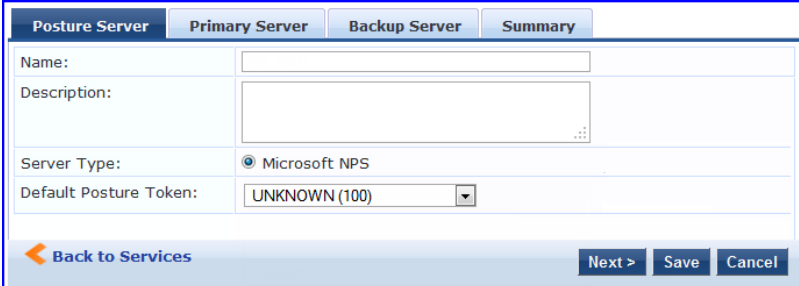
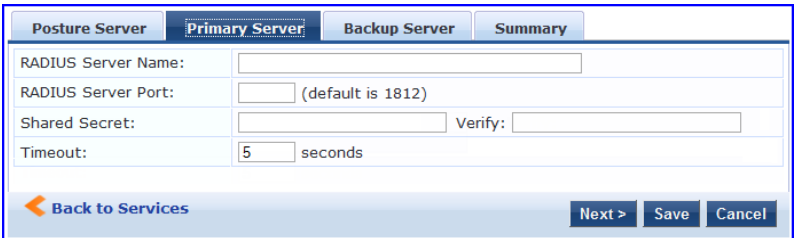
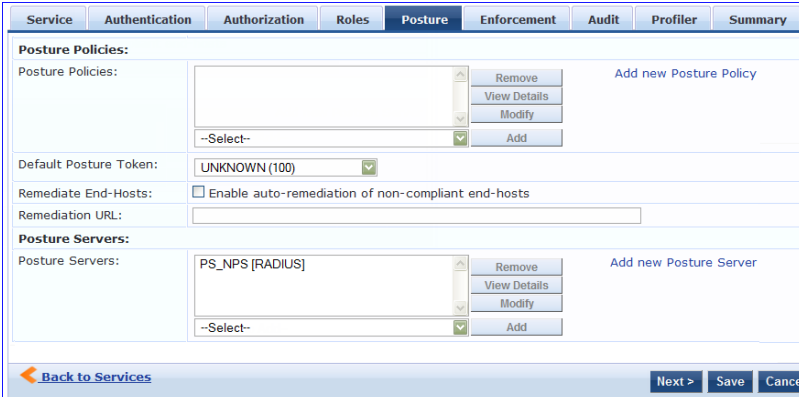
Policy Manager can be configured for a third-party posture server, to evaluate client health based on vendor-specific credentials, typically credentials that cannot be evaluated internally by Policy Manager (that is, not in the form of internal posture policies). Currently, Policy Manager supports the following posture server interface: **Microsoft NPS (RADIUS)**.

Refer to the following table to add the external posture server of type **Microsoft NPS** to the 802.1X service:

ClearPass Policy Manager 6.1 | User Guide

59

**Table 26: Posture Navigation and Settings**

Navigation	Setting
<p>Add a new Posture Server:</p> <ul style="list-style-type: none"> <li>• <b>Posture</b> (tab) &gt;</li> <li>• <b>Add new Posture Server</b> (button) &gt;</li> </ul>	
<p>Configure Posture settings:</p> <ul style="list-style-type: none"> <li>• <b>Posture Server</b> (tab) &gt;</li> <li>• <b>Name</b> (freeform): <b>PS_NPS</b></li> <li>• <b>Server Type</b> (radio button): <b>Microsoft NPS</b></li> <li>• <b>Default Posture Token</b> (selector): <b>UNKNOWN</b></li> <li>• <b>Next</b> (to Primary Server)</li> </ul>	
<p>Configure connection settings:</p> <ul style="list-style-type: none"> <li>• <b>Primary/ Backup Server</b> (tabs): Enter connection information for the RADIUS posture server.</li> <li>• <b>Next</b> (button): from Primary Server to Backup Server.</li> <li>• To complete your work in these tabs, click the <b>Save</b> button.</li> </ul>	
<p>Add the new Posture Server to the Service:</p> <ul style="list-style-type: none"> <li>• Back in the <b>Posture</b> (tab) &gt;</li> <li>• <b>Posture Servers</b> (selector): <b>PS_NPS</b>, then click the <b>Add</b> button.</li> <li>• Click the <b>Next</b> button.</li> </ul>	

## 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 27: Enforcement Policy Navigation and Settings**

Navigation	Setting
Configure the Enforcement Policy: <ul style="list-style-type: none"> <li>● <b>Enforcement</b> (tab) &gt;</li> <li>● <b>Enforcement Policy</b> (selector): <b>Role_Based_Allow_Access_Policy</b></li> </ul>	

For instructions about how to build such an Enforcement Policy, refer to "Configuring Enforcement Policies " on page 221.

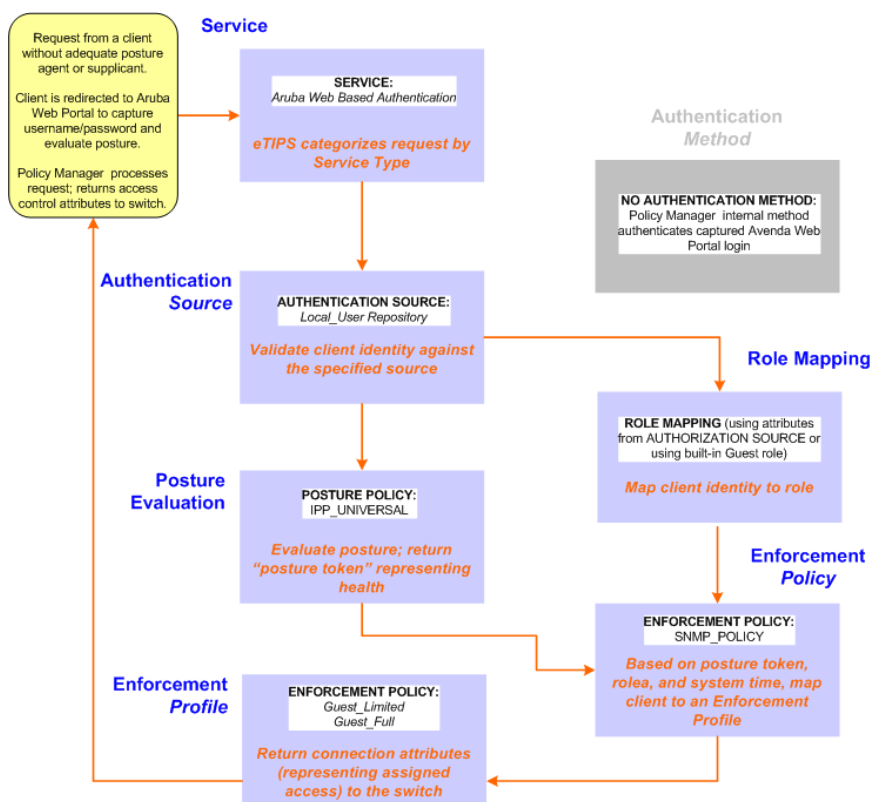
7. Save the Service.

Click **Save**. The Service now appears at the bottom of the **Services** list.



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 40** 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 *Aruba WebAuth* service.  
Refer to your Network Access Device documentation to configure the switch such that it redirects HTTP requests to the *Aruba Guest Portal*, which captures username and password and optionally launches an agent that returns posture data.
2. Create a WebAuth-based Service.

**Table 28:** Service Navigation and Settings

Navigation	Settings
Create a new Service: <ul style="list-style-type: none"> <li>• <b>Services &gt;</b></li> <li>• <b>Add Service &gt;</b></li> </ul>	Configuration » Services Services <div>  Add Service   Import Services   Export Services           </div>

Navigation
Settings

Name the Service and select a pre-configured Service Type:

- **Service** (tab) >
- **Type** (selector): Aruba Web-Based Authentication >
- **Name/Description** (freeform) >
- Upon completion, click **Next**.

Configuration » Services » Add

Services

Service
Authentication
Authorization
Roles
Posture
Enforcement
Summary

Type: Web-based Authentication
Name:
Description: Web Based Authentication for Guests
Monitor Mode: ☐ Enable to monitor network access without enforcement
More Options: ☒ Authorization ☒ Posture Compliance

Service Rule
Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Host	CheckType	MATCHES_ANY	Authentication
2. Click to add...			

Back to Services
Next >
Save
Cancel

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 29: Local Policy Manager Database Navigation and Settings**

Navigation
Settings

Select the local Policy Manager database:

- **Authentication** (tab) >
- **Sources** (Select drop-down list): [Local User Repository] >
- **Add** >
- **Strip Username Rules** (check box) >
- Enter an example of preceding or following separators (if any), with the phrase “user” representing the username to be returned. For authentication, Policy Manager strips the specified separators and any paths or domains beyond them.
- Upon completion, click **Next** (until you reach Enforcement Policy).

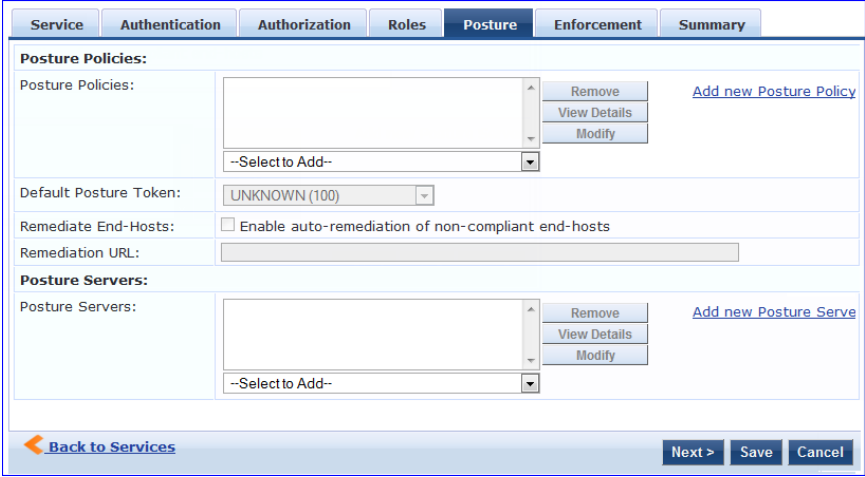
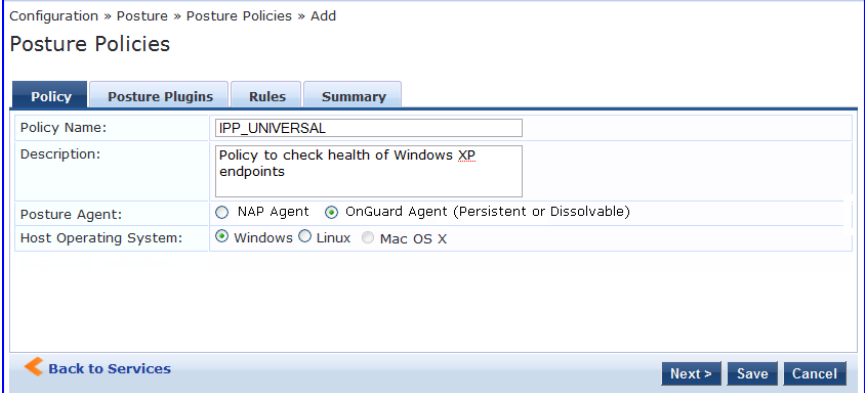
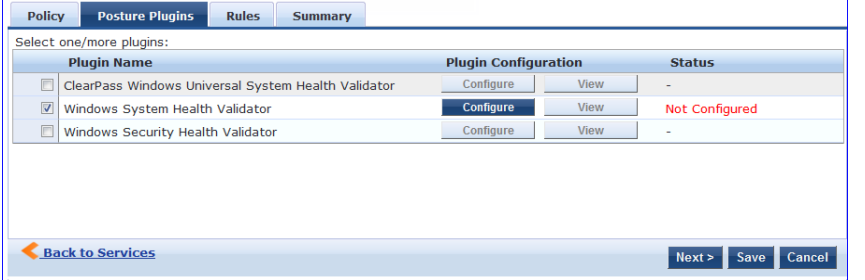
Service
Authentication
Authorization
Roles
Posture
Enforcement
Summary

Authentication Sources: [Local User Repository] [Local SQL DB]
Add new Authentication Source
Move Up
Move Down
Remove
View Details
Modify
--Select to Add--

Strip Username Rules: ☒ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes (user)
If username precedes domain name, use user:<separator> (e.g., user:@)
Otherwise, use <separator>:user (e.g., \user)

Back to Services
Next >
Save
Cancel

**Table 30: Posture Policy Navigation and Settings**

Navigation	Setting
<p>Create a Posture Policy:</p> <ul style="list-style-type: none"> <li>● <b>Posture</b> (tab) &gt;</li> <li>● Enable <b>Validation Check</b> (check box) &gt;</li> <li>● <b>Add new Internal Policy</b> (link) &gt;</li> </ul>	
<p>Name the Posture Policy and specify a general class of operating system:</p> <ul style="list-style-type: none"> <li>● <b>Policy</b> (tab) &gt;</li> <li>● <b>Policy Name</b> (freeform): <i>IPP_UNIVERSAL</i> &gt;</li> <li>● <b>Host Operating System</b> (radio buttons): <b>Windows</b> &gt;</li> <li>● When finished working in the <b>Policy</b> tab, click <b>Next</b> to open the Posture Plugins tab</li> </ul>	
<p>Select a Validator:</p> <ul style="list-style-type: none"> <li>● <b>Posture Plugins</b> (tab) &gt;</li> <li>● Enable <b>Windows Health System Validator</b> &gt;</li> <li>● <b>Configure</b> (button) &gt;</li> </ul>	

Configure the Validator:

- **Windows System Health Validator** (popup) >
- **Enable all Windows operating systems** (check box) >
- Enable Service Pack levels for Windows 7, Vista, XP Server 2008, Server 2008 R2, and Server 2003 (check boxes) >
- **Save** (button) >
- When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)

**Windows System Health Validator**

Client computers can connect to your network, subject to the following checks -

- ☒ **Windows 7**  
Windows 7 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Vista**  
Windows Vista clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows XP**  
Windows XP clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Server 2008**  
Windows Server 2008 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Server 2008 R2**  
Windows Server 2008 R2 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Server 2003**  
Windows Server 2003 clients are allowed

**Reset** **Save** **Cancel**

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.

**Policy** **Posture Plugins** **Rules** **Summary**

Rules Evaluation Algorithm: First applicable

Conditions	Posture Token
1. Passes all SHV checks - Windows System Health Validator	HEALTHY
2. Fails one or more SHV checks - Windows System Health Validator	QUARANTINE

**Add Rule** **Move Up** **Move Down** **Edit Rule** **Remove Rule**

**Rules Editor**

**Conditions**

Select Plugin Checks:

Select Plugins: ☐ Windows System Health Validator

**Actions**

Posture Token:

**Save** **Cancel**

**Back to Services** **Next >** **Save** **Cancel**

### Navigation

Add the new Posture Policy to the Service:  
Back in **Posture** (tab) >  
**Internal Policies** (selector): **IPP\_UNIVERSAL\_XP**, then click the **Add** button

### Setting

Service

Authentication

Authorization

Roles

Posture

Enforcement

Summary

Posture Policies:

Posture Policies:

IPP\_UNIVERSAL

Remove

View Details

Modify

--Select--

Add

Add new Posture Policy

Default Posture Token:

UNKNOWN (100)

Remediate End-Hosts:

☐ Enable auto-remediation of non-compliant end-hosts

Remediation URL:

Posture Servers:

Posture Servers:

Remove

View Details

Modify

--Select--

Add

Add new Posture Server

Back to Services

Next >

Save

Cancel

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 *Aruba 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 31: Enforcement Policy Navigation and Settings**

### Navigation

Add a new Enforcement Policy:

- **Enforcement** (tab) >
- Enforcement Policy (selector): **SNMP\_POLICY**
- Upon completion, click **Save**.

### Setting

Service

Authentication

Authorization

Roles

Posture

Enforcement

Summary

Use Cached Results:

☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy:

SNMP Policy

Modify

Add new Enforcement Policy

Enforcement Policy Details

Description:

-

Default Profile:

Restricted SNMP VLAN

Rules Evaluation Algorithm:

evaluate-all

Conditions

Enforcement Profiles

1. (Tips:Role EQUALS Guest) AND (Tips:Posture EQUALS HEALTHY (0))

Restricted SNMP VLAN

Back to Services

Next >

Save

Cancel

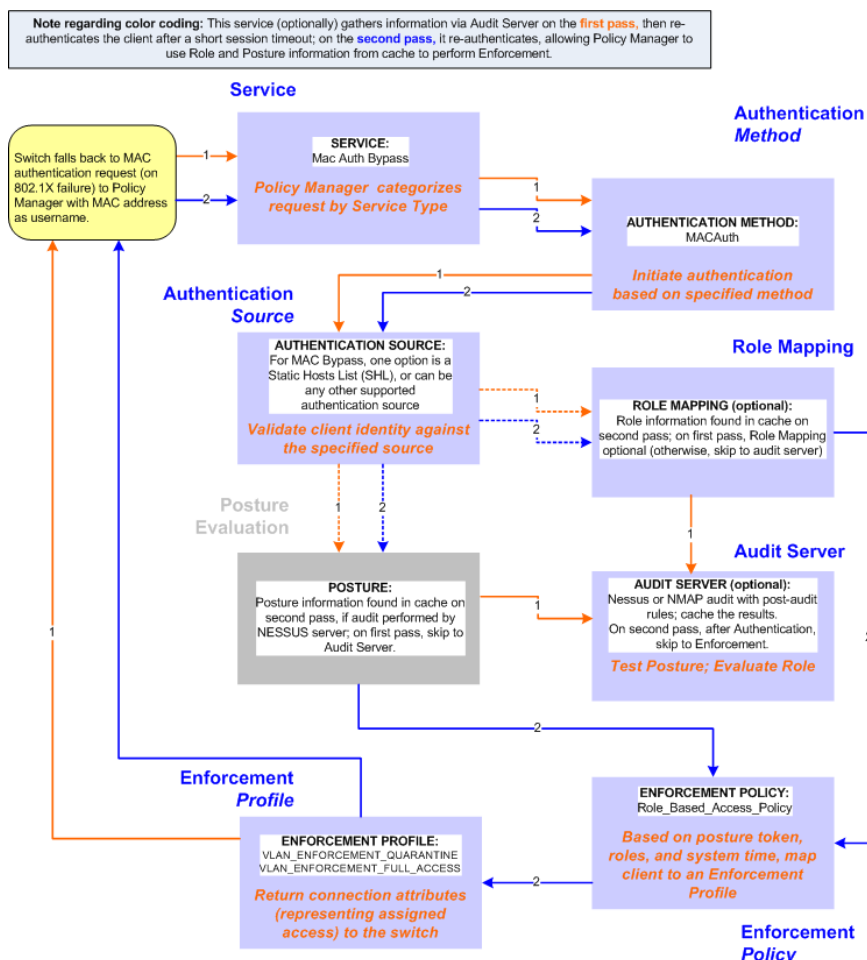
#### 6. Save the Service.

Click **Save**. The Service now appears at the bottom of the **Services** list.



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 41** *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 32: MAC Authentication Service Navigation and Settings**

## Navigation


Create a new Service:

- **Services** >
- **Add Service** (link) >

## Settings

Configuration » Services

### Services



Name the Service and select a pre-configured Service Type:

- **Service** (tab) >
- **Type** (selector): **MAC Authentication** >
- **Name/Description** (freeform) >
- Upon completion, click **Next** to configure Authentication

Configuration » Services » Add

### Services

Service	Authentication	Authorization	Roles	Enforcement	Audit	Profiler	Summary
---------	----------------	---------------	-------	-------------	-------	----------	---------

Type: MAC Authentication

Name:

Description: MAC-based Authentication service

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☒ Authorization ☒ Audit End-hosts ☒ Profile Endpoints

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

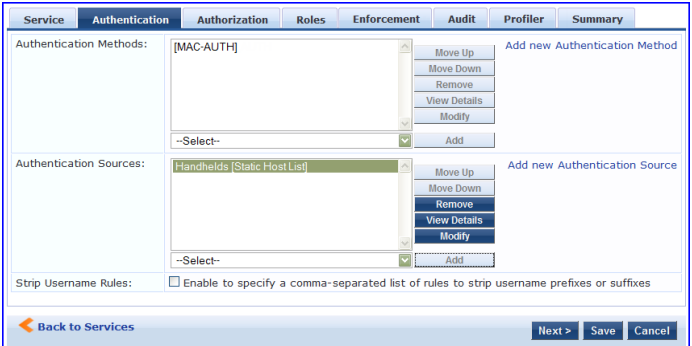
Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2. Radius:IETF	Service-Type	EQUALS	Call-Check (10)
3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4. Click to add...			

[Back to Services](#) [Next >](#) [Save](#) [Cancel](#)

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"](#) on page 167 for more information. You can also select any other supported type of authentication source.

**Table 33: Authentication Method Navigation and Settings**

Navigation	Settings
<p>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):</p> <ul style="list-style-type: none"> <li>• <b>Authentication</b> (tab) &gt;</li> <li>• <b>Methods</b> (This method is automatically selected for this type of service): <b>[MAC AUTH]</b> &gt;</li> <li>• <b>Add</b> &gt;</li> <li>• <b>Sources</b> (Select drop-down list): <b>Handhelds [Static Host List]</b> and Policy Manager Clients White List [Generic LDAP] &gt;</li> <li>• <b>Add</b> &gt;</li> <li>• Upon completion, <b>Next</b> (to Audit)</li> </ul>	

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 34: Audit Server Navigation and Settings**

Navigation	Settings
Configure the Audit Server: <ul style="list-style-type: none"> <li>● <b>Audit</b> (tab) &gt;</li> <li>● <b>Audit End Hosts</b> (enable) &gt;</li> <li>● <b>Audit Server</b> (selector): <b>NMAP</b></li> <li>● <b>Trigger Conditions</b> (radio button): <b>For MAC authentication requests</b></li> <li>● <b>Reauthenticate client</b> (check box): <b>Enable</b></li> </ul>	

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 35: Enforcement Policy Navigation and Settings**

Navigation	Setting
Select the Enforcement Policy: <ul style="list-style-type: none"> <li>● <b>Enforcement</b> (tab) &gt;</li> <li>● <b>Use Cached Results</b> (check box): Select <b>Use cached Roles and Posture attributes from previous sessions</b> &gt;</li> <li>● <b>Enforcement Policy</b> (selector): <b>UnmanagedClientPolicy</b></li> <li>● When you are finished with your work in this tab, click <b>Save</b>.</li> </ul>	

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).

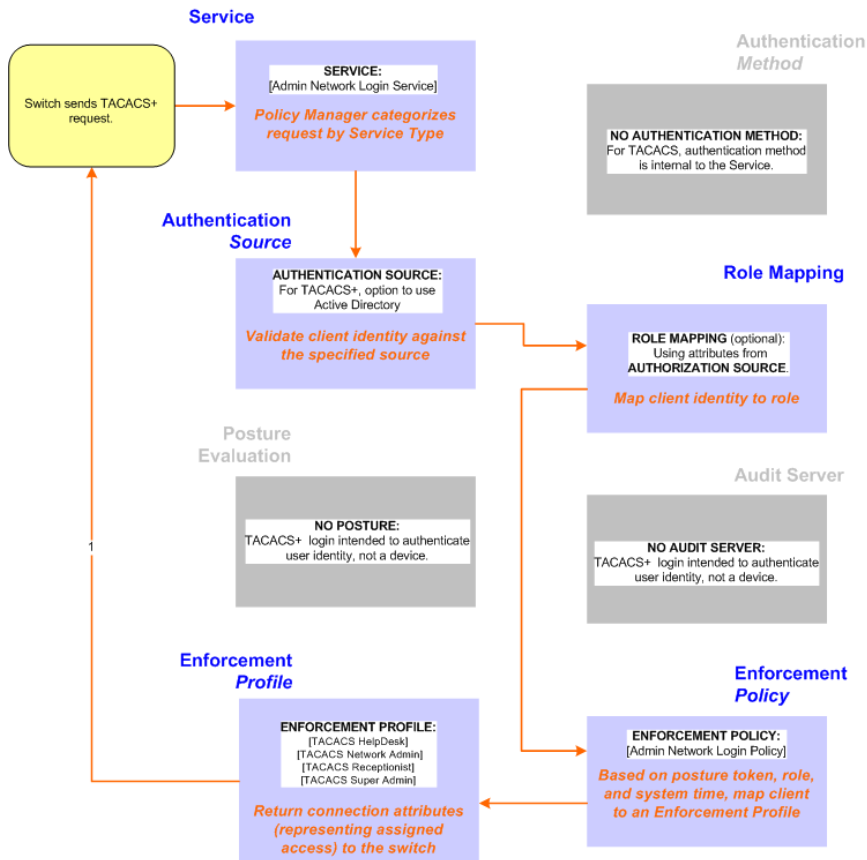
5. Save the Service.

Click **Save**. The Service now appears at the bottom of the **Services** list.



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 42** 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 36:** TACACS+ Navigation and Settings

Navigation	Settings
Create a new Service: <ul style="list-style-type: none"> <li>• <b>Services &gt;</b></li> <li>• <b>Add Service</b> (link) &gt;</li> </ul>	Configuration » Services Services <div>  Add Service              Import Services              Export Services           </div>

Navigation	Settings
<p>Name the Service and select a pre-configured Service Type:</p> <ul style="list-style-type: none"> <li>● <b>Service</b> (tab) &gt;</li> <li>● <b>Type</b> (selector): <b>[Policy Manager Admin Network Login Service]</b> &gt;</li> <li>● <b>Name/Description</b> (freeform) &gt;</li> <li>● Upon completion, click <b>Next</b> (to Authentication)</li> </ul>	

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 37: Active Directory Navigation and Settings**

Navigation	Settings
<p>Select an Active Directory server (that you have already configured in Policy Manager):</p> <ul style="list-style-type: none"> <li>● <b>Authentication</b> (tab) &gt;</li> <li>● <b>Add</b> &gt;</li> <li>● <b>Sources</b> (Select drop-down list): <b>AD (Active Directory)</b> &gt;</li> <li>● <b>Add</b> &gt;</li> <li>● Upon completion, click <b>Next</b> (to Enforcement Policy)</li> </ul>	

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 38: Enforcement Policy Navigation and Settings**

Navigation	Setting
<p>Select the Enforcement Policy:</p> <ul style="list-style-type: none"> <li>● <b>Enforcement</b> (tab) &gt;</li> <li>● <b>Enforcement Policy</b> (selector): <b>Device Command Authorization Policy</b></li> <li>● When you are finished with your work in this tab, click <b>Save</b>.</li> </ul>	

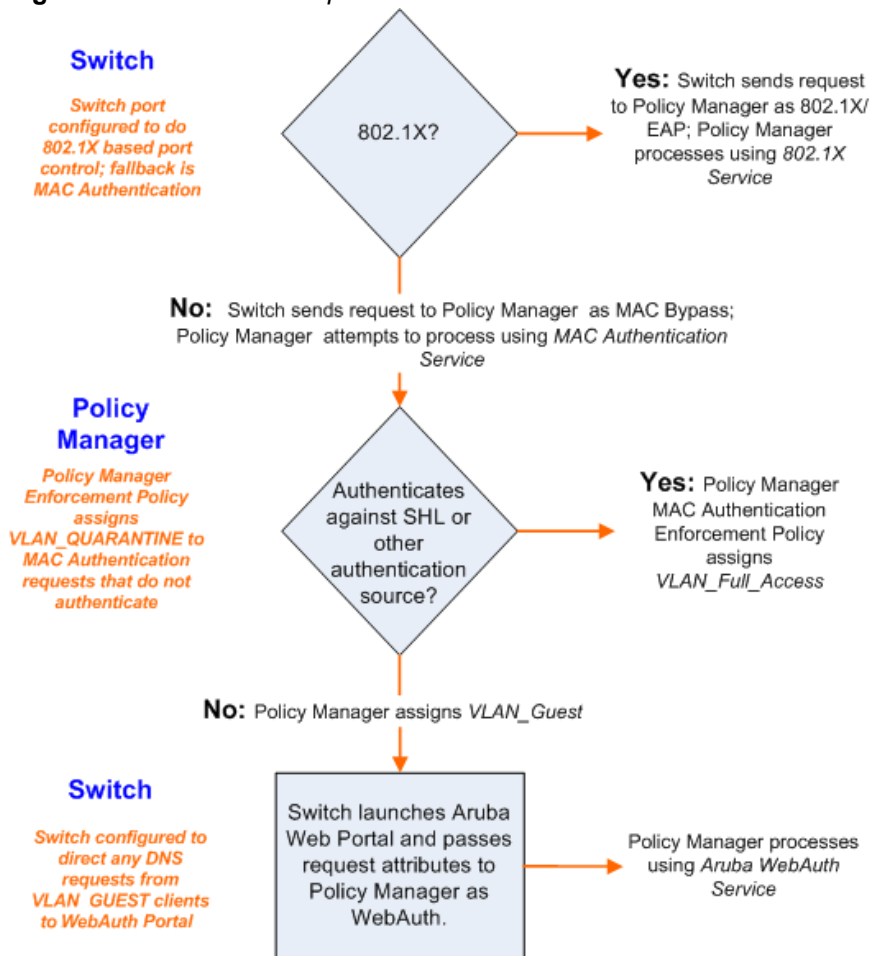
4. Save the Service.
 

Click **Save**. The Service now appears at the bottom of the **Services** list.

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 43** *Flow of the Multiple Protocol Per Port Case*





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. Aruba Networks 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
- Aruba Application Authentication
- Aruba Application Authorization
- Cisco Web Authentication Proxy

Refer to the following sections for more detailed information:

- ["Architecture and Flow " on page 77](#)
- ["Start Here Page " on page 78](#)
- ["Policy Manager Service Types" on page 80](#)
- ["Services " on page 102](#)
  - ["Adding Services " on page 103](#)
  - ["Modifying Services " on page 105](#)
  - ["Reordering Services " on page 107](#)

## 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.

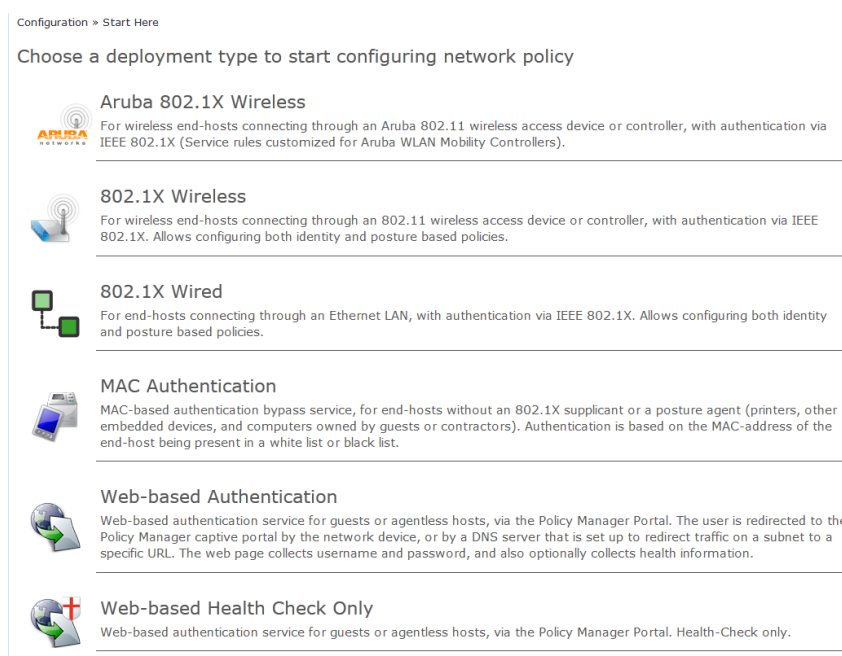
To help you get started, Policy Manager comes pre-configured with 14 different Service types or templates. If these service types do not suit your needs, you can roll your own service with custom service rules.

## 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 44** *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 45** *Service Wizard with Clickable Flow*

Configuration » Services » Add

### Services



Service	Authentication	Authorization	Roles	Posture	Enforcement	Audit	Profiler	Summary
Type:	802.1X Wireless							
Name:								
Description:	802.1X Wireless Access Service							
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement							
More Options:	<input checked="" type="checkbox"/> Authorization <input checked="" type="checkbox"/> Posture Compliance <input checked="" type="checkbox"/> Audit End-hosts <input checked="" type="checkbox"/> Profile Endpoints							
<b>Service Rule</b>								
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:								
	Type	Name	Operator	Value				
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-				
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-Use Authentic				
3.	Click to add...							

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 39: Policy Manager Service Types**

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)																
<div></div> <div>Aruba 802.1X Wireless</div>	<p>Template for wireless hosts connecting through an Aruba 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Service rules are customized for a typical Aruba WLAN Mobility Controller deployment.</p> <p>Refer to the "802.1X Wireless " on page 80 service type for a description of the different tabs.</p>																
<div></div> <div>802.1X Wireless</div>	<p>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 <b>More Options</b> section, click on Authorization, Posture Compliance, Audit End Hosts, or Profile Endpoints to enable additional tabs.</p> <div><div><div>Service</div><div>Authentication</div><div>Roles</div><div>Enforcement</div><div>Summary</div></div><div><div>Type:</div><div>802.1X Wireless</div></div><div><div>Name:</div><div></div></div><div><div>Description:</div><div>802.1X Wireless Access Service</div></div><div><div>Monitor Mode:</div><div><input type="checkbox"/> Enable to monitor network access without enforcement</div></div><div><div>More Options:</div><div><input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints</div></div><div><div>Service Rule</div></div><div><div>Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:</div></div><div><table><tr><th>Type</th><th>Name</th><th>Operator</th><th>Value</th></tr><tr><td>1. Radius:IETF</td><td>NAS-Port-Type</td><td>EQUALS</td><td>Wireless</td></tr><tr><td>2. Radius:IETF</td><td>Service-Type</td><td>BELONGS_TO</td><td>Log</td></tr><tr><td>3. Click to add...</td><td></td><td></td><td></td></tr></table></div></div> <p>To configure authentication methods and authentication source, click on the <b>Authentication</b> tab.</p> <p>The <i>Authentication methods</i> 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.</p> <p>The <i>Authentication sources</i> 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 128.</p> <p>You can enable <b>Strip Username Rules</b> to, optionally, pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.</p> <div><div><div>Service</div><div>Authentication</div><div>Roles</div><div>Enforcement</div><div>Summary</div></div><div><div>Authentication Methods:</div><div><div>[EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS]</div><div>--Select to Add--</div></div><div><div>Move Up Move Down Remove View Details Modify</div></div></div><div><div>Authentication Sources:</div><div><div></div><div>--Select to Add--</div></div><div><div>Move Up Move Down Remove View Details Modify</div></div></div><div><div>Strip Username Rules:</div><div><input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes</div></div></div>	Type	Name	Operator	Value	1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless	2. Radius:IETF	Service-Type	BELONGS_TO	Log	3. Click to add...			
Type	Name	Operator	Value														
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless														
2. Radius:IETF	Service-Type	BELONGS_TO	Log														
3. Click to add...																	

## Service Type

Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)

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 111](#).

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 157](#).

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 an Aruba 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 Policies* and *Posture Servers* refer to topics: ["Adding and Modifying Posture Policies" on page 171](#) and ["Adding and Modifying Posture Servers" on page 197](#).

The screenshot shows the 'Posture' tab of the configuration interface. It contains sections for 'Posture Policies' and 'Posture Servers'. Each section has a list box with 'Remove', 'View Details', and 'Modify' buttons, and a '--Select to Add--' dropdown. Below these are fields for 'Default Posture Token' (set to 'UNKNOWN (100)'), 'Remediate End-Hosts' (checkbox), and 'Remediation URL'.

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.

The screenshot shows the 'Audit' tab of the configuration interface. It includes fields for 'Audit Server' (a dropdown menu), 'Audit Trigger Conditions' (radio buttons for 'Always', 'When posture is not available', and 'For MAC authentication request'), and 'Action after audit' (radio buttons for 'No Action', 'Do SNMP bounce', and 'Trigger RADIUS CoA action').

Select an **Audit Server** - either built-in or customized. Refer to "[Configuring Audit Servers](#)" on page 199 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 221) for a service.

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions Enforcement Policy: [Sample Allow Access Policy] <a href="#">Modify</a> <a href="#">Add new</a>				
<b>Enforcement Policy Details</b>				
Description:		Sample policy to allow network access		
Default Profile:		[Allow Access Profile]		
Rules Evaluation Algorithm:		evaluate-all		
<b>Conditions</b>		<b>Enforcement Profiles</b>		
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)		[Allow Access Profile]		

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	Authentication	Roles	Enforcement	Audit	Profiler	Summary
Endpoint Classification: Select the classification(s) after which an action must be triggered- SmartDevice Home Audio/Video Equipment Projectors -- Select -- <a href="#">Remove</a>						
RADIUS CoA Action: [Aruba Terminate Session] <a href="#">View Details</a> <a href="#">Modify</a> <a href="#">Add new</a>						

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 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 111](#).

Service	Authentication	Authorization	Roles	Enforcement	Summary												
Authorization Details: Authorization sources from which role mapping attributes are fetched (for each authentication source) <table border="1"> <thead> <tr> <th>Authentication Source</th> <th>Attributes Fetched From</th> </tr> </thead> <tbody> <tr> <td colspan="2">Additional authorization sources from which to fetch role-mapping attributes -</td> </tr> <tr> <td></td> <td><a href="#">Remove</a></td> </tr> <tr> <td></td> <td><a href="#">View Details</a></td> </tr> <tr> <td></td> <td><a href="#">Modify</a></td> </tr> <tr> <td colspan="2">--Select to Add--</td> </tr> </tbody> </table>						Authentication Source	Attributes Fetched From	Additional authorization sources from which to fetch role-mapping attributes -			<a href="#">Remove</a>		<a href="#">View Details</a>		<a href="#">Modify</a>	--Select to Add--	
Authentication Source	Attributes Fetched From																
Additional authorization sources from which to fetch role-mapping attributes -																	
	<a href="#">Remove</a>																
	<a href="#">View Details</a>																
	<a href="#">Modify</a>																
--Select to Add--																	

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 157](#).

Configuration » Services » Add					
<b>Services</b>					
Service	Authentication	Roles	Enforcement	Summary	
Role Mapping Policy: --Select-- <a href="#">Modify</a> <a href="#">Add new Role Mapping Policy</a>					
<b>Role Mapping Policy Details</b>					
Description:		-			
Default Role:		-			
Rules Evaluation Algorithm:		-			
<b>Conditions</b>		<b>Role</b>			

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 an Aruba 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 Policies* and *Posture Servers* refer to topics: ["Adding and Modifying Posture Policies "](#) on page 171 and ["Adding and Modifying Posture Servers "](#) on page 197.

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 199](#) 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.

## Service Type

Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)

You must select an enforcement policy (see ["Configuring Enforcement Policies " on page 221](#)) for a service.

Enforcement Policy Details	
Description:	Sample policy to allow network access
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	evaluate-all

Conditions	Enforcement Profiles
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	[Allow Access Profile]

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.

Endpoint Classification	
Select the classification(s) after which an action must be triggered-	<div> <div>SmartDevice</div> <div>Home Audio/Video Equipment</div> <div>Projectors</div> <div>-- Select --</div> </div>

RADIUS CoA Action	
[Aruba Terminate Session]	<a href="#">View Details</a> <a href="#">Modify</a> <a href="#">Add new</a>



### 802.1X Wired

For clients connecting through an Ethernet LAN, with authentication via IEEE 802.1X.

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

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 80](#) service type for a description of the different tabs.



### 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.

Service	Authentication	Roles	Enforcement	Summary
Type:	MAC Authentication			
Name:				
Description:	MAC-based Authentication Service			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints			
<b>Service Rule</b>				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Etherne	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-Us	
3. Connection	Client-Mac-Address	EQUALS	%{Radiu	
4. Click to add...				


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](#)" on page 167), 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.






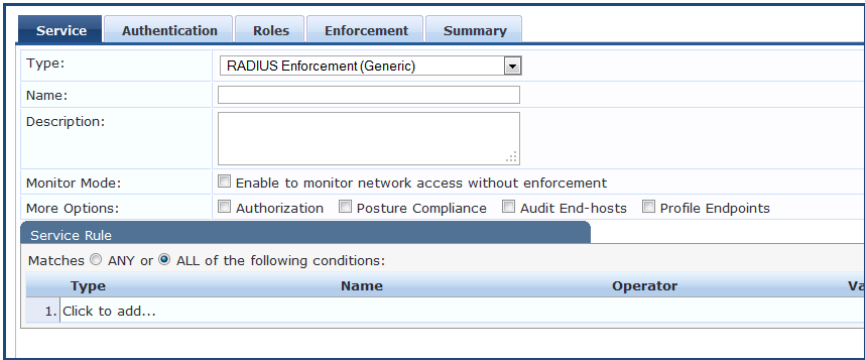
Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:	<div> <div>[MAC AUTH]</div> <div> Move Up Move Down Remove View Details Modify </div> </div> <div>--Select to Add--</div>			
Authentication Sources:	<div> <div>[Endpoints Repository] [Local SQL DB]</div> <div> Move Up Move Down Remove View Details Modify </div> </div> <div>--Select to Add--</div>			
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			

**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.

Service	Authentication	Roles	Enforcement	Audit	Summary
Audit Server:	<div>--Select--</div> <div>View Details    Modify</div>				
Audit Trigger Conditions:	<input type="radio"/> Always <input type="radio"/> When posture is not available <input checked="" type="radio"/> For MAC authentication request <input type="radio"/> For known end-hosts only <input type="radio"/> For unknown end-hosts only <input type="radio"/> For all end-hosts				
Action after audit:	<input type="radio"/> No Action <input type="radio"/> Do SNMP bounce <input checked="" type="radio"/> Trigger RADIUS CoA action <div>[Aruba Terminate Session]    View Details    Modify</div>				

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>No Action:</b> The audit will not apply policies on the network device after this audit.</li> <li>• <b>Do SNMP bounce:</b> 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.</li> <li>• <b>Trigger RADIUS CoA action:</b> This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.</li> </ul> <p>Refer to the <a href="#">"802.1X Wireless " on page 80</a> service type for a description of the other tabs.</p>
 <p>Web-based Authentication</p>	<p>Web-based authentication service for guests or agentless hosts, via the Aruba built-in Portal. The user is redirected to the Aruba 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, Vista, Windows XP, Windows Server 2008, Windows 2000, Windows Server 2003, popular Linux systems). There is an internal service rule (<i>Connection:Protocol EQUALS WebAuth</i>) that categorizes request into this type of service. You can add other rules, if needed.</p> <div data-bbox="436 1031 1295 1402"> </div> <p>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.</p> <div data-bbox="436 1528 1295 1747"> </div> <p>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 <a href="#">"802.1X Wireless " on page 80</a> service type for a description of the other tabs.</p>

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
 <p>Web-based Health Check Only</p>	<p>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 (<i>Connection:Protocol EQUALS WebAuth</i>) 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: <i>Host:CheckType EQUALS Health</i>.</p>
 <p>Web-based Open Network Access</p>	<p>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.</p>
 <p>802.1X Wireless - Identity Only</p>	<p>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.</p>
 <p>802.1X Wired - Identity Only</p>	<p>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.</p>
 <p>RADIUS Enforcement [Generic]</p>	<p>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.</p> <div data-bbox="435 1335 1295 1692">  </div> <p><b>NOTE:</b> 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 <b>Authorization</b>, <b>Posture Compliance</b>, <b>Audit End-hosts</b> and <b>Profile Endpoints</b> options to enable additional tabs. Refer to the "802.1X Wireless " on page 80 service type for a description of the other tabs.</p>

## Service Type

Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)



### 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.



### TACACS+ Enforcement

Template for any kind of TACACS+ request.

## Service Type

Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)

Service	Authentication	Roles	Enforcement	Summary
Type:	TACACS+ Enforcement			
Name:				
Description:				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input checked="" type="checkbox"/> Authorization			
<b>Service Rule</b>				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Click to add...				

**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 329 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 216 for more information.

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	[Admin Network Login Policy]			<a href="#">Modify</a>
<b>Enforcement Policy Details</b>				
Description:	Enforcement policy controlling access to Policy Manager Admin			
Default Profile:	[TACACS Deny Profile]			
Rules Evaluation Algorithm:	evaluate-all			
Conditions	Enforcement Profiles			
1. (Tips:Role MATCHES_ANY [TACACS Help Desk])	[TACACS Help Desk]			
2. (Tips:Role MATCHES_ANY [TACACS Network Admin])	[TACACS Network Admin]			
3. (Tips:Role MATCHES_ANY [TACACS Receptionist])	[TACACS Receptionist]			
4. (Tips:Role MATCHES_ANY [TACACS Super Admin])	[TACACS Super Admin]			



## Aruba Application Authentication

This type of service provides authentication and authorization to users of Aruba applications: GuestConnect and Insight. [Application Enforcement Profiles](#) can be sent to these or other generic applications for authorizing the users.

Service	Authentication	Authorization	Roles	Enforcement	Summary
Type:	Aruba Application Authentication				
Name:					
Description:	Authentication Service for Applications				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement				
More Options:	<input checked="" type="checkbox"/> Authorization				
<b>Service Rule</b>					
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:					
Type	Name	Operator	Value		
1. Application	Name	EQUALS	Enter App Name		
2. Click to add...					



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.

Service Type	Description/ Available Policy Components (in tabs)/ Service Rule (in Rules Editor)/ Service-specific policy components (called out with legend below)
Cisco Web-Authentication Proxy	<p>By default, this service uses the Authentication Method [PAP] [PAP]. You can click on the <b>Authorization</b> and <b>Audit End-hosts</b> options to enable additional tabs. Refer to the "802.1X Wireless" on page 80 service type for a description of these tabs.</p>

## Service Templates

ClearPass Policy Manager Provides the ability to create templates for services where you can define baseline policies and require specific data when you create services. Service templates are for creating services and other components such as role-mapping policies, enforcement policies, and network devices with a fill in the blanks approach. You fill in various fields and Policy Manager creates all the different configuration elements that are needed for the service. These various configuration elements are added back to the service when it is created.

The services templates include

- 802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless
- ClearPass Admin Access
- ClearPass Admin SSO Login
- EDUROAM
- Guest Access - Web Login Pre-Auth
- Guest Access
- Guest MAC Authentication
- Onboard Authorization

**Figure 46** *Service Templates home page*

Configuration » Service Templates

### Service Templates

Select Template Category: All Templates

	<b>802.1X Wired</b> 802.1X Wired Access Service
	<b>802.1X Wireless</b> 802.1X Wireless Access Service
	<b>Aruba 802.1X Wireless</b> Aruba 802.1X Wireless Access Service
	<b>ClearPass Admin Access</b> ClearPass Admin Access Description
	<b>ClearPass Admin SSO Login</b> Application service that allows SAML-based Single Sign-On (SSO) authenticated users to access the application.
	<b>EDUROAM service</b> EDUROAM service
	<b>Guest Access - Web Login Pre-Auth</b> Service for login authentication check at the Guest captive portal (RADIUS pre-auth)
	<b>Guest Access</b> Service for guest access via captive portal (non-802.1x)
	<b>Guest MAC Authentication</b> Service performing authentication for cached MAC entries for guest accounts
	<b>Onboard Authorization</b> Service controlling whether a users device may be provisioned using Onboard

The following sections describe how to create a template.

## 802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless

The 902.1X Wired template is designed for end-hosts connecting through an Ethernet LAN, with authentication via IEEE 802.1X. It allows configuring both identity and posture based policies. The 902.1X Wireless template is intended for wireless end-hosts connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. It allows configuring both identity and posture based policies. The Aruba 802.1X Wireless template is designed for wireless end-hosts connecting through an Aruba 802.11 wireless access device or controller, with authentication via IEEE 802.1X (Service rules customized for Aruba WLAN Mobility Controllers). All three templates are configured using identical parameters.

**Figure 47** *802.1X Wired, 902.1X Wireless, and Aruba 802.1X Wireless Service Template*

Name Prefix:

#### Authentication

AD Name\*:

Description:

Server\*:

Identity\*:

NETBIOS\*:

Base DN\*:

Password\*:

Port\*:

#### Enforcement Details

Attribute Name	Attribute Value	VLAN ID
Department	<input type="text"/>	<input type="text"/>
Department	<input type="text"/>	<input type="text"/>
Department	<input type="text"/>	<input type="text"/>
Default VLAN ID	<input type="text"/>	

#### Wireless Network Settings

Wireless controller name:

Controller IP Address:

Vendor Name:

RADIUS Shared Secret:

Enable RADIUS CoA: ☐

RADIUS CoA Port:

**Table 40:** 802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless Service Template Parameters

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Authentication</b>	
AD Name	Enter your active directory name.
Description	Enter a description that will help you identify the characteristics of this template.
Server	Enter the hostname or the IP address of the Active Directory server.
Identity	Enter the Distinguished Name of the administrator account
NETBIOS	Enter the server Active Directory domain name.
Base DN	.Enter DN of the node in your directory tree from which to start searching for records.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
<b>Enforcement Details</b>	
Attribute Name	The active directory attribute name
Attribute Value	The active directory attribute value.
VLAN ID	Standard RADIUS-IETF VLAN ID.
<b>Wireless Network Settings</b>	
Wireless controller name	The name given to the Wireless Controller.
Controller IP Address	The wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable Radius - Initiated Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device..

## ClearPass Admin Access

This template is designed for TACACS+ service that authenticates users against Active Directory (AD) and uses AD attributes to determine appropriate privilege level for ClearPass Policy Manager admin access.

**Figure 48** *ClearPass Admin Access Service Template*

Configuration > Service Templates

Service Templates - ClearPass Admin Access

TACACS+ service that authenticates users against Active Directory (AD) and uses AD attributes to determine appropriate privilege level for ClearPass Policy Manager admin access.

Name Prefix:

**Authentication**

AD Name\*:

Description:

Server\*:

Identity\*:

NETBIOS\*:

Base DN\*:

Password\*:

Port\*:

**Role Mapping**

Name\*:  Description:

Attribute Name\*:  Super Admin Condition\*:  ex : enter Ad group name for super admin users

Attribute Name\*:  Read Only Admin Condition\*:  ex : enter ad group name for read only users

Attribute Name\*:  Help Desk Condition\*:  ex : enter Ad group name for help desk users

**Table 41:** *ClearPass Admin Access Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Authentication</b>	
AD Name	Enter the hostname or the IP address of the Active Directory server.
Description	Enter a description that will help you identify the characteristics of this template.
Server	Enter the hostname or the IP address of the Active Directory server.
Identity	Enter the Distinguished Name of the administrator account
NETBIOS	Enter the server Active Directory domain name.
Base DN	Enter the Distinguished Name of the administrator account.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
<b>Role Mapping</b>	
Name/Description	Enter a free-form name and description here.
Attribute Name	Select the active directory attribute.
Super Admin Condition	Defines the privilege levels.
Read Only Admin Condition	
Help Desk Condition	

## ClearPass Admin SSO Login

This template is designed for application service that allows SAML-based Single Sign-On (SSO) authenticated users to access the application

**Figure 49** *ClearPass Admin SSO Login Service Template*

The screenshot shows the 'Service Templates - ClearPass Admin SSO Login' configuration page. At the top, there is a breadcrumb 'Configuration » Service Templates'. Below the title, there is a 'Name Prefix:' label followed by an empty text input field. A section titled 'Service Rule' is highlighted with an orange border. Inside this section, there is an 'Application\*:' label followed by a dropdown menu currently showing 'PolicyManager'. At the bottom right of the form are two buttons: 'Add Service' and 'Cancel'.

**Table 42:** *ClearPass Admin SSO Login Service Template Parameters*

Parameter		Description
Name Prefix		Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Service Rule</b>		
Application		Select the application that single-sign-on-authenticated administrative users will be able to access.

## EDUROAM

This template is designed for three types of situations:

- Med Center users connecting to eduroam within the Med Center wireless network.
- Roaming users from other campuses connecting to the Med Center wireless network.
- Roaming Med Center users connecting from UCLA Campus or other campuses that are part of the eduroam federation.

**Figure 50** EDUROAM Service Template

Configuration » Service Templates

### Service Templates - EDUROAM service

Name Prefix:

**Service Rule**

Enter domain details\*:  ex : @edunet.ucla.com  
Select Vendor\*:

**Authentication**

AD Name\*:   
Description:   
Server\*:   
Identity\*:   
NETBIOS\*:   
Base DN\*:   
Password\*:   
Port\*:

**Wireless Network Settings**

Wireless controller name:   
Controller IP Address:   
Vendor Name:   
RADIUS Shared Secret:   
Enable RADIUS CoA: ☐  
RADIUS CoA Port:

**FLRs**

Host Name\*:   
Vendor Name\*:   
RADIUS Shared Secret\*:   
Enable RADIUS CoA\*: ☐  
RADIUS CoA Port\*:   
RADIUS Authentication Port\*:   
RADIUS Accounting Port \*:

Add Service Cancel

**Table 43:** EDUROAM Service Template Parameters

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Service Rule</b>	<b>Service Rule</b>
Enter domain details	Enter the domain name of the network.
Select Vendor	Select the vendor of the network device.

Parameter	Description
<b>Authentication</b>	
AD Name	Enter the hostname or the IP address of the Active Directory server.
Description	Enter a description that will help you identify the characteristics of this template.
Server	Enter the hostname or the IP address of the Active Directory server.
Identity	Enter the Distinguished Name of the administrator account
NETBIOS	Enter the server Active Directory domain name.
Base DN	Enter the Distinguished Name of the administrator account.
Password	Enter the account password.
Port	Enter the TCP port where the server is listening for connection.
<b>Wireless Network Settings</b>	
Wireless controller name	The name given to the Wireless Controller.
Controller IP Address	The wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable Radius - Initiated Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device..
<b>FLRs</b>	
Host Name	The hostname of the federation RADIUS server.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable Radius - Initiated Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device..
RADIUS Authentication Port	Enter a port number here.
RADIUS Accounting Port	Enter a port number here.

## Guest Access - Web Login Pre-Auth

**Figure 51** *Web Login Pre-Auth Service Template*

Configuration > Service Templates

Service Templates - Guest Access - Web Login Pre-Auth

Name Prefix:

**Wireless Network Settings**

Wireless controller name:

Controller IP Address:

Vendor Name:

RADIUS Shared Secret:

Enable RADIUS CoA: ☐

RADIUS CoA Port:

**Guest Access Restrictions**

Days allowed for access\*: ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

**Table 44:** *Web Login Pre-Auth Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Wireless Network Settings</b>	
Wireless controller name	The name given to the Wireless Controller.
Controller IP Address	The wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable Radius - Initiated Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device..
<b>Guest Access Restrictions</b>	
Days allowed for access	Select the days on which access is allowed.

## Guest Access

This template is designed for authenticating guest users who login via captive portal. Guests must re-authenticate after session expiry. Guest Access can be restricted based on day of the week, bandwidth limit and number of unique devices used by the guest user.

**Figure 52** *Guest Access Service Template*

**Table 45:** *Guest Access Service Template Parameters*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Wireless Network Settings</b>	
Wireless SSID for Guest access	Enter the SSID value here.
Wireless controller name	The name given to the Wireless Controller.
Controller IP Address	The wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable Radius - Initiated Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device..
<b>Guest Access Restrictions</b>	
Days allowed for access	Select the days on which access is allowed.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data, in megabytes, a user is allowed per day. A value of 0 (zero). the default, means no limit is set.

## Guest MAC Authentication

This template is designed for authenticating guest accounts based on the cached MAC Addresses used during authentication. A guest can belong to a specific role, such as Contractor, Guest, or Employee, and

each role can have different lifetime for the cached MAC Address.

**Figure 53** *Guest MAC Authentication Service Template*

**Table 46:** *Guest MAC Authentication Service Template Parameters.*

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Wireless Network Settings</b>	<b>Wireless Network Settings</b>
Wireless SSID for Guest access	Enter the SSID name of your network.
Wireless controller name	The name given to the Wireless Controller.
Controller IP Address	The wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable Radius - Initiated Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device..
<b>MAC Caching Settings</b>	
Cache duration for Guest Role	Enter the number of days the MAC account will remain valid for Guest Role. After this the guest will need to re-authenticate via captive portal.

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

## Onboard Authorization

This template is designed for configuration that allows checks to be performed before allowing Onboard provisioning for BYOD use-cases.

**Figure 54** Onboard Authorization Service Template

Configuration » Service Templates

Service Templates - Onboard Authorization

Name Prefix:

**Wireless Network Settings**

Wireless controller name:

Controller IP Address:

Vendor Name:

RADIUS Shared Secret:

Enable RADIUS CoA: ☐

RADIUS CoA Port:

**Guest Access Restrictions**

Days allowed for access\*: ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

**Provisioning Wireless Network Settings**

Wireless SSID for Onboard Provisioning\*:

**Table 47:** Onboard Authorization Service Template Parameters

Parameter	Description
Name Prefix	Enter an optional prefix that will be prepended to services using this template. Use this to identify services that use templates.
<b>Wireless Network Settings</b>	
Wireless controller name	The name given to the Wireless Controller.
Controller IP Address	The wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.

Parameter	Description
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable Radius - Initiated Change of Authorization on the network device.
RADIUS CoA Port	By default this is port 3799 if Radius CoA is enabled. Change this value only if you defined a custom port on the network device..
<b>Guest Access Restrictions</b>	
Days allowed for access	Select the days on which access is allowed.
<b>Provisioning Wireless Network Settings</b>	
Wireless SSID for Onboard Provisioning	Enter the SSID of your network.

## Services

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

**Figure 55** *Service Listing Page*

Services					
Filter: [Name] contains [ ] [Go] [Clear Filter] Show [10] records					
#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	2	[Guest Operator Logins]	Application	Aruba Application Authentication	●
3.	3	Radius Service	RADIUS	RADIUS Enforcement (Generic)	●
Showing 1-3 of 3					

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

**Table 48:** *Services page*

Label	Description
Add Service	Add a service
Import Services	Import previously exported services
Export Service	Export all currently defined services, including all associated policies
Filter	Filter the service listing by specifying values for different listing fields (Name, Type, Template, Status)
Status	The status displays in the last column of the table. A green/red icon indicates enabled/disabled state. Clicking on the icon allows you to toggle the status of a Service between Enabled and Disabled. Note that when a service is in Monitor Mode, an [m] indicator is displayed next to the status icon.

Label	Description
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 103](#)
- ["Modifying Services " on page 105](#)
- ["Reordering Services " on page 107](#)

## 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 56** Add Service Page

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

**Table 49:** Service Page (General Parameters)

Label	Description
Type	<p>Select the desired service type from the drop down menu. When working with service rules, you can select from the following namespace dictionaries:</p> <ul style="list-style-type: none"> <li>• <b>Application:</b> The type of application for this service.</li> <li>• <b>Authentication:</b> The Authentication method to be used for this service.</li> <li>• <b>Connection:</b> Originator address (Src-IP-Address, Src-Port), Destination address (Dest-IP-Address, Dest-Port), and Protocol</li> <li>• <b>Device:</b> Filter the service based on a specific device type, vendor, operating system location, or controller ID.</li> <li>• <b>Date:</b> Time-of-Day, Day-of-Week, or Date-of-Year</li> <li>• <b>Endpoint:</b> Filter based on endpoint information, such as enabled/disabled, device, OS, location, and more.</li> <li>• <b>Host:</b> Filter based on host Name, OSType, FQDN, UserAgent, CheckType, UniqueID,</li> </ul>

Label	Description												
	<p>Agent-Type, and InstalledSHAs,</p> <ul style="list-style-type: none"><li>● <b>RADIUS:</b> Policy Manager ships with a number of vendor-specific namespace dictionaries and distinguishes vendor-specific RADIUS namespaces with the notation <i>RADIUS:vendor</i> (sometimes with an additional suffix for a particular device). To add a dictionary for a vendor-specific RADIUS namespace, navigate to <b>Administration &gt; Dictionaries &gt; Radius &gt; Import Dictionary</b> (link). The notation <b>RADIUS:IETF</b> 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.</li><li>● Any other supported namespace. See <a href="#">"Namespaces" on page 329</a> for an exhaustive list of namespaces and their descriptions.</li></ul> <p>To create new Services, you can copy or import other Services for use <i>as is</i> or as templates, or you can create a new Service from scratch.</p>												
Name	Label for a Service.												
Description	Description for a Service (optional).												
Monitor Mode	<p>Optionally check the <b>Enable to monitor network access without enforcement</b> 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.</p> <p>Policy Manager also allows <i>Policy Simulation</i> (<b>Monitoring &gt; Policy Simulation</b>) where the administrator can test for the results of a particular configuration of policy components.</p>												
More Options	<p>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:</p> <ul style="list-style-type: none"><li>● <b>Authorization:</b> Select an authorization source from the drop down menu to add the source or select the <b>Add new Authentication Source</b> link to create a new source.</li><li>● <b>Posture Compliance:</b> 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 <b>Add new Posture Server</b> link.</li></ul> <div><div>Services</div><div><div>Service</div><div>Authentication</div><div>Authorization</div><div>Roles</div><div>Posture</div><div>Enforcement</div><div>Audit</div><div>Profiler</div><div>Summary</div></div><div>Authorization Details:</div><div>Authorization sources from which role mapping attributes are fetched (for each authentication source)</div><div><table><thead><tr><th>Authentication Source</th><th>Attributes Fetched From</th></tr></thead><tbody><tr><td colspan="2">Additional authorization sources from which to fetch role-mapping attributes -</td></tr><tr><td>[Local User Repository] [Local SQL DB]</td><td>Remove</td></tr><tr><td>[Endpoints Repository] [Local SQL DB]</td><td>View Details</td></tr><tr><td>PTDOMAIN AD [Active Directory]</td><td>Modify</td></tr><tr><td colspan="2">--Select to Add--</td></tr></tbody></table></div><div>Add new</div></div> <ul style="list-style-type: none"><li>● <b>Audit End-hosts:</b> Select an Audit Server - either built-in or customized. Refer to <a href="#">"Configuring Audit Servers" on page 199</a> for audit server configuration steps. For this type of service you can perform audit <b>Always</b>, <b>When posture is not available</b>, or <b>For MAC authentication requests</b>.</li></ul>	Authentication Source	Attributes Fetched From	Additional authorization sources from which to fetch role-mapping attributes -		[Local User Repository] [Local SQL DB]	Remove	[Endpoints Repository] [Local SQL DB]	View Details	PTDOMAIN AD [Active Directory]	Modify	--Select to Add--	
Authentication Source	Attributes Fetched From												
Additional authorization sources from which to fetch role-mapping attributes -													
[Local User Repository] [Local SQL DB]	Remove												
[Endpoints Repository] [Local SQL DB]	View Details												
PTDOMAIN AD [Active Directory]	Modify												
--Select to Add--													

Label	Description																																																																			
	<div data-bbox="402 205 1261 436"> <table border="1"> <thead> <tr> <th>Service</th> <th>Authentication</th> <th>Authorization</th> <th>Roles</th> <th>Posture</th> <th>Enforcement</th> <th>Audit</th> <th>Summary</th> </tr> </thead> <tbody> <tr> <td colspan="2">Audit Server:</td> <td colspan="2">--Select--</td> <td colspan="2">View Details</td> <td colspan="2">Modify</td> </tr> <tr> <td colspan="2">Audit Trigger Conditions:</td> <td colspan="6"> <input type="radio"/> Always  <input type="radio"/> When posture is not available  <input type="radio"/> For MAC authentication request </td> </tr> <tr> <td colspan="2">Action after audit:</td> <td colspan="6"> <input checked="" type="radio"/> No Action  <input type="radio"/> Do SNMP bounce  <input type="radio"/> Trigger RADIUS CoA action </td> </tr> </tbody> </table> </div> <p>You can specify to trigger an audit always, when posture is not available, or for MAC authentication requests. If <b>For MAC authentication requests</b> is specified, then you can perform an audit <b>For known end-hosts only</b> or <b>For unknown end hosts only</b>, or <b>For all end hosts</b>. 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:</p> <ul style="list-style-type: none"> <li>■ <b>No Action:</b> The audit will not apply policies on the network device after this audit.</li> <li>■ <b>Do SNMP bounce:</b> 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.</li> <li>■ <b>Trigger RADIUS CoA action:</b> This option sends a RADIUS Change of Authorization command to the network device by Policy Manager.</li> </ul> <p>● Optionally configure <b>Profiler</b> 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 <b>Add new RADIUS CoA Action</b> link.</p> <div data-bbox="402 1056 1261 1266"> <table border="1"> <thead> <tr> <th>Service</th> <th>Authentication</th> <th>Roles</th> <th>Enforcement</th> <th>Audit</th> <th>Profiler</th> <th>Summary</th> </tr> </thead> <tbody> <tr> <td colspan="2">Endpoint Classification:</td> <td colspan="5">Select the classification(s) after which an action must be triggered-</td> </tr> <tr> <td colspan="2"></td> <td colspan="2"> <input checked="" type="checkbox"/> SmartDevice  <input type="checkbox"/> Home Audio/Video Equipment  <input type="checkbox"/> Projectors  -- Select -- </td> <td colspan="3">Remove</td> </tr> <tr> <td colspan="2">RADIUS CoA Action:</td> <td colspan="2">[Aruba Terminate Session]</td> <td colspan="2">View Details</td> <td>Modify</td> </tr> <tr> <td colspan="2"></td> <td colspan="5"><a href="#">Add new</a></td> </tr> </tbody> </table> </div>	Service	Authentication	Authorization	Roles	Posture	Enforcement	Audit	Summary	Audit Server:		--Select--		View Details		Modify		Audit Trigger Conditions:		<input type="radio"/> Always <input type="radio"/> When posture is not available <input type="radio"/> For MAC authentication request						Action after audit:		<input checked="" type="radio"/> No Action <input type="radio"/> Do SNMP bounce <input type="radio"/> Trigger RADIUS CoA action						Service	Authentication	Roles	Enforcement	Audit	Profiler	Summary	Endpoint Classification:		Select the classification(s) after which an action must be triggered-							<input checked="" type="checkbox"/> SmartDevice <input type="checkbox"/> Home Audio/Video Equipment <input type="checkbox"/> Projectors -- Select --		Remove			RADIUS CoA Action:		[Aruba Terminate Session]		View Details		Modify			<a href="#">Add new</a>				
Service	Authentication	Authorization	Roles	Posture	Enforcement	Audit	Summary																																																													
Audit Server:		--Select--		View Details		Modify																																																														
Audit Trigger Conditions:		<input type="radio"/> Always <input type="radio"/> When posture is not available <input type="radio"/> For MAC authentication request																																																																		
Action after audit:		<input checked="" type="radio"/> No Action <input type="radio"/> Do SNMP bounce <input type="radio"/> Trigger RADIUS CoA action																																																																		
Service	Authentication	Roles	Enforcement	Audit	Profiler	Summary																																																														
Endpoint Classification:		Select the classification(s) after which an action must be triggered-																																																																		
		<input checked="" type="checkbox"/> SmartDevice <input type="checkbox"/> Home Audio/Video Equipment <input type="checkbox"/> Projectors -- Select --		Remove																																																																
RADIUS CoA Action:		[Aruba Terminate Session]		View Details		Modify																																																														
		<a href="#">Add new</a>																																																																		

## 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 57** Service Listing Page

Services					
<div> Add Service  Import Services  Export Services </div>					
Filter: Name contains <input type="text"/> <input type="button" value="Go"/> <input type="button" value="Clear Filter"/> <span>Show 10 records</span>					
#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	<span style="color: green;">●</span>
2.	2	[Guest Operator Logins]	Application	Aruba Application Authentication	<span style="color: green;">●</span>
3.	3	Radius Service	RADIUS	RADIUS Enforcement (Generic)	<span style="color: green;">●</span>
Showing 1-3 of 3 <input type="button" value="Reorder"/> <input type="button" value="Copy"/> <input type="button" value="Export"/> <input type="button" value="Delete"/>					

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 58 Services Configuration**

The screenshot shows the 'Service' configuration page. The 'Name' field is '[Policy Manager Admin Network Login Service]'. The 'Description' is 'Service for access to Policy Manager Admin for network users'. The 'Type' is 'TACACS+ Enforcement', 'Status' is 'Enabled', and 'Monitor Mode' is 'Enable to monitor network access without enforcement'. The 'More Options' section has 'Authorization' checked. The 'Service Rule' table has one rule: '1. Connection' with 'NAD-IP-Address' as the 'Name', 'EQUALS' as the 'Operator', and '127.0.0.1' as the 'Value'. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'.

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

**Table 50: 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. <b>NOTE:</b> You can disable a service by clicking the <b>Disable</b> button on the bottom-right corner of the form. This button will toggle between <b>Enable</b> and <b>Disable</b> 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.
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 51: 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: <ul style="list-style-type: none"> <li>● <b>Application:</b> The type of application for this service.</li> <li>● <b>Authentication:</b> The Authentication method to be used for this service.</li> <li>● <b>Connection:</b> Originator address (Src-IP-Address, Src-Port), Destination address (Dest-IP-Address, Dest-Port), and Protocol</li> <li>● <b>Device:</b> Filter the service based on a specific device type, vendor, operating system location, or controller ID.</li> <li>● <b>Date:</b> Time-of-Day, Day-of-Week, or Date-of-Year</li> </ul>

Label	Description
	<ul style="list-style-type: none"> <li>● <b>Endpoint:</b> Filter based on endpoint information, such as enabled/disabled, device, OS, location, and more.</li> <li>● <b>Host:</b> Filter based on host Name, OSType, FQDN, UserAgent, CheckType, UniqueID, Agent-Type, and InstalledSHAs,</li> <li>● <b>RADIUS:</b> Policy Manager ships with a number of vendor-specific namespace dictionaries and distinguishes vendor-specific RADIUS namespaces with the notation <i>RADIUS:vendor</i> (sometimes with an additional suffix for a particular device). To add a dictionary for a vendor-specific RADIUS namespace, navigate to <b>Administration &gt; Dictionaries &gt; Radius &gt; Import Dictionary</b> (link). The notation <b>RADIUS:IETF</b> 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.</li> <li>● Any other supported namespace. See <a href="#">"Namespaces" on page 329</a> for an exhaustive list of namespaces and their descriptions.</li> </ul>
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 <a href="#">"Operators" on page 335</a> 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 59** *Service Reorder Button*

The screenshot shows the 'Configuration > Services' page. At the top right are links for 'Add Service', 'Import Services', and 'Export Services'. Below these is a filter section with 'Filter: Name' and a 'Go' button. A table lists three services: 1. [Policy Manager Admin Network Login Service] (TACACS, TACACS+ Enforcement), 2. [Guest Operator Logins] (Application, Aruba Application Authentication), and 3. Radius Service (RADIUS, RADIUS Enforcement (Generic)). At the bottom right of the table is a 'Reorder' button, along with 'Copy', 'Export', and 'Delete' buttons.

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	2	[Guest Operator Logins]	Application	Aruba Application Authentication	●
3.	3	Radius Service	RADIUS	RADIUS Enforcement (Generic)	●

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

**Figure 60** *Reordering Services*

Configuration » Services » Reorder

Reorder Services

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

Move Up Move Down

Service Details:

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

Service Rule

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

Back to Services Save Cancel

**Table 52:** *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 method 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.

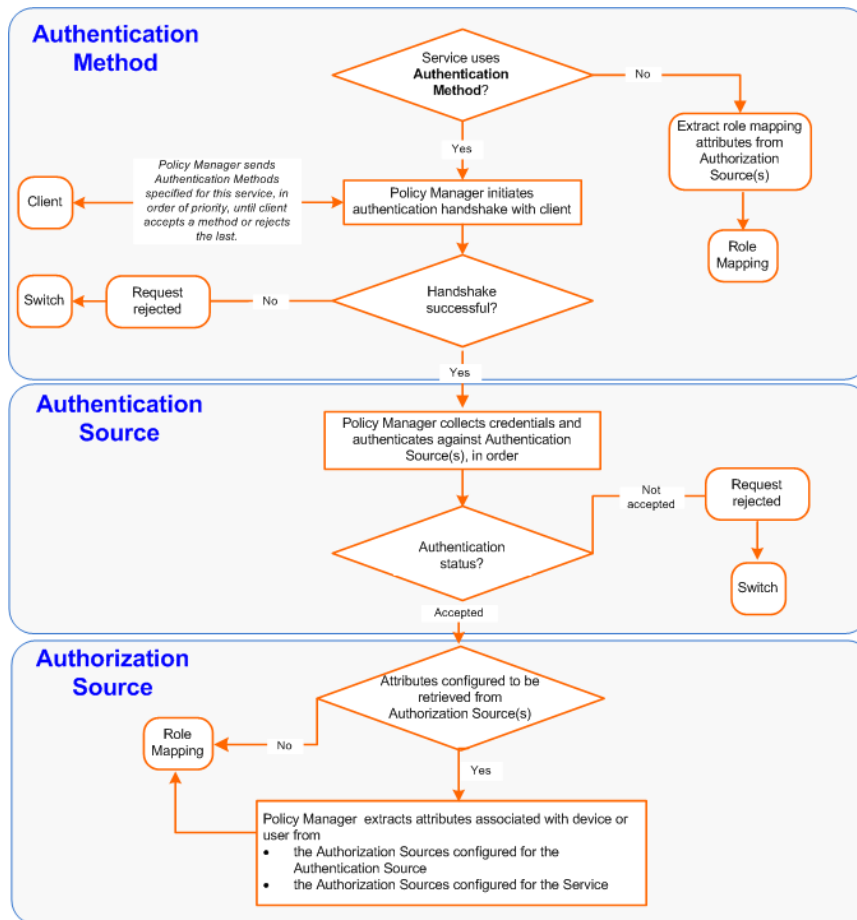


An Authentication Method is only configurable for some service types (Refer to "[Policy Manager Service Types](#)" on page 80). All 802.1X services (wired and wireless) have an associated Authentication Method. An authentication method (of type MAC\_AUTH) can be associated with MAC authentication service 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 61** *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 62** *Authentication Components*

Configuration » Services » Edit - a802.1X Wireless Service

Services - a802.1X Wireless Service

**Authentication**

Authentication Methods:

- eTIPS\_EAP\_PEAP [EAP-PEAP]
- eTIPS\_EAP\_FAST [EAP-FAST]

--Select--

Authentication Sources:

- Avenda\_eTIPS\_Local\_User\_Repository [Local User Repository]
- Avenda AD [Active Directory]

--Select--

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

Back to Services Disable Copy Save Cancel

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

**Table 53:** *Authentication Features at the Service Level*

Configurable Component	Configuration Steps
Sequence of Authentication Methods	<ol style="list-style-type: none"> <li>1. Select a <i>Method</i>, then select <b>Move Up</b>, <b>Move Down</b>, or <b>Remove</b>.</li> <li>2. Select <b>View Details</b> to view the details of the selected method.</li> <li>3. Select <b>Modify</b> to modify the selected authentication method. (This launches a popup with the edit widgets for the select authentication method.) <ul style="list-style-type: none"> <li>■ To add a previously configured <i>Authentication Method</i>, select from the <b>Select</b> drop down list, then click <b>Add</b>.</li> <li>■ To configure a new <i>Method</i>, click the <b>Add New Authentication Method</b> link. Refer to <a href="#">"Adding and Modifying Authentication Methods" on page 111</a> for information about Authentication Methods.</li> </ul> </li> </ol> <p>Note that an Authentication Method is only configurable for some service types. Refer to <a href="#">"Policy Manager Service Types" on page 80</a> for more information.</p>
Sequence of Authentication Sources	<ol style="list-style-type: none"> <li>1. Select a <i>Source</i>, then <b>Move Up</b>, <b>Move Down</b>, or <b>Remove</b>.</li> <li>2. Select <b>View Details</b> to view the details of the selected authentication source.</li> <li>3. Select <b>Modify</b> to modify the selected authentication source. (This launches the authentication source configuration wizard for the selected authentication source.) <ul style="list-style-type: none"> <li>■ To add a previously configured <i>Authentication Source</i>, select from the <b>Select</b> drop down list, then click <b>Add</b>.</li> <li>■ To configure a new <i>Authentication Source</i>, click the <b>Add New Authentication Source</b> link. Refer to <a href="#">"Adding and Modifying Authentication Sources" on page 128</a> for additional information about Authentication Sources.</li> </ul> </li> </ol>
Whether to standardize the form in which usernames are present	<p>Select the <b>Enable to specify a comma-separated list of rules to strip usernames</b> check box to pre-process the user name (and to remove prefixes and suffixes) before authenticating it to the authentication source.</p>

## Adding and Modifying Authentication Methods

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

**Table 54: Policy Manager Supported Authentication Methods**

	EAP	Non-EAP
<b>Tunneled</b>	<ul style="list-style-type: none"> <li>• EAP Protected EAP (EAP-PEAP)</li> <li>• EAP Flexible Authentication Secure Tunnel (EAP-FAST)</li> <li>• EAP Transport Layer Security (EAP-TLS)</li> <li>• EAP Tunneled TLS (EAP-TTLS)</li> </ul>	
<b>Non-Tunneled</b>	<ul style="list-style-type: none"> <li>• EAP Message Digest 5 (EAP-MD5)</li> <li>• EAP Microsoft Challenge Handshake Authentication Protocol version 2 (EAP-MSCHAPv2)</li> <li>• EAP Generic Token Card (EAP-GTC)</li> </ul>	<ul style="list-style-type: none"> <li>• Challenge Handshake Authentication Protocol (CHAP)</li> <li>• Password Authentication Protocol (PAP)</li> <li>• Microsoft CHAP version 1 and version 2</li> <li>• 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 <b>MAC_Authentication</b> request (and not a spoofed request).</li> </ul>




---

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

---




---

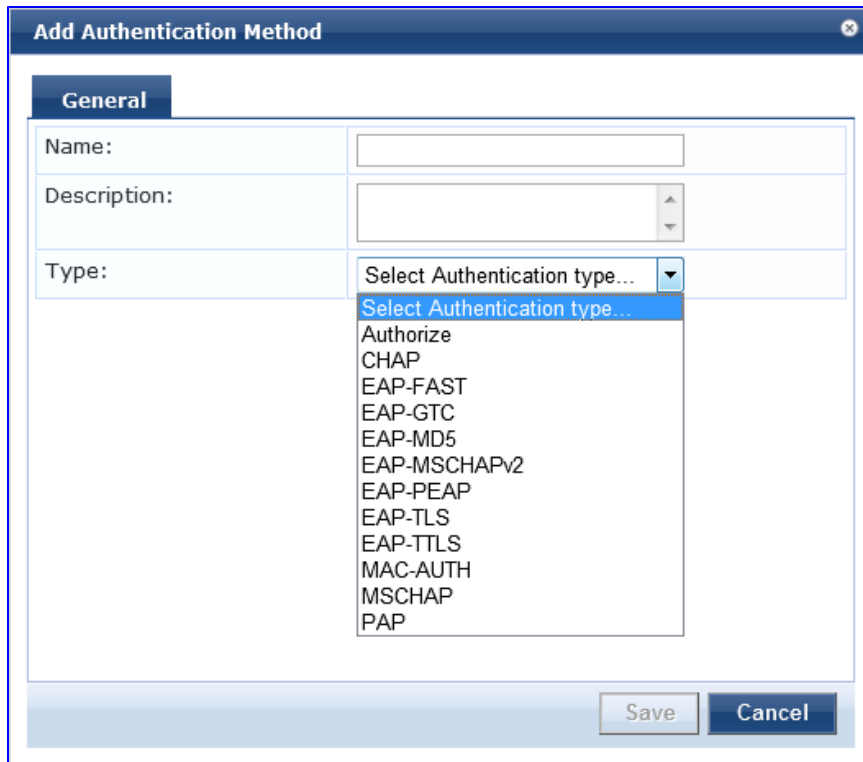
The Authorize authentication method does not fit into any of these categories.

---

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 63** Add Authentication Method dialog box



The image shows a Windows-style dialog box titled "Add Authentication Method". It has a "General" tab selected. The dialog contains three input fields: "Name:" with a text box, "Description:" with a text box and a vertical scrollbar, and "Type:" with a dropdown menu. The dropdown menu is open, showing a list of authentication methods: "Select Authentication type...", "Authorize", "CHAP", "EAP-FAST", "EAP-GTC", "EAP-MD5", "EAP-MSCHAPv2", "EAP-PEAP", "EAP-TLS", "EAP-TTLS", "MAC-AUTH", "MSCHAP", and "PAP". At the bottom right of the dialog are "Save" and "Cancel" buttons.

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

- "PAP " on page 113
- "MSCHAP " on page 114
- "EAP-MSCHAP v2 " on page 115
- "EAP-GTC " on page 115
- "EAP-TLS " on page 116
- "EAP-TTLS " on page 118
- "EAP-PEAP " on page 119
- "EAP-FAST " on page 121
- "MAC-AUTH " on page 126
- "CHAP and EAP-MD5 " on page 126
- Authorize

## PAP

The PAP method contains one tab.

### General Tab

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

**Figure 64** *PAP General Tab*

**Add Authentication Method**

**General**

Name:

Description:

Type: PAP

**Method Details**

Encryption Scheme:

- Clear
- Crypt
- MD5
- SHA1
- Aruba-SSO

Save Cancel

**Table 55:** *PAP General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <b>PAP</b> .
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 65** *MSCHAP General Tab*

**Add Authentication Method**

**General**

Name:

Description:

Type: MSCHAP

Save Cancel

**Table 56:** *MSCHAP General Tab*

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

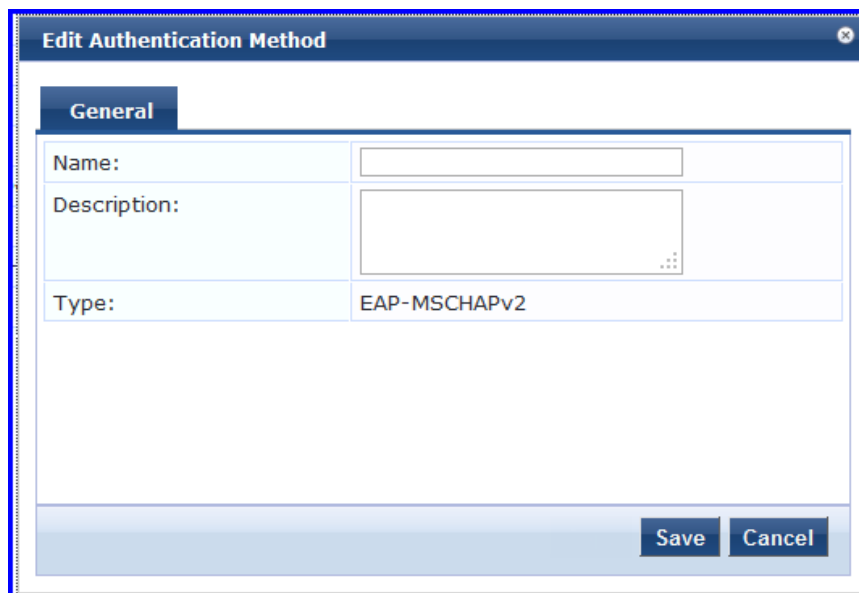
## EAP-MSCHAP v2

The EAP-MSCHAPv2 method contains one tab.

### General Tab

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

**Figure 66** *EAP-MSCHAPv2 General Tab*



**Table 57:** *EAP-MSCHAPv2 General Tab*

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

## EAP-GTC

The EAP-GTC method contains one tab.

### General Tab

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

**Figure 67** *EAP-GTC General Tab*

**Edit Authentication Method**

**General**

Name:

Description:

Type: EAP-GTC

**Method Details**

Challenge:  Password:

Save Cancel

**Table 58:** *EAP-GTCGeneral Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <b>EAP-GTC</b> .
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 68** *EAP\_TLS General Tab*

**Edit Authentication Method**

**General**

Name: [EAP TLS]

Description: Default settings for EAP-TLS

Type: EAP-TLS

**Method Details**

Session Resumption: ☒ Enable

Session Timeout: 6 hours

Authorization Required: ☒ Enable

Certificate Comparison: Do not compare

Verify Certificate using OCSP: None

Override OCSP URL from Client: ☐ Enable

OCSP URL:

Save Cancel

**Table 59:** *EAP\_TLS General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <b>EAP_TLS</b> .
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: <ul style="list-style-type: none"> <li>To skip the certificate comparison, choose <b>Do not compare</b>.</li> <li>To compare specific attributes, choose <b>Compare Common Name (CN)</b>, <b>Compare Subject Alternate Name (SAN)</b>, or <b>Compare CN or SAN</b>.</li> <li>To perform a binary comparison of the stored (in the client record in Active Directory or another LDAP-compliant directory) and presented certificates, choose <b>Compare Binary</b>.</li> </ul>
Verify Certificate using OCSP	Select <b>Optional</b> or <b>Required</b> if the certificate should be verified by the Online Certificate Status Protocol (OCSP). Select <b>None</b> 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 69** *EAP-TTLS General Tab*

The screenshot shows the 'Add Authentication Method' dialog box with the 'General' tab selected. The 'Name' and 'Description' fields are empty. The 'Type' dropdown is set to 'EAP-TTLS'. In the 'Method Details' section, 'Session Resumption' is checked and 'Session Timeout' is set to 6 hours. The 'Save' and 'Cancel' buttons are at the bottom right.

**Table 60:** *EAP-TTLS General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <b>EAP-TTLS</b> .
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 70** *EAP\_TTLS Inner Methods Tab*

Edit Authentication Method

General Inner Methods

Specify inner authentication methods in the preferred order:

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

Default Remove

Select a method...

To set preference for a specific method, use Default button

Save Cancel

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 71** *EAP-PEAP General Tab*

Add Authentication Method

General Inner Methods

Name:

Description:

Type: EAP-PEAP

Method Details

Session Resumption: ☒ Enable

Session Timeout: 6 hours

Fast Reconnect: ☒ Enable

EAPoUDP Support: ☐ Enable

Microsoft NAP Support: ☒ Enable

Enforce Cryptobinding: ☐ Enable

Save Cancel

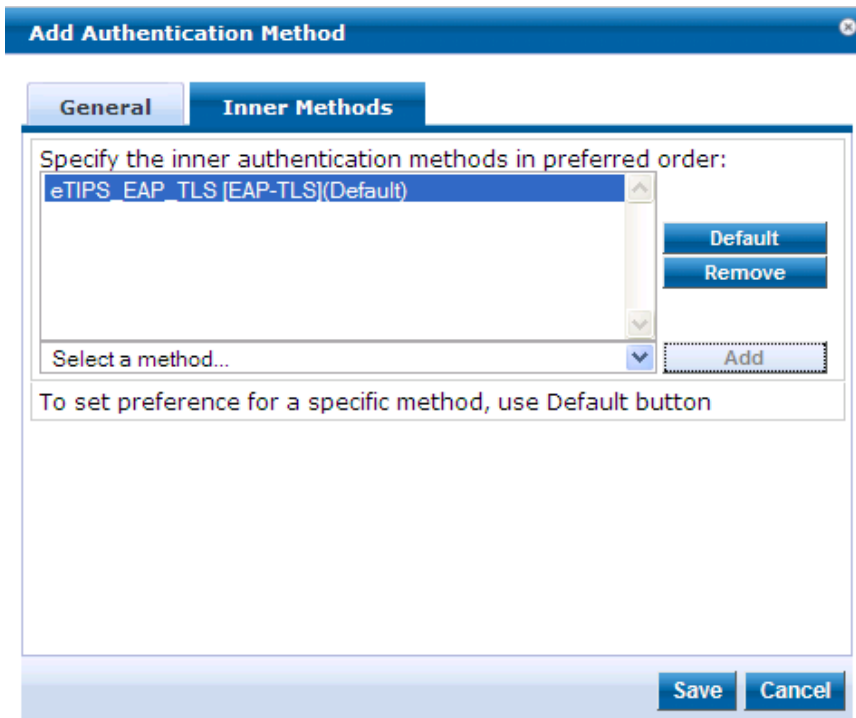
**Table 61: EAP-PEAP General Tab**

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <b>EAP-PEAP</b> .
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 72** *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 73** EAP-FAST General Tab

**Add Authentication Method**

**General** | Inner Methods | PACs | PAC Provisioning

Name:

Description:

Type: **EAP-FAST** ▼

**Method Details**

Session Resumption: ☒ Enable

Session Timeout:  hours

Client Authentication: **Using PACs** ▼

Certificate Comparison: **Do not compare** ▼

**Save** **Cancel**

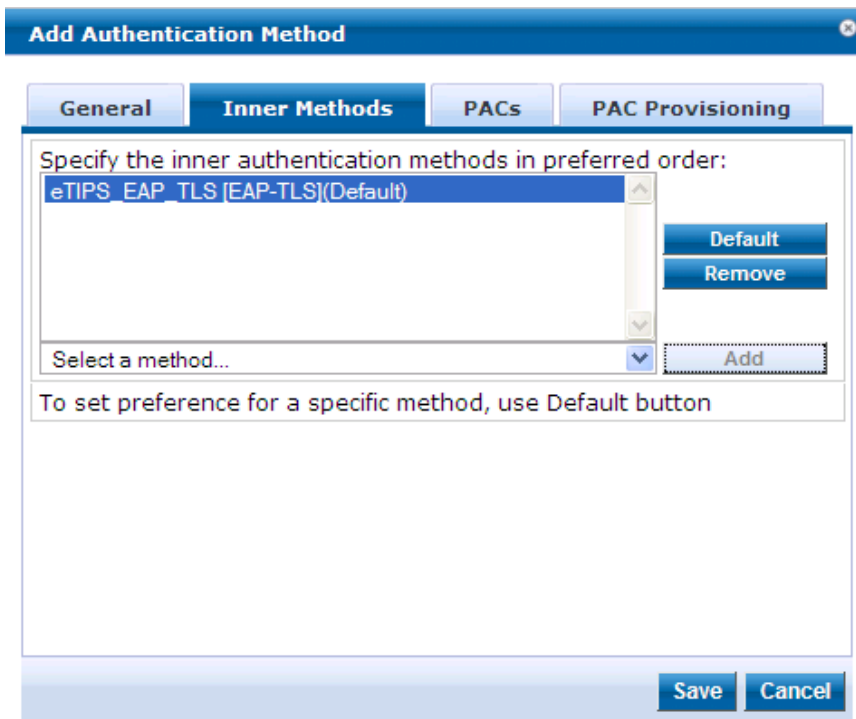
**Table 62:** EAP\_FAST General Tab

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <b>EAP_FAST</b> .
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, <b>session resumption</b> must be enabled.
End-Host Authentication	Refers to establishing the EAP-Fast Phase 1 Outer tunnel: <ul style="list-style-type: none"> <li>Choose <b>Using PACs</b> to use a strong shared secret.</li> <li>Choose <b>Using Client Certificate</b> to use a certificate.</li> </ul>
Certificate Comparison	Type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate: <ul style="list-style-type: none"> <li>To skip the certificate comparison, choose <b>Do not compare</b>.</li> <li>To compare specific attributes, choose <b>Compare Common Name (CN)</b>, <b>Compare Subject Alternate Name (SAN)</b>, or <b>Compare CN or SAN</b>.</li> <li>To perform a binary comparison of the <i>stored</i> (in the end-host record in Active Directory or another LDAP-compliant directory) and <i>presented</i> certificates, choose <b>Compare Binary</b>.</li> </ul>

## Inner Methods Tab

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

**Figure 74** *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 75** *EAP\_FAST PACs Tab*

The screenshot shows the 'Add Authentication Method' dialog box with the 'PACs' tab selected. The dialog contains the following fields and options:

- Tunnel PAC Expire Time:** 1 days
- ☒ **Machine PAC**  
**Machine PAC Expire Time:** 1 days
- ☒ **Authorization PAC**  
**Authorization PAC Expire Time:** 1 days
- ☒ **Posture PAC**  
**Posture PAC Expire Time:** 1 days

Buttons at the bottom: Save, Cancel

- 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 76** *EAP\_FAST PAC Provisioning tab*

The screenshot shows the 'Add Authentication Method' dialog box with the 'PAC Provisioning' tab selected. Under the 'In-Band PAC Provisioning' section, the following options are checked: 'Allow anonymous mode (requires no server certificate)', 'Allow authenticated mode (requires server certificate)', and 'Accept end-host after authenticated provisioning'. The option 'Require end-host certificate for provisioning' is unchecked. The 'Save' and 'Cancel' buttons are located at the bottom right of the dialog.

**Table 63:** *EAP\_FAST PAC Provisioning Tab*

Parameter	Description	Considerations
Allow Anonymous Mode	When in anonymous mode, <i>phase 0</i> 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 <i>phase 0</i> 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): <ul style="list-style-type: none"> <li>• 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.</li> </ul>
Allow Authenticated Mode	Enable to allow authenticated mode provisioning. When in Allow Authenticated Mode <i>phase 0</i> , Policy Manager establishes the outer tunnel inside of a server-authenticated tunnel. The end-host authenticates the server by validating the Policy Manager certificate.	<ul style="list-style-type: none"> <li>• Otherwise, if the appropriate cipher suite is supported by the end-host, Policy Manager performs anonymous provisioning.</li> </ul>
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 77** MAC-AUTH General Tab

**Table 64:** MAC-Auth General Tab

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, always <b>MAC-AUTH</b> .
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 <a href="#">"Configuring Audit Servers" on page 199</a> ), 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 78** CHAP General Tab

The screenshot shows a dialog box titled "Add Authentication Method" with a close button in the top right corner. Inside the dialog, there is a tab labeled "General". Below the tab, there are three input fields: "Name:" with a text box, "Description:" with a text box and a vertical scrollbar, and "Type:" with a dropdown menu showing "CHAP". At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

**Figure 79** EAP-MD5 General Tab

The screenshot shows a dialog box titled "Add Authentication Method" with a close button in the top right corner. Inside the dialog, there is a tab labeled "General". Below the tab, there are three input fields: "Name:" with a text box, "Description:" with a text box and a vertical scrollbar, and "Type:" with a dropdown menu showing "EAP-MD5". At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

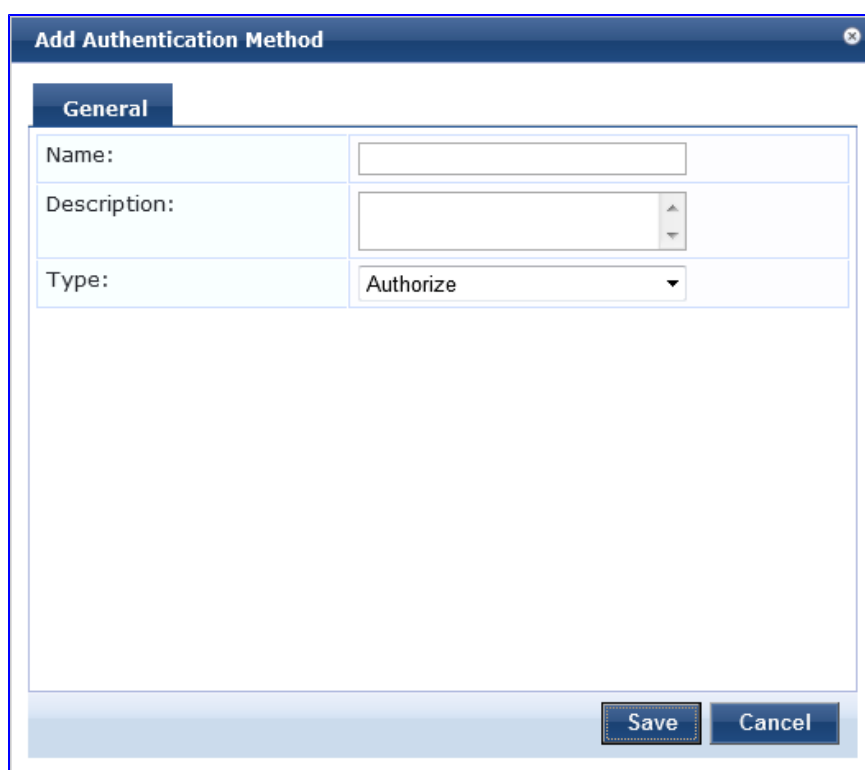
**Table 65:** CHAP and EAP-MD5 General Tab Parameters

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

## Authorize

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

**Figure 80** Authorize General Tab



**Table 66:** Authorize General Tab Parameters

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

## Adding and Modifying Authentication Sources

Policy Manager supports the following Authentication Sources:

- "Generic LDAP or Active Directory " on page 129
- "Generic SQL DB (Open Data Base Connectivity (ODBC) compliant SQL Databases) " on page 139

- "HTTP" on page 143
- "Kerberos " on page 146
- "Okta" on page 148
- "Static Host List " on page 150
- "Token Server " on page 151

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 81** *Authentication Sources Listing Page*

Configuration » Authentication » Sources

Authentication Sources

[Add Authentication Source](#)  
[Import Authentication Sources](#)  
[Export Authentication Sources](#)

Filter: Name contains [ ] Go Clear Filter Show 10 records

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
3.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
4.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
5.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
6.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database

Showing 1-6 of 6

Copy Export Delete

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

**Figure 82** *Add Authentication Source Page*

Configuration » Authentication » Sources » Add

Authentication Sources

General

Name: [ ]

Description: [ ]

Type: [Select] (Dropdown menu open showing: -- Select --, Generic SQL DB, Generic LDAP, Active Directory, Kerberos, Token Server, Static Host List, HTTP)

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

Authorization Sources: [ ]

Remove View Details

Back to Authentication Sources

Next > Save Cancel

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 157](#)

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 83** Generic LDAP or Active Directory (General Tab)

Configuration » Authentication » Sources » Add

### Authentication Sources

**General** Primary Attributes Summary

Name:

Description:

Type:

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

Authorization Sources:

-- Select --

Server Timeout:  seconds

Cache Timeout:  seconds

Backup Servers Priority:

[Back to Authentication Sources](#)

**Table 67:** Generic LDAP or Active Directory (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <b>General LDAP</b> or <b>Active Directory</b> .
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	<p>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 <b>Add</b> to add it to the list of authorization sources. Click <b>Remove</b> to remove it from the list.</p> <p>If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.</p> <p><b>NOTE:</b> As described in “,” 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.</p>
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	<p>To add a backup server, click <b>Add Backup</b>. When the <b>Backup 1</b> tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click <b>Remove</b>. Select <b>Move Up</b> or <b>Move Down</b> 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.</p>

## Primary Tab

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

**Figure 84** Generic LDAP or Active Directory (Primary Tab)

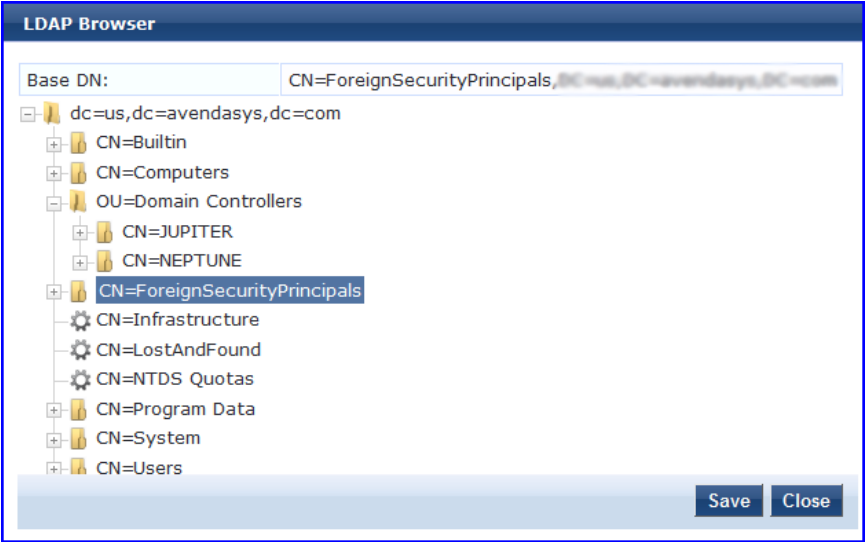
Configuration » Authentication » Sources » Add

### Authentication Sources

General	Primary	Attributes	Summary
<b>Connection Details</b>			
Hostname:	<input type="text"/>		
Connection Security:	None		
Port:	389		
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection		
Bind DN:	<input type="text"/>		
Bind Password:	<input type="password"/>		
Base DN:	<input type="text"/> <a href="#">Search Base Dn</a>		
Search Scope:	SubTree Search		
LDAP Referrals:	<input type="checkbox"/> Follow referrals		
Bind User:	<input type="checkbox"/> Allow bind using user password		
Password Attribute:	userPassword		
Password Type:	Cleartext		
Password Header:	<input type="text"/>		
User Certificate :	userCertificate		
<a href="#">Back to Authentication Sources</a> <span>Next &gt;</span> <span>Save</span> <span>Cancel</span>			

**Table 68:** Generic LDAP or active Directory (Primary Tab)

Parameter	Description
Host Name/Port	<ul style="list-style-type: none"> <li>• Hostname or IP address of the LDAP or Active Directory server.</li> <li>• 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).</li> </ul>
Connection Security	<ul style="list-style-type: none"> <li>• Select <b>None</b> for default non-secure connection (usually port 389)</li> <li>• Select <b>StartTLS</b> for secure connection that is negotiated over the standard LDAP port. This is the preferred way to connect to an LDAP directory securely.</li> <li>• Select <b>LDAP over SSL</b> or <b>AD over SSL</b> to choose the legacy way of securely connecting to an LDAP directory. Port 636 must be used for this type of connection.</li> </ul>
Bind DN/Password	<p>Distinguished Name (DN) of the administrator account. Policy Manager uses this account to access all other records in the directory.</p> <p><b>NOTE:</b> For Active Directory, the bind DN can also be in the administrator@domain format (e.g., administrator@acme.com).</p> <p>Password for the administrator DN entered in the Bind DN field.</p>

Parameter	Description
NetBIOS Domain Name	<p>The AD domain name for this server. Policy Manager prepends this name to the user ID to authenticate users found in this Active Directory.</p> <p><b>NOTE:</b> This setting is only available for Active Directory.</p>
Verify Server Certificate	<p>Select this checkbox if you want to verify the Server Certificate as part of the authentication.</p>
Base DN	<p>Enter DN of the node in your directory tree from which to start searching for records.</p> <p>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.</p>  <p>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.</p> <p><b>NOTE:</b> 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</p>
Search Scope	<p>Scope of the search you want to perform, starting at the Base DN.</p> <ul style="list-style-type: none"> <li>• <b>Base Object Search</b> allows you to search at the level specified by the base DN.</li> <li>• <b>Subtree Search</b> allows you to search the entire subtree under the base DN (including at the base DN level).</li> <li>• <b>One Level Search</b> allows you to search up to one level below (immediate children of) the base DN.</li> </ul>
LDAP Referral	<p>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.</p>
Bind User	<p>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.</p>

Parameter	Description
Password Attribute (Available only for <b>Generic LDAP</b> 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 85** Active Directory Attributes Tab (with default data)

General	Primary	Attributes	Summary
Specify filter queries used to fetch authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	Attribute
	title	Title	Attribute
	company	company	-
	memberOf	memberOf	-
	telephoneNumber	Phone	Attribute
	mail	Email	Attribute
	displayName	Name	Attribute
2. Group	cn	Groups	Attribute
3. Machine	dNSHostName	HostName	Attribute
	operatingSystem	OperatingSystem	Attribute
	operatingSystemServicePack	OSServicePack	Attribute
4. Onboard Device Owner	memberOf	Onboard memberOf	-
5. Onboard Device Owner Group	cn	Onboard Groups	Attribute

**Figure 86** Generic LDAP Directory Attributes Tab

General	Primary	Attributes	Summary
Specify filters used to query for authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enable as role
1. Authentication	dn	UserDN	false
2. Group	cn	groupName	false

**Table 69:** AD/LDAP Attributes Tab (Filter Listing Screen)

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enable as Role	Listing column descriptions: <ul style="list-style-type: none"> <li>● <b>Filter Name:</b> Name of the filter.</li> <li>● <b>Attribute Name:</b> Name of the LDAP/AD attributes defined for this filter.</li> <li>● <b>Alias Name:</b> For each attribute name selected for the filter, you can specify an alias name.</li> </ul>

Tab	Parameter/Description
	<ul style="list-style-type: none"> <li>• <b>Enabled As:</b> 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.</li> </ul>
Add More Filters	Brings up the filter creation popup. This is described in the next image.

The following table describes the available directories.

**Table 70: AD/LDAP Default Filters Explained**

Directory	Default Filters
Active Directory	<ul style="list-style-type: none"> <li>• <b>Authentication:</b> This is the filter used for authentication. The query searches in objectClass of type <i>user</i>. This query finds both user and machine accounts in Active Directory:  <code>(&amp;(objectClass=user)(sAMAccountName={Authentication:Username}))</code>  When a request arrives, Policy Manager populates <code>{Authentication:Username}</code> with the authenticating user or machine. This filter is also set up to fetch the following attributes based on this filter query: <ul style="list-style-type: none"> <li>■ <b>dn</b> (aliased to UserDN): This is an internal attribute that is populated with the user or machine record's Distinguished Name (DN)</li> <li>■ <b>department</b></li> <li>■ <b>title</b></li> <li>■ <b>company</b></li> <li>■ <b>memberOf:</b> In Active Directory, this attribute is populated with the groups that the user or machine belongs to. This is a multi-valued attribute.</li> <li>■ <b>telephoneNumber</b></li> <li>■ <b>mail</b></li> <li>■ <b>displayName</b></li> </ul> </li> <li>• <b>Group:</b> This is filter used for retrieving the name of the groups a user or machine belongs to.  <code>(distinguishedName={memberOf})</code>  This query fetches all group records, where the distinguished name is the value returned by the <b>memberOf</b> variable. The values for the <b>memberOf</b> attribute are fetched by the first filter (Authentication) described above. The attribute fetched with this filter query is <b>cn</b>, which is the name of the group</li> <li>• <b>Machine:</b> This query fetches the machine record in Active Directory.  <code>(&amp;(objectClass=computer)(sAMAccountName={Host:Name}\$))</code>  <code>{Host:Name}</code> is populated by Policy Manager with name of the connecting host (if available). <code>dnsHostName</code>, <code>operatingSystem</code> and <code>operatingSystemServicePack</code> attributes are fetched with this filter query.</li> <li>• <b>Onboard Device Owner:</b></li> <li>• <b>Onboard Device Owner Group:</b></li> </ul>
Generic LDAP Directory	<p><b>Authentication:</b> This is the filter used for authentication.  <code>(&amp;(objectClass=*)(uid={Authentication:Username}))</code></p> <p>When a request arrives, Policy Manager populates <code>{Authentication:Username}</code> with the authenticating user or machine. This filter is also set up to fetch the following attributes based on this filter query:</p> <ul style="list-style-type: none"> <li>■ <b>dn</b> (aliased to UserDN): This is an internal attribute that is populated with the user record's Distinguished Name (DN)</li> </ul> <p><b>Group:</b> This is filter used for retrieving the name of the groups a user belongs to.  <code>(&amp;(objectClass=groupOfNames)(member={UserDn}))</code></p> <ul style="list-style-type: none"> <li>■ This query fetches all group records (of objectClass <code>groupOfNames</code>), where member</li> </ul>

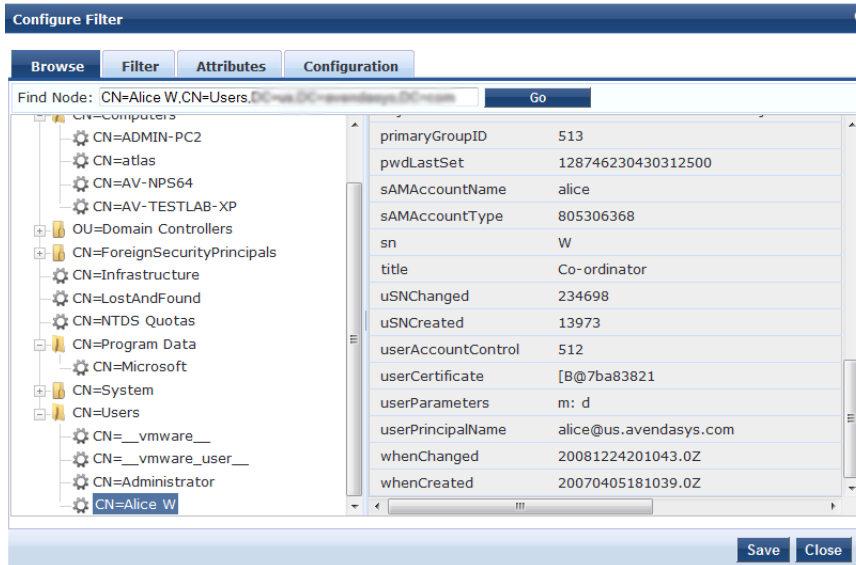
Directory	Default Filters
	field contains the DN of the user record (UserDN, which is populated after the Authentication filter query is executed. The attribute fetched with this filter query is cn, which is the name of the group (this is aliased to a more readable name: groupName)

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



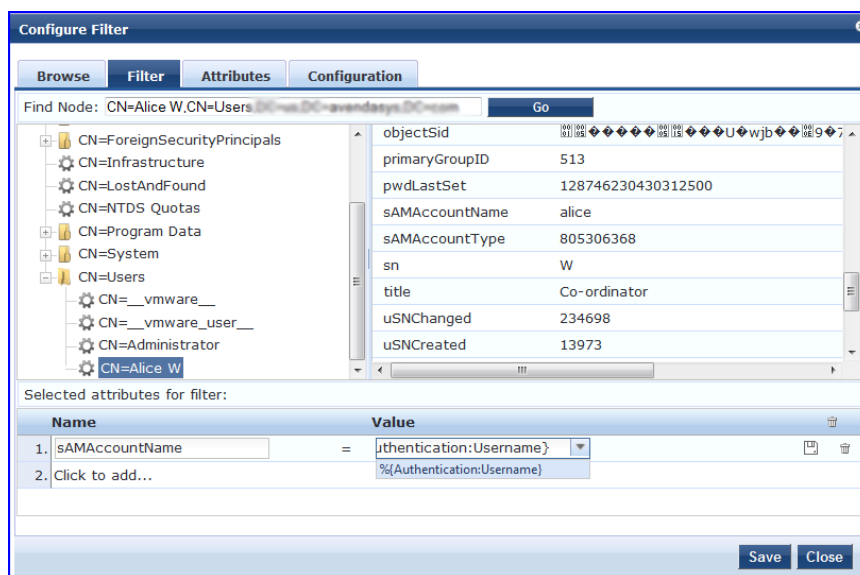
**Table 71:** AD/LDAP Configure Filter Popup (Browse Tab)

Navigation	Description
Find Node / Go	Go directly to a given node by entering its Distinguished Name (DN) and clicking on the <b>Go</b> 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 88** AD/LDAP Create Filter Popup (Filter Tab)



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



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

**Table 72:** 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.
Select the attributes for filter	<p>This table has a name and value column. There are two ways to enter the attribute name</p> <ul style="list-style-type: none"> <li>By going to a node of interest, inspecting the attributes, and then manually entering the attribute name by clicking on <b>Click to add...</b> in the table row.</li> <li>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.</li> </ul> <p>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).</p>

Parameter	Description

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

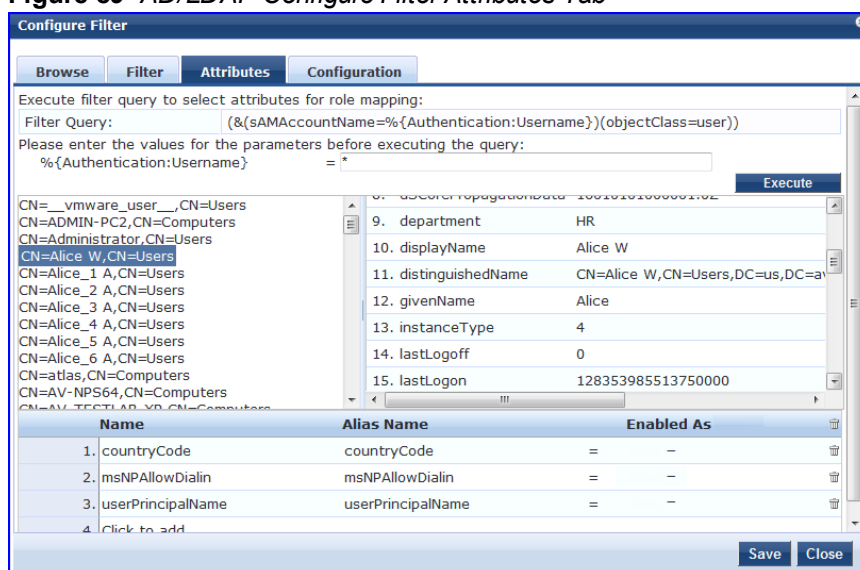
**Table 73: Filter Creation Steps**

Step	Description
<b>Step 1</b> 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.
<b>Step 2</b> 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).
<b>Step 3</b> 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.
<b>Step 4</b>	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 221.)

**Figure 89 AD/LDAP Configure Filter Attributes Tab**



**Table 74: AD/LDAP Configure Filter Popup (Attributes Tab)**

Parameter	Description
Enter values for parameters	<p>Policy Manager parses the filter query (created in the <b>Filter</b> tab and shown at the top of the <b>Attributes</b> 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.</p> <p><b>NOTE:</b> If there are thousands of entries in the directory, entering the wildcard character (*) can take a while to fetch all matching entries.</p>
Execute	<p>Once you have entered the values for all dynamic parameters, click on <b>Execute</b> 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.</p>
Name / Alias Name / Enable as Role	<p><b>Name:</b> This is the name of the attribute</p> <p><b>Alias Name:</b> A friendly name for the attribute. By default, this is the same as the attribute name.</p> <p><b>Enabled As:</b> 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.</p>

### 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 90** *Configure Filter Popup (Configuration Tab)*

Configure Filter

Filter Name:

Filter Query:

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

Save Close

### 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.



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 91** *Modify Default Filters*

Configure Filter

Filter Name:

Filter Query:

Name	Alias Name	Data type	Enabled As	Role	Attribute
1. dn	UserDN	String	-		
2. department	Department	String		<input type="checkbox"/>	<input checked="" type="checkbox"/>
3. title	Title	String	Attribute		
4. company	company	Integer			
5. memberOf	memberOf	Boolean	-		
6. telephoneNumber	Phone	String	Attribute		
7. mail	Email	String	Attribute		
8. displayName	Name	String	Attribute		
9. Click to add...					

Save Close

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 PostgreSQL). 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 92** *Generic SQL DB (General Tab)*

The screenshot shows the 'Authentication Sources' configuration interface. It has four tabs: 'General' (selected), 'Primary', 'Attributes', and 'Summary'. The 'General' tab contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field with a vertical ellipsis icon on the right.
- Type:** A dropdown menu currently showing 'Generic SQL DB'.
- Use for Authorization:** A checkbox labeled 'Enable to use this authentication source to also fetch role mapping attributes', which is checked.
- Authorization Sources:** A list box with a '-- Select --' dropdown and buttons for 'Remove' and 'View Details'.
- Cache Timeout:** A text input field showing '36000' with a unit dropdown set to 'seconds'.
- Backup Servers Priority:** A list box with buttons for 'Move Up', 'Move Down', 'Add Backup', and 'Remove'.

At the bottom of the form are four buttons: 'Back to Authentication Sources' (with a left arrow), 'Next >', 'Save', and 'Cancel'.

**Table 75:** *General SQL DB (General Tab)*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <b>Generic SQL DB</b> .
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 <b>Add</b> to add it to the list of authorization sources. Click <b>Remove</b> to remove it from the list.

Parameter	Description
	<p>If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.</p> <p><b>NOTE:</b> 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.</p>
Backup Servers	<p>To add a backup server, click <b>Add Backup</b>. When the <b>Backup 1</b> tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click <b>Remove</b>. Select <b>Move Up</b> or <b>Move Down</b> to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.</p>
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 93** General SQL DB (Primary Tab)

The screenshot shows the 'Authentication Sources' dialog box with the 'Primary' tab selected. The 'Connection Details' section contains the following fields:

- Server Name: [Text input field]
- Port (Optional): [Text input field] (Specify only if you want to override the default value)
- Database Name: [Text input field]
- Login Username: [Text input field]
- Login Password: [Text input field]
- Timeout: 10 seconds
- ODBC Driver: MySQL (dropdown menu)

At the bottom, there are four buttons: 'Back to Authentication Sources' (with a left arrow), 'Next >' (with a right arrow), 'Save', and 'Cancel'.

**Table 76:** 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	<p>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.</p> <p>Enter the password for the user account entered in the field above.</p>

Parameter	Description
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 or MSSQL in this release) to connect to database.

### Attributes Tab

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

**Figure 94** Generic SQL DB (Attributes Tab)

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

**Table 77:** Generic SQL DB Attributes Tab (Filter List)

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enabled As	<p>Listing column descriptions:</p> <ul style="list-style-type: none"> <li>• <b>Filter Name:</b> Name of the filter.</li> <li>• <b>Attribute Name:</b> Name of the SQL DB attributes defined for this filter.</li> <li>• <b>Alias Name:</b> For each attribute name selected for the filter, you can specify an alias name.</li> <li>• <b>Enabled As:</b> Indicates whether the filter is enabled as a role or attribute type. Note that this can also be blank.</li> </ul>
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 95** Generic SQL DB Filter Configure Popup

Name	Alias Name	Data type	Enabled As
1. sponsor_name	Owner	String	-

**Table 78: 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	<p><b>Name:</b> This is the name of the attribute</p> <p><b>Alias Name:</b> A friendly name for the attribute. By default, this is the same as the attribute name.</p> <p><b>Data Type:</b> Specify the data type for this attribute, such as String, Integer, Boolean, etc.</p> <p><b>Enabled As:</b> 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.</p>

## 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 96 HTTP (General Tab)**

Configuration » Authentication » Sources » Add

### Authentication Sources

**General** Primary Attributes Summary

Name:

Description:

Type:

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

Authorization Sources:

Backup Servers Priority:

[Back to Authentication Sources](#)

**Table 79: HTTP (General Tab)**

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <b>HTTP</b> .
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	<p>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 <b>Add</b> to add it to the list of authorization sources. Click <b>Remove</b> to remove it from the list.</p> <p>If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.</p> <p><b>NOTE:</b> 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.</p>
Backup Servers	<p>To add a backup server, click <b>Add Backup</b>. When the <b>Backup 1</b> tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click <b>Remove</b>. Select <b>Move Up</b> or <b>Move Down</b> to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.</p>

## Primary Tab

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

**Figure 97 HTTP (Primary Tab)**
**Table 80: HTTP (Primary Tab)**

Parameter	Description
Server Name	Enter the hostname or IP address of the database server.

Parameter	Description
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 98** HTTP (Attributes Tab)

**Table 81:** HTTP Attributes Tab (Filter List)

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enabled As	Listing column descriptions: <ul style="list-style-type: none"> <li>● <b>Filter Name:</b> Name of the filter.</li> <li>● <b>Attribute Name:</b> Name of the SQL DB attributes defined for this filter.</li> <li>● <b>Alias Name:</b> For each attribute name selected for the filter, you can specify an alias name.</li> <li>● <b>Enabled As:</b> Indicates whether an attribute has been enabled as a role.</li> </ul>
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 99** HTTP Filter Configure Popup

**Table 82:** HTTP 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	<b>Name:</b> This is the name of the attribute <b>Alias Name:</b> A friendly name for the attribute. By default, this is the same as the attribute name. <b>Data Type:</b> Specify the data type for this attribute, such as String, Integer, Boolean, etc. <b>Enabled As:</b> 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 100** Kerberos General Tab

Authentication Sources

The screenshot shows the 'Authentication Sources' configuration window with the 'General' tab selected. The form contains the following fields and controls:

- Name:** A text input field.
- Description:** A text area with a vertical ellipsis icon at the bottom right.
- Type:** A dropdown menu currently showing 'Kerberos'.
- Use for Authorization:** A checkbox labeled 'Enable to use this authentication source to also fetch role mapping attributes'.
- Authorization Sources:** A list box with a 'Remove' button and a 'View Details' button to its right. Below the list box is a dropdown menu showing '-- Select --'.
- Backup Servers Priority:** A list box with 'Move Up' and 'Move Down' buttons to its right. Below the list box are 'Add Backup' and 'Remove' buttons.

At the bottom of the window, there is a 'Back to Authentication Sources' link on the left and 'Next >', 'Save', and 'Cancel' buttons on the right.

**Table 83: Kerberos (General Tab)**

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <b>Kerberos</b>
Use for Authorization	Disabled in this context.
Authorization Sources	<p>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.</p> <p><b>NOTE:</b> 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.</p>
Backup Servers	<p>To add a backup kerberos server, click <b>Add Backup</b>. When the <b>Backup 1</b> tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).</p> <p>To remove a backup server, select the server name and click <b>Remove</b>. Select <b>Move Up</b> or <b>Move Down</b> to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.</p>

### Primary Tab

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

**Figure 101 Kerberos (Primary Tab)**
**Table 84: 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.

Parameter	Description
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 Aruba Application Authentication. You configure Okta authentication sources on the following tabs:

- [General Tab](#)
- [Primary Tab](#)
- [Attributes Tab](#)

### General Tab

**Figure 102** *Okta General Tab*

Configuration » Authentication » Sources » Add

#### Authentication Sources

General	Primary	Attributes	Summary
Name:	<input type="text"/>		
Description:	<input type="text"/>		
Type:	Okta		
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this authentication source to also fetch role mapping attributes		
Authorization Sources:	<div> <input type="text"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> </div> <div> -- Select -- </div>		
Server Timeout:	10 seconds		
Cache Timeout:	36000 seconds		
Backup Servers Priority:	<div> <input type="text"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> </div> <div> <input type="button" value="Add Backup"/> <input type="button" value="Remove"/> </div>		

[Back to Authentication Sources](#)

### Okta (General Tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <b>Okta</b>
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.

Parameter	Description
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 <b>Add Backup</b> . When the <b>Backup 1</b> 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 <b>Remove</b> . Select <b>Move Up</b> or <b>Move Down</b> 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 103** *Okta Primary Tab*

Configuration » Authentication » Sources » Add

### Authentication Sources

**Table 85:** *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 104** *Okta Attributes Tab*

Configuration » Authentication » Sources » Add

### Authentication Sources

**Table 86:** *Okta (Attributes Tab)*

Tab	Parameter/Description
Filter Name / Attribute Name / Alias Name / Enable as Role	<p>Listing column descriptions:</p> <ul style="list-style-type: none"><li>● <b>Filter Name:</b> Name of the filter. (Only Group can be configured for Okta.)</li><li>● <b>Attribute Name:</b> Name of the LDAP/AD attributes defined for this filter.</li><li>● <b>Alias Name:</b> For each attribute name selected for the filter, you can specify an alias name.</li><li>● <b>Enabled As:</b> 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.</li></ul>
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 105** *Static Host List (General Tab)*

The screenshot shows the 'Configuration > Authentication > Sources > Add' page. The title is 'Authentication Sources'. There are three tabs: 'General' (selected), 'Static Host Lists', and 'Summary'. The 'General' tab contains the following fields:

- Name:** A text input field.
- Description:** A text input field.
- Type:** A dropdown menu with 'Static Host List' selected.
- Use for Authorization:** A checkbox labeled 'Enable to use this authentication source to also fetch role mapping attributes'.
- Authorization Sources:** A list box with a 'Remove' button and a 'View Details' button.

At the bottom, there is a 'Back to Authentication Sources' link and 'Next >', 'Save', and 'Cancel' buttons.

**Table 87:** *Static Host List (General Tab)*

Parameter	Description
Name/ Description	Freeform label
Type	<b>Static Host List</b> , 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 106** *Static Host List (Static Host Lists Tab)*

**Table 88:** *Static Hosts List (Static Host Lists Tab)*

Parameter	Description
Host List	Select a Static Host List from the drop down and <b>Add</b> to add it to the list. Click on <b>Remove</b> to remove the selected static host list. Click on <b>View Details</b> to view the contents of the selected static host list. Click on <b>Modify</b> to modify the selected static host list.



Only Static Host Lists of type MAC Address List or MAC Address Regular Expression can be configured as authentication sources. Refer to ["Adding and Modifying Static Host Lists "](#) on [page 167](#) 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 329](#).

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 107** *Token Server (General Tab)*

Configuration » Authentication » Sources » Add

### Authentication Sources

**General** Primary Attributes Summary

Name:

Description:

Type:

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

Authorization Sources:

Server Timeout:  seconds

Backup Servers Priority:

[Back to Authentication Sources](#)

**Table 89:** *Token Server General Tab*

Parameter	Description
Name/Description	Freeform label and description.
Type	In this context, <b>Token Server</b>
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	<p>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 <b>Add</b> to add it to the list of authorization sources. Click <b>Remove</b> to remove it from the list.</p> <p>If Policy Manager authenticates the user or device from this authentication source, then it also fetches role mapping attributes from these additional authorization sources.</p> <p><b>NOTE: Note:</b> 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.</p>
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 <b>Add Backup</b> . When the <b>Backup 1</b> tab appears, you can specify connection details for a backup server (same fields as for primary server, specified below).

Parameter	Description
	To remove a backup server, select the server name and click <b>Remove</b> . Select <b>Move Up</b> or <b>Move Down</b> 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 108** Token Server (Primary Tab)

**Table 90:** 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 155 for more information.) Policy Manager load all RADIUS vendor dictionaries in the type drop down to help select the attributes.

**Figure 109** Token Server (Attributes Tab)



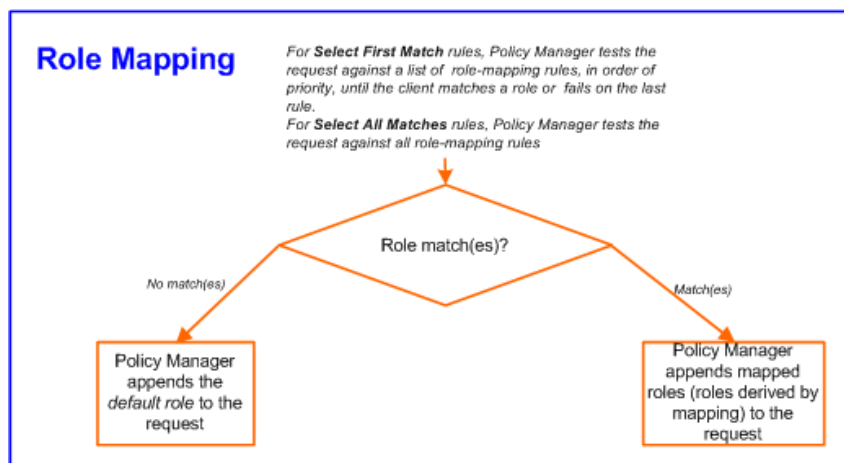
A Role Mapping Policy reduces client (user or device) identity or attributes associated with the request to *Role(s)* for Enforcement Policy evaluation. The roles ultimately determine differentiated access.

## 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 "](#) on page 157). 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 128)
- Associated directly with a user in the Policy Manager *local user* database (["Adding and Modifying Local Users "](#) on page 161 and ["Adding and Modifying Guest Users "](#) on page 162).
- Associated directly with a *static host list*, again through *role mapping* (["Adding and Modifying Static Host Lists "](#) on page 167).

**Figure 110** 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.



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



Additional roles are available with AirGroup and Onboard licenses

You can also configure other roles. Refer to ["Adding and Modifying Roles "](#) on page 160.

## Configuring Single Sign-On

Single Sign-On allows ClearPass users to access the Policy Manager, Guest, and Insight applications without re-signing in once they have signed in to one of the applications.

To configure single sign-on

1. Go to **Configuration > Identity > Single Sign-On**.

2. Enter the IdP (Identity Provider) Single sign-on URL. (See below for details.)
3. In the Enable SSO for section, select the check box for the applications you want users to access with single sign-on.
4. If you want to do a certificate comparison, select the IdP Certificate to use.
5. Click **Save**.

**Table 91: Single Sign-On parameters.**

Parameter	Description
IdP SSO URL	This is the Identity Provider's HTTP-REDIRECT URI, which is the URL a user is redirected to with a SAMLRequest when that user accesses a SAML protected resource.
IdP Certificate	Single sign-on will operate with or without a certificate comparison. The certificates you can choose in this list are the ones defined in <a href="#">"Certificate Trust List "</a> on page 289.

## 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.



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 160](#) 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 111** *Role Mapping Policies*

Configuration > Identity > Role Mappings			
Role Mappings			
Filter: Name contains		Go	Clear Filter
		Show 20 records	
#	Name	Description	Default Role
1.	Employee Roles	Role mapping policies for employees	Role_Engineer
2.	Enterprise Role Mapping Policy	Role mapping policy for all managed users	eTIPS_Guest
3.	Handheld Roles	Roles for handheld devices	Not_Handhelds
4.	RMP_DEPARTMENT		eTIPS_Guest
5.	Switch Port Role Mapping Policy		Unknown Client
6.	TG Role Mapping (AD)	AD Roles for traffic generator	eTIPS_Guest
7.	Unmanaged Clients Role Mapping	Roles for handheld devices	Not_Handhelds
Showing 1-7 of 7			
		Copy	Export Delete

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 112** *Role Mapping (Policy Tab)*

**Table 92:** *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 <b>View Details</b> to view the details of the default role. Click on <b>Modify</b> to modify the default role. Click on <b>Add new Role</b> 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 113** *Role Mapping (Mapping Rules Tab)*

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

**Figure 114** *Rules Editor*

**Table 93:** *Role Mappings Page (Rules Editor)*

Label	Description
Type	<p>The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to <a href="#">"Namespaces" on page 329.</a>) In the role mapping context, Policy Manager allows attributes from following namespaces:</p> <ul style="list-style-type: none"> <li>• Application</li> <li>• Authentication</li> <li>• Authorization</li> <li>• Authorization:&lt;authorization_source_instance&gt; - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (<a href="#">"Adding and Modifying Authentication Sources " on page 128</a>). Only those attributes that have been configured to be fetched are shown in the attributes dropdown.</li> <li>• Certificate</li> <li>• Connection</li> <li>• Date</li> <li>• Device</li> <li>• Endpoint</li> <li>• GuestUser</li> <li>• Host</li> <li>• LocalUser</li> <li>• Onboard</li> <li>• TACACS</li> <li>• RADIUS - All enabled RADIUS vendor dictionaries</li> </ul>
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 <a href="#">"Operators" on page 335.</a>
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 115** Roles

Configuration » Identity » Roles

Roles

Filter: Description contains Role Go Clear Filter Show 10 records

#	Name	Description
1.	[Contractor]	Default role for a Contractor
2.	[Employee]	Default role for an Employee
3.	[Guest]	Default role for a Guest
4.	[Other]	Default role for other user or device
5.	[TACACS API Admin]	API administrator role for Policy Manager Admin
6.	[TACACS Help Desk]	Help desk role for Policy Manager Admin
7.	[TACACS Network Admin]	Network administrator role for Policy Manager Admin
8.	[TACACS Read-only Admin]	Read-only administrator role for Policy Manager Admin
9.	[TACACS Receptionist]	Receptionist role for Policy Manager Admin
10.	[TACACS Super Admin]	Super administrator role for Policy Manager Admin

Showing 1-10 of 10 Export Delete

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 116** Add New Role

Add New Role

Name: [Text Field]

Description: [Text Area]

Save Cancel

**Table 94:** 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.



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 161 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 117** *Fig: Local Users Listing*

#	User ID	Name	Role	Status
1.	001e4cc18254	India Test Laptop	Role_Engineer	Enabled
2.	Akira	Akira Kurosawa	Senior_Mgmt	Enabled
3.	arthur	Arthur Denver	Senior_Mgmt	Enabled
4.	ashwath	Ashwath Murthy	[TACACS Super Admin]	Enabled
5.	avendaconference	Avenda Conference Room	ConferenceLaptop	Enabled
6.	bhprasad	Bhagya Prasad NR	TestQA	Enabled
7.	bob	Bill Gecko	Device SuperAdmin	Enabled
8.	carrie	Carrie Lipton	Senior_Mgmt	Enabled
9.	clay	Clay Pepp	Role_Engineer	Enabled
10.	david	David Hamel	Senior_Mgmt	Enabled

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

**Figure 118** *Add Local User*

Attribute	Value
1. Phone	= 408-555-1212
2. Email	= gabriel@acme.com
3. Designation	= Network Admin Consultant
4. Location	= HQ
5. Click to add...	

**Table 95:** *Add Local User*

Parameter	Description
User ID/ Name /Password/ Verify Password	Freeform labels and password.

Parameter	Description
Enable User	Uncheck to disable this user account.
Role	Select a static role for this local user.
Attributes	<p>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.</p> <p><b>NOTE:</b> All attributes entered for a local user are available in the role mapping rules editor under the LocalUser namespace.</p>

### 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 119** *Guest Users Listing*

#	Username	Sponsor Name	Guest Type	Status	Expired	Source Application
1.	abartz	admin	USER	Enabled	Valid	Policy Manager
2.	dmoore	admin	USER	Enabled	Valid	Policy Manager
3.	mohara	admin	USER	Enabled	Valid	Policy Manager
4.	skale	admin	USER	Enabled	Valid	Policy Manager

**Table 96:** *Guest Users Listing*

Parameter	Description
User Name	Guest user name.
Sponsor Name	Sponsor who sponsored the guest.
Guest Type	USER (for guest users) and DEVICE (for devices registered from the GuestConnect product).
Status	Enabled/Disabled status.

Parameter	Description
Expired	Whether the guest/device account has expired
Source Application	Where this account was created: From Policy Manager or the GuestConnect 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 120** Add New Guest User

**Figure 121** Add New Guest Device

**Table 97:** Add New Guest User/Device

Parameter	Description
Guest Type	Add a guest user or a guest device
User ID/ Name /Password/ Verify Password (Guest User only)	Freeform labels and password. Click <b>Auto Generate</b> to auto-generate a password for the guest user.

Parameter	Description
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	<p>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 <b>Attribute</b> drop down for all guest users.</p> <p><b>NOTE:</b> All attributes entered for a guest user are available in the role mapping rules editor under the GuestUser namespace.</p>

- 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 122** *Onboard Devices*

Configuration > Identity > Onboard Devices

Onboard Devices [Export Onboard Devices](#)

Filter: Device Name contains    Show 10 records

#	Device Name	Owner	Status	Expired	Expiry Time
1.	ios:172:mdps_generic		Enabled	Valid	Apr 25, 2013 17:24:34 PDT
2.	ios:174:mdps_generic		Enabled	Valid	Apr 25, 2013 17:35:25 PDT
3.	iOS:177:mdps_generic		Enabled	Valid	Apr 25, 2013 17:42:32 PDT
4.	sam:178:mdps_generic		Enabled	Valid	Apr 26, 2013 09:28:26 PDT
5.	Sam:180:mdps_generic		Enabled	Valid	Apr 26, 2013 09:31:25 PDT
6.	sam:182:mdps_generic		Enabled	Valid	Apr 26, 2013 09:43:03 PDT
7.	Sam:184:mdps_generic		Enabled	Valid	Apr 26, 2013 09:47:46 PDT
8.	sam:185:mdps_generic		Enabled	Valid	Apr 26, 2013 09:49:48 PDT
9.	sam:186:mdps_generic		Enabled	Valid	Apr 26, 2013 10:09:38 PDT
10.	sam:187:mdps_generic		Enabled	Valid	Apr 26, 2013 10:13:30 PDT

Showing 1-10 of 11

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 123** *View Onboard Devices*

View Onboard Devices

Device Name :	ios:174:mdps_generic
Password:	
Start Time:	Apr 25, 2012 17:05:25 PDT
Expiry Time:	Apr 25, 2013 17:35:25 PDT
Owner:	
Enable Device	<input checked="" type="checkbox"/>

Attribute	Value
1. Device Serial	=
2. Device UDID	=
3. Product Name	= iPod4,1
4. Product Version	= 9A405

Save Cancel

## Adding and Modifying Endpoints

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

**Figure 124** Endpoints Listing

Endpoints

Add Endpoint  
Import Endpoints  
Export All Endpoints

Filter: MAC Address contains Go Clear Filter Show 20 records

#	<input type="checkbox"/> MAC Address	Hostname	Category	OS Family	Status	Profiled
1.	<input checked="" type="checkbox"/> 001644b19320				Unknown	No
2.	<input type="checkbox"/> 001a927f8fcf				Unknown	No
3.	<input type="checkbox"/> 247703478518				Unknown	No

Showing 1-3 of 3

Authentication Records Export Delete

- 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 125** Endpoint Authentication Details

Endpoint Authentication Details

MAC Address	001644b19320				
Username	Device	Authentication	Start Time	Policy Manager Server	Session ID
1	10.2.50.29	ACCEPT	2012/04/25 11:23:17	10.2.50.177	R00000175-01-4f984115
2	10.2.50.29	ACCEPT	2012/04/25 11:23:03	10.2.50.177	R00000174-01-4f984107
3	10.2.50.29	ACCEPT	2012/04/25 11:17:45	10.2.50.177	R00000173-01-4f983fc9
4	10.2.50.29	ACCEPT	2012/04/25 11:17:31	10.2.50.177	R00000172-01-4f983fba
5	10.2.50.29	ACCEPT	2012/04/25 11:11:59	10.2.50.177	R00000171-01-4f983e6e
6	10.2.50.29	ACCEPT	2012/04/25 11:06:39	10.2.50.177	R00000170-01-4f983d2f
7	10.2.50.29	ACCEPT	2012/04/25 11:06:26	10.2.50.177	R0000016f-01-4f983d22

Close

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

**Figure 126** *Add Endpoint*

**Add Endpoint**

MAC Address: 00-21-70-9C-85-2B

Description:

Status: ☒ Known client ☐ Unknown client ☐ Disabled client

Attribute	Value
1. Device Type	= Turnstile
2. Click to add...	

Add Cancel

**Table 98:** *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 <b>"Click to add..."</b> 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. <b>NOTE:</b> 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 127** *Endpoint Popup*

**Edit Endpoint**

MAC Address: 90840d6da04e

Description:

Status: ☐ Known client ☒ Unknown client ☐ Disabled client

Attribute	Value
1. Click to add...	

**Policy Cache Values**

Roles: [User Authenticated], Senior\_Mgmt

Posture Status: UNKNOWN (100)

Last Updated at: Nov 18, 2010 17:24:07 PST

Cache Expires at: Nov 18, 2010 17:24:07 PST

Clear Cache Save Cancel

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 128** Static Host Lists (Listing Page)

Configuration > Identity > Static Host Lists

Static Host Lists

Filter: Name contains [ ] Go Clear Filter Show 10 records

Buttons: Add Static Host List, Import Static Host Lists, Export Static Host Lists

#	<input type="checkbox"/>	Name ▲	Format	Type	Description
1.	<input type="checkbox"/>	Handhelds	List	MACAddress	Handhelds Whitelist
2.	<input type="checkbox"/>	IP-Whitelist	List	IPAddress	
3.	<input type="checkbox"/>	Macintosh and iPhone Clients	Regex	MACAddress	MAC Address list for Apple vendor endpoints
4.	<input type="checkbox"/>	MAC Whitelist - No Posture	List	MACAddress	MAC Address list where posture rules are ignored
5.	<input type="checkbox"/>	SJ and Bangalore Endpoints	Regex	IPAddress	All San Jose & Bangalore Endpoints
6.	<input type="checkbox"/>	SJ Endpoints	Subnet	IPAddress	All San Jose Endpoints

Showing 1-6 of 6

Buttons: Export, Delete

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

**Figure 129** Add Static Host List

**Add Static Host List**

Name: Handhelds

Description: Handhelds Whitelist

Host Format: ☐ Subnet ☐ Regular Expression ☒ List

Host Type: ☐ IP Address ☒ MAC Address

List: 00-23-df-21-9b-a7  
00-21-e9-40-46-a5

Buttons: Remove Host, Add Host

Buttons: Save, Cancel

**Table 99:** *Add Static Host List*

Parameter	Description
Name/ Description	Freeform labels and descriptions.
Host Format	Select a format for expression of the address: <b>subnet</b> , <b>IP address</b> or <b>regular expression</b> .
Host Type	Select a host type: <b>IP Address</b> or <b>MAC Address</b> (radio buttons).
List	Use the <b>Add Host</b> and <b>Remove Host</b> 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

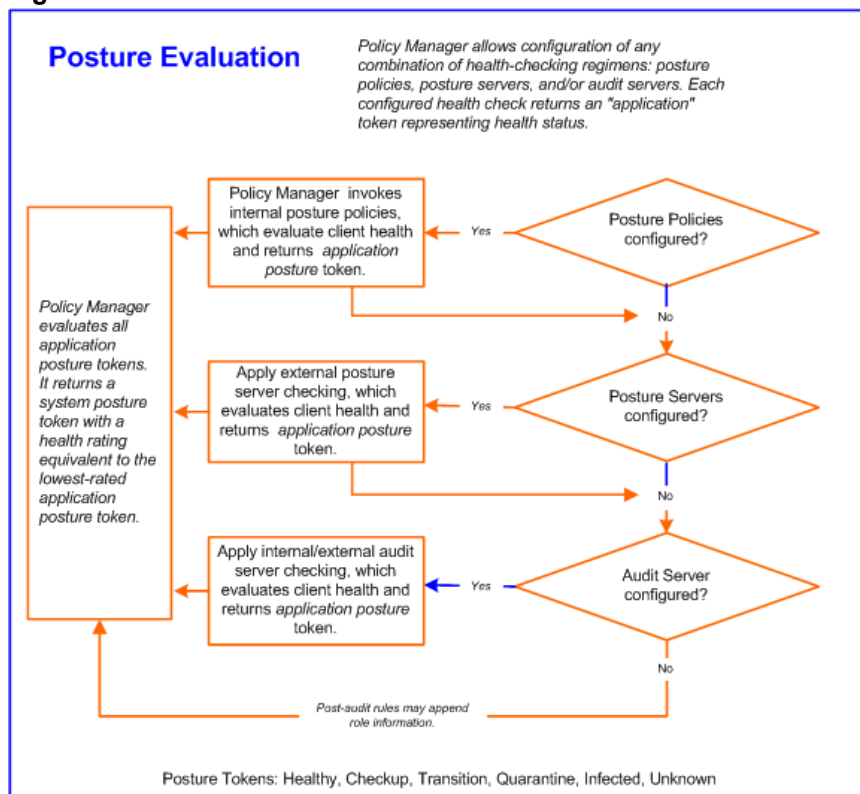
Policy Manager provides several *posture* methods for health evaluation of clients requesting access. These methods all return *Posture Tokens* (E.g., Healthy, Quarantine) for use by Policy Manager for input into *Enforcement Policy*. One or more of these posture methods may be associated with a *Service*.

## 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 130** *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/antispysware/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 131** *Posture Features at the Service Level*

The screenshot shows the 'Posture' tab in the ClearPass Policy Manager configuration interface. The 'Service' tab is selected, and the 'Posture' sub-tab is active. The configuration is divided into two main sections: 'Posture Policies' and 'Posture Servers'.

**Posture Policies:**

- Posture Policies:** A list box containing 'Basic Linux Health Check'. To the right of the list are buttons for 'Remove', 'View Details', and 'Modify'.
- Select to Add--**: A dropdown menu to add new policies.
- Default Posture Token:** A dropdown menu currently set to 'UNKNOWN (100)'.
- Remediate End-Hosts:** A checkbox labeled 'Enable auto-remediation of non-compliant end-hosts'.
- Remediation URL:** A text field containing 'http://remediation\_internal.us.acme.com'.

**Posture Servers:**

- Posture Servers:** A list box containing 'PS\_NPS [RADIUS] [Microsoft NPS]'. To the right of the list are buttons for 'Remove', 'View Details', and 'Modify'.
- Select to Add--**: A dropdown menu to add new servers.

You can configure the following features of posture:

**Table 100: Posture Features at the Service Level**

Configurable Component	How to Configure
Sequence of Posture Policies	<p>Select a Policy, then select <b>Move Up</b>, <b>Move Down</b>, <b>Remove</b>, or <b>View Details</b>.</p> <ul style="list-style-type: none"> <li>To add a previously configured Policy, select from the <b>Select</b> drop-down list, then click <b>Add</b>.</li> <li>To configure a new Policy, click the <b>Add New Policy</b> link and refer to <a href="#">"Adding and Modifying Posture Policies " on page 171</a>.</li> <li>To edit the selected posture policy, click <b>Modify</b> and refer to <a href="#">"Adding and Modifying Posture Policies " on page 171</a>.</li> </ul>
Default Posture Token	
Remediation End-Hosts	
Remediation URL	
Sequence of Posture Servers	<p>Select a Posture Server, then select <b>Move Up</b>, <b>Move Down</b>, <b>Remove</b>, or <b>View Details</b>.</p> <ul style="list-style-type: none"> <li>To add a previously configured Posture Server, select from the <b>Select</b> drop-down list, then click <b>Add</b>.</li> <li>To configure a new Posture Server, click <b>Add New Posture Server</b> (link) and refer to <a href="#">"Adding and Modifying Posture Servers " on page 197</a>.</li> <li>To edit the selected posture server, click <b>Modify</b> and refer to <a href="#">"Adding and Modifying Posture Servers " on page 197</a>.</li> </ul>
Enable auto-remediation of non-compliant end-hosts	<p>Select the <b>Enable auto-remediation of non-compliant end-hosts</b> 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.</p>

## 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 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 172 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 132** Add Posture Policy (Policy Tab)

**Table 101: Add Posture Policy**

Parameter	Description
Policy Name/Description	Freeform label and description.
Posture Agent	<ul style="list-style-type: none"> <li>• <b>NAP Agent</b> - 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: Microsoft Windows 8, Microsoft Windows 7, Microsoft Windows Vista, Microsoft Windows XP SP3, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, and Linux OSes supported by ClearPass Linux NAP Agent.</li> <li>• <b>OnGuard Agent</b> - 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: Microsoft Windows 8, Microsoft Windows 7, Microsoft Windows Vista, Microsoft Windows XP SP3, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2003, MAC OS X 10.5 or above, and Linux OSes supported by ClearPass Linux NAP Agent.</li> </ul>
Host Operating System	Select <b>Linux</b> , <b>Windows</b> or <b>Mac OS X</b> . Note that Mac OS X is not available if the Posture Agent is NAP.
Restrict by Roles	<p>Select role(s) that the Posture policy will apply to. Leave empty for the Posture policy to apply to all roles.</p> <ul style="list-style-type: none"> <li>• To add a role, select a role from the drop-down list, and then click <b>Add</b>.</li> <li>• To remove a role, select a role in the list, and then click <b>Remove</b>.</li> </ul>

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

**Figure 133 Add Posture Policy (Posture Plugins Tab) - Windows NAP Agent**

Policy | **Posture Plugins** | Rules | Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input checked="" type="checkbox"/> ClearPass Windows Universal System Health Validator	Configure View	-
<input type="checkbox"/> Windows System Health Validator	Configure View	-
<input type="checkbox"/> Windows Security Health Validator	Configure View	-

Back to Posture Policies Next > Save Cancel

**Figure 134 Add Posture Policy (Posture Plugins Tab) - Linux NAP Agent**

Policy | **Posture Plugins** | Rules | Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input checked="" type="checkbox"/> ClearPass Linux Universal System Health Validator	Configure View	-

Back to Posture Policies Next > Save Cancel

**Figure 135** Add Posture Policy (Posture Plugins Tab) - Windows OnGuard Agent

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Windows Universal System Health Validator	Configure View	-
<input type="checkbox"/> Windows System Health Validator	Configure View	-
<input type="checkbox"/> Windows Security Health Validator	Configure View	-

**Figure 136** Add Posture Policy (Posture Plugins Tab) - Linux OnGuard Agent

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Linux Universal System Health Validator	Configure View	-

**Figure 137** Add Posture Policy (Posture Plugins Tab) - Mac OS X OnGuard Agent

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> ClearPass Mac OS X Universal System Health Validator	Configure View	-

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

- "ClearPass Windows Universal System Health Validator - NAP Agent " on page 175
- "Windows System Health Validator - NAP Agent " on page 196
- "Windows Security Health Validator - NAP Agent " on page 195
- "ClearPass Windows Universal System Health Validator - OnGuard Agent " on page 191
- "ClearPass Linux Universal System Health Validator - NAP Agent" on page 191
- "ClearPass Linux Universal System Health Validator - OnGuard Agent " on page 193
- "Windows System Health Validator - OnGuard Agent " on page 196
- "Windows Security Health Validator - OnGuard Agent " on page 195
- "ClearPass Mac OS X Universal System Health Validator - OnGuard Agent " on page 193

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 138** *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 139** *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" on page 176
- "Processes" on page 177
- "Registry Keys" on page 180
- "AntiVirus" on page 181
- "AntiSpyware" on page 183
- "Firewall" on page 184
- "Peer To Peer" on page 185
- "Patch Management" on page 186
- "Windows Hotfixes" on page 187
- "USB Devices" on page 188
- "Virtual Machines" on page 188
- "Network Connections" on page 189

## Services

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

**Figure 140** *Services Page*

**Table 102:** *Services Page*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop or start services based on the entries in <b>Service to run</b> and <b>Services to stop</b> 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 <b>Services to run</b> or <b>Services to stop</b> 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 <b>Service to run</b> or <b>Services to stop</b> 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 <b>Insert</b> .
Delete	To remove a service from the list of available services, select it and click <b>Delete</b> .

## Processes

The **Processes** page provides a set of widgets for specifying specific processes to be explicitly present or absent on the system.

**Figure 141** *Processes Page (Overview)*

The screenshot shows the 'Processes' page overview. At the top, there are checkboxes for 'Remediation checks', 'Auto Remediation', and 'User Notification'. Below this, there are two main sections: 'Processes to be Present' and 'Processes to be Absent'. Each section contains a table with columns for 'Process Path' and 'Process Name', and an 'Add' button to the right of the table header.

**Table 103:** *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 <b>Registry keys to be present</b> and <b>Registry keys to be absent</b> configuration).
User Notification	Enable to allow user notifications for registry check policy violations.
Processes to be present/absent	Click <b>Add</b> to specify a process to be added, either to the <b>Processes to be present</b> or <b>Processes to be absent</b> lists.

Click **Add** for Process to be present to display the **Process** page detail.

### Processes to be Present

**Figure 142** *Process to be Present Page (Detail)*

The screenshot shows the 'Process to be Present - Add' page. It has a title bar 'Process to be Present - Add'. Below the title bar, there is a 'Process Location' dropdown menu with 'SystemDrive' selected. There are two text input fields: 'Enter the Process name' and 'Enter the Display name'. At the bottom, there are 'Save' and 'Cancel' buttons.

**Table 104:** *Process to be Present Page (Detail)*

Parameter	Description
Process Location	Choose from one of the pre-defined paths, or choose None. <ul style="list-style-type: none"> <li>SystemDrive - For example, C:</li> <li>SystemRoot - For example, C:\Windows</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• ProgramFiles - For example, "C:\Program Files"</li> <li>• HOMEDRIVE - For example, C:</li> <li>• HOMEPATH - For example, \Users\JohnDoe</li> <li>• None - By selecting None, you can enter a custom path name in the Process Name field.</li> </ul>
Enter the Process name	<p>A pathname containing the process executable name. Some valid examples are listed below:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 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"</li> <li>• 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"</li> </ul> <p>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.</p>
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 143** *Process to be Absent Page (Detail)*

The figure consists of two screenshots of a web form titled "Process to be Absent - Add".

The top screenshot shows the "Check Type :" section with two radio buttons: "Process Name" (selected) and "MD5 Sum". Below this are two text input fields: "Enter the Process name" and "Enter the Display name". At the bottom are "Save" and "Cancel" buttons.

The bottom screenshot shows the "Check Type :" section with two radio buttons: "Process Name" and "MD5 Sum" (selected). Below this is a large text area labeled "MD5 Sum". At the bottom is a text input field labeled "Enter the Display name" and "Save" and "Cancel" buttons.

**Table 105:** *Process to be Absent Page (Detail)*

Parameter	Description
Check Type	Select the type of process check to perform. The agent can look for <ul style="list-style-type: none"><li>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.</li><li>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.</li></ul>
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

**Figure 144** *Process Page (Overview - Post Add)*

Remediation checks	<input checked="" type="checkbox"/> Auto Remediation	<input checked="" type="checkbox"/> User Notification
Processes to be Present <span>Add</span>		
Process Path	Process Name	
SystemDrive	system32\notepad.exe	
Processes to be Absent <span>Add</span>		
Process MD5 Sum	Process Name	
-	usurf.exe	
e1ab298bafc8ecca8c322a29c5fdc68c	UltraSurf	
3f0ebc940fa292bb5f1d87dd544b5d60		

## Registry Keys

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

**Figure 145** *Registry Keys Page (Overview)*

Remediation checks	<input checked="" type="checkbox"/> Auto Remediation	<input checked="" type="checkbox"/> User Notification	
Registry keys to be present <span>Add</span>			
Key	Name	Value	Type
Registry keys to be absent <span>Add</span>			
Key	Name	Value	Type

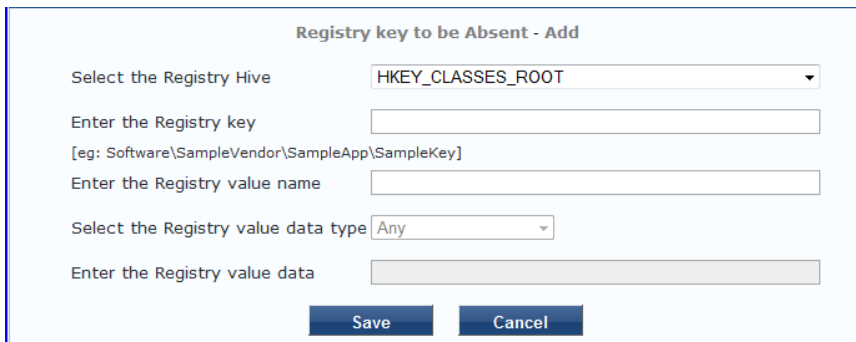
**Table 106:** *Registry Keys Page (Overview - Pre-Add)*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for registry checks (Automatically add or remove registry keys based on the entries in <b>Registry keys to be present</b> and <b>Registry keys to be absent</b> configuration).
User Notification	Enable to allow user notifications for registry check policy violations.
Registry keys to be present/absent	Click <b>Add</b> to specify a registry key to be added, either to the <b>Registry keys to be present</b> or <b>Registry keys to be absent</b> lists.

Click **Add** for either condition to display the **Registry** page detail.

## Registry Keys to be Absent

**Figure 146** Registry Keys Page (Detail)



The form is titled "Registry key to be Absent - Add". It contains the following fields and controls:

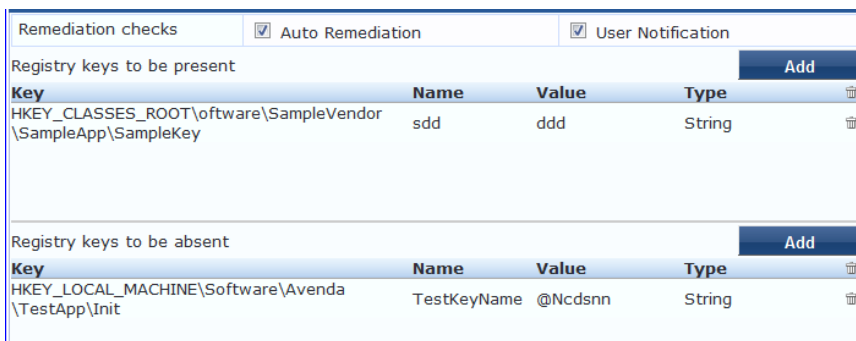
- "Select the Registry Hive": A dropdown menu with "HKEY\_CLASSES\_ROOT" selected.
- "Enter the Registry key": A text input field with a placeholder example "[eg: Software\SampleVendor\SampleApp\SampleKey]".
- "Enter the Registry value name": A text input field.
- "Select the Registry value data type": A dropdown menu with "Any" selected.
- "Enter the Registry value data": A text input field.
- "Save" and "Cancel" buttons at the bottom.

**Table 107:** 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 147** Registry Keys Page (Overview - Post Add)



The screenshot shows the "Registry Keys" page with two sections: "Registry keys to be present" and "Registry keys to be absent".

**Registry keys to be present:**

Key	Name	Value	Type	
HKEY_CLASSES_ROOT\oftware\SampleVendor\SampleApp\SampleKey	sdd	ddd	String	

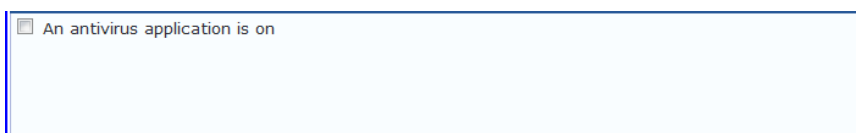
**Registry keys to be absent:**

Key	Name	Value	Type	
HKEY_LOCAL_MACHINE\Software\Avenda\TestApp\Init	TestKeyName	@Ncdsnn	String	

## AntiVirus

In the **Antivirus** page, you can 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 148** Antivirus Page (Overview - Before)



The screenshot shows a single checkbox labeled "An antivirus application is on".

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

**Figure 149** Antivirus Page (Detail 1)

The screenshot shows the top section of the Antivirus configuration page. At the top, there are four checkboxes: "An antivirus application is on" (checked), "Remediation checks" (unchecked), "Auto Remediation" (checked), "User Notification" (checked), and "Display Update URL" (checked). Below these is an "Add" button. Underneath is a table with the following columns: "Antivirus", "Prd Version", "Eng Version", "Dat Version", "Dat Update", "Last Scan", "Rtp Check", and a trashcan icon. The table is currently empty.

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

**Figure 150** Antivirus Page (Detail 2)

The screenshot shows the "Product-specific checks" section. It includes a checkbox "(Uncheck to allow any product)" which is checked. Below it is a dropdown menu "Select the antivirus product" with "Symantec AntiVirus" selected. There are three more dropdown menus: "Product version check" (set to "Is Latest"), "Engine version check" (set to "No Check"), and "Data file version check" (set to "No Check"). Below these are two input fields for "Data file has been updated in" and "Last scan has been done before", both set to "2" with "Hour(s)" dropdowns. At the bottom, there are radio buttons for "Real-time Protection Status Check": "No Check" (unchecked), "On" (checked), and "Off" (unchecked). "Save" and "Cancel" buttons are at the bottom right.

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

**Figure 151** Antivirus Page (Overview - After)

The screenshot shows the same table as in Figure 149, but now it contains one row of data. The row has the following values: "Symantec AntiVirus" in the "Antivirus" column, "isLatest" in "Prd Version", "no check" in "Eng Version", "no check" in "Dat Version", "2 Hour(s)" in "Dat Update", "2 Hour(s)" in "Last Scan", and "on" in "Rtp Check". The trashcan icon is visible at the end of the row.

**Table 108:** Antivirus Page

Interface	Parameter	Description
Antivirus Page	<ul style="list-style-type: none"> <li>An Antivirus Application is On</li> <li>Auto Remediation</li> <li>User Notification</li> <li>Display Update URL</li> </ul>	<ul style="list-style-type: none"> <li>Check the <b>Antivirus Application is On</b> check box to enable testing of health data for configured Antivirus application(s).</li> <li>Check the <b>Auto Remediation</b> check box to enable auto remediation of anti-virus status.</li> <li>Check the <b>User Notification</b> check box to enable user notification of policy violation of anti-virus status.</li> <li>Check the <b>Display Update URL</b> check box to show the origination URL of the update.</li> </ul>
Antivirus Page (Detail 1)	<ul style="list-style-type: none"> <li>Add</li> <li>Trashcan icon</li> </ul>	<ul style="list-style-type: none"> <li>To configure Antivirus application attributes for testing against health data, click <b>Add</b>.</li> <li>To remove configured Antivirus application attributes from the list, click the <b>trashcan icon</b> in that row.</li> </ul>

Interface	Parameter	Description
Antivirus Page (Detail 2)	Product/Version/Last Check	<p>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.</p> <ul style="list-style-type: none"> <li>• Select the antivirus product - Select a vendor from the list</li> <li>• Product version check - No Check, Is Latest (requires registration with ClearPass portal), At Least, In Last N Updates (requires registration with ClearPass Portal)</li> <li>• Engine version check - Same choices as product version check.</li> <li>• Data file version check - Same choices as product version check</li> <li>• Data file has been updated in - Specify the interval in hours, days, weeks, or months.</li> <li>• Last scan has been done before - Specify the interval in hours, days, weeks, or months.</li> <li>• Real-time Protection Status Check - No Check, On, or Off.</li> </ul>

## 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 Antipware Application is On** to configure the AntiSpyware application information.

**Figure 152** AntiSpyware Page (Overview Before)

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

**Figure 153** AntiSpyware Page (Detail 1)

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

**Figure 154** AntiSpyware Page (Detail 2)

**Figure 155 AntiSpyware Page (Overview After)**

☒ An antispyware application is on

Remediation checks ☒ Auto Remediation ☒ User Notification ☒ Display Update URL

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	
AVG Anti-Malware [AntiSpyware]	isLatest	isLatest	no check	2 Hour(s)	no check	nocheck	<input type="button" value=""/>

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 156 Firewall Page (Overview Before)**

☐ A firewall application is on

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

**Figure 157 Firewall Page (Detail 1)**

☒ A firewall application is on

Remediation checks ☒ Auto Remediation ☒ User Notification

Product-specific checks ☒ (Uncheck to allow any product)

Firewall Product Name	Product Version	
-----------------------	-----------------	--

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

**Figure 158 Firewall Page (Detail 2)**

Select the firewall product

Product version is at least

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

**Figure 159 Firewall Page (Overview After)**

☒ A firewall application is on

Remediation checks ☒ Auto Remediation ☒ User Notification

Product-specific checks ☒ (Uncheck to allow any product)

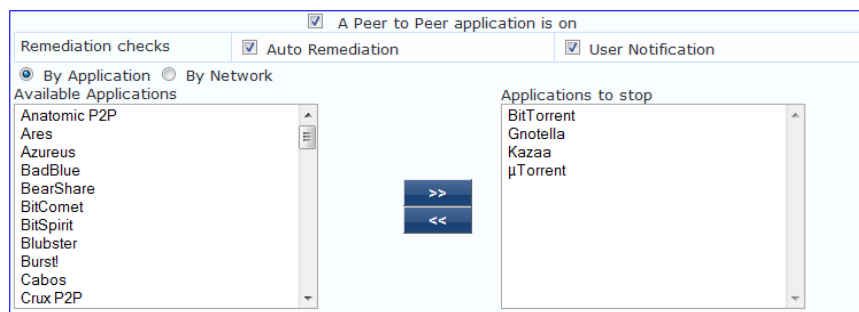
Firewall Product Name	Product Version	
BitDefender Internet Security 2009	12	<input type="button" value=""/>

**Table 109: Firewall Page**

Interface	Parameter	Description
Firewall Page	<ul style="list-style-type: none"> <li>A Firewall Application is On</li> <li>Auto Remediation</li> <li>User Notification</li> <li>Uncheck to allow any product</li> </ul>	<ul style="list-style-type: none"> <li>Check the <b>Firewall Application is On</b> check box to enable testing of health data for configured firewall application(s).</li> <li>Check the <b>Auto Remediation</b> check box to enable auto remediation of firewall status.</li> <li>Check the <b>User Notification</b> check box to enable user notification of policy violation of firewall status.</li> <li>Uncheck the <b>Uncheck to allow any product</b> check box to check whether any firewall application (any vendor) is running on the end host.</li> </ul>
Firewall Page (Detail 1)	<ul style="list-style-type: none"> <li>Add</li> <li>Trashcan icon</li> </ul>	<ul style="list-style-type: none"> <li>To configure firewall application attributes for testing against health data, click <b>Add</b>.</li> <li>To remove configured firewall application attributes from the list, click the <b>trashcan icon</b> in that row.</li> </ul>
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. <ul style="list-style-type: none"> <li>Select the firewall product - Select a vendor from the list</li> <li>Product version is at least - Enter the version of the product.</li> </ul>

## 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 160 Peer to Peer Page****Table 110: 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 <b>Applications to stop</b> 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 <b>Applications to stop</b> panel. Click the >> or << to add or remove, respectively, the applications or networks from the <b>Applications to stop</b> 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 161** *Patch Management Page (Overview - Before)*

☐ A patch management application is on

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

**Figure 162** *Patch Management Page (Detail 1)*

☒ A patch management application is on

Remediation checks ☒ Auto Remediation ☒ User Notification

Product-specific checks ☒ (Uncheck to allow any product)

**PM Product Name** **Product Version** **Status Check** **Add**

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

**Figure 163** *Patch Management Page (Detail 2)*

Select the Patch Mgmt product

Product version is at least

Status Check Type

**Save** **Cancel**

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

**Figure 164** *Patch Management Page (Overview - After)*

☒ A patch management application is on

Remediation checks ☒ Auto Remediation ☒ User Notification

Product-specific checks ☒ (Uncheck to allow any product)

**PM Product Name** **Product Version** **Status Check** **Add**

BigFix Enterprise Client	3.0	Enabled	
--------------------------	-----	---------	--

**Table 111: Patch Management Page**

Interface	Parameter	Description
Patch Management Page	<ul style="list-style-type: none"> <li>A patch management application is on</li> <li>Auto Remediation</li> <li>User Notification</li> <li>Uncheck to allow any product</li> </ul>	<ul style="list-style-type: none"> <li>Check the <b>Patches / Hot fixes Application is On</b> check box to enable testing of health data for configured Antivirus application (s).</li> <li>Check the <b>Auto Remediation</b> check box to enable auto remediation of patch management status.</li> <li>Check the <b>User Notification</b> check box to enable user notification of policy violation of patch management status.</li> <li>Uncheck the <b>Uncheck to allow any product</b> check box to check whether any patch management application (any vendor) is running on the end host.</li> </ul>
Patch Management Page (Detail 1)	<ul style="list-style-type: none"> <li>Add</li> <li>Trashcan icon</li> </ul>	<ul style="list-style-type: none"> <li>To configure patch management application attributes for testing against health data, click <b>Add</b>.</li> <li>To remove configured patch management application attributes from the list, click the <b>trashcan icon</b> in that row.</li> </ul>
Patch Management Page (Detail 2)	Product/Version	<p>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.</p> <ul style="list-style-type: none"> <li>Select the Patch Mgmt product - Select a vendor from the list</li> <li>Product version is at least - Enter version number</li> <li>Status check type - No check, Enabled, Disabled</li> </ul>

## Windows Hotfixes

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

**Figure 165 Windows Hotfixes Page**

☒ Enable checks for Windows 7

Windows Hotfixes

Remediation checks ☒ Auto Remediation ☒ User Notification

Available Hotfixes

Critical  
Important  
Moderate  
Low  
Unspecified

KB2032276 (CRITICAL)  
KB2079403 (CRITICAL)  
KB2160841 (CRITICAL)  
KB2183461 (CRITICAL)  
KB2281679 (CRITICAL)  
KB2286198 (CRITICAL)  
KB2296199 (CRITICAL)

Hotfixes to be present

**Table 112: 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 <b>Hotfixes to be present</b> panel (using their associated widgets). Click the >> or << to add or remove, respectively, the hotfixes from the <b>Hotfixes to run</b> boxes.

## USB Devices

The **USB Devices** page provides configuration to control USB mass storage devices attached to an endpoint.

**Figure 166** *USB Devices*

**Table 113:** *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	<ul style="list-style-type: none"> <li>• No Action - Take no action; do not eject or disable the attached devices.</li> <li>• Remove USB Mass Storage Devices - Eject the attached devices.</li> <li>• Remove USB Mass Storage Devices - Stop the attached devices.</li> </ul>

## Virtual Machines

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

**Figure 167** *USB Devices*

**Table 114:** *Virtual Machines*

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.
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	<ul style="list-style-type: none"> <li>• No Action - Take no action; do not stop or pause virtual machines.</li> <li>• Stop all Virtual Machines running on Host - Stop the VM clients that are running on Host.</li> <li>• Pause all Virtual Machines running on Host - Pause the VM clients that are running on Host.</li> </ul>

## Network Connections

The **Network Connections** page provides configuration to control network connections based on connection type.

**Figure 168** *Network Connections*

☒ Network Connections Check is on

Remediation checks ☒ Auto Remediation ☒ User Notification

☐ Check for Network Connection Types **Configure**

Network Connections Type	Network Connections Allowed	Remediation Action For Network Connections Not Allowed
-	-	-

☒ Allow Bridge Network Connection  
Remediation Action for Bridge Network Connection No Action

☒ Allow Internet Connection Sharing  
Remediation Action for Internet Connection Sharing No Action

☒ Allow Adhoc/Hosted Wireless Networks  
Remediation Action for Adhoc/Hosted Wireless Networks No Action

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

### Configure Network Connection Type

**Figure 169** Network Connection Type Configuration

Network Connection Types

Allowed Network Connections Type: Allow Only One Network Connection

Network Connections Types: Others, Wired, Wireless

Network Connections Allowed:

Remediation Action For Network Connection Types Not Allowed: No Action

Save Cancel

**Table 115:** 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	<ul style="list-style-type: none"><li>No Action - Take no action; do not eject or disable the attached devices.</li><li>Disable Network Connections - Disable network connections for the configured network type.</li></ul>

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 116:** 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 <b>Allow Bridge Network Connection</b> 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 <b>Allow Internet Connection Sharing</b> 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 <b>Allow Adhoc/Hosted Wireless Networks</b> 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 170** *Fig: ClearPass Linux Universal system Health Validator - NAP Agent*

The screenshot shows the 'Linux Universal System Health Validator' configuration window. On the left, there's a sidebar with a tree view containing 'CentOS', 'Services', 'Fedora', 'Red Hat Enterprise Linux', 'SUSE Linux Enterprise Desktop', and 'General Configuration'. The 'CentOS' option is selected. The main area has a checkbox 'Enable checks for CentOS' which is checked. Below it, there are three checkboxes: 'Remediation checks' (checked), 'Auto Remediation' (checked), and 'User Notification' (checked). There are two list boxes: 'Available Services' on the left and 'Services to run' on the right. The 'Available Services' list contains: auditd, autofs, avahi-daemon, connman, crond, cups, dovecot, haldaemon, httpd, nfslock, ntpd. There are 'Insert', '>>', '<<', and 'Delete' buttons between the two list boxes. At the bottom, there is a 'Quarantine Message' text field and 'Reset', 'Save', and 'Cancel' buttons.

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 117:** *Services View*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically start or stop services based on the entries in <b>Service to run</b> and <b>Service to stop</b> 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 <b>Services to run</b> or <b>Services to stop</b> 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 <b>Insert</b> .
Delete	To remove a service from the list of selectable services, select it and click <b>Delete</b> .

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 171** *General Configuration Section*

The screenshot shows a sidebar with a list of operating systems: CentOS, Fedora, Red Hat Enterprise Linux, SUSE Linux Enterprise Desktop, and General Configuration. Below this list are two expandable sections: AntiVirus and Firewall. To the right of the sidebar, there is a checkbox labeled 'Antivirus Check'.

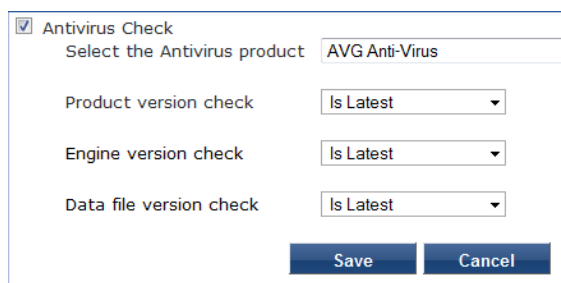
Select **Firewall Check** to display a view where you can specify Firewall parameters, specifically with respect to which ports may be open or blocked.

**Figure 172** *Firewall view*

The screenshot shows the 'Firewall Check' configuration window. It has a title bar with a checked checkbox and the text 'Firewall Check'. Below the title bar, there are three tabs: 'Remediation checks', 'Auto Remediation' (which is selected), and 'User Notification'. Under the 'Auto Remediation' tab, there are several input fields: 'TCP ports to open', 'UDP ports to open', a checkbox for 'Block all other ports', 'TCP ports to block', and 'UDP ports to block'. At the bottom, there is an example text: 'Example: 90,100-200,256,1000-2000'.

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

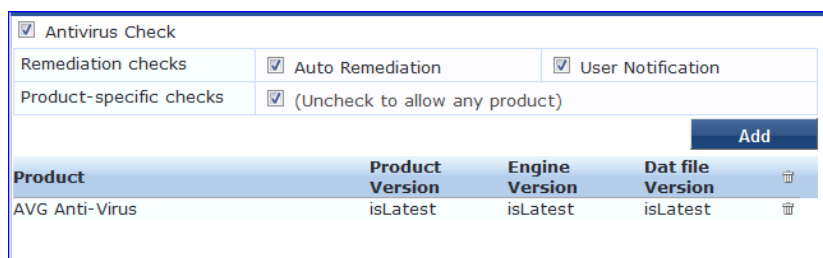
**Figure 173** *Antivirus Check view*

A dialog box titled "Antivirus Check" with a checked checkbox. It contains a "Select the Antivirus product" field with "AVG Anti-Virus" selected. Below are three version check options, each with a dropdown menu set to "Is Latest": "Product version check", "Engine version check", and "Data file version check". At the bottom are "Save" and "Cancel" buttons.

<input checked="" type="checkbox"/> Antivirus Check
Select the Antivirus product: <input type="text" value="AVG Anti-Virus"/>
Product version check: <input type="text" value="Is Latest"/>
Engine version check: <input type="text" value="Is Latest"/>
Data file version check: <input type="text" value="Is Latest"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>

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

**Figure 174** *Antivirus Check*

A configuration interface for Antivirus Check. It includes checkboxes for "Remediation checks" (Auto Remediation, User Notification) and "Product-specific checks" (unchecked, with a note "(Uncheck to allow any product)"). Below is a table with columns: Product, Product Version, Engine Version, Dat file Version, and an Add button. The table contains one row for "AVG Anti-Virus" with version "isLatest".

<input checked="" type="checkbox"/> Antivirus Check				
Remediation checks	<input checked="" type="checkbox"/> Auto Remediation	<input checked="" type="checkbox"/> User Notification		
Product-specific checks	<input type="checkbox"/> (Uncheck to allow any product)			
<input type="button" value="Add"/>				
Product	Product Version	Engine Version	Dat file Version	
AVG Anti-Virus	isLatest	isLatest	isLatest	<input type="button" value="Add"/>

**Table 118:** *Antivirus Check*

Interface	Parameter	Description
Antivirus Main view	Add	To configure Antivirus application attributes for testing against health data, click <b>Add</b> .
	Trashcan icon	To remove configured Antivirus application attributes from the list, click the <b>trashcan icon</b> 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).

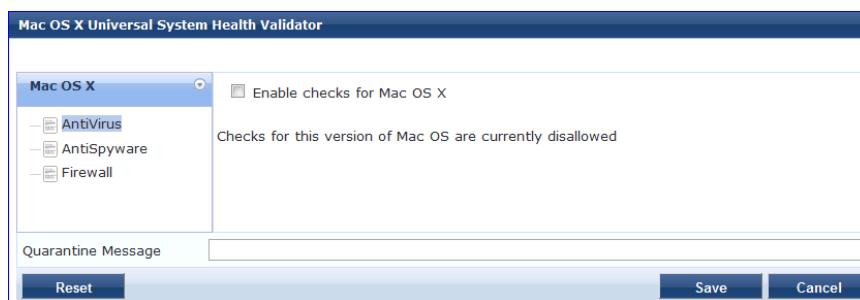
The dissolvable agent version of the ClearPass Linux Universal System Health Validator supports all the features supported by the "[ClearPass Linux Universal System Health Validator - NAP Agent](#)" on page 191 except for the following:

- 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.

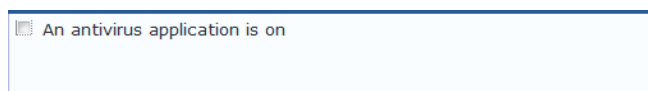
**Figure 175** ClearPass Mac OS X Universal System Health Validator - OnGuard Agent

The screenshot shows the 'Mac OS X Universal System Health Validator' window. On the left, there's a sidebar with 'Mac OS X' selected, containing sub-items: 'Antivirus', 'AntiSpyware', and 'Firewall'. The main area has a checkbox 'Enable checks for Mac OS X' which is unchecked. Below it, a message states 'Checks for this version of Mac OS are currently disallowed'. At the bottom, there's a 'Quarantine Message' text field and three buttons: 'Reset', 'Save', and 'Cancel'.

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 176** Antivirus Page (Overview - Before)

This is a snippet of the 'Antivirus' configuration page. It shows a single item in a list: 'An antivirus application is on'.

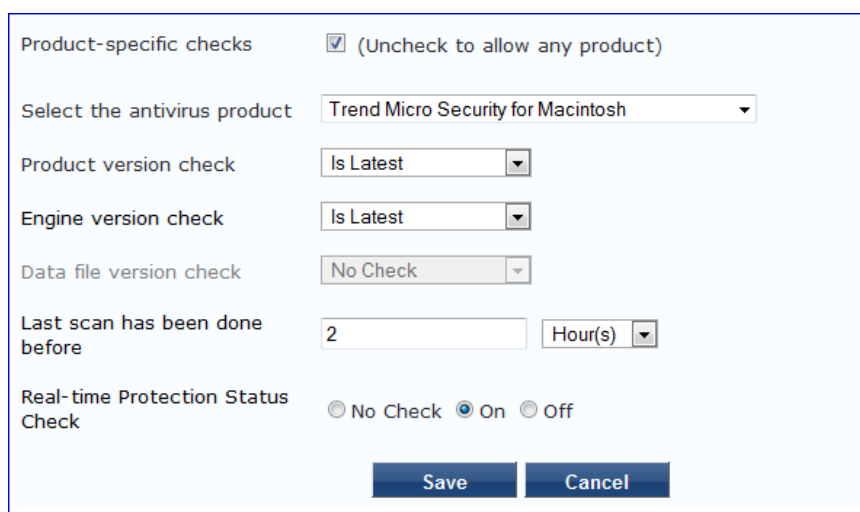
When enabled, the **Antivirus** detail page appears.

**Figure 177** Antivirus Page (Detail 1)

This snippet shows the top part of the 'Antivirus' detail page. It includes a header 'An antivirus application is on' with sub-sections 'Remediation checks' (containing 'Auto Remediation') and 'User Notification' (containing 'User Notification'). There is an 'Add' button and a table header with columns: 'Antivirus', 'Prd Version', 'Eng Version', 'Dat Version', 'Last Scan', and 'Rtp Check'.

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

**Figure 178** Antivirus Page (Detail 2)

This is a detailed configuration form for the 'Antivirus' page. It contains several sections: 'Product-specific checks' with a checkbox '(Uncheck to allow any product)'; 'Select the antivirus product' with a dropdown menu showing 'Trend Micro Security for Macintosh'; 'Product version check' with a dropdown menu showing 'Is Latest'; 'Engine version check' with a dropdown menu showing 'Is Latest'; 'Data file version check' with a dropdown menu showing 'No Check'; 'Last scan has been done before' with a text input '2' and a dropdown menu 'Hour(s)'; and 'Real-time Protection Status Check' with radio buttons for 'No Check', 'On' (selected), and 'Off'. At the bottom are 'Save' and 'Cancel' buttons.

When you save your Antivirus configuration, it appears in the **Antivirus** page list. See "[ClearPass Windows Universal System Health Validator - NAP Agent](#) " on page 175 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 175 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 179** 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 180** *Windows Security Health Validator*

The screenshot shows the 'Windows Security Health Validator' window. On the left, there is a sidebar with a tree view containing 'Configuration' (selected), 'Windows 8', 'Windows 7', 'Windows Vista', and 'Windows XP'. The main area is titled 'Enable checks for Windows 8' and lists several security checks that can be enabled or disabled. The checks are: Firewall, Virus Protection, Spyware Protection, Automatic Updates, and Security Updates. Each check has a checkbox and a description of what the client must have. For example, 'Firewall' requires the client to have a firewall enabled. 'Security Updates' includes a dropdown for 'Important and above' and a text box for '22 hours'. At the bottom, there are 'Reset', 'Save', and 'Cancel' buttons.

## 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 181** *Windows System Health Validator (Overview)*

The screenshot shows the 'Windows System Health Validator' window. The main area is titled 'Client computers can connect to your network, subject to the following checks -'. It lists several operating systems and their corresponding service pack levels. The checks are: Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2008, and Windows Server 2008 R2. Each check has a checkbox and a description of what the client must have. For example, 'Windows 8' requires the client to have Service Pack less than a certain level. At the bottom, there are 'Reset', 'Save', and 'Cancel' buttons.

## 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 Windows 2000 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 182** Windows System Health Validator - OnGuard Agent (Overview)

Client computers can connect to your network, subject to the following checks -

- ☒ **Windows 8**  
Windows 8 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows 7**  
Windows 7 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Vista**  
Windows Vista clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows XP**  
Windows XP clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Server 2008**  
Windows Server 2008 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Server 2008 R2**  
Windows Server 2008 R2 clients are allowed

## Adding and Modifying Posture Servers

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

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

**Figure 183** Posture Servers Listing Page

Configuration > Posture > Posture Servers

Posture Servers

Filter: Server Type contains    Show 10 records

#	Name	Description	Server Type	Default State
1.	Avenda CCA CAM	Cisco Clean Access Manager GAMEV2 server	Cisco CCA	UNKNOWN
2.	PS_NPS	NAP Posture Server	Microsoft NPS	UNKNOWN

Showing 1-2 of 2

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

**Figure 184** Add Posture Server Page

Configuration > Posture > Posture Servers > Add

Posture Servers

Name:

Description:

Server Type: ☒ Microsoft NPS

Default Posture Token:

Depending on the **Protocol** and **Requested Credentials**, different tabs and fields appear. Refer to "Microsoft NPS " on page 197.

## 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 119:** *Microsoft NPSSettings (Posture Server tab)*

Parameter	Description
Name/Description	Freeform label and description.
Server Type	Always <b>Microsoft NPS</b> .
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 185** *Microsoft NPS Settings (Primary and Backup Server tabs)*

**Table 120:** *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 <b>Enable to use backup when primary does not respond</b> check box.

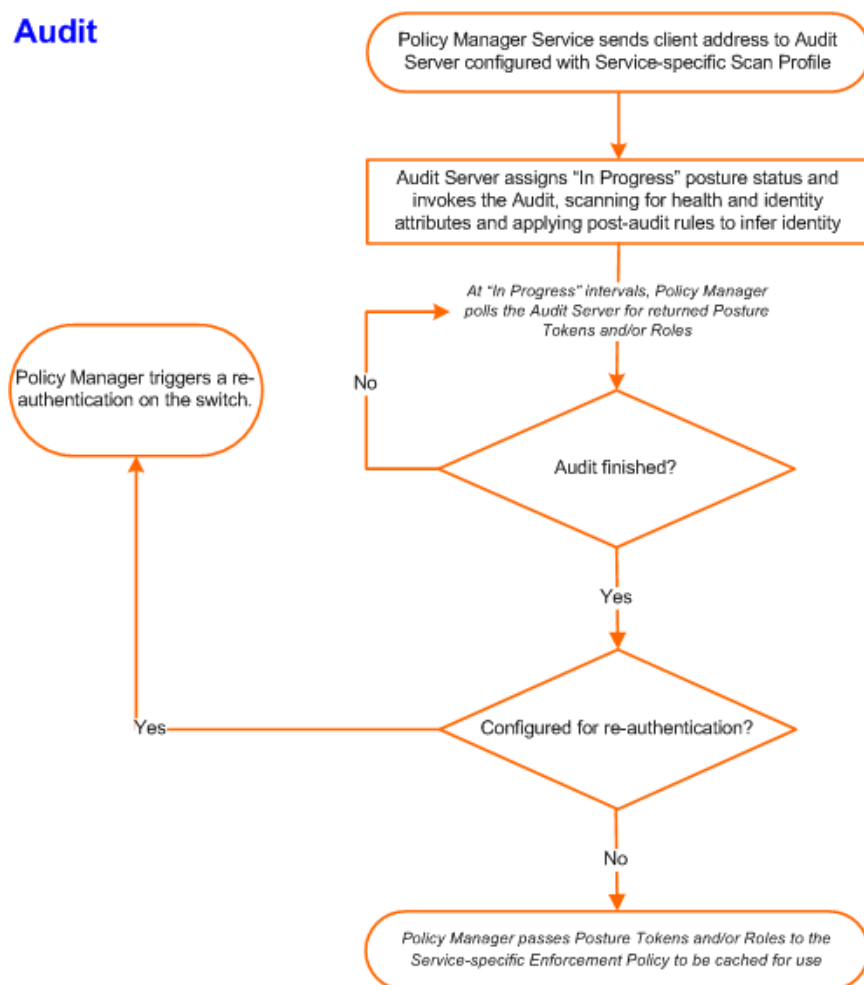
Audit Servers evaluate posture and/or role for unmanaged or unmanageable clients; that is, clients that lack an adequate posture agent or 802.1X supplicant (for example, printers, PDAs, or guest users may not be able to send posture credentials or identify themselves.) A Policy Manager Service can trigger 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 186** *Flow of Control of Policy Manager Auditing*

### Audit



Refer to "Configuring Audit Servers" on page 199 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" on page 200
- "Custom Audit Servers" on page 202
- "Nessus Scan Profiles" on page 205

## 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 187** *Audit Tab*

Configuration > Services > Add  
Services

Service Authentication Roles Enforcement **Audit** Summary

Audit Server: --Select-- View Details Modify Add new Audit Server

Audit Trigger Conditions:  
☐ Always  
☐ When posture is not available  
☐ For MAC authentication request

Action after audit:  
☒ No Action  
☐ Do SNMP bounce  
☐ Trigger RADIUS CoA action

[Back to Services](#) Next > Save Cancel

**Table 121:** *Audit Tab*

Parameter	Description
Audit Server/Add new Audit Server	<p>Select a built-in server profile from the list:</p> <ul style="list-style-type: none"><li>• The <i>[Nessus Server]</i> performs vulnerability scanning. It returns a Healthy/Quarantine result.</li><li>• The <i>[Nmap Audit]</i> performs network port scans. The health evaluation always returns <b>Healthy</b>. The port scan gathers attributes that allow determination of Role(s) through post-audit rules.</li></ul> <p><b>NOTE:</b> 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.</p>

Parameter	Description
	To audit devices that have a static IP address assigned, it is recommended that a static binding between the MAC and IP address of the endpoint be created in your DHCP server. Refer to your DHCP Server documentation for configuring such static bindings. Note 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	<ul style="list-style-type: none"> <li>● <b>Always:</b> Always perform an audit</li> <li>● <b>When posture is not available:</b> Perform audit only when posture credentials are not available in the request.</li> <li>● <b>For MAC Authentication Request,</b> If you select this option, then Policy Manager presents three additional settings: <ul style="list-style-type: none"> <li>■ <b>For known end-hosts only.</b> 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.</li> <li>■ <b>For unknown end-hosts only.</b> 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.</li> <li>■ <b>For all end-hosts.</b> For both known and unknown end-hosts.</li> </ul> </li> </ul>
Re-authenticate client	<p>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).</p> <p><b>NOTE:</b> 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.</p>

## 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 188** *Audit Servers Listing*

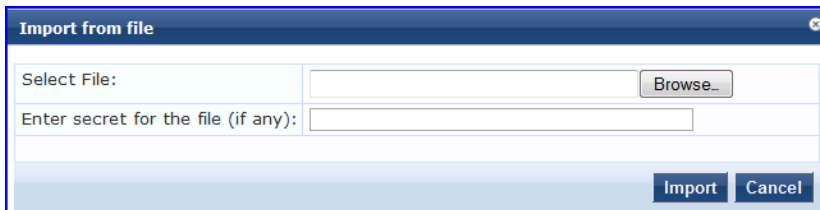
#	Name	Description	Type
1.	External Nessus Server (Sample)		NESSUS
2.	[Nessus Server]	Nessus server running in the Policy Manager server	NESSUS
3.	[Nmap Audit]	Nmap default configuration	NMAP

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 205 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 189** Upload Nessus Plugins Popup

A dialog box titled "Import from file" with a close button in the top right corner. It contains two input fields: "Select File:" with a "Browse..." button to its right, and "Enter secret for the file (if any):" with an empty text box. At the bottom right are "Import" and "Cancel" buttons.

- 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:

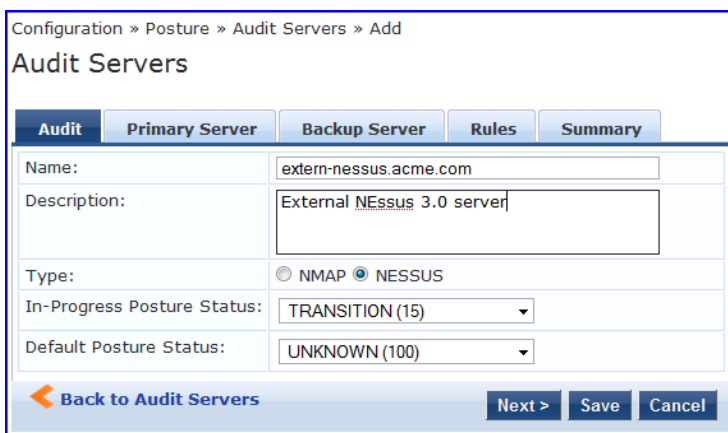
- "NESSUS Audit Server" on page 202
- "NMAP Audit Server" on page 203

## 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 190** NESSUS Audit Server (Audit Tab)

A screenshot of the "Add Audit Servers" page in the Policy Manager interface. The breadcrumb trail at the top reads "Configuration » Posture » Audit Servers » Add". The page title is "Audit Servers". Below the title are five tabs: "Audit" (selected), "Primary Server", "Backup Server", "Rules", and "Summary". The "Audit" tab contains the following fields:

- Name: A text box containing "extern-nessus.acme.com".
- Description: A text box containing "External NEssus 3.0 server".
- Type: Radio buttons for "NMAP" and "NESSUS", with "NESSUS" selected.
- In-Progress Posture Status: A dropdown menu showing "TRANSITION (15)".
- Default Posture Status: A dropdown menu showing "UNKNOWN (100)".

At the bottom of the form are three buttons: "Back to Audit Servers" (with a left arrow), "Next >" (disabled), "Save", and "Cancel".

**Table 122: 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 191 Fig: NESSUS Audit Server (Primary & Backup Tabs)**

The screenshot displays the configuration interface for the NESSUS Audit Server. It features two tabs: 'Primary Server' and 'Backup Server'. The 'Primary Server' tab is active, showing fields for 'Nessus Server Name' (extern-nessus.acme.com), 'Nessus Server Port' (1241), 'Username' (admin), 'Password' (masked), and 'Verify' (masked). It also includes a 'Scan Profile' dropdown set to 'default' with buttons for 'View Details', 'Modify', and 'Add/Edit Scan Profile'. The 'In-Progress Timeout' is set to 30 seconds. The 'Backup Server' tab is also visible, showing a checkbox for 'Enable to use backup when primary does not respond' which is checked, and similar configuration fields. At the bottom, there are navigation buttons: 'Back to Audit Servers', 'Next >', 'Save', and 'Cancel'.

**Table 123: NESSUS Audit Server - Primary and Backup Server tabs**

Parameter	Description
Server Name and Port/ Username/ Password	Standard NESSUS server configuration fields. <b>NOTE:</b> For the backup server to be invoked on primary server failover, check the <b>Enable to use backup when primary does not respond</b> check box.
Scan Profile	You can accept the default Scan Profile or select <b>Add/Edit Scan Profile</b> to create other profiles and add them to the Scan Profile list. Refer to " <a href="#">Nessus Scan Profiles</a> " on page 205.

The **Rules** tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to "[Post-Audit Rules](#)" on page 207.

## 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 192** *Audit Tab (NMAP)*

Configuration » Posture » Audit Servers » Add

### Audit Servers

**Audit** | NMAP Options | Rules | Summary

Name: Custom NMAP Profile

Description: Customized NMAP profile for custom port scans

Type: ☒ NMAP ☐ NESSUS

In-Progress Posture Status: TRANSITION (15)

Default Posture Status: UNKNOWN (100)

[Back to Audit Servers](#) [Next >](#) [Save](#) [Cancel](#)

**Table 124:** *Audit Tab (NMAP)*

Parameter	Description
Name/Description	Freeform label and description.
Type	For purposes of an NMAP-type Audit Server, always <b>NMAP</b> .
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 193** *Options Tab (NMAP)*

Configuration » Posture » Audit Servers » Add

### Audit Servers

Audit | **NMAP Options** | Rules | Summary

TCP Scan: None

UDP Scan: ☒ Enabled

Service Scan: ☒ Enabled

Detect Host Operating System: ☒ Enabled

Port Range:

Host Timeout: 30 seconds

In-Progress Timeout: 30 seconds

[Back to Audit Servers](#) [Next >](#) [Save](#) [Cancel](#)

**Table 125: Options Tab (NMAP)**

Parameter	Description
TCP Scan	To specify a TCP scan, select from the <b>TCP Scan</b> drop-down list. Refer to NMAP documentation for more information on these options. NMAP option --scanflags.
UDP Scan	To enable, check the <b>UDP Scan</b> check box. NMAP option -sU.
Service Scan	To enable, check the <b>Service Scan</b> check box. NMAP option -sV.
Detect Host Operating System	To enable, check the <b>Detect Host Operating System</b> check box. NMAP option -A.
Port Range/ Host Timeout/ In Progress Timeout	<ul style="list-style-type: none"><li>Port Range - Range of ports to scan. NMAP option -p.</li><li>Host Timeout - Give up on target host after this long. NMAP option --host-timeout</li><li>In Progress Timeout - How long to wait before polling for NMAP results.</li></ul>

The **Rules** tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to "[Post-Audit Rules](#)" on page 207.

## Nessus Scan Profiles

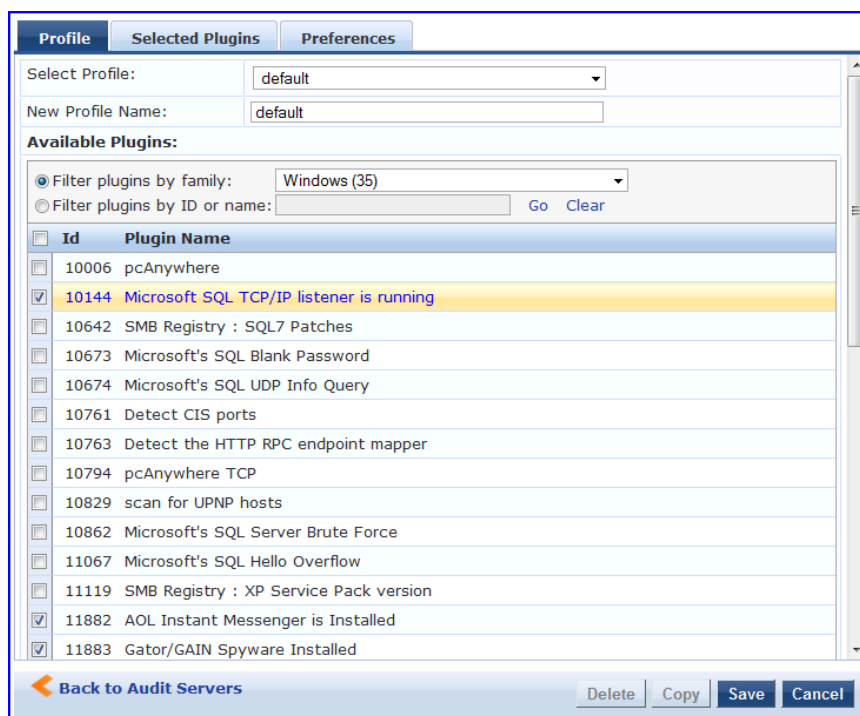
A scan profile contains a set of scripts (plugins) that perform specific audit functions. To Add/Edit Scan Profiles, select **Add/Edit Scan Profile** (link) from the **Primary Server** tab of the Nessus Audit Server configuration. The **Nessus Scan Profile Configuration** page displays.

**Figure 194** 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:

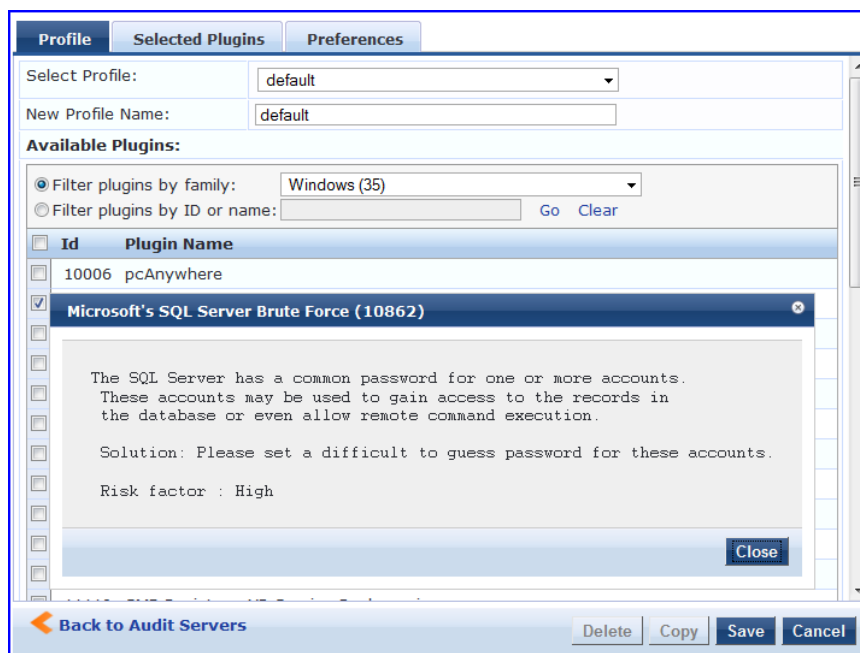
- The **Profile** tab identifies the profile and provides a mechanism for selection of plugins:
  - From the **Filter plugins by family** drop-down list, select a family to display all available member plugins in the list below. You may also enter the name of a plugin in **Filter plugins by ID** or name 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 195** Nessus Scan Profile Configuration (Profile Tab)



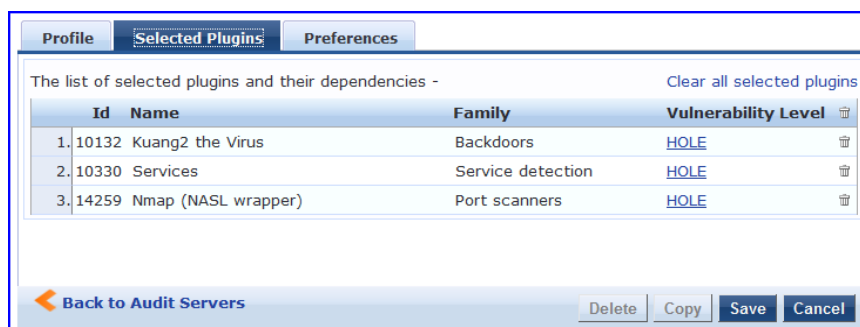
- The **Selected Plugins** tab displays all selected plugins, plus any dependencies. To display a synopsis of any listed plugin, click on its row.

**Figure 196** Nessus Scan Profile Configuration (Profile Tab) - Plugin Synopsis

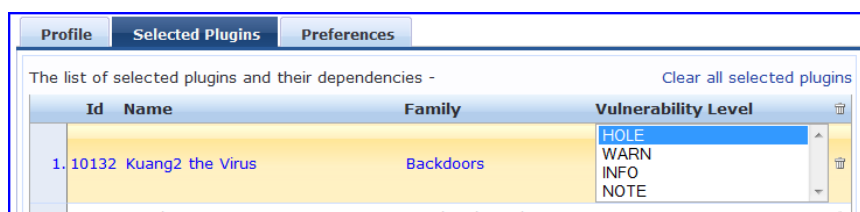


Of special interest is the section of the synopsis entitled **Risks**. To delete any listed plugin, click on its corresponding trashcan icon. To change the vulnerability level of any listed plugin click on the link to change the level to one of HOLE, WARN, INFO, NOTE. This tells Policy Manager the vulnerability level that is considered to be assigned QUARANTINE status.

**Figure 197** Nessus Scan Profile Configuration (Selected Plugins Tab)



**Figure 198** Nessus Scan Profile Configuration (Selected Plugins Tab) - Vulnerability Level

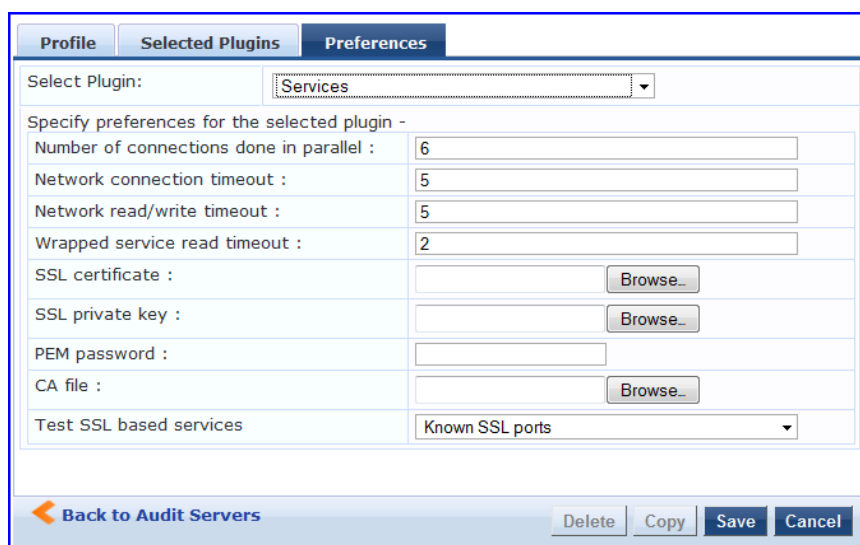


For each selected plugin, the Preferences tab contains a list of fields that require entries.

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 199** 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 200** All Audit Server Configurations (Rules Tab)

Rules Evaluation Algorithm: ☐ Select first match ☒ Select all matches

Post-Audit Rules:

Conditions	Role Name
<input type="button" value="Add Rule"/>	<input type="button" value="Move Up"/> <input type="button" value="Move Down"/>
<input type="button" value="Edit Rule"/>	<input type="button" value="Remove Rule"/>

**Table 126:** All Audit Server Configurations (Rules Tab)

Parameter	Description
Rules Evaluation Algorithm	<b>Select first matched</b> rule and return the role or <b>Select all matched</b> rules and return a set of roles.
Add Rule	Add a rule. Brings up the rules editor. See below.
Move Up/Down	Reorder the rules.
Edit Rule	Brings up the selected rule in edit mode.
Remove Rule	Remove the selected rule.

**Figure 201** All Audit Server Configurations (Rules Editor)

Rules Editor

Conditions

Matches ☒ ANY or ☐ ALL of the following conditions:

Name	Operator	Value
1. OS-Info	CONTAINS	Linux
2. <input type="text"/>		
3. <input type="text"/>		

Audit-Status  
Device-Type  
Output-Msgs  
Network-Apps  
Mac-Vendor  
OS-Info  
Open-Ports

Actions

**Table 127:** All Audit Server Configurations (Rules Editor)

Parameter	Description
Conditions	The <b>Conditions</b> list includes five dictionaries: Audit-Status, Device-Type, Output-Msgs, Mac-Vendor, Network-Apps, Open-Ports, and OS-Info.. Refer to <a href="#">"Namespaces" on page 329</a> .
Actions	The <b>Actions</b> list includes the names of the roles configured in Policy Manager.
Save	To commit a Condition/Action pairing, click <b>Save</b> .

Policy Manager controls network access by sending a set of access-control attributes to the request-originating Network Access Device (NAD).

Policy Manager sends these attributes by evaluating an *Enforcement Policy* associated with the service. The evaluation of Enforcement Policy results in one or more *Enforcement Profiles*; each Enforcement Profile wraps the access control attributes sent to the Network Access Device. For example, for RADIUS requests, commonly used Enforcement Profiles include attributes for VLAN, Filter ID, Downloadable ACL and Proxy ACL.

## 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.

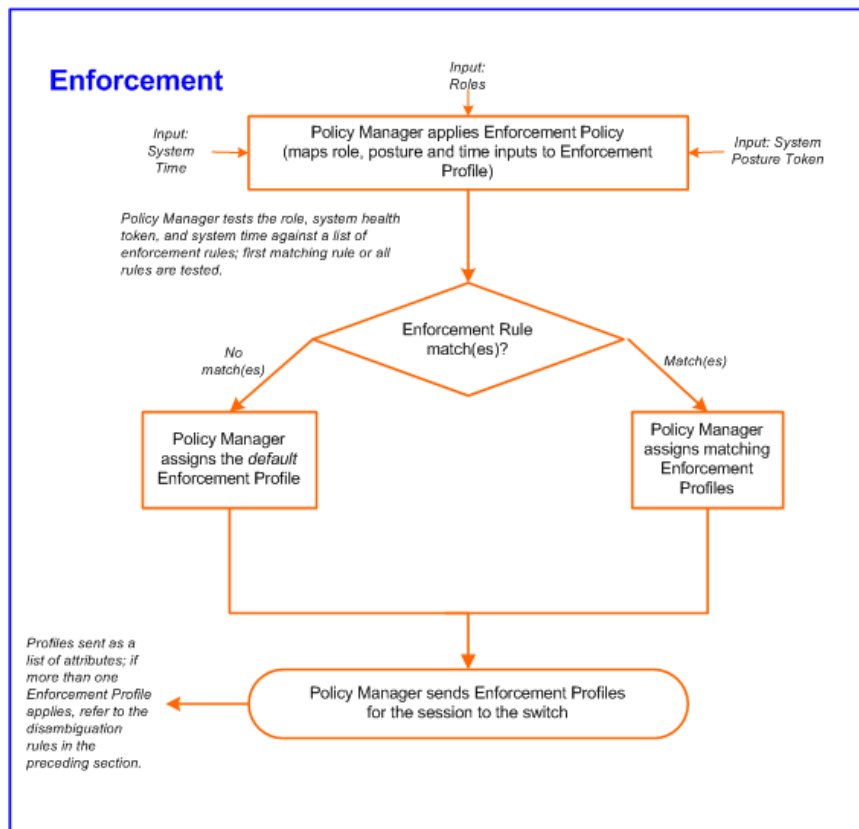


---

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 202** *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 203** *Enforcement Profiles Page*

Configuration > Enforcement > Profiles

Enforcement Profiles

[Add Enforcement Profile](#)  
[Import Enforcement Profiles](#)  
[Export Enforcement Profiles](#)

Filter: Type contains Go Clear Filter

Show 10 records

#	Name	Type	Description
1.	Access Switches Control	TACACS	TACACS+ Enforcement Profile for Access Switches
2.	AirGroup Device Owner	RADIUS	RADIUS attributes returned for all valid AirGroup requests
3.	AirGroup Location Sharing	RADIUS	RADIUS attributes returned for devices shared by location name
4.	AirGroup Response	RADIUS	RADIUS attributes returned for empty AirGroup responses
5.	AirGroup Role Sharing	RADIUS	RADIUS attributes returned for devices shared by role name
6.	AirGroup User Sharing	RADIUS	RADIUS attributes returned for devices shared with other users
7.	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
8.	Allow All Commands	TACACS	Allow all commands on the device
9.	ArubaGuest	RADIUS	
10.	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)

Showing 1-10 of 68 records

Copy Export Delete

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 - Reauthenticate-Session]** - Trigger a session reauthentication on a Cisco device.
  - **[HP - Terminate Session]** - Terminate a session on an HP device.
  - **[Aruba - Terminate Session]** - Terminate a session on an Aruba 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 204** Add Enforcement Profile Page

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Aruba RADIUS Enforcement	
Description:	Aruba Downloadable Role Enforcement	
Type:	VLAN Enforcement	
Action:	Filter ID Based Enforcement	
Device Group List:	RADIUS Based Enforcement	
	RADIUS Change of Authorization (CoA)	
	Agent Enforcement	
	SNMP Based Enforcement	
	CLI Based Enforcement	
	TACACS+ Based Enforcement	
	Cisco Downloadable ACL Enforcement	
	Cisco Web Authentication Enforcement	
	ClearPass Insight Enforcement	
	Generic Application Enforcement	
	ClearPass Entity Update Enforcement	
	Session Restrictions Enforcement	

Remove View Details Modify

[Add new Device Group](#)

[Back to Enforcement Profiles](#) [Next >](#) [Save](#) [Cancel](#)

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

- **VLAN Enforcement** - All RADIUS attributes for VLAN enforcement are pre-filled in this template.
- **Aruba RADIUS Enforcement** - RADIUS template that can be filled with attributes from the Aruba RADIUS dictionaries loaded into Policy Manager.

- Aruba 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 template 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.
- Aruba GuestConnect Enforcement - Application specific enforcement profile with pre-loaded attributes for authorization of GuestConnect users.
- Aruba 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 Aruba 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 128:** *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.
Device Group List	Associate the profile with pre-configured Device Groups. <ul style="list-style-type: none"> <li>• <b>Add New Device Group</b> to add a new device group.</li> <li>• <b>Add</b> to add a device group from this drop-down list.</li> <li>• <b>Remove, View Details, Modify</b> to remove, view the details of, or modify the selected enforcement profile, respectively</li> </ul> <b>NOTE:</b> 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 213
- "RADIUS CoA Enforcement Profiles" on page 215
- "SNMP Enforcement Profiles " on page 216
- "TACACS+ Enforcement Profiles " on page 216
- "Application Enforcement Profiles " on page 218
- "CLI Enforcement Profile " on page 219
- "Agent Enforcement Profiles " on page 219
- 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** - Aruba Downloadable Role Enforcement

**Figure 205** *RADIUS Enforcement Profile (Attributes Tab)*

The screenshot displays the 'Attributes' tab of a RADIUS Enforcement Profile configuration. It shows four distinct rule sets, each with a table of attributes and their values. The rules are labeled A, B, C, and D on the right side of the image.

**Rule A (VLAN Enforcement):**

Type	Name	Value
1. Radius:IETF	Session-Timeout	= 3600
2. Radius:IETF	Termination-Action	= RADIUS-Request (1)
3. Radius:IETF	Tunnel-Type	= VLAN (13)
4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5. Radius:IETF	Tunnel-Private-Group-Id	= Enter VLAN
6.	Click to add...	

**Rule B (Filter ID Based Enforcement):**

Type	Name	Value
1. Radius:IETF	Filter-Id	= Enter Filter Name
2.	Click to add...	

**Rule C (Cisco Downloadable ACL Enforcement):**

Type	Name	Value
1. Radius:Cisco	Cisco-IP-Downloadable-	= permit ip any any
2.	Click to add...	

**Rule D (Cisco We Authentication Enforcement):**

Type	Name	Value
1. Radius:Cisco	Cisco-AVPair	= priv-lvl=15
2. Radius:Cisco	Cisco-AVPair	= proxyacl# 10=permit ip any any
3.	Click to add...	

At the bottom of the configuration window, there are buttons for 'Back to Enforcement Profiles', 'Next >', 'Save', and 'Cancel'.

**Figure 206** RADIUS Enforcement Profile (Attributes Tab) - Generic RADIUS Enforcement Profile

Type	Name	Value
Radius:IETF	User-Name	%(Authorization:Avenda AD:countryCode) %(Authorization:Avenda AD:department) %(Authorization:Avenda AD:distinguishedName) %(Authorization:Avenda AD:memberOf) %(Authorization:Avenda AD:msNPAllowDialin) %(Authorization:Avenda AD:name) %(Authorization:Avenda AD:title) %(Authorization:Test RSA Token Server:IETF.Class) %(Authorization:Test RSA Token Server:IETF.Service-Type)
2. Click to add...		

Back to Enforcement Profiles    Next >    Save    Cancel

**Figure 207** Aruba Downloadable Role Enforcement

Type	Name	Value
Radius:Aruba	Aruba-CPPM-Role	ip access-list stateless denying any any svc-icmp deny ! user-role cppm1 access-list stateless denying !
2. Click to add...		

Back to Enforcement Profiles    Next >    Save    Cancel

**Table 129:** RADIUS Enforcement Profile (Attributes tab)

Enforcement Profile Template	Description
<b>A</b> —VLAN Enforcement	Enforcement profile template to set IETF RADIUS standard VLAN attributes.
<b>B</b> —Filter ID Based Enforcement	Enforcement profile template to set IETF RADIUS standard filter ID attribute.
<b>C</b> —Cisco Downloadable ACL Enforcement	Enforcement profile template for Cisco IOS downloadable ACLs.

Enforcement Profile Template	Description
<b>D</b> —Cisco Web Authentication Enforcement	Enforcement profile template to set Cisco Web Authentication ACLs.
<b>E</b> —(Generic) RADIUS-Based Authentication	<p><b>Type</b> 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.</p> <p><b>Name</b> is the name of the attribute from the dictionary selected in the Type field. The attribute names are prepopulated from the dictionary.</p> <p><b>Value</b> is the value of the attribute. If the value has prepopulated values in the dictionary, these appear in a drop-down list. Otherwise, you can enter freeform text.</p> <p>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).</p> <p>For example, to set the name of the VLAN to the name of the role, enter <code>%{Tips:Role}</code> as the value for <code>RADIUS:IETF:Tunnel-Private-Group-Id</code>. These dynamic values must be entered in the following format, without any spaces: <code>%{namespace:attribute-name}</code>.</p> <p>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.</p>
<b>F</b> —Aruba Downloadable Role Enforcement	<p>Enforcement profile template for ClearPass Policy Manager to create user roles at the time of user authentication.</p> <p><b>Type</b> is Aruba RADIUS dictionary.</p> <p><b>Name</b> is the Aruba downloadable role.</p> <p><b>Value</b> is attribute for the downloadable role. You can enter freeform text to define the role and policy.</p> <p>For more information on defining roles and policies, refer to Aruba OS7.X User Guide. The following is an example of an Aruba downloadable role:</p> <pre>ip access-list stateless denying any any svc-icmp deny user-role cppm1 access-list stateless denying</pre>

## 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	<p>The supported template types are:</p> <ul style="list-style-type: none"> <li>• Cisco - Disable-Host-Port</li> <li>• Cisco - Bounce-Host-Port</li> <li>• Cisco - Reauthenticate-Session</li> <li>• HP - Change-VLAN</li> <li>• HP - Generic-CoA</li> </ul>
Attributes	<p>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.</p>

## SNMP Enforcement Profiles

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

**Figure 208** *Fig: SNMP Enforcement Profile (SNMP Tab)*

Attribute Name	Attribute Value
1. VLAN ID	= 150
2. Session Timeout (in seconds)	= 3600
3. <input type="text" value="VLAN ID"/>	

[Back to Enforcement Profiles](#) [Next >](#) [Save](#) [Cancel](#)

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

**Table 130:** *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 209** TACACS+ Enforcement Profiles (Services Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

Profile Services Commands Summary

Privilege Level: 15 (Privileged)

Selected Services:

Shell

Remove

--Select--

Add

--Select--

PIX Shell

PPP:IP

PPP:IPX

PPP:LCP

ARAP

eTIPS:HTTP

Service Attributes

Type	Name	=	Value	
1. Shell	priv_lvl	=	15	
2. Shell	timeout	=	180	
3. Shell				
4. Shell				

Back to Enforcement Profiles

Next > Save Cancel

**Table 131:** TACACS+ Enforcement Profile (Services tab)

Container	Description
Privilege Level	Enter a value, from 0 to 15. <b>NOTE:</b> Refer to your network device documentation for definitions of the different privilege levels.
Selected Services	To add supported services, click <b>Add</b> . To remove a service, select it and click <b>Remove</b> . 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 attributes (which are automatically populated by Policy Manager in a drop down list in the <b>Name</b> field). You can also add custom attributes in the Name field. Add service attributes corresponding to the services selected in <b>Selected Services</b> . 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 210** TACACS+ Enforcement Profiles (Commands tab)

The screenshot shows the 'Commands' tab of the TACACS+ Enforcement Profiles configuration. At the top, there are tabs for 'Summary', 'Profile', 'Services', and 'Commands'. Below the tabs, the 'Service Type' is set to 'Shell'. The 'Unmatched Commands' section has a checkbox 'Enable to permit unmatched commands' which is checked. The main area is a table titled 'Commands' with columns: 'Command', 'Arguments', 'Permit Action', and 'Unmatched Arguments'. There are two rows: 1. 'show' with argument 'vlan' and action 'Deny'; 2. 'show' with argument 'interface' and action 'Deny'. A 'Configure Tacacs Command Authorization' popup is open, showing a 'Shell Command' field with 'interface' entered. Below it is a table with 'Command Arguments' and 'Action'. The first row is 'vlan' with action 'Deny'. The second row is 'Click to add...'. At the bottom of the popup, 'Unmatched Arguments' is set to 'Permit'.

**Table 132:** Commands tab (TACACS+ Enforcement Profiles)

Container	Description
Service Type	Select <b>Shell</b> or <b>PIX shell</b> 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 <b>Commands</b> field.
Commands	<p>Contains a list of the commands recognized for the specified <b>Service Type</b>: To add a command, click <b>Add</b>. In the <b>Configure Tacacs Command Authorization</b> popup, enter values for:</p> <ul style="list-style-type: none"> <li>• <b>Command</b>. A string for the command. This is followed by one or more command argument rows.</li> <li>• <b>Command Arguments</b>. The arguments for the command.</li> <li>• <b>Action</b>. Click on <b>Enable to permit</b> check box to permit use of this command argument. If this box is unchecked the column shows <b>Deny</b> and the command argument is not allowed.</li> <li>• Click <b>Trashcan</b> to delete the command argument.</li> <li>• <b>Unmatched Arguments</b>. Select <b>Permit</b> radio button to permit this command even if Policy Manager receives arguments for the command that it does not recognize. Select <b>Deny</b> radio button to deny the command if Policy Manager receives unrecognized arguments.</li> </ul> <p>To save and exit, click outside the row you are editing. To delete a command, click the <b>Trashcan</b> icon for that row.</p>

## Application Enforcement Profiles

Application Enforcement Profiles contain attribute-value pairs and other permissions related to authorization of users of Aruba Applications - GuestConnect 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 211** Application Enforcement Profiles (Attributes Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Attribute Name	Attribute Value
1. Privilege-Level	= Sponsor
2. Sponsor-Profile-Name	= Enter Profile Name
3. Privilege-Level	= Sponsor-Profile-Name

**Table 133:** Application Enforcement Profiles (Attributes tab)

Container	Description
Privilege-Level	Enter a predefined value: <b>Admin</b> , <b>Sponsor</b> , <b>Helpdesk</b> ; or enter an application-specific custom value. <b>NOTE:</b> Sponsor is only valid for the GuestConnect application
Sponsor-Profile-Name	Valid only for GuestConnect application. This is the (case-sensitive) name of the sponsor profile defined in the GuestConnect 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 212** CLI Enforcement Profile (Attributes Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Attribute Name	Attribute Value
1. Target Device	= %{Connection:NAD-IP-Address}
2. Command	= Enter Command
3. Click to add...	

**Table 134:** 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 Aruba OnGuard Agent.

**Figure 213** Agent Enforcement Profile (Attributes Tab)

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Attribute Name	Attribute Value
1. Bounce Client	= false
2. Message	= Enter message here
3. Click to add...	

**Table 135:** 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 reauthentication 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 214** Post Authentication Enforcement Profiles

This figure illustrates rules for the two sample profiles:

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

Profile Attributes Summary

**A**

Type	Name	Value
1. Endpoint	Device Type	= Dell
2. Status-Update	GuestUser	= Enabled
3. Click to add...		

**B**

Type	Name	Value
1. Bandwidth-Check	Start-Date	= 2012-10-10
2. Bandwidth-Check	Stop-Date	= 2012-10-11
3. Post-Auth-Check	Action	= Disconnect
4. Click to add...		

**Table 136:** Post Authentication Enforcement Profiles

Enforcement Profile Template	Description
<b>A</b> — ClearPassEntity Update Enforcement	Enforcement profile template used to update tags in endpoints and guest users. <b>Type</b> is any endpoint, guest user, or a session update. <b>Name</b> 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.

Enforcement Profile Template	Description
	<b>Value</b> is the value of the attribute.
<b>B</b> —Session Restrictions Enforcement	<p>Enforcement profile template used to restrict users based on bandwidth usage and also disconnect users when the specified limits are crossed.</p> <p><b>Type</b> is any post authentication check or session check that is applicable to the user.</p> <p><b>Name</b> is the name of any specific check related the selected <b>Type</b>.</p> <p><b>Value</b> is the value of the attribute.</p> <p>For example, if <b>Bandwidth-Check</b> is selected as the <b>Type</b>, you can select <b>Start-Date</b> from the <b>Name</b> drop-down list, and specify the start date in the <b>Value</b> field.</p>

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 215** *Enforcement Policies Listing Page*

Configuration > Enforcement > Policies  
Enforcement Policies

[Add Enforcement Policy](#)  
[Import Enforcement Policies](#)  
[Export Enforcement Policies](#)

Filter: Name contains    Show 10 records

#	Name ▲	Type	Description
1.	<input type="checkbox"/> [Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin
2.	<input type="checkbox"/> [AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	<input type="checkbox"/> [Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device
4.	<input type="checkbox"/> Guest - MAC Caching - Limit 1 Device	RADIUS	Limits guests to maximum 1 device for MAC caching purposes
5.	<input type="checkbox"/> Guest - MAC Caching - Limit 2 Devices	RADIUS	Limits guests to maximum 2 devices for MAC caching purposes
6.	<input type="checkbox"/> Guest Operator Logins	Application	Enforcement policy controlling access to Guest application
7.	<input type="checkbox"/> [MAC Caching - 24 Hours]	RADIUS	Sample policy for MAC caching specifying a 24 hour lifetime
8.	<input type="checkbox"/> [MAC Caching - 5 Days]	RADIUS	Sample policy for MAC caching specifying a 5 day lifetime
9.	<input type="checkbox"/> [MAC Caching - 8 Hours]	RADIUS	Sample policy for MAC caching specifying a 8 hour lifetime
10.	<input type="checkbox"/> [MAC Caching By Role]	RADIUS	Sample policy for MAC caching specifying a lifetime depending on role

Showing 1-10 of 15

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

**Figure 216** Add Enforcement Policy (Enforcement tab)

Configuration » Enforcement » Policies » Add

### Enforcement Policies

Enforcement

Rules

Summary

Name:

Employee Access Enforcement

Description:

Enforcement policy for employee access

Type:

☒ RADIUS
 ☐ TACACS+
 ☐ WEBAUTH (SNMP/CLI)
 ☐ Application

Default Profile:

--Select--

View Details

Modify

Add new Enforcement Profile

Back to Enforcement Policies

Next >

Save

Cancel

**Table 137:** Add Enforcement Policy (Enforcement tab)

Parameter	Description
Name/Description	Freeform label and description.
Type	Select: <b>RADIUS</b> , <b>TACACS+</b> , <b>WebAuth (SNMP/CLI)</b> or <b>Application</b> . 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 Aruba 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 <b>Add new Enforcement Profile</b> 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 217** Add Enforcement Policy (Rules Tab)

Enforcement

Rules

Summary

Rules Evaluation Algorithm:

☐ Select first match
 ☒ Select all matches

Enforcement Policy Rules:

Conditions	Actions
1. (Tips:Role MATCHES_ANY Role_Engineer Senior_Mgmt)	EMPLOYEE_VLAN
2. (Tips:Role EQUALS eTIPS_Guest) AND (Tips:Posture EQUALS HEALTHY (0))	INTERNET_VLAN

Add Rule

Move Up

Move Down

Edit Rule

Remove Rule

Back to Enforcement Policies

Next >

Save

Cancel

**Figure 218** Add Enforcement Policy (Rules Editor)

**Rules Editor**

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	Posture	EQUALS	HEALTHY (0)
2.	Tips	Role	MATCHES_ANY	Remote Worker role_engineer testqa
3.				
4.	Date			

Enforcement Profiles

Profile Names:

- EMPLOYEE\_VLAN
- Remote Employee ACL

--Select--

Move Up  
Move Down  
Remove  
Add

Save Cancel

**Table 138:** 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 139:** Add Enforcement Policy (Rules Editor)

Field	Description
Conditions/Enforcement Profiles	<p>Select conditions for this rule. For each condition, select a matching action (Enforcement Profile).</p> <p><b>NOTE:</b> A condition in an Enforcement Policy rule can contain attributes from the following namespaces: Tips:Role, Tips:Posture, and Date.</p> <p><b>NOTE:</b> 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 <b>Save</b>.</p>
Enforcement Profiles	<p>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.</p>



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 225
- "Adding and Modifying Device Groups " on page 229
- "Adding and Modifying Proxy Targets " on page 231

## 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 219** *Network Devices page*

#	Name	IP or Subnet Address	Description
1.	Aruba Controller 1	192.168.5.68	
2.	Aruba Controller Building 1341	10.6.2.252	
3.	Aruba Controller Building 1341-2	10.6.2.241	

## 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 220** *Device tab*

Attribute	Value
1. Location	= Building 1
2. Device Type	= iOS 12.2
Device Vendor	
OS Version	
Location	
Controller Id	

**Table 140: 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	<p>Optionally, specify the dictionary to be loaded for this device.</p> <p><b>NOTE:</b> RADIUS:IETF, the dictionary containing standard the set of RADIUS attributes, is always loaded.</p> <p>When you specify a vendor here, the RADIUS dictionary associated with this vendor is automatically enabled.</p>
Enable RADIUS CoA RADIUS CoA Port	<p>Enable RADIUS Change of Authorization (RFC 3576/5176) for this device.</p> <p>Set the UDP port on the device to send CoA actions. Default value is 3799.</p>
Attributes	<p>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.</p> <p><b>NOTE:</b> All attributes entered for a device are available in the role mapping rules editor under the Device namespace.</p>
Add/Cancel	Click Add to commit or Cancel to dismiss the popup.

**Figure 221** SNMP Read/Write Settings tabs

**Figure 222** SNMP Read/Write Settings tabs - SNMP v3 Details

**Table 141: 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: <ul style="list-style-type: none"> <li>• DES-CBC</li> <li>• AES-128</li> </ul>
Add/Cancel	Click <b>Add</b> to commit or <b>Cancel</b> 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 223** CLI Settings tab

**Table 142:** 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 <b>Add</b> to commit or <b>Cancel</b> 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 224** *Device Groups Page*

Configuration > Network > Device Groups

Network Device Groups

☐ Select ALL matches
 ☒ Select ANY match

Filter: Name 
 Filter: Name 
 Filter: Format 
 Filter: Format 
 Filter: Name 


 Show 10 records

#	<input type="checkbox"/>	Name ▲	Format	Description
1.	<input type="checkbox"/>	ArubaControllers	List	All Aruba Controllers
2.	<input type="checkbox"/>	Bangalore Devices	Subnet	Devices in Bangalore
3.	<input type="checkbox"/>	Remote Bangalore	Subnet	Remote Bangalore Devices
4.	<input type="checkbox"/>	Remote San Jose	Subnet	San Jose VPN Devices
5.	<input type="checkbox"/>	San Jose Devices	List	San Jose Switches

Showing 1-5 of 5

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

**Figure 225** Add New Device Group Popup

The figure shows three overlapping screenshots of the 'Add New Device Group' popup, illustrating different configuration options for the 'Format' field.

- Top Screenshot:** The 'Format' field is set to 'Subnet'. The 'Subnet' field contains the example '192.168.1.1/24'.
- Middle Screenshot:** The 'Format' field is set to 'Regular Expression'. The 'Regular Expression' field contains the example '^192([0-9]\*){3}\$'.
- Bottom Screenshot:** The 'Format' field is set to 'List'. It shows two lists: 'Available Devices' (containing IP addresses like 192.168.150.204) and 'Selected Devices' (empty). Arrows allow moving items between the lists. A 'Filter' box is present for each list.

Each screenshot also shows the 'Name' and 'Description' fields, which are filled with test data like 'TestDevice Group' and 'This is a test device group'.

**Table 143:** 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 <b>Filter</b> to filter the list based on the text in the associated text box.
Save/Cancel	Click <b>Save</b> to commit or <b>Cancel</b> to dismiss the popup.



For SNMP enforcement on the network device, one or more of the following traps have to be configured on the device: Link Up trap, Link Down trap, MAC Notification trap. In addition, one or more of the following SNMP MIBs must be supported by the device: RFC-1213 MIB, IF-MIB, BRIDGE-MIB, ENTITY-MIB, Q-BRIDGE-MIB, CISCO-VLAN-MEMBERSHIP-MIB, CISCO-STACK-MIB, CISCO-MAC-NOTIFICATION-MIB.

These traps and MIBs enable Policy Manager to correlate the MAC address, IP address, switch port, and switch information.

## Additional Available Tasks

- To import a Device Group, click **Import 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" on page 80.](#))

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

**Figure 226** Proxy Targets Page

Configuration > Network > Proxy Targets

Proxy Targets

Filter: Name contains Go Clear Filter Show 10 records

#	Name	Hostname	Description
1.	SJ Branch Office Proxy	acme.com	SJ branch office

Showing 1-1 of 1

Export Delete

## 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 227** Add Proxy Target Popup

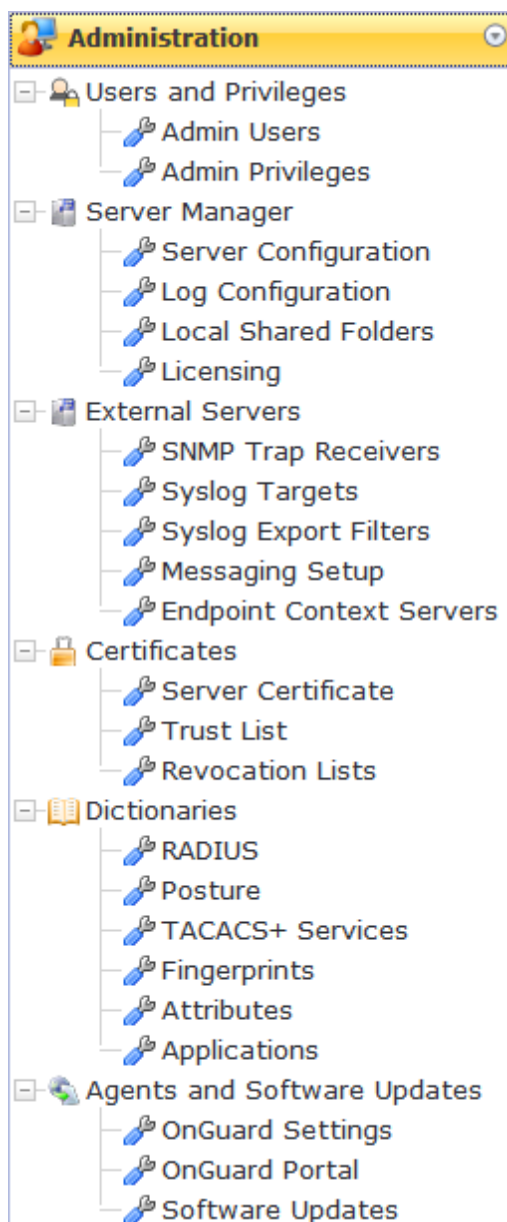
**Table 144:** *Add Proxy Target popup*

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 " on page 233
- "Admin Privileges " on page 236
- "Server Configuration" on page 240
- "Log Configuration " on page 268
- "Local Shared Folders " on page 270
- "Application Licensing " on page 271
- "SNMP Trap Receivers " on page 273
- "Syslog Targets " on page 275
- "Syslog Export Filters " on page 277
- "Server Certificate " on page 284
- "Messaging Setup " on page 281
- "Endpoint Context Servers" on page 282
- "Certificate Trust List " on page 289
- "Revocation Lists " on page 290
- "RADIUS Dictionaries " on page 291
- "Posture Dictionaries " on page 292
- "TACACS+ Services " on page 293
- "Fingerprints " on page 294
- "Attributes " on page 295
- "Application Dictionaries" on page 298
- "OnGuard Settings " on page 298
- "OnGuard Portal " on page 300
- "Update Portal " on page 302

## Admin Users

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

- "Add User" on page 234

- "Import Users " on page 235
- "Export Users " on page 235
- "Export " on page 235

**Figure 228** Admin Users

#	User ID	Name	Privilege Level
1.	admin	Super Admin	Super Administrator
2.	apiadmin	API Access	Super Administrator
3.	ashwath	ashwath	Super Administrator
4.	bh prasad	Bhagya Prasad NR	Super Administrator
5.	carlos	Carlos Gomez Gallego	Super Administrator
6.	cesdale	Cameron Esdaile	Super Administrator
7.	choppe	Carlen Hoppe	Super Administrator
8.	david	David Hamel	Super Administrator
9.	frontdesk	frontdesk	Receptionist
10.	helpdesk	Helpdesk	Help Desk

**Table 145:** Admin Users

Container	Description
Add User	Opens the <b>Add User</b> popup form.
Import Users	Opens the <b>Import Users</b> 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 229** Add Admin User

**Add Admin User**

User ID:

Name:

Password:

Verify Password:

Privilege Level: 

- Super Administrator
- Super Administrator
- Network Administrator
- Help Desk
- Receptionist

**Table 146:** *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 <ul style="list-style-type: none"> <li>• Super Administrator</li> <li>• Network Administrator</li> <li>• Receptionist</li> </ul> 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 230** *Import (Admin) Users*
**Table 147:** *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

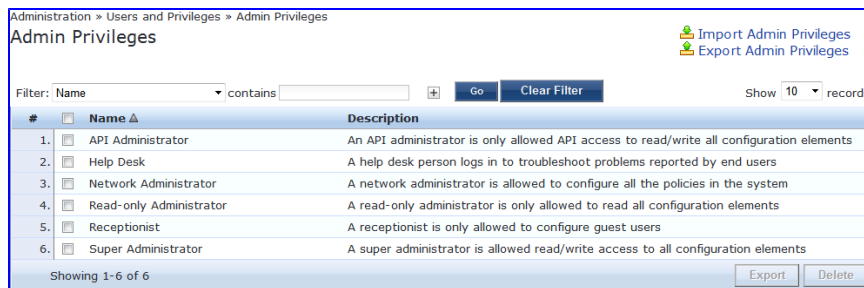
Select the **Export** button on the lower right portion of the page.

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 231** *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 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 place 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 Trending: taskId="mon.li.sp"
    - Endpoint Profiles: taskId="mon.li.ep"
    - System Monitor: taskId="mon.li.sy"
  - Audit Viewer: taskId="mon.av"
  - Event Viewer: taskId="mon.ev"
  - Data Filters: taskId="mon.df"
- Configuration: taskId="con"
  - Start Here (Services Wizard): taskId="con.sh"
  - Services: taskId="con.se"
  - Service Templates: taskId="con.st"
  - Authentication: taskId="con.au"
    - Methods: taskId="con.au.am"
    - Sources: taskId="con.au.as"
  - Identity: taskId="con.id"
    - Single Sign-On: taskId="con.id.sso"
    - Local Users: taskId="con.id.lu"
    - Guest Users: taskId="con.id.gu"
    - Onboard Devices: taskId="con.id.od"
    - Endpoints: taskId="con.id.ep"
    - Static Host Lists: taskId="con.id.sh"

- Roles: taskId="con.id.rs"
- Role Mappings: taskId="con.id.rm"
- Posture: taskId="con.pv"
  - Posture Policies: taskId="con.pv.in"
  - Posture Servers: taskId="con.pv.ex"
  - Audit Servers: taskId="con.pv.au"
- Enforcements: taskId="con.en"
  - Policies: taskId="con.en.epo"
  - Profiles: taskId="con.en.epr"
- Network: taskId="con.nw"
  - Devices: taskId="con.nw.nd"
  - Device Groups: taskId="con.nw.ng"
  - Proxy Targets: taskId="con.nw.pr"
- Policy Simulation: taskId="con.ps"
- Profile Settings: taskId="con.prs"
- Administration: taskId="adm"
  - User and Privileges: taskId="adm.us"
    - Admin Users: taskId="adm.us.au"
    - Admin Privileges: taskId="adm.us.ap"
  - Server Manager: taskId="adm.mg"
    - Server Configuration: taskId="adm.mg.sc"
    - Log Configuration: taskId="adm.mg.ls"
    - Local Shared Folders: taskId="adm.mg.sf"
    - Licensing: taskId="adm.mg.sf"
  - External Servers: taskId="adm.xs"
    - SNMP Trap Receivers: taskId="adm.xs.st"
    - Syslog Targets: taskId="adm.xs.es"
    - Syslog Export Filters: taskId="adm.xs.sx"
    - Messaging Setup: taskId="adm.xs.me"
  - Certificates: taskId="adm.cm"
    - Server Certificate: taskId="adm.cm.mc"
    - Trust List: taskId="adm.cmctl"
    - 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>

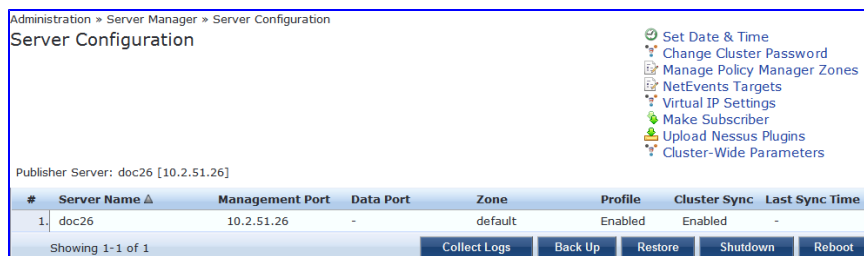
```

## Server Configuration

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

- "Set Date/Time " on page 241
- "Change Cluster Password " on page 242
- "Manage Policy Manager Zones " on page 243
- "NetEvents Targets" on page 244
- "Virtual IP Settings" on page 244
- "Make Subscriber " on page 245
- "Upload Nessus Plugins " on page 246
- "Cluster-Wide Parameters " on page 246
- "Collect Logs " on page 250
- "Backup " on page 252
- "Restore" on page 253
- "Shutdown/Reboot " on page 254
- "Drop Subscriber " on page 254

**Figure 232** *Server Configuration*



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

- "System Tab " on page 254
- "Services Control Tab " on page 257
- "Service Parameters Tab " on page 257
- "System Monitoring Tab " on page 264
- "Network Tab" on page 266

## 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 233** *Change Date and Time - Date & Time tab*

**Change Date and Time**

This will change Date & Time for all nodes in the cluster

**Date & Time** | Time zone on publisher

☐ Synchronize time with NTP server

**Date**  
Use yyyy-mm-dd  
2012-09-28

**Time**  
Hour: 14 Minute: 50 Second: 16

**Date & Time** | Time zone on publisher

☒ Synchronize time with NTP server

NTP server (primary): time.nist.gov

NTP server (secondary):

**WARNING:** After command execution Policy Manager services need to be restarted. This may take a while.

Save Cancel

**Table 148:** *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**. Note that 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 234** Time zone on publisher

**Change Date and Time**

This will change Date & Time for all nodes in the cluster

**Date & Time** | **Time zone on publisher**

To change the time zone, select your area from the list below

- Africa/Abidjan
- Africa/Accra
- Africa/Addis\_Ababa
- Africa/Algiers
- Africa/Asmara
- Africa/Bamako
- Africa/Bangui
- Africa/Banjul
- Africa/Bissau
- Africa/Blantyre

Current time zone: Etc/UTC(GMT 0:00)

**WARNING:** After command execution Policy Manager services need to be restarted. This may take a while.

**Save** **Cancel**

## 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 235** Change Cluster Password

**Change Cluster Password**

This will change Cluster Password for all nodes in the cluster

New Password

Verify Password

**Save** **Cancel**

**Table 149:** *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:

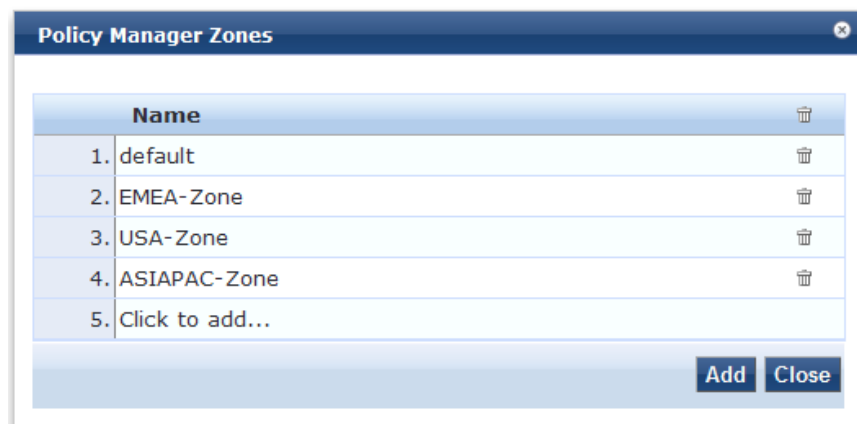
- Roles and Postures of connected entities
- Connection status of all endpoints running OnGuard
- Endpoint details gathered by

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 236** *Policy Manager Zones***Table 150:** *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 237** *NetEvents Targets*

NetEvents Targets

External targets can be configured to which ClearPass NetEvents will be sent periodically

Target URL	Username
No external targets have been configured.	

NetEvent Target Details -

Target URL:

Username:

Password:  Verify Password:

Note: For an external Insight server, you may input https://<Insight-server-IP>/insight/netevents in Target URL

**Table 151:** *NetEvents targets*

Parameter	Description
Target URL	HTTP URL for the service that support POST and requires Authentication using Username / Password. <b>NOTE:</b> For an external Insight server, you may input https://<Insight-server-IP>/insight/netevents in Target URL
Username	Credentials configured for authentication for the HTTP service that is provided in the Target URL.
Password	
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. Once the primary node becomes available again, the Virtual IP address is released to the primary.

**Figure 238** *Virtual IP Settings*

Virtual IP Settings

Configure Virtual IPs for ClearPass High Availability

Virtual IP	Primary Node	Secondary Node	Status
No Virtual IP have been configured			

Virtual IP Details -

Virtual IP:

Node:  Interface:  Subnet:

Primary Node:  Secondary Node:

Enabled: ☒

Reset Delete Save Close

**Table 152:** *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 239** *Add Subscriber Node*

Add Subscriber Node

Publisher IP: 10.4.33.168

Publisher Password: .....

☒ Restore the local log database after this operation

☐ Do not backup the existing databases before this operation

**WARNING :** All application licenses on this server will be removed. Please contact support to add and activate these licenses.

Save Cancel

**Table 153:** *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 <i>appadmin</i>
Publisher Password	
Restore the local log database after this operation	Enable to restore the log database following addition of a subscriber node.
Do not backup the existing databases before this operation	Enable this check box only if you do not require a backup to the existing database.

## Upload Nessus Plugins

Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Upload Nessus Plugins** link.

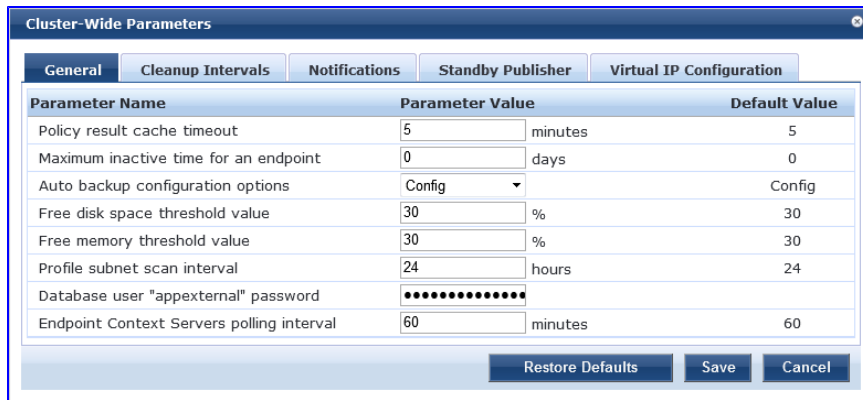
**Figure 240** *Upload Nessus Plugins*
**Table 154:** *Upload Nessus Plugins*

Container	Description
Select File	Click <b>Browse</b> 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 241** *Cluster-Wide Parameters dialog box, General tab*

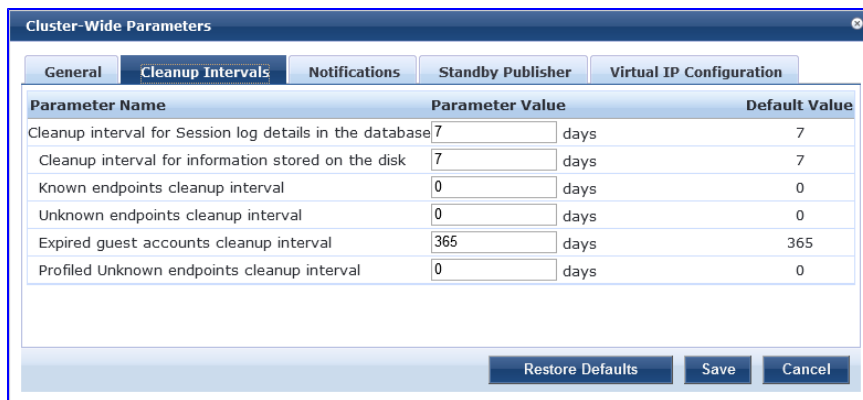


The dialog box shows the General tab with the following parameters:

Parameter Name	Parameter Value	Default Value
Policy result cache timeout	5 minutes	5
Maximum inactive time for an endpoint	0 days	0
Auto backup configuration options	Config	Config
Free disk space threshold value	30 %	30
Free memory threshold value	30 %	30
Profile subnet scan interval	24 hours	24
Database user "appexternal" password	••••••••••	
Endpoint Context Servers polling interval	60 minutes	60

Buttons: Restore Defaults, Save, Cancel

**Figure 242** *Cluster-Wide Parameters dialog box, Cleanup Interval tab*

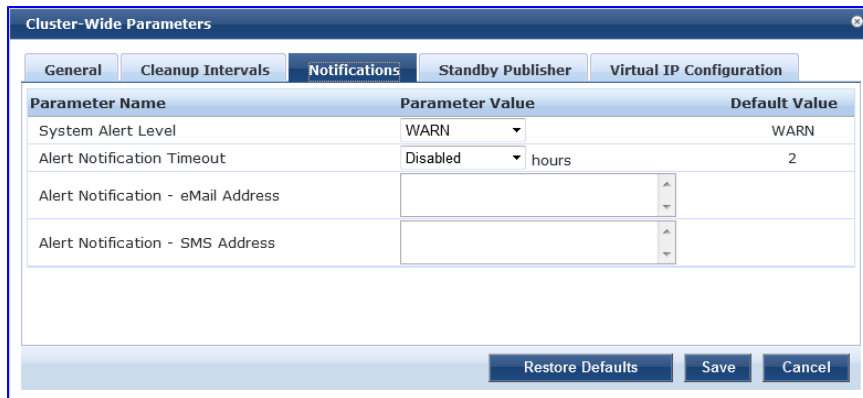


The dialog box shows the Cleanup Intervals tab with the following parameters:

Parameter Name	Parameter Value	Default Value
Cleanup interval for Session log details in the database	7 days	7
Cleanup interval for information stored on the disk	7 days	7
Known endpoints cleanup interval	0 days	0
Unknown endpoints cleanup interval	0 days	0
Expired guest accounts cleanup interval	365 days	365
Profiled Unknown endpoints cleanup interval	0 days	0

Buttons: Restore Defaults, Save, Cancel

**Figure 243** *Cluster-Wide Parameters dialog box, Notification tab*



The dialog box shows the Notifications tab with the following parameters:

Parameter Name	Parameter Value	Default Value
System Alert Level	WARN	WARN
Alert Notification Timeout	Disabled hours	2
Alert Notification - eMail Address		
Alert Notification - SMS Address		

Buttons: Restore Defaults, Save, Cancel

**Figure 244** *Cluster-Wide Parameters dialog box, Standby Publisher tab*

Parameter Name	Parameter Value	Default Value
Enable Publisher Failover	FALSE	FALSE
Designated Standby Publisher		0
Failover Wait Time	10 minutes	10

**Figure 245** *Cluster-Wide Parameters dialog box, Virtual IP Configuration tab*

Parameter Name	Parameter Value	Default Value
Failover Wait Time	10 seconds	10

**Table 155:** *Cluster-Wide Parameters*

Parameter	Description
<b>General</b>	
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	<ul style="list-style-type: none"> <li>Off - Do not perform periodic backups.</li> <li>Config - Perform a periodic backup of only the configuration database.</li> <li>Config SessionInfo - Perform a backup of both the configuration database and the session log database.</li> </ul>
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.

Parameter	Description
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.
Endpoint Context Servers polling interval	Enter the number of minutes between polling of endpoint context servers. The default is 60.
<b>Cleanup Intervals</b>	
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.

Parameter	Description
<b>Notifications</b>	
System Alert Level	Alert notifications are generated for system events logged at this level or higher. Selecting INFO generates alerts for INFO, WARN and ERROR messages. Selecting WARN generates alerts for WARN and ERROR messages. Selecting ERROR generates alerts for ERROR messages.
Alert Notification Timeout	This indicates how often (in hours) alert messages are generated and sent out. Selecting 'Disabled' disables alert generation.
Alert Notification - eMail Address	Comma separated list of email addresses to which alert messages are sent.
Alert Notification - SMS Address	Comma separated list of SMS addresses to which alert messages are sent. For example, 4085551212@txt.att.net.
<b>Standby Publisher</b>	
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.
<b>Virtual IP Configuration</b>	
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 246** *Collect Logs*

Collect Logs

Output file name (ending with .zip or .tar.gz)

Collect the following logs

- ☒ System logs
- ☒ Logs from all Policy Manager services
- ☐ Capture network packets Duration of dump: 60 secs.
- ☒ Diagnostic dumps from Policy Manager services

☐ Specify date range

For number of days until today: 1

Start date in yyyy-mm-dd format

End date in yyyy-mm-dd format

Start Cancel

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.

---

Aruba Networks 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.

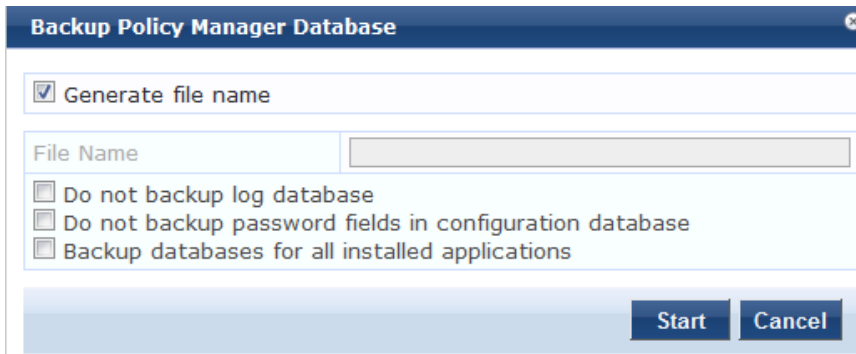
3. Open the .tar file and extract the files within it. The result will be a folder named the same as the .tar file.

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

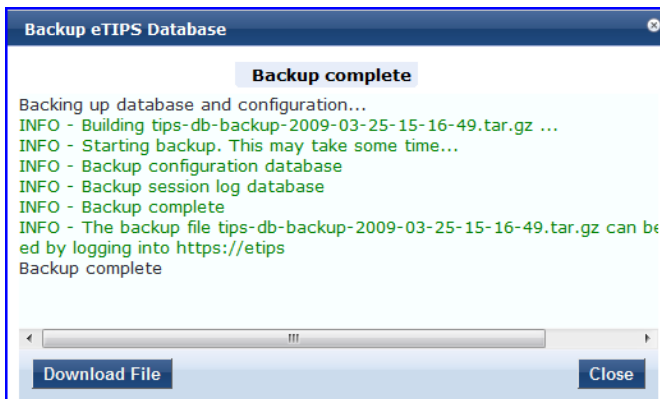
Navigate to the **Administration > Server Manager > Server Configuration** page, and click on the **Back Up** button. Note that this action can also be performed using the "backup" CLI command

**Figure 247** Backup Popup



The screenshot shows a window titled "Backup Policy Manager Database". It contains a checkbox labeled "Generate file name" which is checked. Below this is a text field labeled "File Name". Underneath the text field are three unchecked checkboxes: "Do not backup log database", "Do not backup password fields in configuration database", and "Backup databases for all installed applications". At the bottom right of the window are two buttons: "Start" and "Cancel".

**Figure 248** Post-Backup Popup



The screenshot shows a window titled "Backup eTIPS Database". It displays a "Backup complete" status. The text inside the window reads: "Backing up database and configuration...", "INFO - Building tips-db-backup-2009-03-25-15-16-49.tar.gz ...", "INFO - Starting backup. This may take some time...", "INFO - Backup configuration database", "INFO - Backup session log database", "INFO - Backup complete", and "INFO - The backup file tips-db-backup-2009-03-25-15-16-49.tar.gz can be ed by logging into https://etips". At the bottom of the window are two buttons: "Download File" and "Close".

**Table 156:** 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 " on page 270).
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 249** *Restore*

**Table 157:** *Restore*

Container	Description
Restore file location	Select either <b>Upload file to server</b> or <b>File is on server</b> .
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 " <a href="#">Local Shared Folders</a> " on page 270). This is shown only when <b>File on server</b> 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 250** *Fig: System Tab*

Administration » Server Manager » Server Configuration - cppm52  
 Server Configuration - cppm52 (10.100.8.52) [Import Updates](#)

System	Services Control	Service Parameters	System Monitoring	Network Interfaces												
Hostname: <input type="text" value="cppm52"/> Policy Manager Zone: <input type="text" value="default"/> <a href="#">Manage Policy Manager Zones</a> Enable Profile: <input checked="" type="checkbox"/> Enable to allow this node to perform endpoint classification Enable Insight: <input checked="" type="checkbox"/> Enable to use insight on this node																
<table border="1"> <thead> <tr> <th colspan="2">Management Port:</th> <th>Data/External Port:</th> </tr> </thead> <tbody> <tr> <td>IP Address:</td> <td><input type="text" value="10.100.8.52"/></td> <td><input type="text" value="10.2.152.178"/></td> </tr> <tr> <td>Subnet Mask:</td> <td><input type="text" value="255.255.255.0"/></td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td>Default Gateway:</td> <td><input type="text" value="10.100.8.1"/></td> <td><input type="text" value="10.2.152.201"/></td> </tr> </tbody> </table>					Management Port:		Data/External Port:	IP Address:	<input type="text" value="10.100.8.52"/>	<input type="text" value="10.2.152.178"/>	Subnet Mask:	<input type="text" value="255.255.255.0"/>	<input type="text" value="255.255.255.0"/>	Default Gateway:	<input type="text" value="10.100.8.1"/>	<input type="text" value="10.2.152.201"/>
Management Port:		Data/External Port:														
IP Address:	<input type="text" value="10.100.8.52"/>	<input type="text" value="10.2.152.178"/>														
Subnet Mask:	<input type="text" value="255.255.255.0"/>	<input type="text" value="255.255.255.0"/>														
Default Gateway:	<input type="text" value="10.100.8.1"/>	<input type="text" value="10.2.152.201"/>														
<table border="1"> <thead> <tr> <th colspan="2">DNS Settings:</th> </tr> </thead> <tbody> <tr> <td>IP Address:</td> <td><input type="text" value="10.100.8.82"/></td> </tr> </tbody> </table>					DNS Settings:		IP Address:	<input type="text" value="10.100.8.82"/>								
DNS Settings:																
IP Address:	<input type="text" value="10.100.8.82"/>															
AD Domains: Policy Manager is not part of any domain. Join to domain here. <a href="#">Join AD Domain</a>																

[Back to Server Configuration](#) [Save](#) [Cancel](#)

**Table 158:** *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 <b>Policy Manager Timezone</b> 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: <ul style="list-style-type: none"> <li>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.</li> <li>When enabling the checkbox for other servers in the cluster, they will be added as backups for the same auth source.</li> <li>The order of the primary and backup servers in the [Insight Repository] is the same in which the user enables Insight on the server.</li> </ul>
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.



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.



For most use cases, if you have multiple nodes in the cluster, you must join each node to the same Active Directory domain.

**Figure 251** *Join Active Directory Domain*

**Table 159:** *Join AD Domain*

Container	Description
Domain Controller	<i>Fully qualified</i> 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 <b>Leave Domain</b> button (which replaces the <b>Join Domain</b> 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: <ul style="list-style-type: none"><li>Continue to use the domain controller name that you entered</li><li>Use the domain controller name returned by the DNS query</li><li>Abort the Join Domain operation.</li></ul>
Use default domain admin user	Check this box to use the <i>Administrator</i> 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 252** *Services Control Tab*

System	Services Control	Service Parameters	System Monitoring	Network Interfaces
Service Name	Status	Action		
1. Async DB write service	Running	Stop		
2. Async network services	Running	Stop		
3. DB change notification server	Running	Stop		
4. DB replication service	Running	Stop		
5. Domain service	Running	Stop		
6. Policy server	Running	Stop		
7. Radius server	Running	Stop		
8. System auxiliary services	Running	Stop		
9. System monitor service	Running	Stop		
10. Tacacs server	Running	Stop		

[Back to Server Configuration](#)
[Save](#)
[Cancel](#)

## Service Parameters Tab

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

**Figure 253** *Policy Server Service Parameters*

System	Services Control	Service Parameters	System Monitoring	Network Interfaces
Select Service: <input type="text" value="Policy server"/>				
Parameter Name	Parameter Value	Default Value		
Machine Authentication Cache Timeout	<input type="text" value="86400"/>	seconds	86400	
Authentication Thread Pool Size	<input type="text" value="20"/>	threads	20	
LDAP Primary Retry Interval	<input type="text" value="600"/>	seconds	600	
External Posture Server Thread Pool Size	<input type="text" value="5"/>	threads	5	
External Posture Server Primary Retry Interval	<input type="text" value="600"/>	seconds	600	
Audit SPT Default Timeout	<input type="text" value="600"/>	seconds	600	
Number of request processing threads	<input type="text" value="4"/>	threads		
Audit Primary Retry Interval	<input type="text" value="600"/>	seconds	600	
Audit IP Lookup Session Timeout	<input type="text" value="120"/>	seconds	120	

**Table 160:** *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 254** *RADIUS Server Service Parameters*

Administration » Server Manager » Server Configuration - testlab178  
 Server Configuration - testlab178 (10.2.50.178) [Import Updates](#)

System Services Control **Service Parameters** System Monitoring Network Interfaces

Select Service: RADIUS server

Parameter Name	Parameter Value	Default Value	Allowed Values
<b>Proxy</b>			
Maximum Response Delay	5 seconds	5	1-5
Maximum Reactivation Time	120 seconds	120	60-3600
Maximum Retry Counts	5 retries	5	2-10
<b>Security</b>			
Reject Packet Delay	1 seconds	1	0-5
Maximum Attributes	200 attributes	200	0-512
Process Server-Status Request	FALSE	FALSE	
<b>Main</b>			
Authentication Port	1812, 1645	1812, 1645	
Accounting Port	1813, 1646	1813, 1646	
Maximum Request Time	30 seconds	30	5-120
Cleanup Time	5 seconds	5	2-10
Local DB Authentication Source Connection Count	32	32	5-150
AD/LDAP Authentication Source Connection Count	64	64	5-300
SQL DB Authentication Source Connection Count	32	32	5-100
EAP-TLS Fragment Size	1024 bytes	1024	512-1500
Use Inner Identity in Access-Accept Reply	FALSE	FALSE	
TLS Session Cache Limit	10000 sessions	10000	1000-100000

[Back to Server Configuration](#) Save Cancel

**Table 161:** *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)
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
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 255** TACACS+ Service Parameters

Parameter Name	Parameter Value	Default Value
TACACS+ Profiles Cache Timeout	86400 seconds	86400

**Table 162:** *Service Parameters tab - TACACS server*

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

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 Aruba update portal in order to download the latest version information for posture services.

**Figure 256** *ClearPass System Services Parameters*

System	Services Control	Service Parameters	System Monitoring	Network Interfaces
Select Service: <span>ClearPass system services</span>				
Parameter Name	Parameter Value	Default Value	Allowed Values	
<b>PHP System Configuration</b>				
Memory Limit	<input type="text" value="256"/> Megabytes	256	256-1024	
Form POST Size	<input type="text" value="10"/> Megabytes	10	1-256	
File Upload Size	<input type="text" value="5"/> Megabytes	5	1-256	
Input Time	<input type="text" value="60"/> seconds	60	0-600	
Socket Timeout	<input type="text" value="60"/> seconds	60	5-600	
Enable zlib output compression	<input type="checkbox"/> FALSE	FALSE		
Include PHP header in web server response	<input type="checkbox"/> TRUE	TRUE		
<b>HTTP Proxy</b>				
Proxy Server	<input type="text"/>			
Port	<input type="text" value="3128"/>	3128		
Username	<input type="text"/>			
Password	<input type="text"/>			

**Table 163:** *Service Parameters - ClearPass system services*

Service Parameter	Description
PHP System Configuration	
Memory Limit	Maximum memory that can be used by the PHP applications.
Form POST Size	Maximum HTTP POST content size that can be sent to the PHP application.
File Upload Size	Maximum file size that can be uploaded into the PHP application.
Input Time	Time limit after which the server will detect no activity from the user and will take some action.
Socket Timeout	Maximum time for any socket connections.
Enable zlib output compression	Setting to compress the output files.
Include PHP header in web server response	Setting to include PHP header in the HTTP responses.
HTTP Proxy	
Proxy Server	Hostname or IP address of the proxy server

Service Parameter	Description
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 257** ClearPass Network Services Parameters

Select Service:	ClearPass network services ▼			
Parameter Name	Parameter Value		Default Value	Allowed Values
<b>DhcpSnooper</b>				
MAC to IP Request Hold time	120	seconds	120	60-300
DHCP Request Probation Time	30	seconds	30	10-60
<b>SnmpService</b>				
SNMP Timeout	4	seconds	4	2-30
SNMP Retries	1	retries	1	1-5
LinkUp Timeout	5	seconds	5	3-15
IP Address Cache Timeout	600	seconds	600	12-1200
Uplink Port Detection Threshold	5		5	0-20
SNMP v2c Trap Community	*****		public	
SNMP v3 Trap Username	aruba		aruba	
SNMP v3 Trap Authentication Protocol				
SNMP v3 Trap Privacy Protocol				
SNMP v3 Trap Authentication Key				
SNMP v3 Trap Privacy Key				
Device Info Poll Interval	60	minutes	60	10-1500
<b>WebAuthService</b>				
Max time to determine network device where client is connected	5	seconds	5	0-100
<b>PostureService</b>				
Audit Thread Pool Size	20	threads	20	5-40

**Table 164:** Service Parameters - ClearPass network services

Service Parameters	Description
<b>DhcpSnooper</b>	
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
<b>SnmpService</b>	

Service Parameters	Description
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)
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 specifies the time (in minutes) between polling for device information.
<b>PostureService</b>	
Audit Thread Pool Size	This specifies the number of threads to use for connections to audit servers.

Service Parameters	Description
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.
<b>WebAuthService</b>	
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 258** System Monitor Service Parameters

System	Services Control	Service Parameters	System Monitoring	Network Interfaces
Select Service:	System monitor service			
Parameter Name	Parameter Value	Default Value		
Free Disk Space Threshold	30 %	30		
1 Min CPU load average Threshold	3 %	3		
5 Min CPU load average Threshold	2 %	2		
15 Min CPU load average Threshold	1 %	1		

**Table 165:** Services Parameters tab - System monitor service

Service Parameter	Description
Free Disk Space Threshold	This parameter monitors the available disk space. If the available disk free space falls below the specified threshold (default 30%), then system sends SNMP traps to the configured trap servers.
1 Min CPU load average Threshold	These parameters monitor the CPU load average of the system, specifying thresholds for 1-min, 5-min and 15-min averages, respectively. If any of these loads exceed the associated maximum value, then system sends traps to the configured trap servers.
5 Min CPU load average Threshold	
15 Min CPU load average Threshold	

## 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 259** System Monitoring Tab

The screenshot shows the 'System Monitoring' tab selected. The form includes the following fields:

- System Location: [Text Field]
- System Contact: [Text Field]
- SNMP Configuration:
  - Version: [V3]
  - User Name: [Text Field]
  - Security Level: [NOAUTH\_NOPRIV]
  - Authentication Protocol: [MD5]
  - Authentication key: [Text Field] Verify: [Text Field]
  - Privacy Protocol: [DES]
  - Privacy Key: [Text Field] Verify: [Text Field]

A red box highlights the System Location, System Contact, and SNMP Configuration fields.

**Table 166:** System Monitoring tab details

Service Parameter	Description
System Location	Policy Manager appliance location and contact information
System Contact	
SNMP Configuration: Version	V1, V2C or V3
SNMP Configuration: Community String	Read community string.
SNMP Configuration: SNMP v3: Username	Username to use for SNMP v3 communication
SNMP Configuration: SNMP v3: Security Level	One of NOAUTH_NOPRIV (no authentication or privacy), AUTH_NOPRIV (authenticate, but no privacy), 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 260** *Network Interfaces Tab*

The screenshot shows the 'Network' tab selected in the top navigation bar. Below the navigation bar, there are three sections: 'GRE Tunnels:', 'VLANs:', and 'Application Access Control:'. Each section has a status message and a corresponding button. 'GRE Tunnels:' shows 'No GRE Tunnel created on this node' with a 'Create Tunnel' button. 'VLANs:' shows 'No VLANs present' with a 'Create VLAN' button. 'Application Access Control:' shows 'No Access Restrictions added to this node' with a 'Restrict Access' button. At the bottom, there is a 'Back to Server Configuration' link and 'Save' and 'Cancel' buttons.

### 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 261** *Creating GRE Tunnel*

The screenshot shows the 'Create Tunnel' dialog box. It has a title bar with a close button. Inside, there are four input fields: 'Display Name', 'Local Inner IP', 'Remote Outer IP', and 'Remote Inner IP'. At the bottom right, there are 'Create' and 'Cancel' buttons.

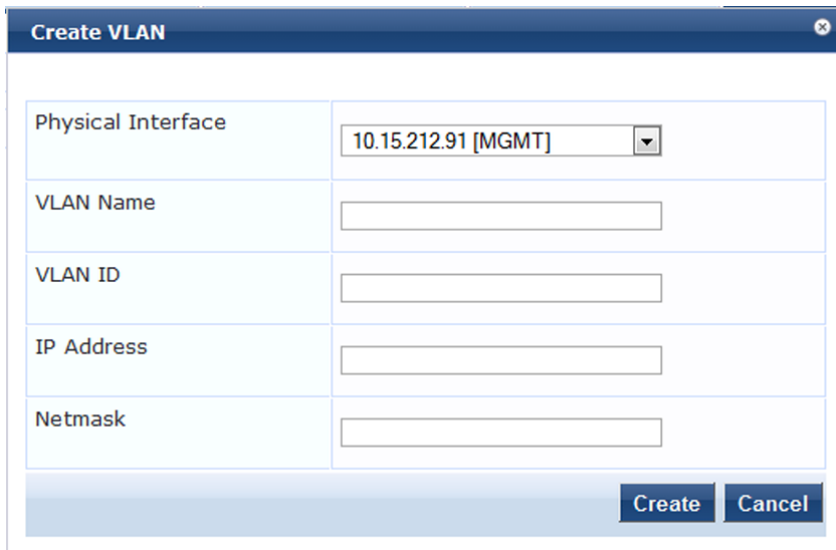
**Table 167:** *Creating GRE Tunnel*

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 262** *Creating VLAN*



**Table 168:** *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 263** *Restrict Access dialog box*

**Restrict Access**

Resource Name: -- Select --

Access: Allow

Network: Deny access for all except -

**Note:** Network supports Hostname / IP Address / IP Subnet only

Create Cancel

**Table 169:** *Restrict Access Parameters*

Parameter	Description
Resource Name	Select the application you want to allow or deny access to.
Access	Select: <ul style="list-style-type: none"><li>● <b>Allow</b> to define allowed access</li><li>● <b>Deny</b> to define denied access.</li></ul>
Network	Enter one or more hostnames, IP addresses, or IP 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 264** Log Configuration (Services Level tab)

Administration » Server Manager » Log Configuration

### Log Configuration

Select Server: 10.2.50.178

**Service Log Configuration** | System Level

Select Service: Policy server

Module Log Level Settings: ☒ Enable to override default log level

Default Log Level: WARN

Module Name	Log Level
1. Rules Engine	WARN
2. Xpip Server	WARN
3. Database	INFO
4. AD/LDAP	INFO
5. Request Handling	INFO
6. Common Framework	INFO
7. External Posture Validation	INFO
8. Internal Posture Validation	INFO
9. Audit Server support	INFO
10. SOAP API	INFO

**Table 170:** 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	<p><b>Enable</b> 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):</p> <ul style="list-style-type: none"> <li>• DEBUG</li> <li>• INFO</li> <li>• WARN</li> <li>• ERROR</li> <li>• FATAL</li> </ul> <p>If this option is disabled, then all module level logs are set to the default log level.</p>
Default Log Level	<p>This drop down is available if the <b>Module Log Level Settings</b> option is disabled. This sets the default logging level for all modules. Available options include the following:</p> <ul style="list-style-type: none"> <li>• DEBUG</li> <li>• INFO</li> <li>• WARN</li> <li>• ERROR</li> <li>• FATAL</li> </ul> <p>Set this option first, and then override any modules as necessary.</p>
Module Name & Log Level	<p>If the <b>Module Log Level Settings</b> option is enabled, select log levels for each of the available modules (listed in decreasing level of verbosity):</p> <ul style="list-style-type: none"> <li>• DEBUG</li> <li>• INFO</li> <li>• WARN</li> <li>• ERROR</li> <li>• FATAL</li> </ul>
Restore Defaults/Save	Click <b>Save</b> to save changes or <b>Restore Defaults</b> to restore default settings.

**Figure 265** Log Configuration (System Level tab)

Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 10.2.50.178

**Service Log Configuration** **System Level**

Number of log files: 6 (default is 6 files)

Limit each log file size to: 10 MB (default is 10 MB)

**Syslog Settings:**

Syslog Server:

Syslog Server Port: 514 (default is 514)

Service Name	Enable Syslog	Syslog Filter Level
1. Policy server	<input type="checkbox"/>	WARN
2. Radius server	<input type="checkbox"/>	WARN
3. Tacacs server	<input type="checkbox"/>	WARN
4. Admin server	<input type="checkbox"/>	WARN
5. Syslog client service	<input type="checkbox"/>	WARN
6. ClearPass network services	<input type="checkbox"/>	WARN

**Table 171:** 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.
Service Name Enable Syslog Syslog Filter Level	For each service, you can select the <b>Enable Syslog</b> check box and then override the Syslog Filter level. The current Syslog Filter level is based on the default log level specified on the <b>Service Log Configuration</b> tab.
Restore Defaults/Save	Click <b>Save</b> to save changes or <b>Restore Defaults</b> to restore default settings.

## Local Shared Folders

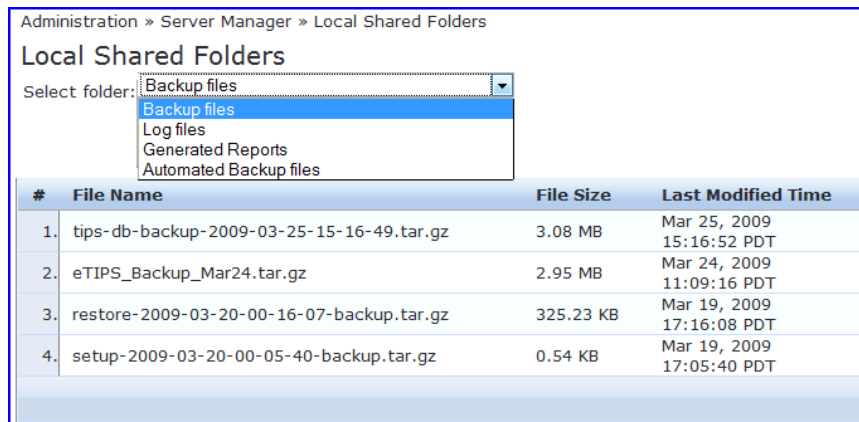
To view backup files, log files, and generated reports, navigate to **Administration > Server Manager > Local Shared Folders**.

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 266** Local Shared Folders



## Application Licensing

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

- [Adding a License](#)
- [Activating an Application License](#)
- [Updating a License](#)



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.

In this release, you can add and activate OnGuard, Guest, Onboard, and Enterprise application licenses. The Summary section shows the number of purchased licenses for Policy Manager, OnGuard, Guest, and Onboard.

**Figure 267** Licensing Page - License Summary tab

Licensing

Add License

License Summary

Servers

Applications

Cluster License Summary

	License Type	Total Count	Used Count	Updated At
1	PolicyManager	5000	264	2012/09/27 00:06:51
2	OnGuard	100	1	2012/09/27 00:06:51
3	ClearPass Enterprise	25	1	2012/09/27 00:06:51

Note: The ClearPass Enterprise license count is inclusive of 25 endpoints for each server node.

Server License Summary

	Server	License Type	Total Count	Used Count	Updated At
1	192.168.1.100	PolicyManager	5000	264	2012/09/27 00:06:51
2	192.168.1.101	OnGuard	100	1	2012/09/27 00:06:51
3	192.168.1.102	ClearPass Enterprise	25	1	2012/09/27 00:06:51

**Figure 268** Licensing Page - Servers tab

License Summary		Servers	Applications					
#	Server IP Address	Product	License Type	Native	Number of Endpoints	Duration	Activation Status	License Added On
1		Policy Manager	Permanent	No	5000	2 years	Activated	Mar 11, 2013 12:13:42 PDT



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.

## Adding a License

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

**Figure 269** Add License dialog box

**Table 172:** Add a License

Container	Description
Product	Select a product from the drop down menu.
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.

## Activating 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.

License Summary		Servers	Applications			
#	Product	License Type	Number of Endpoints	Duration	Activation Status	License Added On
1	OnGuard	Permanent	100	-	Activated	Sep 26, 2012 17:26:54 PDT
2	Guest	Permanent	100	-	Activated	Sep 26, 2012 17:25:40 PDT
3	Onboard	Permanent	100	-	Activate	Sep 26, 2012 17:25:15 PDT

3. Click **Activate** in the Activation Status column.
4. Click **OK**.

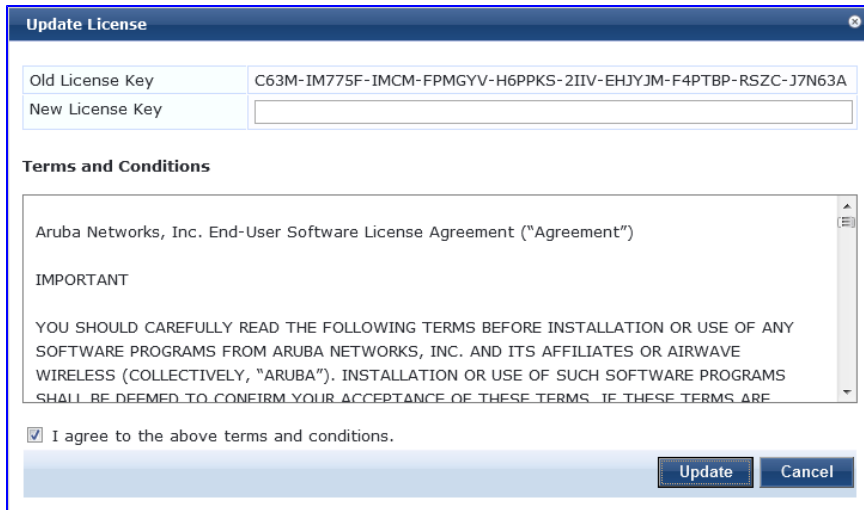
## Updating a License

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.

- Click an application anywhere except in the Activation Status column. The Update License dialog box appears.



The 'Update License' dialog box contains the following elements:

- Old License Key:** C63M-IM775F-IMCM-FPMGYV-H6PPKS-2IIV-EHJYJM-F4PTBP-RSZC-J7N63A
- New License Key:** An empty text input field.
- Terms and Conditions:** A scrollable text area containing the 'Aruba Networks, Inc. End-User Software License Agreement ("Agreement")'. The text includes an 'IMPORTANT' notice stating that users should read the terms before installation or use of any software programs from Aruba Networks, Inc. and its affiliates or Airwave Wireless (collectively, 'Aruba'). It also states that installation or use of such software programs shall be deemed to confirm acceptance of these terms.
- Agreement:** A checkbox labeled 'I agree to the above terms and conditions.' which is checked.
- Buttons:** 'Update' and 'Cancel' buttons at the bottom right.

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

## SNMP Trap Receivers

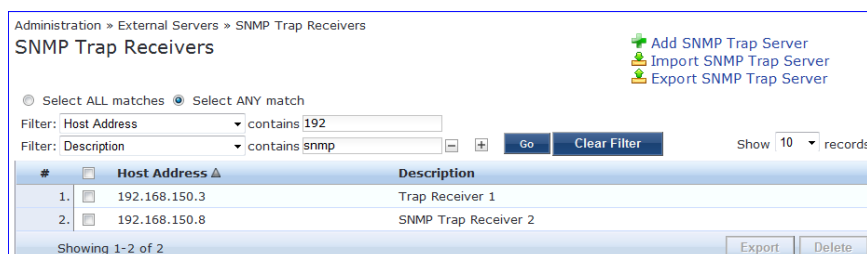
Policy Manager sends SNMP traps that expose the following server information:

- 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 274
- "Import SNMP Trap Server " on page 275
- "Export all SNMP Trap Servers " on page 275
- "Export a Single SNMP Trap Server " on page 275

**Figure 270** SNMP Trap Receivers Listing Page



The 'SNMP Trap Receivers' listing page shows the following interface:

- Breadcrumbs:** Administration > External Servers > SNMP Trap Receivers
- Page Title:** SNMP Trap Receivers
- Actions:** Add SNMP Trap Server, Import SNMP Trap Server, Export SNMP Trap Server
- Filters:**
  - Select ALL matches (radio button) / Select ANY match (radio button)
  - Filter: Host Address contains 192
  - Filter: Description contains snmp
  - Buttons: Go, Clear Filter
  - Show 10 records
- Table:**

#	Host Address	Description
1.	192.168.150.3	Trap Receiver 1
2.	192.168.150.8	SNMP Trap Receiver 2
- Footer:** Showing 1-2 of 2, Export, Delete

**Table 173: SNMP Trap Receivers**

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

## 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 271** Add SNMP Trap Server

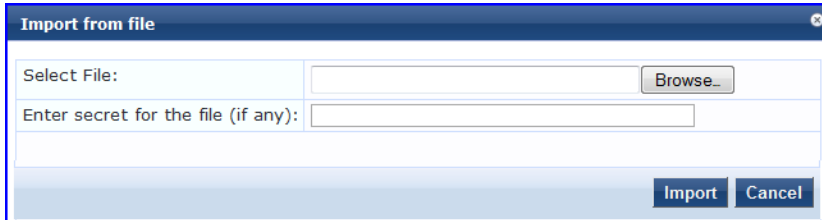
**Table 174: Add SNMP Trap Server fields**

Container	Description
Host Address	Trap destination hostname or ip address. <b>NOTE:</b> This server must have an SNMP trap receiver or trap viewer installed.
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. <b>NOTE:</b> Configure the trap server firewall for traffic on this port.
Save/Cancel	Click <b>Save</b> to commit the configuration or <b>Cancel</b> 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 272** Fig: Import SNMP Trap Server



**Table 175:** 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 <b>Import</b> to commit, or <b>Cancel</b> 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 276](#)
- ["Import Syslog Target " on page 276](#)
- ["Export Syslog Target " on page 277](#)
- ["Export " on page 277](#)

**Figure 273** Syslog Target Listing Page

Administration » External Servers » Syslog Targets

Syslog Targets

Select ALL matches Select ANY match

Filter: Host Address contains 192

Filter: Description contains kiwi

Go Clear Filter

Show 10 records

#	Host Address	Description
1.	10.6.132.138	Kiwi syslog target
2.	192.168.5.233	My Test Syslog Target

Showing 1-2 of 2

Export Delete

**Table 176:** Syslog Target Configuration

Container	Description
Add Syslog Target	Opens the <b>Add Syslog Target</b> popup.
Import Syslog Target	Opens the <b>Import Syslog Target</b> popup.
Export Syslog Target	Opens the <b>Export Syslog Target</b> popup.
Export	Opens the <b>Export</b> popup.
Delete	To delete a Syslog Target, select it (check box at left) and click <b>Delete</b> .

## Add Syslog Target

To add a Syslog Target, navigate to **Administration > External Servers > Syslog Targets** and select **Add Syslog Target**.

**Figure 274** Add Syslog Target

Add Syslog Target

Host Address: 192.168.12.44

Description: Kangaroo Syslog Target

Server Port: 514

Save Cancel

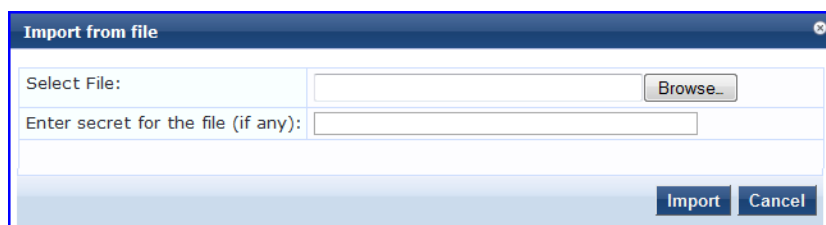
**Table 177:** Add Syslog Target

Container	Description
Host Address	Syslog server hostname or IP address.
Description	Freeform description.
Server Port	Port number for sending the syslog messages; by default, port 514.
Save/Cancel	Click <b>Save</b> to commit the configuration or <b>Cancel</b> to dismiss.

## Import Syslog Target

Navigate to **Administration > External Servers > Syslog Targets** and select **Import Syslog Target**.

**Figure 275** *Import Syslog Target*



**Table 178:** *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 <b>Import</b> to commit, or <b>Cancel</b> 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 278](#)
- ["Import Syslog Filter " on page 280](#)
- ["Export Syslog Filter " on page 280](#)
- ["Export " on page 280](#)

**Figure 276 Syslog Filters Listing page**

Administration » External Servers » Syslog Export Filters

Syslog Export Filters

☐ Select ALL matches
 ☒ Select ANY match

Filter: Name 
 Filter: Description 
 Filter: Export Template 
 Filter: Status

#	<input type="checkbox"/>	Name	Description	Export Template	Status
1.	<input type="checkbox"/>	Audit Syslog Server	This is the syslog export filter to stream all the failed authentications to syslog target.	Audit Records	<input type="button" value="Disable"/>
2.	<input type="checkbox"/>	Failed Authentications Stream	Stream all failed requests to external syslog.	Session Logs	<input type="button" value="Disable"/>
3.	<input type="checkbox"/>	Failed Requests Stream	This is the syslog export filter to stream all the logged in session information to the syslog target.	Session Logs	<input type="button" value="Disable"/>
4.	<input type="checkbox"/>	Logged in Session Stream		Session Logs	<input type="button" value="Disable"/>
5.	<input type="checkbox"/>	Syslog Accounting		Session Logs	<input type="button" value="Disable"/>
6.	<input type="checkbox"/>	Syslog Export Filter for Audit		Audit Records	<input type="button" value="Disable"/>

Showing 1-6 of 6

**Table 179: Syslog Export Filters Configuration**

Container	Description
Add Syslog Filter	Opens <b>Add Syslog Filter</b> page ( <b>Administration &gt; External Servers &gt; Syslog Export Filters &gt; Add</b> ).
Import Syslog Filter	Opens <b>Import Syslog Filter</b> popup.
Export Syslog Filter	Opens <b>Export Syslog Filter</b> popup.
Enable/Disable	Click the toggle button <b>Enable/Disable</b> to enable or disable the syslog filter.
Export	Opens <b>Export</b> popup.
Delete	<b>To delete a Syslog Filter</b> , select it (check box at left) and click <b>Delete</b> .

## Add Syslog Filter

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

**Figure 277 Add Syslog Filters (General tab)**

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

General
  Filter and Columns
  Summary

Name: 
 Description: 
 Export Template: 
 Syslog Server: 

[Add new Syslog target](#)

**Table 180: Syslog Export Filters Configuration**

Container	Description
Name/Description	Freeform label.
Export Template	Session Logs, Audit Records or System Events
Syslog Server	A drop down list shows all Syslog Targets configured. (Refer to <a href="#">"Add Syslog Target"</a> on page 276).
Modify/Add new syslog target	Click to <b>Modify</b> the selected syslog target, or select the <b>Add new syslog target</b> link to add a new syslog target.
Save/Cancel	Click <b>Save</b> to commit the configuration or <b>Cancel</b> to dismiss.

If you selected Session Logs as the export template 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.



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 278 Add Syslog Filters (Filter and Columns tab)**

Administration » External Servers » Syslog Export Filters » Add

**Syslog Export Filters**

General **Filter and Columns** Summary

**Option 1:** For common use-cases, select Data Filter and Columns for export:

Data Filter: [All Requests] [Modify](#) [Add new Data filter](#)

Columns Selection:

Predefined Field Groups -

- Logged in users
- Failed Authentications
- RADIUS Accounting
- TACACS+ Administration

Available Columns -

Type: Common

Common Alerts

Common Alerts-Present

Common Audit-Posture-Token

Common Auth-Type

Common Connection-Status

Common Enforcement-Profiles

Common Error-Code

**Option 2:** For advanced use-cases, specify custom SQL query for export:

Custom SQL:

```
SELECT "Common.Username", "Common.Service", "Common.Roles", "Common.Host-MAC-Address", "RADIUS.Acct-Framed-IP-Address", "Common.NAS-IP-Address", "Common.Request-Timestamp", "Common.Alerts" FROM dblink ( --DB-CONNECTION-STRING-- , "SELECT T1.user_name as "Common.Username", T1.service_name as "Common.Service", T3.roles as "Common.Roles", T1.host_mac as "Common.Host-MAC-Address", T8.framed_ip_address as "RADIUS.Acct-Framed-IP-Address".
```

As an example, [click here](#) to copy a sample SQL

[Back to Syslog Filters](#) [Next >](#) [Save](#) [Cancel](#)

**Table 181: 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.

Container	Description
Modify/ Add new Data filter	Modify the selected data filter, or add a new one.
Columns Selection	<p>This provides a way to limit the type of columns sent to syslog.</p> <p>There are Predfined Field Groups, which are column names grouped together for quick addition to the report. For example, <i>Logged in users</i> field group seven pre-defined columns. When you click <i>Logged in users</i> the seven columns automatically appear in the <b>Selected Columns</b> list.</p> <p>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 <b>Available Columns Type</b> 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 <b>Available Columns Type</b>, the columns appear in the box below. From here you can click &gt;&gt; to add the selected column to the <b>Selected Columns</b> list. Click &lt;&lt; to remove a column from the <b>Selected Columns</b> list.</p>

## Import Syslog Filter

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

**Figure 279** *Import Syslog Filter*

**Table 182:** *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 <b>Import</b> to commit, or <b>Cancel</b> 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 Filter 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 280** *Messaging Setup (SMTP Servers)*

**Table 183:** *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 281** *Messaging Setup (Mobile Service Providers tab)*

Administration » External Servers » Messaging Setup

**Messaging**

Configure the SMTP mail servers for email and SMS notifications : Select Server : 192.168.5.217

**SMTP Servers** **Mobile Service Providers**

[Add](#)

#	Provider Name	Mail Address
1.	Illinois Valley Cellular	ivctext.com
2.	Verizon	vtext.com
3.	Nextel	
4.	SunCom	
5.	Centennial Wi	
6.	Omnipoint	
7.	Alltel	
8.	Cingular	
9.	CellularOne	mobile.celloneusa.com

**Edit Mobile Service Provider**

Provider Name: Verizon

Mail Address: vtext.com

[Save](#) [Close](#)

[Save](#)

**Table 184:** *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 Aruba 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 282** *Endpoint Context Servers*

Administration » External Servers » Endpoint Context Servers

**Endpoint Context Servers**

[Add Context Server](#)  
[Import Context Servers](#)  
[Export Context Servers](#)

Filter: Server Name contains [ ] [Go](#) [Clear Filter](#) Show 10 records

#	Server Name	Server Type
1.	activate.arubanetworks.com	Aruba Activate
2.	MobileIron.com	MobileIron
3.	168.0.0.1	Palo Alto Networks Firewall
4.	168.0.0.2	SOTI

Showing 1-4 of 4 [Export](#) [Delete](#)

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 185:** *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.

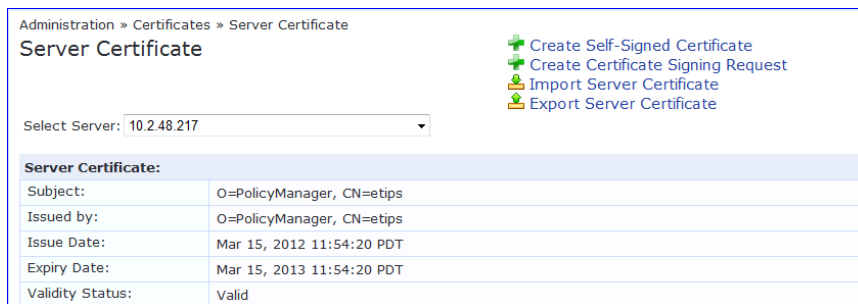
Item	Description
Device Filter (Aruba Activate)	This field is populated with a default regex to retrieve only the information of RAP and IAP information.
Folder Filter (Aruba Activate)	This field is set to "*" by default.
API Key (airwatch) Customer ID (JAMF) Group ID (SOTI)	Enter the values (provided 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 285](#)
- ["Create Certificate Signing Request " on page 286](#)
- ["Export Server Certificate " on page 288](#)
- ["Import Server Certificate " on page 288](#)

**Figure 283** *Server Certificates*



Administration > Certificates > Server Certificate

### Server Certificate

Select Server: 10.2.48.217

Server Certificate:	
Subject:	O=PolicyManager, CN=etips
Issued by:	O=PolicyManager, CN=etips
Issue Date:	Mar 15, 2012 11:54:20 PDT
Expiry Date:	Mar 15, 2013 11:54:20 PDT
Validity Status:	Valid

**Table 186:** *Server Certificate*

Container	Description
Create Self-Signed Certificate	Opens the <b>Create Self-Signed Certificate</b> popup.
Create Certificate Signing Request	Opens the <b>Create Certificate Signing Request</b> popup.

Container	Description
Select Server	Select a server in the cluster for server certificate operations.
Export	Opens the <b>Export</b> popup.
Import	Opens the <b>Import</b> 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 284** *Create Self-Signed Certificate*

Common Name (CN):	clearpass
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
State (ST):	CA
Country (C):	US
Location (L):	San Jose
Subject Alternate Name (SAN):	email:admin@acme.com
Private Key Password:	.....
Verify Private Key Password:	.....
Key Length:	1024 bits
Digest Algorithm:	SHA-1
Valid for:	180 days

**Submit** **Cancel**

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

**Figure 285** *Generated Self Signed Certificate*

Subject DN:	L=San Jose, C=US, ST=CA, O=Acme Systems, OU=Engineering, CN=clearpass
Issuer DN:	L=San Jose, C=US, ST=CA, O=Acme Systems, OU=Engineering, CN=clearpass
Subject Alternate Name (SAN):	email:admin@acme.com
Issue Date/Time:	Sep 28, 2012 17:16:30 UTC
Expiry Date/Time:	Mar 27, 2013 17:16:30 UTC
Validity Status:	Valid
Signature Algorithm:	SHA1WithRSAEncryption
Public Key Format:	X.509

**Install** **Cancel**

**Table 187: 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: <i>email_address</i> , URI: <i>uri</i> , IP: <i>ip_address</i> , dns: <i>dns_name</i> , or rid: <i>id</i> . 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: <b>512</b> , <b>1024</b> , or <b>2048</b> .
Digest Algorithm	Select message digest algorithm to use: <b>SHA-1</b> , <b>MD5</b> , and <b>MD2</b> .
Valid for	Specify duration in days.
Submit/Cancel	On submit, Policy Manager generates a popup containing the self-signed certificate. Click on the <b>Install</b> button to install the certificate on the selected server. <b>NOTE:</b> 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 286** 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 287** Generated Certificate Signing Request

**Table 188:** 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.
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.

Container	Description
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: <b>512</b> , <b>1024</b> , or <b>2048</b> .
Digest Algorithm	Select message digest algorithm to use: <b>SHA-1</b> , <b>MD5</b> , and <b>MD2</b> .
Submit/Cancel	<p>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.</p> <ul style="list-style-type: none"> <li>To create a file containing the certificate signing request, click <b>Download CSR File</b>. A .csr file is downloaded to your local computer.</li> <li>To download the generated private key file, click <b>Download Private Key File</b>.</li> </ul> <p><b>NOTE:</b> Make sure that you save the downloaded private key in a secure place.</p>

## 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 **ServerCertificate.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 288** *Import Server Certificate*

The screenshot shows a dialog box titled "Import Server Certificate". It has a light blue header bar. Below the header, there are three rows of input fields. The first row is "Certificate File:" followed by a text input field and a "Browse..." button. The second row is "Private Key File:" followed by a text input field and a "Browse..." button. The third row is "Private Key Password:" followed by a text input field. At the bottom right of the dialog, there are two buttons: "Import" and "Cancel".

**Table 189: 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 <b>Import</b> to commit, or <b>Cancel</b> 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 289 Certificate Trust List**

#	Subject	Validity	Enabled
1.	C=US, O=GeoTrust Inc., CN=GeoTrust Global CA	valid	Enabled
2.	C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority	valid	Enabled
3.	C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority	valid	Enabled
4.	C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2	valid	Enabled
5.	C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority	valid	Enabled
6.	C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority	valid	Enabled
7.	C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA 2	valid	Enabled
8.	C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA	valid	Enabled
9.	C=AT, O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, OU=A-Trust-nQual-03, CN=A-Trust-nQual-03	valid	Enabled
10.	C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority	valid	Enabled

**Table 190: 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.

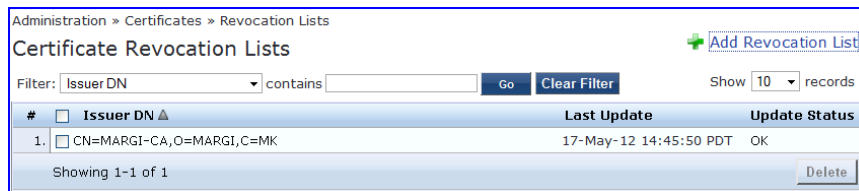
**Figure 290 Add Certificate**

**Table 191: Add Certificate**

Container	Description
Certificate File	Browse to select certificate file.
Add Certificate/Cancel	Click <b>Add Certificate</b> to commit, or <b>Cancel</b> to dismiss the popup.

## Revocation Lists

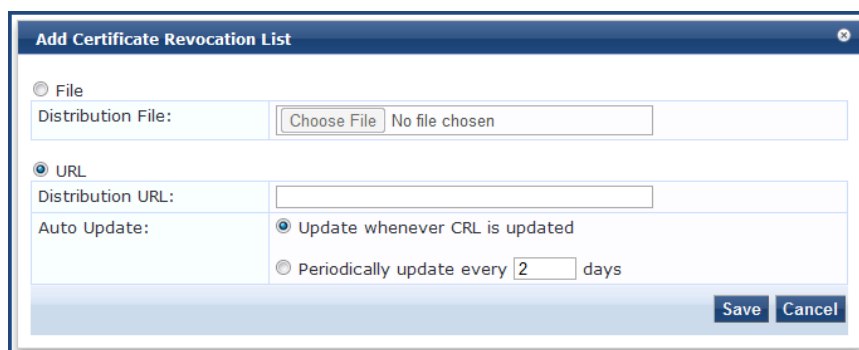
To display available Revocation Lists, navigate to **Administration > Certificates > Revocation Lists**. To add a revocation list, click **Add Revocation List**. To delete a revocation list, select the check box to the left of the list and then click **Delete**.

**Figure 291 Revocation Lists****Table 192: 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 <b>Delete</b> .

## Add Revocation List

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

**Figure 292 Add Certificate Revocation List****Table 193: Add Revocation List**

Container	Description
File	File enables the Distribution File option.

Container	Description
Distribution File	Specify the distribution file (e.g., <b>C:/distribution/crl.verisign.com/Class3InternationalServer.crl</b> ) to fetch the certificate revocation list.
URL	URL enables the Distribution URL option.
Distribution URL	Specify the distribution URL (e.g., <b>http://crl.verisign.com/Class3InternationalServer.crl</b> ) to fetch the certificate revocation list.
Auto Update	Select <b>Update whenever CRL is updated</b> to update the CRL at intervals specified in the list. Or select <b>Periodically update</b> 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 293** *RADIUS*

Administration > Dictionaries > RADIUS

RADIUS Dictionaries [Import Dictionary](#)

Filter:  contains    Show  records

#	Vendor Name	Vendor ID	Vendor Prefix	Enabled ▾
1.	FreeRADIUS	11344	FreeRADIUS	false
2.	Aruba	14823	Aruba	true
3.	Cisco	9	Cisco	true
4.	Alvarion	12394	Alvarion	true
5.	Microsoft	311	Microsoft	true
6.	Airespace	14179	Airespace	true
7.	Juniper	2636	Juniper	true
8.	IETF	0	IETF	true
9.	Ascend	529	Ascend	false
10.	Cosine	3085	Cosine	false

Showing 1-10 of 103

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 294** *RADIUS IETF Dictionary Attributes*

**RADIUS Attributes**

Vendor Name:

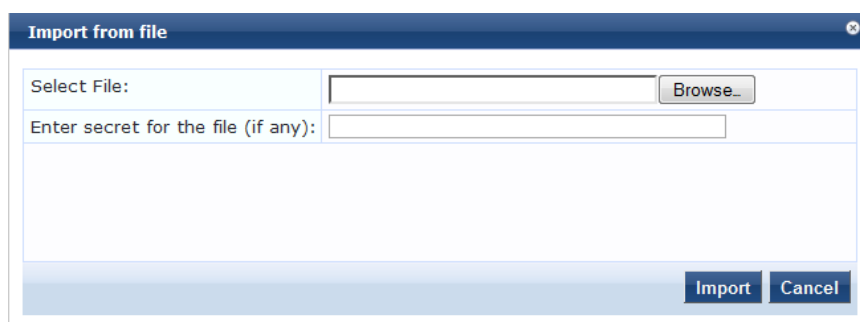
#	Attribute Name	ID	Type	In/Out
1.	User-Name	1	String	in out
2.	User-Password	2	String	in
3.	CHAP-Password	3	String	in
4.	NAS-IP-Address	4	IPv4Address	in
5.	NAS-Port	5	Integer32	in
6.	Service-Type	6	Integer32	in out
7.	Framed-Protocol	7	Integer32	in out
8.	Framed-IP-Address	8	IPv4Address	in out
9.	Framed-IP-Netmask	9	IPv4Address	in out
10.	Framed-Routing	10	Integer32	out

**Table 194:** *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 tool. 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 295** *Import RADIUS Dictionary***Table 195:** *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

Administration > Dictionaries > Posture  
Posture Dictionaries [Import Dictionary](#)

Filter: Vendor Name contains  Go Clear Filter Show 10 records

#	Vendor Name	Vendor ID	Application Name	Application ID
1.	Avenda	25427	Audit	6
2.	Avenda	25427	MacSHV	65282
3.	Avenda	25427	WindowsSHV	65281
4.	Avenda	25427	LinuxSHV	65280
5.	Cisco	9	Anti-Virus	3
6.	Cisco	9	Posture Agent	1
7.	Cisco	9	Firewall	4
8.	Cisco	9	Host	2
9.	Cisco	9	Audit	6
10.	Cisco	9	Host Intrusion Protection Service	5

Showing 1-10 of 16 records

Table 196: Posture

Container	Description
Import Dictionary	Click to open the <b>Import Dictionary</b> 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 296 Fig: Posture Dictionary

**Posture Attributes**

Vendor Name: Microsoft (311)  
Application Name: SystemSHV (65280)

#	Attribute Name	ID	Type	In/Out
1.	Application-Posture-Token	1	Unsigned32	out
2.	System-Posture-Token	2	Unsigned32	out
3.	SoH	3	SoH	in
4.	SoHR	4	SoH	out

Export Close

Table 197: Posture Dictionary Attributes

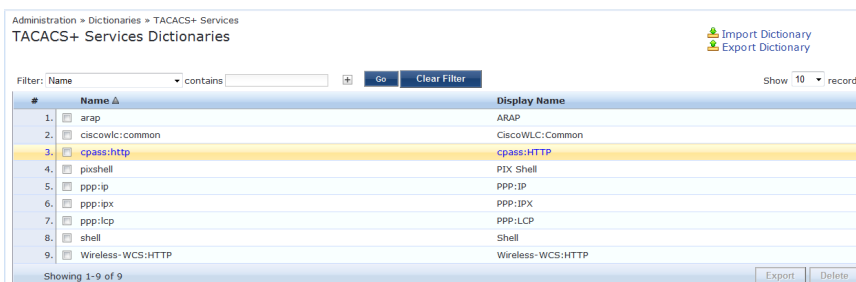
Container	Description
Export	Click to save the posture dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.

## 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 297 TACACS+ Services**



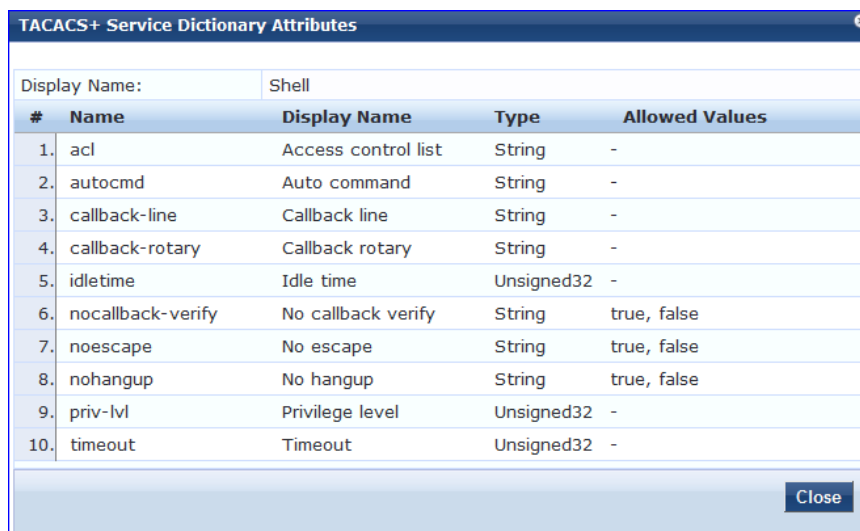
**Table 198: TACACS+ Services Dictionary**

Container	Description
Import Dictionary	Click to open the <b>Import Dictionary</b> 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 298 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 Aruba Update Portal (See "[Update Portal](#) " on [page 302](#) for more information.)

**Figure 299** *Device Fingerprints*

Administration » Dictionaries » Fingerprints

### Device Fingerprints

Filter:  contains    Show  records

#	Category ▲	Family	Name
1	Access Points	Symbol	Symbol AP
2	Access Points	Aruba	Aruba AP
3	Access Points	Cisco	Cisco AP
4	Access Points	Trendnet	Trendnet AP
5	Access Points	Enterasys	Enterasys HiPath AP
6	Access Points	Trapeze	Trapeze AP
7	Access Points	AeroHive	AeroHive AP
8	Access Points	Ruckus	Ruckus Wireless
9	Access Points	Enterasys/Trapeze	Enterasys/Trapeze AP
10	Access Points	Bluesocket	Bluesocket Controller

Showing 1-10 of 111

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

**Figure 300** *Fig: Device Fingerprints*

Device Fingerprint Dictionary Attributes		
Category:	Computer	
Family:	Linux	
Name:	Fedora	
#	Field	Value
1	DHCP Option55	1,28,2,3,15,6,12,40,41,42 28,2,3,15,6,12,40,41,42 1,28,2,3,15,6,12,40,41,42,26,119 1,28,2,3,15,6,12,40,41,42,26 1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42 1,28,2,121,15,6,12,40,41,42,26,119,3 1,28,2,3,15,6,12,40,41,42,26,119,121,249,252,42
<input type="button" value="Close"/>		

## 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 296
- "Import Attributes" on page 297
- "Export Attributes" on page 297
- "Export " on page 297

**Figure 301** *Attributes page*

Administration » Dictionaries » Attributes

Attributes

 Add Attribute  
 Import Attributes  
 Export Attributes

Filter: Name contains [ ] + Go Clear Filter Show 10 records

#	Name	Entity	Data Type	Is Mandatory	Allow Multiple
1.	[Company Name]	GuestUser	String	No	Yes
2.	[Conference]	GuestUser	String	Yes	No
3.	[Controller Id]	Device	String	No	Yes
4.	[Department]	LocalUser	String	No	Yes
5.	[Designation]	GuestUser	String	No	Yes
6.	[Designation]	LocalUser	String	No	Yes
7.	Device IMEI	Endpoint	String	No	Yes
8.	Device IMEI	GuestUser	String	No	Yes
9.	Device Serial	GuestUser	String	No	Yes
10.	[Device Type]	Device	String	No	Yes

Showing 1-10 of 40 Export Delete

**Table 199:** *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 302** *Add Attributes*

Add Attribute

Entity: GuestUser

Name: [vendor]

Data Type: String

Is Mandatory: ☒ Yes ☐ No

Allow Multiple: ☐ Yes ☒ No

Default Value (optional): conferenceroom (Enter String without special characters e.g., firstfloor)

Add Cancel

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 200:** *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 <b>Is Mandatory</b> is specified as <b>Yes</b> .

## 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 303** *Import from file*

A screenshot of a Windows-style dialog box titled "Import from file". It contains two input fields: "Select File:" with a "Browse..." button to its right, and "Enter secret for the file (if any):" with an empty text box. At the bottom right, there are two buttons: "Import" and "Cancel".

**Table 201:** *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 <b>Import</b> to commit, or <b>Cancel</b> 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.

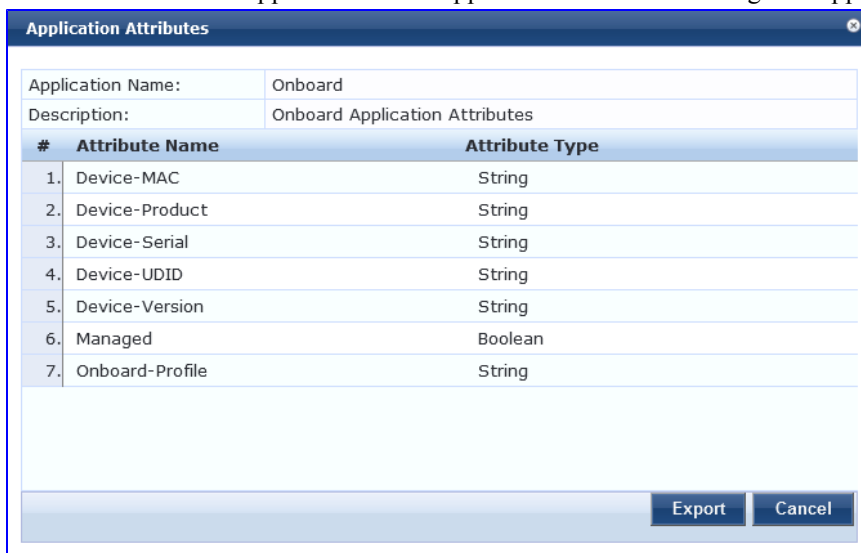
You can

- [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.



#	Attribute Name	Attribute Type
1.	Device-MAC	String
2.	Device-Product	String
3.	Device-Serial	String
4.	Device-UDID	String
5.	Device-Version	String
6.	Managed	Boolean
7.	Onboard-Profile	String

### Delete an application dictionary

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

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 Microsoft 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 304 OnGuard Settings**

Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings - [Global Agent Settings](#) [Policy Manager Zones](#)

Agent Version: 6.1.0.49783

**Agent Installers**

Agent Installers updated at Mar 29, 2013 21:44:19 UTC

OS	Installer URL	Format	Size
Windows	<a href="http://10.2.51.26/agent/installer/windows/ClearPassOnGuardInstall.exe">http://10.2.51.26/agent/installer/windows/ClearPassOnGuardInstall.exe</a>	(Full Install - EXE)	13MB
Windows	<a href="http://10.2.51.26/agent/installer/windows/ClearPassOnGuardInstall.msi">http://10.2.51.26/agent/installer/windows/ClearPassOnGuardInstall.msi</a>	(Full Install - MSI)	13MB
Mac OS X	<a href="http://10.2.51.26/agent/installer/mac/ClearPassOnGuardInstall.dmg">http://10.2.51.26/agent/installer/mac/ClearPassOnGuardInstall.dmg</a>	(Full Install)	8MB

**Agent Customization**

Managed Interfaces: ☒ Wired ☒ Wireless ☒ VPN ☐ Other

Mode: Authenticate with health checks

Username Text:

Password Text:

Client Certificate Check: ☐ Enable to use a certificate from User keystore during authentication

Agent action when an update is available: Ignore

**External Captive Portal Support**

Enter the URL of a web page that can be accessed only after a successful authentication (e.g., <http://www.arubanetworks.com>). A network device that is configured for captive portal-based authentication redirects requests to this URL to an authentication page.

URL:

[Save](#) [Cancel](#)

**Table 202: OnGuard Settings**

Container	Description
Global Agent Settings	<p>Configure global parameters for OnGuard agents. Parameters include the following:</p> <ul style="list-style-type: none"> <li>CacheCredentialsForDays : Select the number of days the user credentials should be cached on OnGuard agents.</li> <li>WiredAllowedSubnets : Add a comma-separated list of IP or subnet addresses.</li> <li>WirelessAllowedSubnets : Add a comma-separated list of IP or subnet addresses</li> <li>KeepAliveIntervalSeconds : Add a keep alive interval for OnGuard agents</li> <li>EnableClientLoadBalance : Enable this option to load balance OnGuard authentication requests across ClearPass Policy Servers in a cluster</li> <li>AllowRemoteDesktopSession : Enable this option to allow OnGuard access via a Remote Desktop session.</li> <li>HideLogoutButton : Enable this option to hide the Logout button.</li> </ul>
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 MacOS.
Managed Interfaces	Select the type of interfaces that OnGuard will manage on the endpoint.
Mode	<p>Select one of:</p> <ul style="list-style-type: none"> <li>Authenticate - no health checks.</li> <li>Check health - no authentication. OnGuard does not collect username/password.</li> <li>Authenticate with health checks. OnGuard collects username/password and also performs health checks on the endpoint.</li> </ul>

Container	Description
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 305** *OnGuard Portal*

Administration > Agents and Software Updates > OnGuard Portal

Global Portal Settings

Name: default

Portal URL: https://testlab32/agent/portal/

Select Mode: Authenticate - no health checks (HTML form)

Enter authentication details

Username:

Password:

Submit

Usage Terms Text: ☐ Enable to show terms and conditions of use

Resource Files: No resource files were uploaded. A ZIP archive containing resource files is supported [Upload](#)

Customize Portal: ☒ Use default template ☐ Upload custom template

Title: ClearPass OnGuard Health Check Portal - Aruba Networks

Logo Image:

Header: Users must pass the health checks to access the network

Footer: **Note:** If you cannot access an enterprise resource, it may be because you are in the quarantine network. Please visit [User Policy Example](#) for more information




Copyright: © Copyright 2013 Aruba Networks. All rights reserved.

Save Cancel

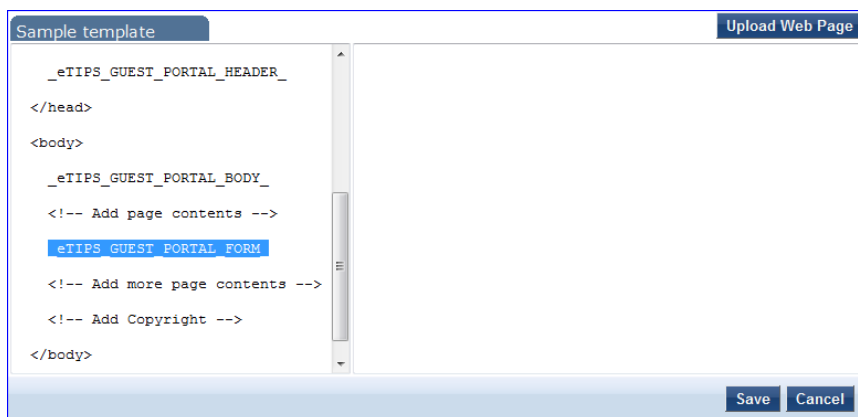
**Figure 306** *OnGuard Portal parameters*

Parameter	Description
Global Portal Settings	Attribute names and value configuration for the portal.

Parameter	Description
	<ul style="list-style-type: none"> <li>• <i>UsernameFormat</i>: 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.</li> <li>• <i>SharedSecret</i>: 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.</li> <li>• <i>ShowOriginalPageRedirectLink</i>: Show a link that will take the user to the original page (prior to being redirected to the captive portal).</li> </ul>
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	<p>Select from the following for different modes of the portal:</p> <ul style="list-style-type: none"> <li>• <b>Authenticate - no health validation (HTML Form)</b> - Policy Manager presents a simple HTML form with the username and password. Health credentials are not collected from the client.</li> <li>• <b>Authenticate - no health validation (Java Applet)</b> - 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.</li> <li>• <b>Check Health - no authentication (Java applet)</b> - Username/password are not collected. Health is evaluated via a Java applet.</li> <li>• <b>Authenticate with health checks (Java Applet)</b> - 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.</li> <li>• <b>Authenticate with optional health checks (Dual mode)</b> - 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.</li> <li>• <b>No Authentication and no health checks (HTML form)</b> - User is presented with a simple HTML form for the username, which is hidden.</li> </ul>
Authentication Details	Click within the Enter Authentication Details field to enter credential details. Note that 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.
Resource Files	<p>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 <code>_eTIPS_GUEST_PORTAL_RESOURCE_</code> to the patch component. For example, if there is a file named <code>logo.jpg</code> in the zipped archive, refer to this resource as "<code>_eTIPS_GUEST_PORTAL_RESOURCE_/logo.jpg</code>" on the OnGuard portal page.</p> <p>After the zipped archive is successfully uploaded, a screen showing the contained files is shown:</p>

Parameter	Description															
	<div><div>Resource Files:</div><div>4 resource files are uploaded (Size: 211.8 KB)<div> Update  Download  Delete</div></div><div><div>Resource Files Details</div><table><thead><tr><th>Name</th><th>Size</th><th>Modified</th></tr></thead><tbody><tr><td>cam.jpg</td><td>51.2 KB</td><td>2010/10/26 17:33:00</td></tr><tr><td>chappatte.jpg</td><td>70 KB</td><td>2010/10/26 17:34:02</td></tr><tr><td>dcr0656l.jpg</td><td>24.9 KB</td><td>2010/10/26 17:30:56</td></tr><tr><td>keefe.jpg</td><td>68.9 KB</td><td>2010/10/26 17:33:16</td></tr></tbody></table><div>To reference the uploaded resource, use <code>&lt;eTIPS_GUEST_PORTAL_RESOURCE /&gt;&lt;filename&gt;</code></div></div></div>	Name	Size	Modified	cam.jpg	51.2 KB	2010/10/26 17:33:00	chappatte.jpg	70 KB	2010/10/26 17:34:02	dcr0656l.jpg	24.9 KB	2010/10/26 17:30:56	keefe.jpg	68.9 KB	2010/10/26 17:33:16
Name	Size	Modified														
cam.jpg	51.2 KB	2010/10/26 17:33:00														
chappatte.jpg	70 KB	2010/10/26 17:34:02														
dcr0656l.jpg	24.9 KB	2010/10/26 17:30:56														
keefe.jpg	68.9 KB	2010/10/26 17:33:16														
Customize Portal	<p><b>Use default template</b> to edit the different fields as described above. To import a custom HTML file to be used as the OnGuard portal, select <b>Upload custom template</b>. Note that the following macros must be present in the custom HTML template:</p> <ul style="list-style-type: none"><li>• <code>_eTIPS_GUEST_PORTAL_HEADER_</code></li><li>• <code>_eTIPS_GUEST_PORTAL_BODY_</code></li><li>• <code>_eTIPS_GUEST_PORTAL_FORM_</code></li></ul>															
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 307** 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 ClearPass Policy Manager server periodically communicates with the webservice about available updates. It downloads any available updates to the ClearPass Policy Manager server. The administrator can install these updates directly from this Software Updates page. The first time the Subscription ID is saved, 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 308** *Software Updates*

**Table 203:** *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	
Import Updates	Use <b>Import Updates</b> 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: <a href="https://clearpass.arubanetworks.com/cppm/appupdate/cppm_apps_updates.zip">https://clearpass.arubanetworks.com/cppm/appupdate/cppm_apps_updates.zip</a> . When prompted, enter the provided Subscription ID for the username and the password for authentication. <b>NOTE:</b> This button is enabled only on publisher node.
Firmware & Patch Updates	

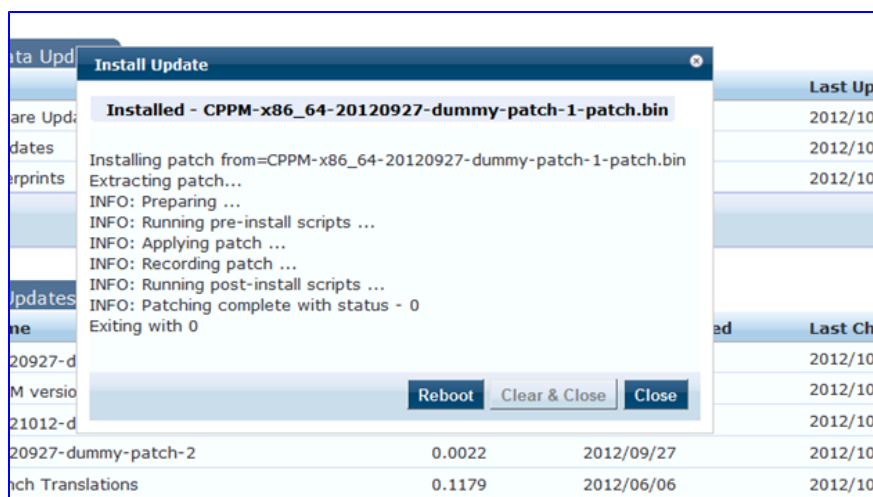
Container	Description
Import Updates	<p>If the server is not able to reach the webservice server, click <b>Import Updates</b> to import the latest Firmware and Update patch binaries (obtained via support or other means) into this server. When logged in as appadmin, the Upgrade and Patch binaries imported can be installed manually via the CLI using the following commands:</p> <ul style="list-style-type: none"> <li>• <code>system update</code> (for patches)</li> <li>• <code>system upgrade</code> (for upgrades)</li> </ul> <p><b>NOTE:</b> The Onboard, Guest Plugins and Skins can only be downloaded and installed via webservice.</p>
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 309** *Install Update*



**Table 204:** *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 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.

### 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). 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:

- "Cluster Commands" on page 309
- "Configure Commands" on page 312
- "Network Commands" on page 314
- "Service commands" on page 316
- "Show Commands" on page 317
- "System commands" on page 320
- "Miscellaneous Commands" on page 322

## Available Commands

**Table 205:** *Command Categories*

Command
<code>ad auth</code> See "Miscellaneous Commands" on page 322
<code>ad netleave</code> See "Miscellaneous Commands" on page 322
<code>ad netjoin</code> See "Miscellaneous Commands" on page 322
<code>ad testjoin</code> See "Miscellaneous Commands" on page 322
<code>alias</code> See "Miscellaneous Commands" on page 322
<code>backup</code> See "Miscellaneous Commands" on page 322
<code>cluster drop-subscriber</code>
<code>cluster list</code>
<code>cluster make-publisher</code>
<code>cluster make-subscriber</code>
<code>cluster reset-database</code>
<code>cluster set-cluster-passwd</code>
<code>cluster set-local-passwd</code>

Command
<i>configure date</i>
<i>configure dns</i>
<i>configure hostname</i>
<i>configure ip</i>
<i>configure timezone</i>
dump certchain See <a href="#">"Miscellaneous Commands"</a> on page 322
dump logs See <a href="#">"Miscellaneous Commands"</a> on page 322
dump servercert See <a href="#">"Miscellaneous Commands"</a> on page 322
exit See <a href="#">"Miscellaneous Commands"</a> on page 322
help See <a href="#">"Miscellaneous Commands"</a> on page 322
krb auth See <a href="#">"Miscellaneous Commands"</a> on page 322
krb list See <a href="#">"Miscellaneous Commands"</a> on page 322
ldapsearch See <a href="#">"Miscellaneous Commands"</a> on page 322
<i>network ip</i>
<i>network nslookup</i>
<i>network ping</i>
<i>network traceroute</i>
<i>network reset</i>
quit See <a href="#">"Miscellaneous Commands"</a> on page 322
restore See <a href="#">"Miscellaneous Commands"</a> on page 322
<i>service activate</i>
<i>service deactivate</i>
<i>service list</i>

Command
<i>service restart</i>
<i>service start</i>
<i>service status</i>
<i>service stop</i>
<i>show date</i>
<i>show dns</i>
<i>show domain</i>
<i>show all-timezones</i>
<i>show hostname</i>
<i>show ip</i>
<i>showlicense</i>
<i>show timezone</i>
<i>show version</i>
<i>system boot-image</i>
<i>system gen-support-key</i>
<i>system update</i>
<i>system restart</i>
<i>system shutdown</i>
<i>system install-license</i>
<i>system upgrade</i>

## Cluster Commands

The Policy Manager command line interface includes the following *cluster* commands:

- ["drop-subscriber" on page 309](#)
- ["list" on page 310](#)
- ["make-publisher" on page 310](#)
- ["make-subscriber" on page 310](#)
- ["reset-database" on page 311](#)
- ["set-cluster-passwd" on page 311](#)
- ["set-local-passwd" on page 311](#)

### drop-subscriber

Removes specified subscriber node from the cluster.

## Syntax

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

Where:

**Table 206:** *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 207: 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 312
- "dns" on page 312
- "hostname" on page 313
- "ip" on page 313
- "timezone" on page 313

### 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 208:** *Date Commands*

Flag/Parameter	Description
-s <ntpserver>	Optional. Synchronize time with specified NTP server.
-d <date>	Required. <i>Syntax:</i> yyyy-mm-dd
-t <time>	Optional. <i>Syntax:</i> hh:mm:ss
-z <timezone>	Optional. <i>Syntax:</i> 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 address>
```

Where:

**Table 209: IP Commands**

Flag/Parameter	Description
ip <mgmt data> <ip address>	Network interface type: <i>mgmt</i> or <i>data</i> <ul style="list-style-type: none"><li>• Server ip address.</li></ul>
netmask <netmask address>	Netmask address.
gateway <gateway address>	Gateway address.

### Example

```
[appadmin]# configure ip data 192.168.5.12 netmask 255.255.255.0 gateway 192.168.5.1
```

## timezone

Configures time zone interactively.

## Syntax

```
configure timezone
```

### Example

```
[appadmin]# configure timezone
```

```
configure timezone
*****
* WARNING: When the command is completed Policy Manager services *
* are restarted to reflect the changes.                          *
*****
Continue? [y|Y]: y
```

## Network Commands

The Policy Manager command line interface includes the following *network* commands:

- ["ip" on page 314](#)
- ["nslookup" on page 315](#)
- ["ping" on page 315](#)
- ["reset" on page 316](#)
- ["traceroute" on page 316](#)

### 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 210: 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 211: 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 212: 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 213: Ping Commands**

Flag/Parameter	Description
-i <SrcIpAddr>	Optional. Originating IP address for ping.
-t	Optional.

Flag/Parameter	Description
	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 214: 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 215: 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 216: Action Commands**

Flag/Parameter	Description
action	Choose an action: <i>activate</i> , <i>deactivate</i> , <i>list</i> , <i>restart</i> , <i>start</i> , <i>status</i> , or <i>stop</i> .
service-name	Choose a service: <i>tips-policy-server</i> , <i>tips-admin-server</i> , <i>tips-system-auxiliary-server</i> , <i>tips-radius-server</i> , <i>tips-tacacs-server</i> , <i>tips-dbwrite-server</i> , <i>tips-repl-server</i> , or <i>tips-sysmon-server</i> .

### 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 318
- "date" on page 318
- "dns" on page 318
- "domain" on page 318
- "hostname" on page 319
- "ip" on page 319
- "license" on page 319
- "timezone" on page 319

- ["version" on page 320](#)

## all-timezones

Interactively displays all available timezones

### Syntax

```
show all-timezones
```

### Example

```
[appadmin]# show all-timezones
Africa/Abidjan
Africa/Accra
.....
WET
Zulu
```

## date

Displays *System Date*, *Time*, and *Time Zone* information.

### Syntax

```
show date
```

### Example

```
[appadmin]# show date
Wed Oct 31 14:33:39 UTC 2012
```

## dns

Displays DNS servers.

### Syntax

```
show dns
```

### Example

```
[appadmin]# show dns
show dns
=====
DNS Information
-----
Primary   DNS   :   192.168.5.3
Secondary DNS : <not configured>
Tertiary  DNS : <not configured>
=====
```

## domain

Displays *Domain Name*, *IP Address*, and *Name Server* information.

### Syntax

```
show domain
```

### Example

```
[appadmin]# show domain
```

## hostname

Displays hostname.

### Syntax

```
show hostname
```

### Example

```
[appadmin]# show hostname
show hostname
wolf
```

## ip

Displays IP and DNS information for the host.

### Syntax

```
show ip
```

### Example

```
[appadmin]# show ip
show ip
=====
Device Type      :   Management Port
-----
IP Address       :   192.168.5.227
Subnet Mask      :   255.255.255.0
Gateway          :   192.168.5.1
=====
Device Type      :   Data Port
-----
IP Address       :   <not configured>
Subnet Mask      :   <not configured>
Gateway          :   <not configured>
=====
DNS Information
-----
Primary  DNS    :   192.168.5.3
Secondary DNS   :   <not configured>
Tertiary  DNS   :   <not configured>
=====
```

## license

Displays the license key.

### Syntax

```
show license
```

### Example

```
[appadmin]# show license
show license
```

## timezone

Displays current system timezone.

### Syntax

```
show timezone
```

## Example

```
[appadmin]# show timezone
show timezone
```

## version

Displays Policy Manager software version hardware model.

## Syntax

```
show version
```

## Example

```
[appadmin]# show version
=====
Policy Manager software version : 2.0(1).6649
Policy Manager model number    : ET-5010
=====
```

# System commands

The Policy Manager command line interface includes the following *system* commands:

- ["boot-image" on page 320](#)
- ["gen-support-key" on page 320](#)
- ["install-license" on page 321](#)
- ["restart" on page 321](#)
- ["shutdown" on page 321](#)
- ["update" on page 322](#)
- ["upgrade" on page 322](#)

## boot-image

Sets system boot image control options.

## Syntax

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

Where:

**Table 217:** *Boot-Image Commands*

Flag/Parameter	Description
-l	Optional. List boot images installed on the system.
-a <version>	Optional. Set active boot image version, in <i>A.B.C.D</i> 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 218:** *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 [-u <patch-name>]
system update [-l]
```

Where:

**Table 219: Update Commands**

Flag/Parameter	Description
-i user@hostname:/<filename>   http://hostname/<filename>	Optional. Install the specified patch on the system.
-u <patch-name>	Optional. Uninstall the patch. (For exact patch names, refer to [-l] in this table.)
-l	Optional. List the patches installed on the system.

### Example

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

## upgrade

Upgrades the system.

### Syntax

```
system upgrade <filepath>
```

Where:

**Table 220: 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" on page 323
- "ad netjoin" on page 323
- "ad netleave" on page 324
- "ad testjoin" on page 324
- "alias" on page 324
- "backup" on page 324
- "dump certchain" on page 325
- "dump logs" on page 325
- "dump servercert" on page 326
- "exit" on page 326
- "help" on page 326
- "krb auth" on page 327
- "krb list" on page 327
- "ldapsearch" on page 327
- "quit" on page 328
- "restore" on page 328

## ad auth

Authenticate the user against AD.

### Syntax

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

Where:

**Table 221:** *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 222:** *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 223:** *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 224: 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 225: 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 226: 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).

Flag/Parameter	Description
-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 227:** *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
```

<code>exit</code>	Exit the shell
<code>help</code>	Display the list of supported commands
<code>netjoin</code>	Join host to the domain
<code>netleave</code>	Remove host from the domain
<code>network</code>	Network troubleshooting commands
<code>quit</code>	Exit the shell
<code>restore</code>	Restore Policy Manager database
<code>service</code>	Control Policy Manager services
<code>show</code>	Show configuration details
<code>system</code>	System commands

## krb auth

Does a kerberos authentication against a kerberos server (such as Microsoft AD)

### Syntax

```
krb auth <user@domain>
```

Where:

**Table 228:** Kerberos Authentication Commands

Flag/Parameter	Description
<code>&lt;user@domain&gt;</code>	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 229:** LDAP Search commands

Flag/Parameter	Description
<code>&lt;user@hostname&gt;</code>	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 230:** *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 291 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 292](#) 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 prepopulated 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 128](#) 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 128](#) 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-polluted 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 231:** *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 232:** *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	<ul style="list-style-type: none"> <li>● <b>None</b> - No PAC was used to establish the outer tunnel in the EAP-FAST authentication method</li> <li>● <b>Tunnel</b> - A tunnel PAC was used to establish the outer tunnel in the EAP-FAST authentication method</li> <li>● <b>Machine</b> - 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 <a href="#">"Adding and Modifying Authentication Methods" on page 111</a>).</li> </ul>
Phase2PAC	<ul style="list-style-type: none"> <li>● <b>None</b> - No PAC was used instead of an inner method handshake in the EAP-FAST authentication method</li> <li>● <b>UserAuthPAC</b> - A user authentication PAC was used instead of the user authentication inner method handshake in the EAP-FAST authentication method</li> <li>● <b>PosturePAC</b> - A posture PAC was used instead of the posture credential handshake in the EAP-FAST authentication method</li> </ul>
Posture	<ul style="list-style-type: none"> <li>● <b>Capable</b> - The client is capable of providing posture credentials</li> <li>● <b>Collected</b> - Posture credentials were collected from the client</li> <li>● <b>Not-Capable</b> - The client is not capable of providing posture credentials</li> <li>● <b>Unknown</b> - It is not known whether the client is capable of providing credentials</li> </ul>
Status	<ul style="list-style-type: none"> <li>● <b>None</b> - No authentication took place</li> <li>● <b>User</b> - The user was authenticated</li> <li>● <b>Machine</b> - The machine was authenticated</li> <li>● <b>Failed</b> - Authentication failed</li> <li>● <b>AuthSource-Unreachable</b> - The authentication source was unreachable</li> </ul>
MacAuth	<ul style="list-style-type: none"> <li>● <b>NotApplicable</b> - Not a MAC Auth request</li> <li>● <b>Known Client</b> - Client MAC address was found in an authentication source</li> </ul>

Attribute Name	Values
	<ul style="list-style-type: none"> <li>• <b>Unknown Client</b> - Client MAC address was not found in an authentication source</li> </ul>
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 233:** *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-RegisteredID, 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 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 199 for 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 234:** *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
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: GuestConnect, Insight, Edge.

## 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 235:** *Policy Manager Variables*

Variable	Description
<code>%{attribute-name}</code>	<i>attribute-name</i> is the alias name for an attribute that you have configured to be retrieved from an authentication source. See <a href="#">"Adding and Modifying Authentication Sources "</a> on page 128.
<code>%{RADIUS:IETF:MAC-Address-Colon}</code>	MAC address of client in aa:bb:cc:dd:ee:ff format
<code>%{RADIUS:IETF:MAC-Address-Hyphen}</code>	MAC address of client in aa-bb-cc-dd-ee-ff format
<code>%{RADIUS:IETF:MAC-Address-Dot}</code>	MAC address of client in aabb.ccdd.eeff format
<code>%{RADIUS:IETF:MAC-Address-NoDelim}</code>	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 236: 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 237: 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., <code>RADIUS:IETF:NAS-Identifier EQUALS "SJ-VPN-DEVICE"</code>
CONTAINS	For string data type, true if the run-time value of the attribute is a substring of the configured value. E.g., <code>RADIUS:IETF:NAS-Identifier CONTAINS "VPN"</code>
BEGINS_WITH	For string data type, true if the run-time value of the attribute begins with the configured value. E.g., <code>RADIUS:IETF:NAS-Identifier BEGINS_WITH "SJ-"</code>
ENDS_WITH	For string data type, true if the run-time value of the attribute ends with the configured value. E.g., <code>RADIUS:IETF:NAS-Identifier ENDS_WITH "DEVICE"</code>
BELONGS_TO	For string data type, true if the run-time value of the attribute matches a set of configured string values.

Operator	Description
	<p>E.g., <code>RADIUS:IETF:Service-Type BELONGS_TO Login-User,Framed-User,Authenticate-Only</code></p> <p>For integer data type, true if the run-time value of the attribute matches a set of configured integer values.</p> <p>E.g., <code>RADIUS:IETF:NAS-Port BELONGS_TO 1,2,3</code></p> <p>For day data type, true if run-time value of the attribute matches a set of configured days of the week.</p> <p>E.g., <code>Date:Day-of-Week BELONGS_TO MONDAY,TUESDAY,WEDNESDAY</code></p> <p>When Policy Manager is aware of the values that can be assigned to <code>BELONGS_TO</code> 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.</p>
<code>EQUALS_IGNORE_CASE</code>	<p>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.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier EQUALS_IGNORE_CASE "sj-vpn-device"</code></p>
<code>MATCHES_REGEX</code>	<p>For string data type, true if the run-time value of the attribute matches the regular expression in the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier MATCHES_REGEX sj-device[1-9]-dev*</code></p>
<code>EXISTS</code>	<p>For string data type, true if the run-time value of the attribute exists. This is a unary operator.</p> <p>E.g., <code>RADIUS:IETF:NAS-Identifier EXISTS</code></p>
<code>GREATER_THAN</code>	<p>For integer, time and date data types, true if the run-time value of the attribute is greater than the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Port GREATER_THAN 10</code></p>
<code>GREATER_THAN_OR_EQUALS</code>	<p>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.</p> <p>E.g., <code>RADIUS:IETF:NAS-Port GREATER_THAN_OR_EQUALS 10</code></p>
<code>LESS_THAN</code>	<p>For integer, time and date data types, true if the run-time value of the attribute is less than the configured value.</p> <p>E.g., <code>RADIUS:IETF:NAS-Port LESS_THAN 10</code></p>
<code>LESS_THAN_OR_EQUALS</code>	<p>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.</p> <p>E.g., <code>RADIUS:IETF:NAS-Port LESS_THAN_OR_EQUALS 10</code></p>
<code>IN_RANGE</code>	<p>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.</p> <p>E.g., <code>Date:Date-of-Year IN_RANGE 2007-06-06,2007-06-12</code></p>
<code>MATCHES_ANY</code>	<p>For list data types, true if any of the run-time values in the list matches one of the configured values.</p> <p>E.g., <code>Tips:Role MATCHES_ANY HR,ENG,FINANCE</code></p>
<code>MATCHES_ALL</code>	<p>For list data types, true if all of the run-time values in the list are found in the configured values.</p> <p>E.g., <code>Tips:Role MATCHES_ALL HR,ENG,FINANCE</code>. In this example, if the run-time values of <code>Tips:Role</code> are <code>HR,ENG,FINANCE,MGR,ACCT</code> the condition evaluates to true.</p>

Operator	Description
MATCHES_ EXACT	<p>For list data types, true if all of the run-time values of the attribute match all of the configured values.</p> <p>E.g., <code>Tips:Role MATCHES_ALL HR,ENG,FINANCE</code>. In this example, if the run-time values of <code>Tips:Role</code> are <code>HR,ENG,FINANCE,MGR,ACCT</code> the condition evaluates to false, because there are some values in the configured values that are not present in the run-time values.</p>
BELONGS_ TO_ GROUP	<p>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).</p> <p>E.g., <code>RADIUS:IETF:Calling-Station-Id BELONGS_TO_GROUP Printers</code>.</p>

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

- [Error Codes](#)
- [SNMP Trap Details](#)
- [Important 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 348](#) 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 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](mailto: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

## Lighttpd 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](mailto: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 aheared 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 acknowledgement:
- \* "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 acknowledgement:
- \* "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 licence and distribution terms for any publically available version or
- \* derivative of this code cannot be changed. i.e. this code cannot simply be
- \* copied and put under another distribution licence
- \* [including the GNU Public Licence.] \*/

## OpenLDAP License

The OpenLDAP Public License

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."