Dell Networking W-ClearPass Policy Manager 6.5

User Guide

Copyright Information

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

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

The Dell Networking W-ClearPass Policy Manager (CPPM) platform provides role and device-based network access control across wired, wireless, and Virtual Private Network (VPN) networks. Dell Networking W-ClearPass Policy Manager provides device registration, device profiling, endpoint health assessments, and comprehensive reporting. Dell Networking W-ClearPass Policy Manager also automatically enforce user and endpoint access policies when devices connect to the network using RADIUS, SNMP, or TACACS+ authentication.

Dell Networking W-ClearPass Policy Manager offers user and device authentication based on 802.1X, non-802.1X, and web portal access methods. Multiple authentication protocols like PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP Public can be used concurrently to strengthen security in any environment. Attributes from multiple identity stores such as Microsoft Active Directory, LDAP-compliant directory, ODBC-compliant SQL database, token servers, and internal databases across domains can be used within a single policy for fine-grained control. Additionally, posture assessments and remediation can be added to existing policies at any time.

Dell Networking W-ClearPass Policy Manager, referred as Policy Manager, is the main application of the ClearPass access management platform, and is used to create and enforce policies across a network for all devices and applications. Dell Networking W-ClearPass Policy Manager also includes links to Guest, Insight, and Onboard. OnGuard, Profile features, and some AirGroup configuration items are included within the Policy Manager user interface.

Policy Manager has a built-in profiling service that discovers and classifies all endpoints, regardless of device type. A variety of contextual data such as MAC OUIs, DHCP fingerprinting, and other identity-centric device data can be obtained and used within policies. Stored profiling data is used to identify device profile changes and to dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, ClearPass Policy Manager can automatically deny access. Unmanaged non-802.1X devices such as printers and IP phones can be identified as known or unknown when they connect to the network. The identity of these devices is based on the presence of their MAC address in an external or internal database.

About this Document

The Dell Networking W-ClearPass Policy Manager User Guide provides a general overview of Dell Networking W-ClearPass Policy Manager features and detailed descriptions of the configuration settings used to manage and monitor your Policy Manager deployment.

Getting Started

If you are new to Dell Networking W-ClearPass Policy Manager, refer to the following sections:

- For general descriptions of Dell Networking W-ClearPass Policy Manager features, refer to Dell Networking W-ClearPass Policy Manager Service Components on page 26.
- For a list of common configuration tasks, and information about how to perform each task, refer to Configuration on page 85.

If you are planning a new Dell Networking W-ClearPass Policy Manager deployment, refer to the ClearPass Deployment Guide for work flows, best practices, and example configurations to help you to plan your deployment.

The content in the following sections of this document are presented in an order that matches the Policy Manager WebUI.

To learn more about the specific configurations, fields, and forms available in these sections, refer to the appropriate sections of the following chapters:

- Monitoring on page 1
- Configuration on page 85
- Administration on page 389

Feature Overview

The following sections give a general overview of some of 's features:

- Dell Networking W-ClearPass Policy Manager Service Components on page 26
- Services Architecture and Flow on page 29
- Authentication and Authorization Architecture and Flow on page 30
- Enforcement Architecture and Flow on page 31
- Posture Architecture and Flow on page 33
- Audit Servers on page 34

Dell Networking W-ClearPass Policy Manager Service Components

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

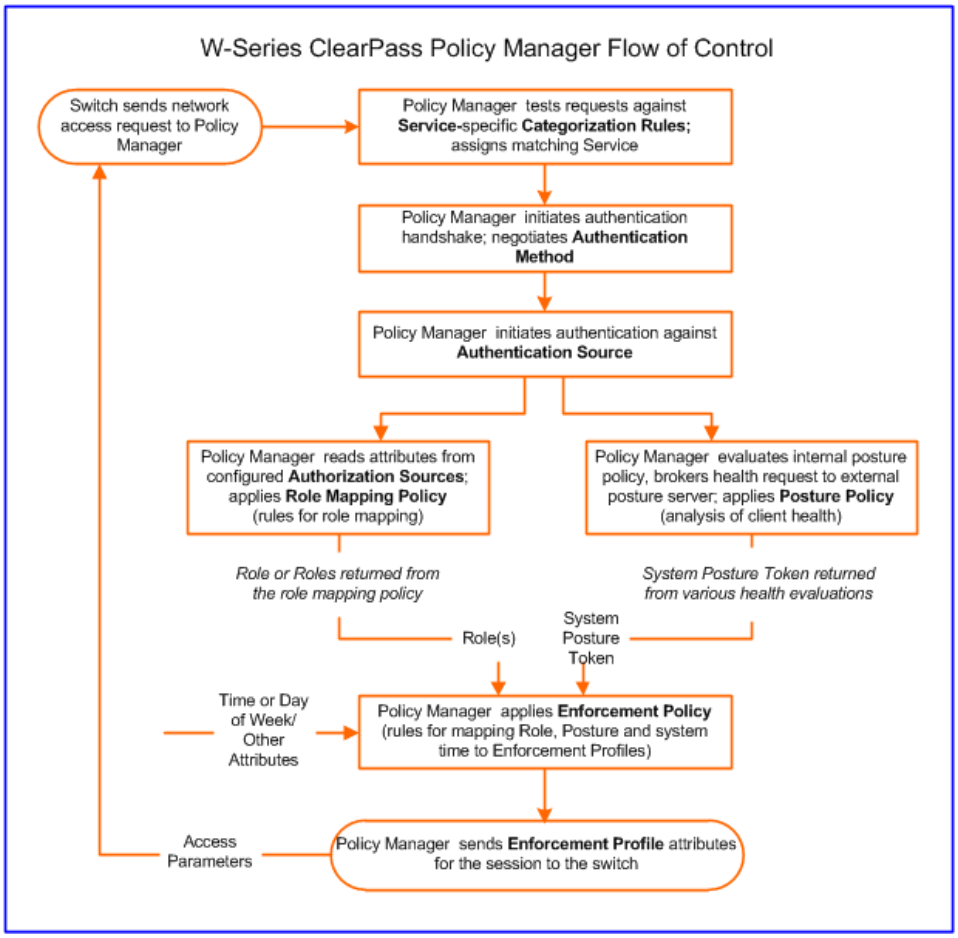
- Unique categorization rules (per service) enable Policy Manager to test access requests (requests) against available services to provide robust differentiation of requests by access method, location, or other network vendor-specific attributes.

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

- By wrapping a specific set of policy components, a service can coordinate the flow of a request from authentication to role and health evaluation to determine the enforcement parameters for network access.

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

Figure 1: *Generic Policy Manager Service Flow of Control*



The following table describes the Policy Manager service components:

Table 1: *Policy Manager Service Components*

Component	Service: Component Ratio	Description

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

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

Table 1: *Policy Manager Service Components (Continued)*

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

Services Architecture and Flow

Architecturally, Policy Manager services are classified into the following:

- **Parents** of their policy components, which are wrapped (hierarchically) and coordinated in processing requests.
- **Siblings** of other Policy Manager services within an order that determines the sequence in which they are tested against requests.

- **Children** of Policy Manager, which test requests against their rules to find a matching service for each request.

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

- Policy Manager tests for the first request-to-service-rule match.
- The matching service coordinates execution of its policy components.
- Those policy components process the request to return enforcement profiles to the network access device and, optionally, posture results to the client.

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

- **Bottom-Up**: Create all policy components (authentication method, authentication source, role mapping policy, posture policy, posture servers, audit servers, enforcement profiles, and enforcement policy) first, as needed, and then create the service using the **Service** creation wizard.
- **Top-Down**: Start with the **Service** creation wizard and create the associated policy components as and when required, all in the same flow.

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

Authentication and Authorization Architecture and Flow

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

- Authentication method
- Authentication source
- Authorization source

Authentication Method

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

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

An authentication method is configurable only for some service types. For more information, see Policy Manager Service Types on page 122. All 802.1X wired and wireless services have an associated authentication method. For example, the MAC_AUTH authentication method can be associated with the MAC authentication service type.

Authentication Source

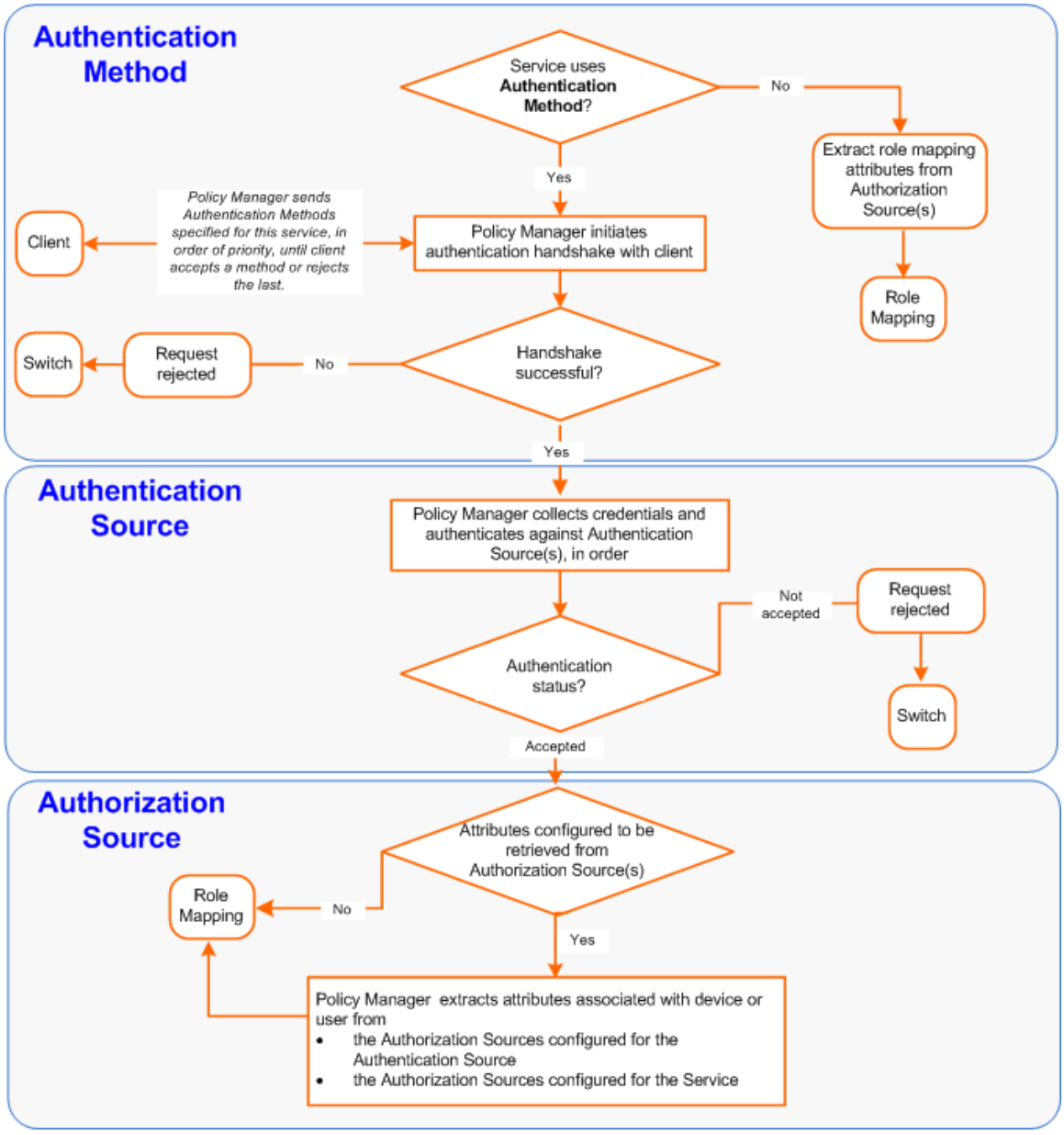
In Policy Manager, an authentication source is the identity store (Active Directory, LDAP directory, SQL DB, token server) against which users and devices are authenticated. Policy Manager first tests whether the connecting entity (the device or user) is present in the ordered list of configured authentication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

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

- Where no authentication source is specified (for example, for unmanageable devices), Policy Manager passes the request to the next configured policy component for this service.
- If Policy Manager does not find the connecting entity in any of the configured authentication sources, it rejects the request.

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

Figure 2: *Authentication and Authorization Flow of Control*



Enforcement Architecture and Flow

To evaluate a request, Policy Manager 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

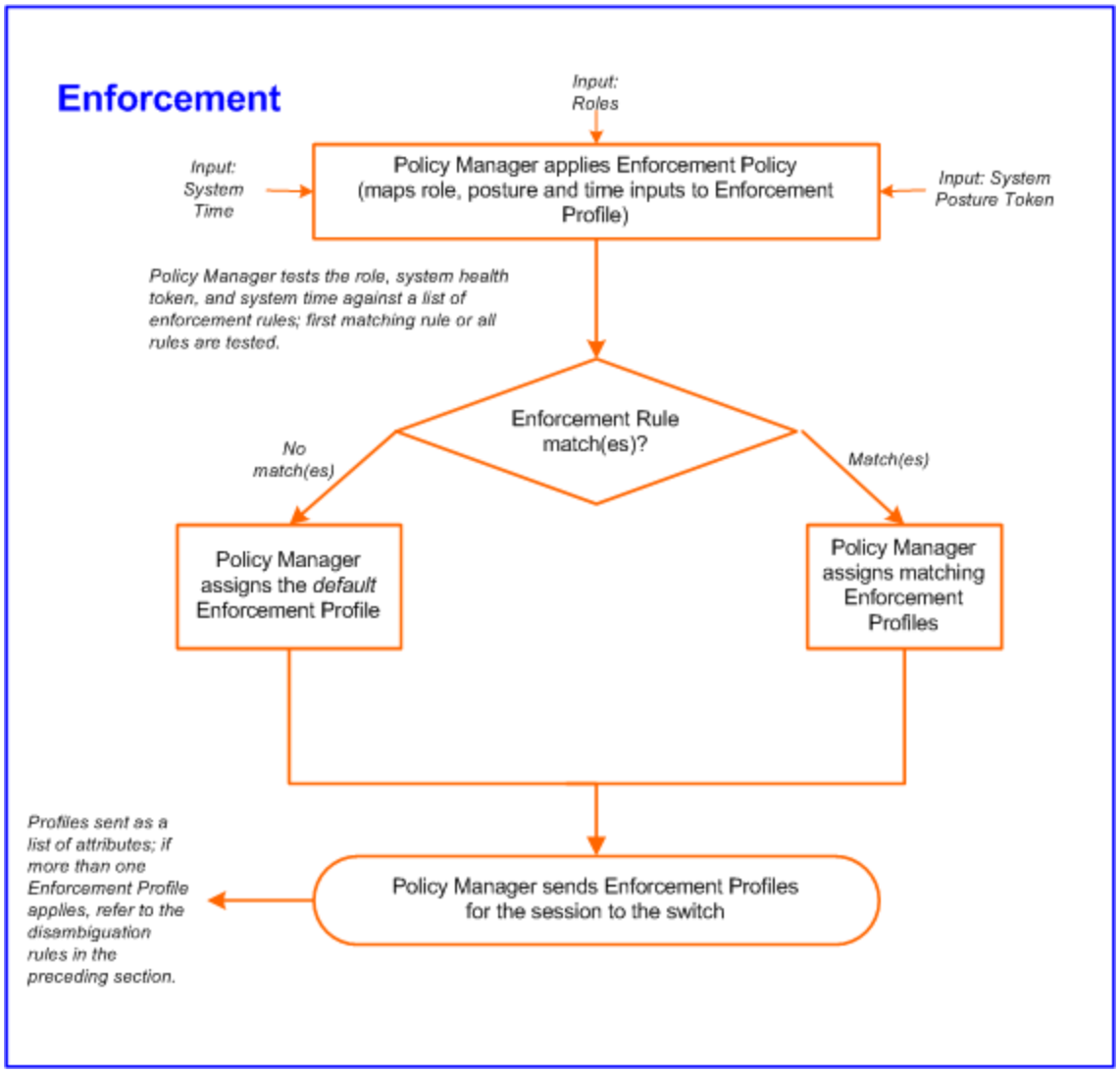
occurs inside of a black box called an enforcement policy.

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 3: *Flow of Control of Policy Manager Enforcement*



Posture Architecture and Flow

Policy Manager supports three types of posture checking: posture policies, posture servers, and audit servers.

Posture Policy

Policy Manager supports four pre-configured posture plug-ins for Windows, one plug-in for Linux®, and one plug-in for Mac OS® X, against which administrators can configure rules that test for specific attributes of client health and correlate the results to return application posture tokens for processing by enforcement policies.

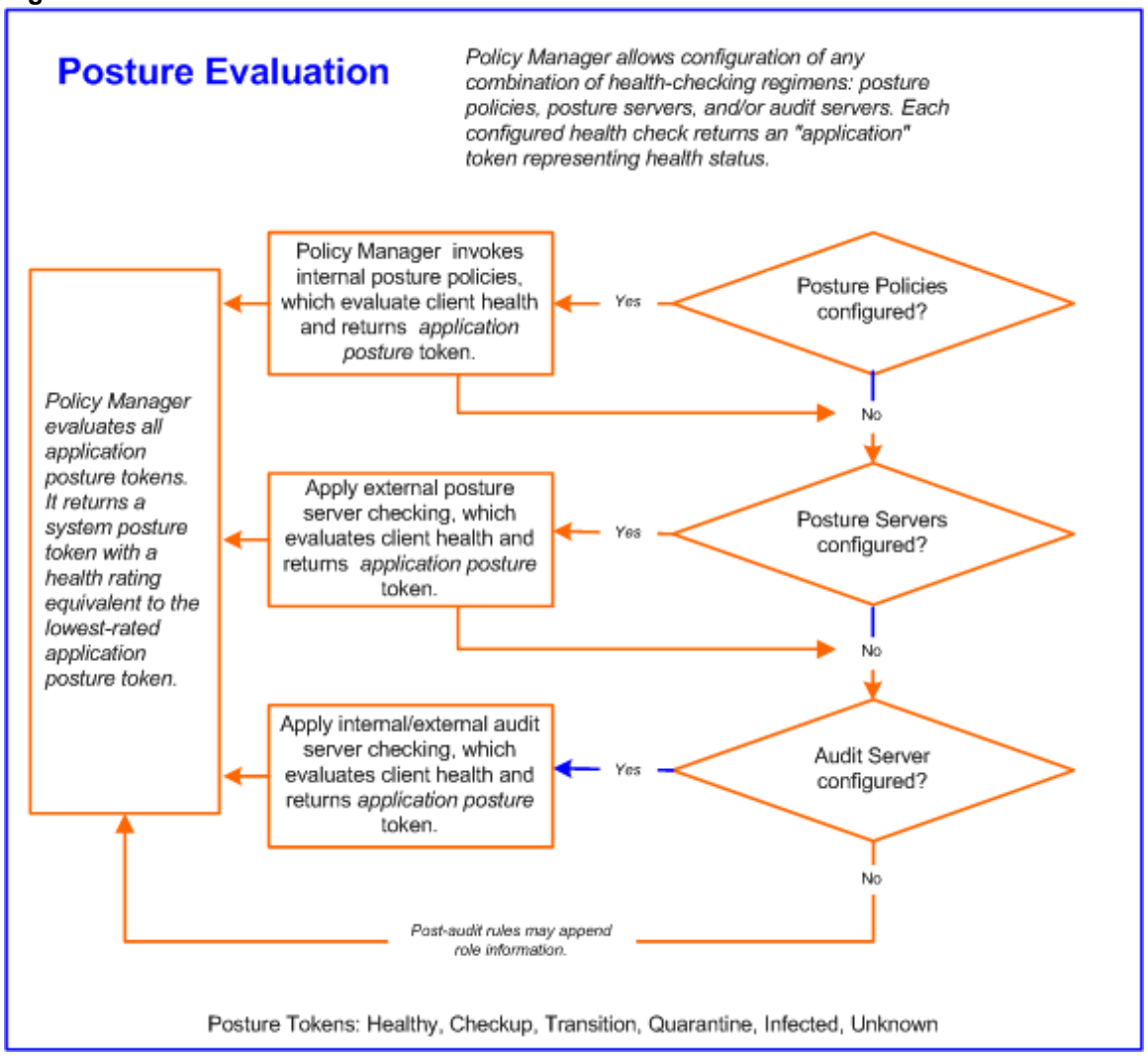
Posture Server

Policy Manager can forward all or part of the posture data received from the client to a posture server. The posture server evaluates the posture data and returns application posture tokens. Policy Manager supports the Microsoft NPS server for Microsoft NAP integration.

Audit Server

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

Figure 4: *Posture Evaluation Process*



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

- Operating system version/type
- Registry keys/services present (or absent)
- Antivirus/antispyware/firewall configuration
- Patch level of different software components
- Peer-to-Peer (P2P) 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.

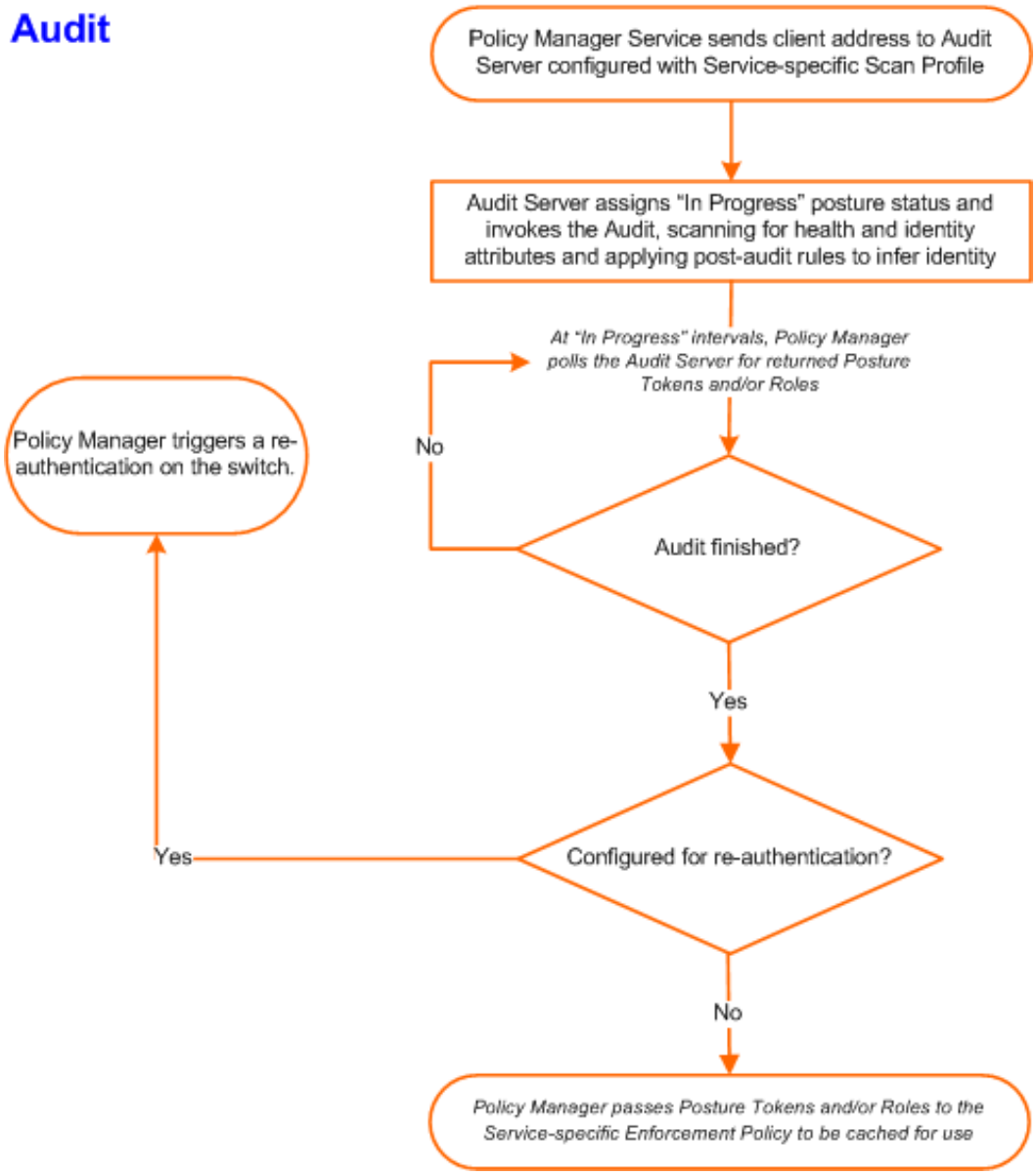
Audit Servers

Audit Servers evaluate posture, role, or both, for unmanaged or unmanageable clients. One example could be clients that lack an adequate posture agent or 802.1X supplicant. For example, printers, PDAs, or guest users might not be able to send posture credentials or identify themselves. A Policy Manager Service can trigger an audit by sending a client ID to a pre-configured audit server, and the server returns attributes for role mapping and posture evaluation.

Audit servers are configured at a global level. Only one audit server can be associated with a service. The flow-of-control of the audit process is shown in the figure.

For more information, see Configuring Audit Servers on page 285.

Figure 5: *Flow of Control of Policy Manager Auditing*



Common Tasks in Policy Manager

When you use Dell Networking W-ClearPass Policy Manager, you may observe many common fields with similar functions in different locations. For example, the option to import or export is available from a list of items such as services, authentication methods, authentication sources, and enforcement policies. This section explains how to perform the following common tasks:

- Importing on page 35
- Exporting on page 36

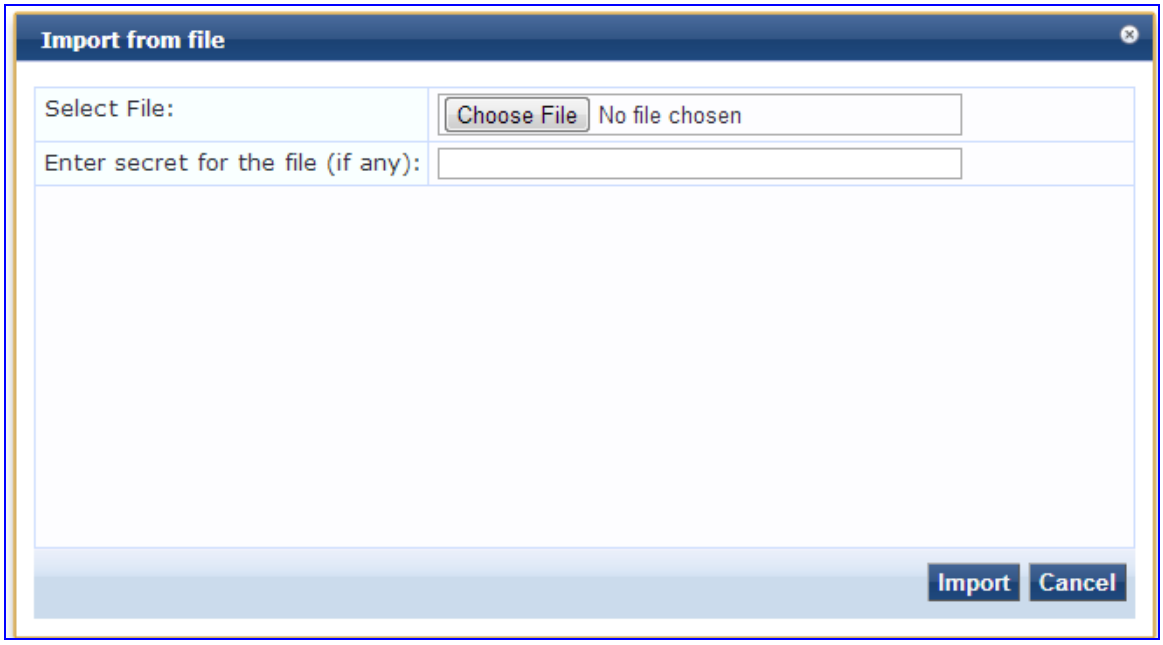
Importing

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

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

1. Click the **Import** link at the top right corner of the configuration page. The **Import from file** dialog box appears.

Figure 6: *Import from file Page*



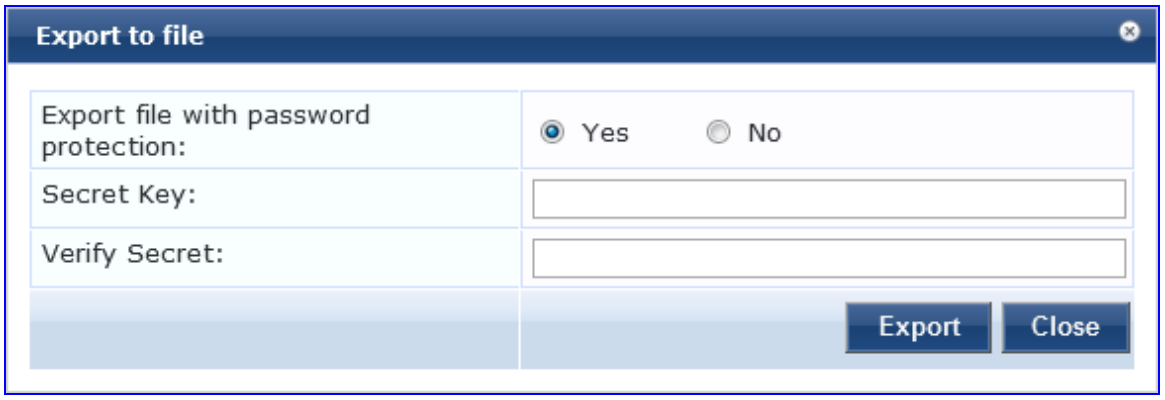
2. Click **Choose File**.
3. Select the file you want to import. You must select an XML file in the correct format. If you have exported files from different places from Policy Manager, ensure that you are selecting the correct file. See the *Dell Networking W-ClearPass Policy Manager Configuration API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

Exporting

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

1. Click the **Export** link at the top-right corner of the configuration page. The **Export to File** dialog appears.

Figure 7: *Export to File*



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

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

NOTE

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

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

Table 2: *Dashboard Layout Parameters*

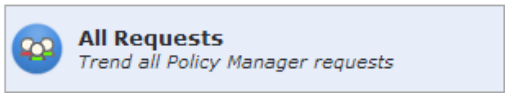
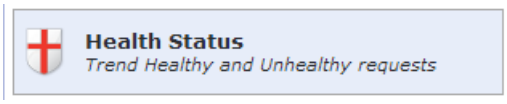
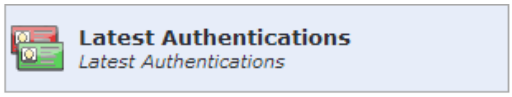
	Drag and drop the **All Requests** widget to **Dashboard** to view the graph that displays all requests processed by Policy Manager over the past week. Processed requests include RADIUS, TACACS+, and WebAuth requests. Clicking on each bar in the graph drills down to the **Access Tracker** page and shows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

Table 2: *Dashboard Layout Parameters (Continued)*

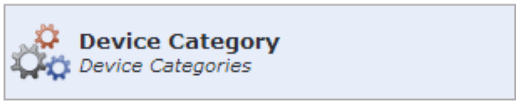
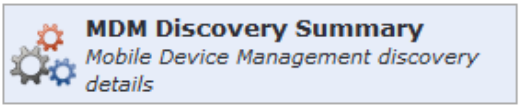
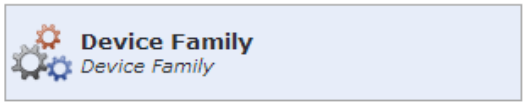
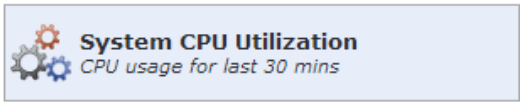
	Drag and drop the **Device Category** widget to **Dashboard** to view the chart that shows the graph of all profiled devices categorized into the following built-in categories: • SmartDevices • Access Points • Computer • VOIP phone • Datacenter Appliance • Printer • Physical Security • Game Console • Routers • Unknown • Conflict **Unknown** devices are the devices that are not profiled by the profiler. **Conflict** indicates a conflict occurred in the categorization of the device. For example, if the device category derived from the HTTP User Agent string does not match with the category derived from DHCP fingerprinting, then a conflict is flagged and the device is marked as **Conflict**.
	Drag and drop the **MDM Discovery Summary** widget to **Dashboard** to view the charts that show the endpoints discovered. The endpoints are displayed in separate charts based on the endpoint's operating system. Clicking a chart drills down to the **Configuration** > **Identity** > **Endpoints** page with the results with the filters applied depends on the operating system selected. For example, if you click the Android devices chart, you can view the list of only Android devices in the **Configuration** > **Identity** > **Endpoints** page.
	Drag and drop the **Device Family** widget to **Dashboard** to view each of the built-in device categories. For example, selecting **SmartDevice** shows the different kinds of smart devices identified by **Profile**.
	Drag and drop the **System CPU Utilization** widget to **Dashboard** to view the CPU usage for the last 30 minutes. The utilization is presented in ten-minute increments. The widget displays the CPU utilization time in minutes and percentage for users, system, IO Wait time, and Idle time. For example, if you want to view the system CPU utilization for the period from 14:50 to 15:00, hover the mouse over the red line in the graph.
	Drag and drop the **Request Processing Time** widget to **Dashboard** to view the trend of total request processing time.

Table 2: *Dashboard Layout Parameters (Continued)*

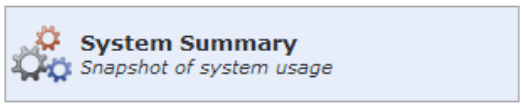
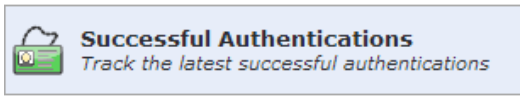
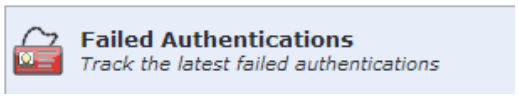
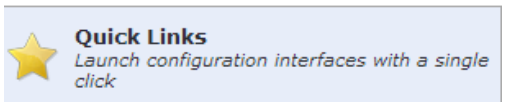
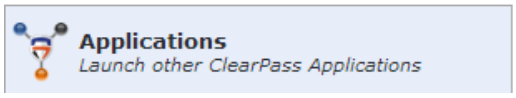
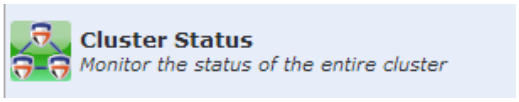
	Drag and drop the **System Summary** widget to **Dashboard** to view the **Percentage Used** statistics for the following: • Main Memory • Swap Memory • Disk • Swap Disk
	Drag and drop the **Successful Authentications** widget to **Dashboard** to view a table with the latest successful authentications.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

Table 2: *Dashboard Layout Parameters (Continued)*

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

The Monitoring features in Policy Manager provide access to live monitoring of components and other functions. Dell Networking W-ClearPass Policy Manager includes the following Monitoring features:

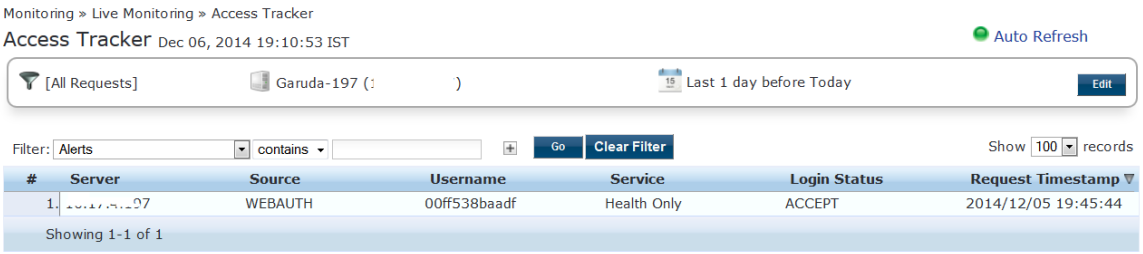
- Live Monitoring
  - Live Monitoring: Access Tracker on page 43
  - Live Monitoring: Accounting on page 52
  - Live Monitoring: Analysis and Trending on page 68
  - Live Monitoring: Endpoint Profiler on page 69
  - Live Monitoring: OnGuard Activity on page 62
  - Live Monitoring: System Monitor on page 70
- Audit Viewer
  - Audit Viewer on page 75
- Event Viewer
  - Event Viewer on page 77
- Data Filters
  - Data Filters on page 79
- Blacklisted Users
  - Blacklisted Users on page 82

Live Monitoring: Access Tracker

The **Access Tracker** table provides a real-time display of per-session access activity on the selected server or domain. To view this page, navigate to **Monitoring > Live Monitoring > Access Tracker**.

The following figure displays the **Access Tracker** table:

Figure 8: *Live Monitoring > Access Tracker Table*



The following table describes the information in the **Access Tracker** table:

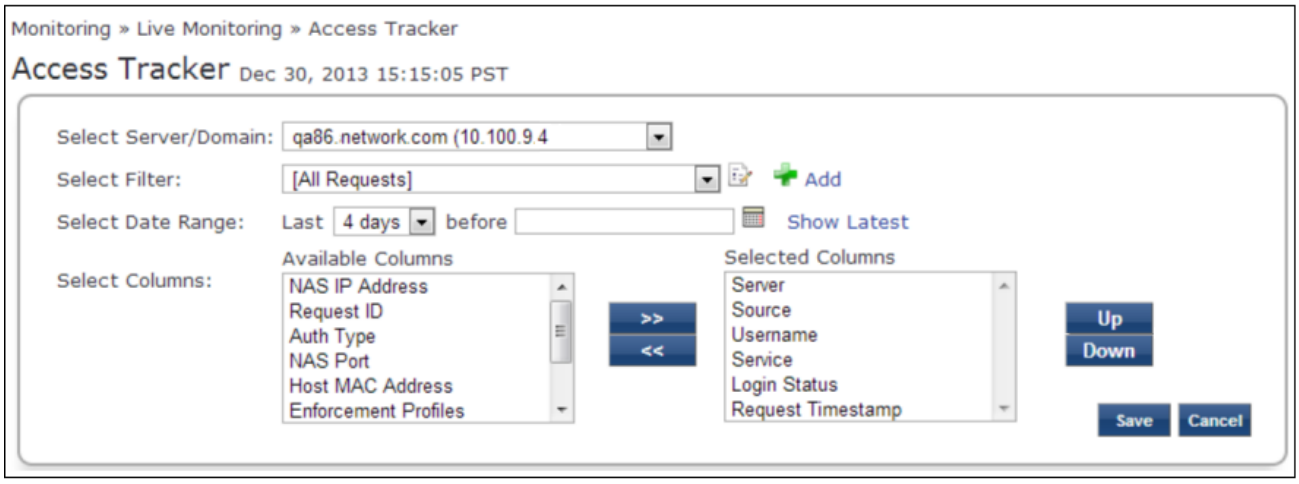
Table 3: *Access Tracker Table Parameters*

Parameter	Description
Server	Displays the IP address of the server.
Source	Displays the authentication source for the session. For example, TACACS or web authentication.
Username	Displays the username or MAC address of the user.
Service	Displays the name of the service. For example, Health Only, MAC authentication, or AirGroup Authorization.
Login Status	Displays the status of the request, such as **accept**, **reject**, or **timeout**.
Request Timestamp	Displays the date and time when the status was last updated.

Editing the Access Tracker

Change the **Access Tracker** parameters by clicking the **Edit** button. The **Access Tracker edit** page appears, as displayed in the following figure:

Figure 9: *Access Tracker Page (edit mode)*



The table below describes the configuration parameters on the **Access Tracker Edit** page:

Table 4: *Access Tracker Edit Page Parameters*

Parameter	Description
Select Server/Domain	Displays information for the selected server or domain on the **Access Tracker** page. Select all the servers to display transactions from all nodes in the Policy Manager cluster.
Select Filter	Select a filter category to filter the displayed data. For a description of available filters, see Data Filters on page 79.
Modify Filter	Click the  icon to modify the current data filter. For more information, see Data Filters on page 79.
Add Filter	Click the  icon to add a data filter. The **Data Filters** page opens. For more information, see Data Filters on page 79.
Select Date Range	Click the **Last** drop-down list to select the start of the range of dates for which the **Access Tracker** table displays data. Available options are 1-6 days, or 1 week.
Select Date	Click the  icon to select a date.
Show Latest	Click **Show Latest** to set the date in the **before** field to the current date.
Select Columns	This section displays the following two fields: • **Available Columns**: displays the data column available to display in an **Access Tracker** table. • **Selected Columns:** displays the data columns currently selected for display. To move a column name from one field to another, select the column name and click the left or right arrows. To change the order in which the columns are displayed, click a column name in the **Selected Columns** field and click the **Up** or **Down** buttons.

Viewing Access Tracker Session Details

Click any session in the **Access Tracker** table to display the **Request Details** window with details about that session. The information in this window varies, depending upon the session selected. Refer to the following sections for more information specific types of information that can appear on each tab of the **Request Details** page:

- Summary Tab on page 45
- Input Tab on page 46
- Output Tab on page 48
- Alerts Tab on page 49
- Viewing Access Tracker Session Details on page 45
- Access Control Capabilities on page 50

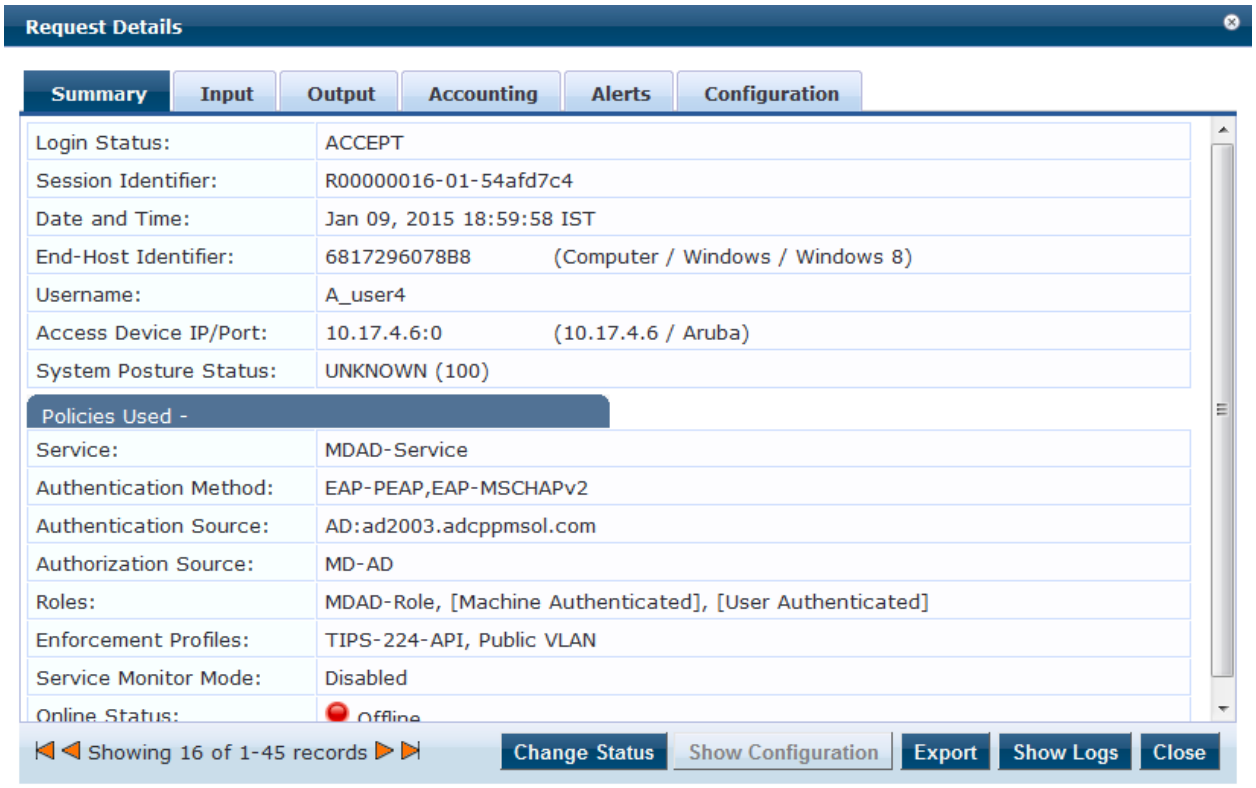
Summary Tab

This tab shows a summary view of the transaction including policies that are applied and protocol-specific attributes. Click any table row in the **Monitoring > Live Monitoring > Access Tracker** page to view the

Summary tab.

The following figure displays the **Summary** tab:

Figure 10: *Request Details - Summary Tab*

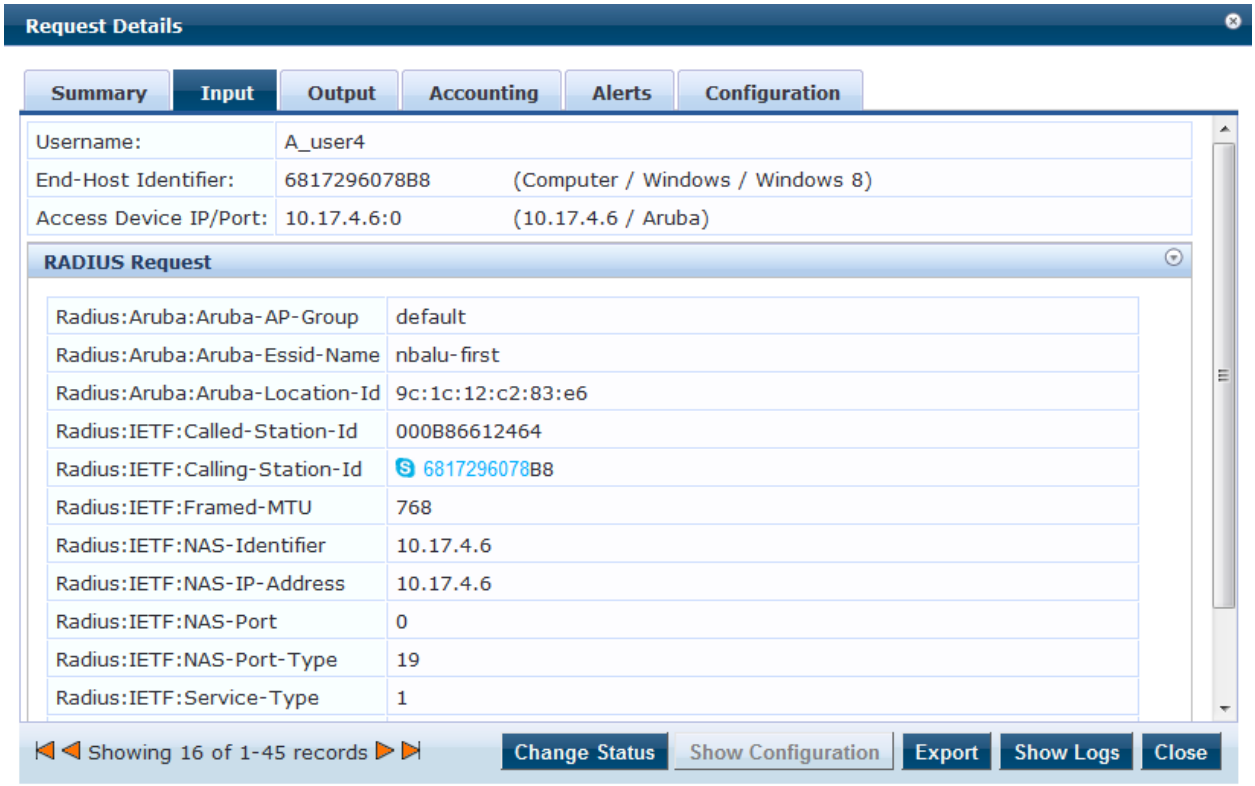


Input Tab

This tab shows protocol-specific attributes that Policy Manager received in a transaction request, including authentication and posture details (if available). The **Input** tab also shows computed attributes that Policy Manager derived from the request attributes. Click any table row in the **Monitoring > Live Monitoring > Access Tracker** page to view the **Input** tab. All of these attributes can be used in role mapping rules.

The following figure displays the **Request Details - Input** tab:

Figure 11: *Request Details - Input tab*

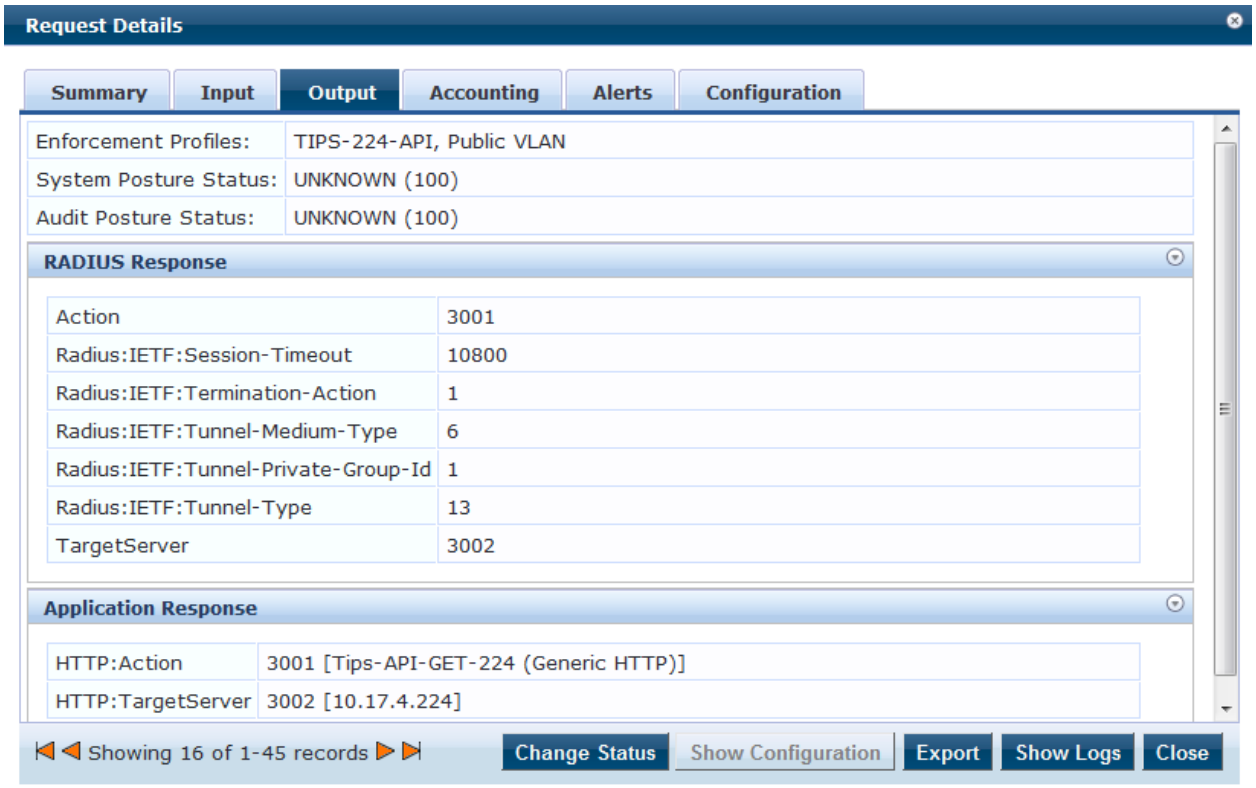


Output Tab

This tab shows the attributes that were sent to the network device (switch or controller) and the posture-capable endpoint (For example, MAC devices). Click any table row in the **Monitoring > Live Monitoring > Access Tracker** page to view the **Output** tab.

The following figure displays the **Request Details - Output** tab:

Figure 12: *Request Details - Output tab*



NOTE

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

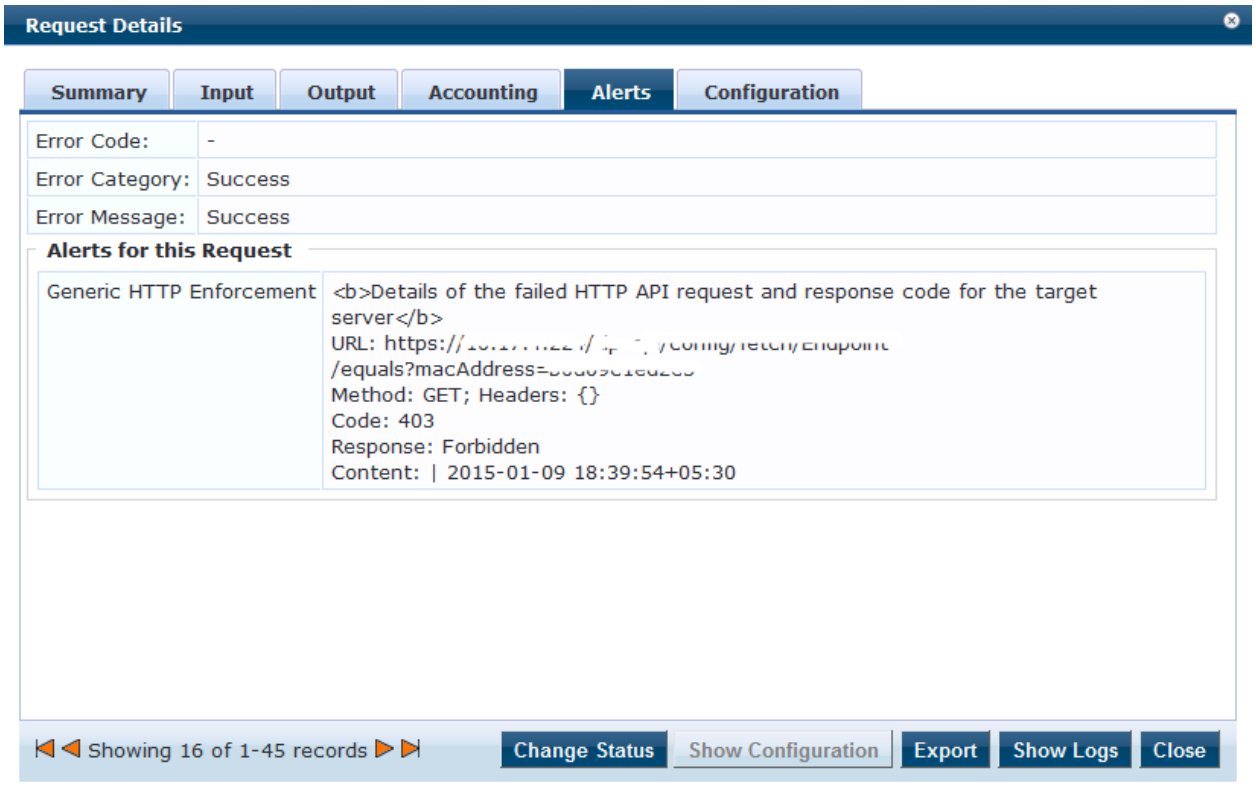
Administrators can view the posture response and posture evaluation with accurate results. For example, the administrator can view details such as missing registry keys and the reasons for a failed registry key check.

Alerts Tab

This tab shows information about a session with an error. The **Alerts** tab only appears in the **Request Details** window when you access the **Monitoring > Live Monitoring > Access Tracker** page. Click a table row for a session that has an error to view the **Alerts** tab. For example, if you select a row where the **Login** status displays a TIMEOUT or REJECT status.

The following figure displays the **Request Details - Alerts** tab:

Figure 13: *Request Details - Alerts tab*

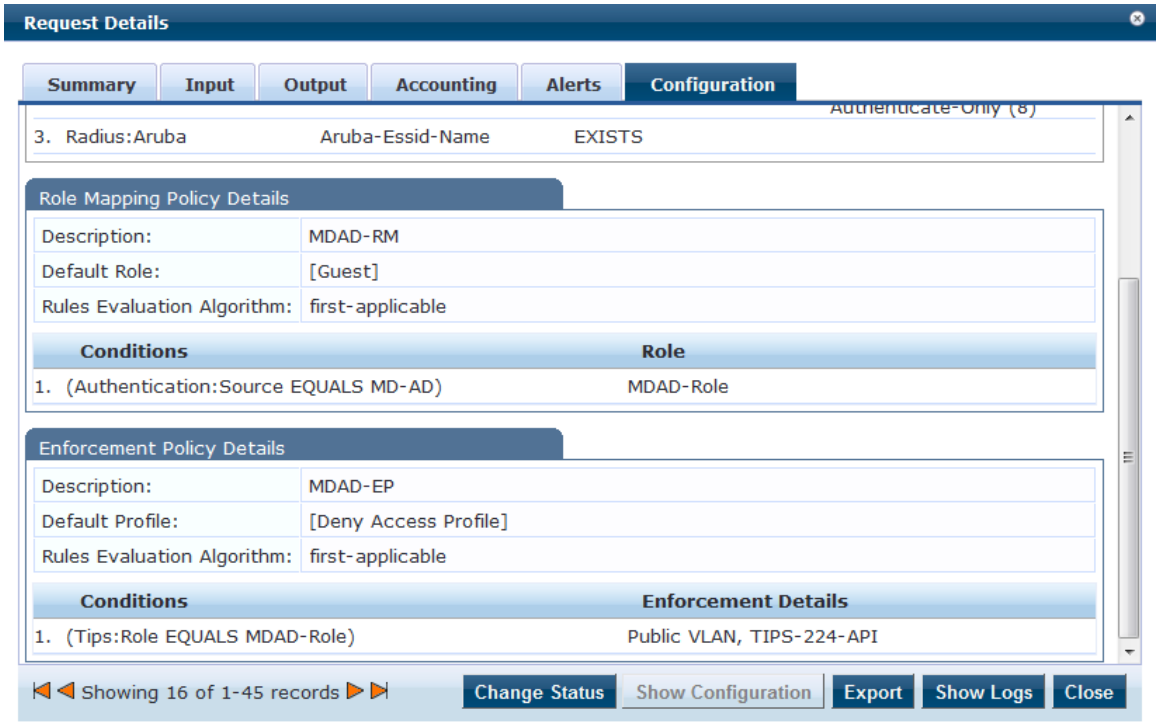


Configuration Tab

This tab shows the attributes that Policy Manager received in a transaction request, including service rules, role mapping policies used, authorization sources, and enforcement policies used (if available). Click any table row in the **Monitoring** > **Live Monitoring** > **Access Tracker** page to view the **Configuration** tab.

The following figure displays the **Request Details - Configuration** tab:

Figure 14: *Request Details - Configuration Tab*

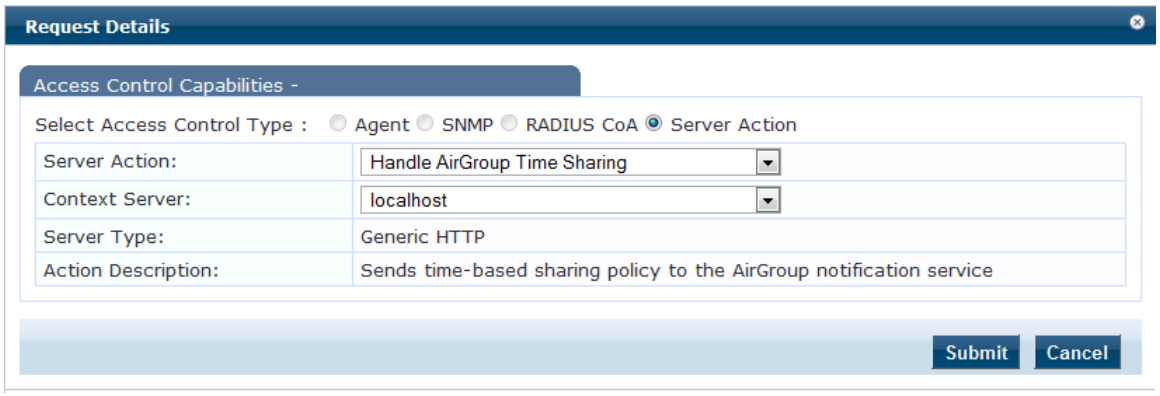


Access Control Capabilities

This page shows a summary view of the transaction, including policies that are applied and protocol-specific attributes. You can use the **Access Control Capabilities** page to view or change the access control type. The **Access Control Capabilities** page is displayed if you click the **Change Status** button in the **Request Details** screen. The **Change Status** button is enabled only if you use the RADIUS and WebAuth authentication types.

The following figure displays the **Access Control Capabilities** tab:

Figure 15: *Access Control Capabilities*



The following table describes the **Request Details - Access Control Capabilities** page parameters:

Table 5: *Request Details - Access Control Capabilities Page Parameters*

Parameter	Description

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

Server Action	Select the server action that is performed on endpoints. You can select from the following options: • Check Point Login • Check Point Logout • Fortinet Login • Fortinet Logout • Handle AirGroup Time Sharing • Nmap scan (Appears only if the server action contains a valid IP address) • Snmp Scan (Appears only if the server action contains a valid IP address)
Context Server	Enter a valid server name. You can enter an IP address or domain name.

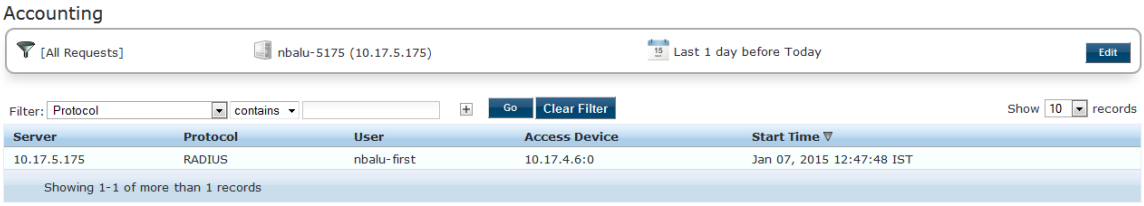
Table 5: *Request Details - Access Control Capabilities Page Parameters (Continued)*

Parameter	Description
Server Type	Displays the server type configured when the server action was configured.
Action Description	Specifies the description of the action. For example, the description can be "Delete all information stored" if the configured action is **Remote Wipe**.

Live Monitoring: Accounting

The **Monitoring > Live Monitoring > Accounting** page provides a dynamic report that describes session access, as reported by the network access device by means of RADIUS or TACACS+ accounting records. The following figure displays the **Live Monitoring** > **Accounting** page:

Figure 16: *Live Monitoring > Accounting Page*



The following table describes the **Accounting** parameters:

Table 6: *Accounting Page Parameters*

Parameter	Description
Server	Specifies the IP address of the host name.
Protocol	Specifies the protocol used.
User	Displays the user name.
Access Device	Displays the IP address of the device.
Start Time	Displays the date and time.

NOTE

You can click any row in this table to drill down and display the corresponding **Accounting Record Details** page for the session. For details, see RADIUS Accounting Details on page 53 and TACACS+ Accounting Details on page 60

Modifying the Accounting Table

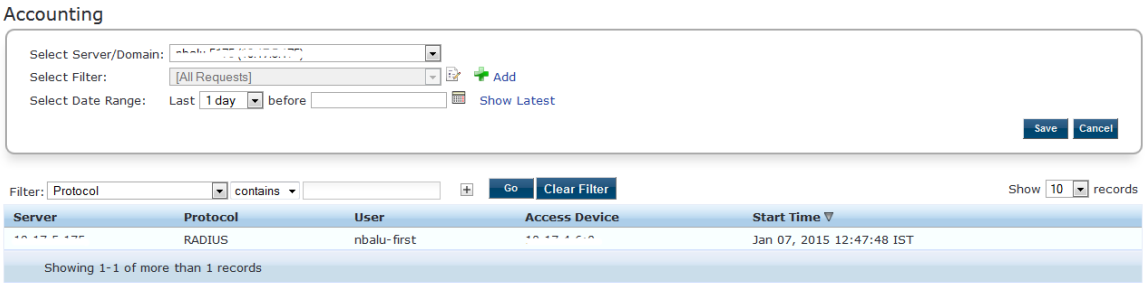
You can filter or modify the information displayed in this table by creating a filter, or selecting a different server, domain, or time range. To filter the data currently displayed in the **Accounting** table,

1. Navigate to the **Monitoring > Live Monitoring > Accounting** page.
2. Click the **Filter** field and select **Protocol**, **User**, or **Access Device** to filter the data by a string in the protocol, user name or access device fields.

3. Click the **Contains** drop-down list and indicate whether the table should display data that contains or does not contain the text string in the adjacent field.
4. Enter an alphanumerical string into the filter text box.
5. Click **Go**.

The following figure displays the **Accounting Page - Edit Mode**:

Figure 17: *Accounting Page - Edit Mode*



The following table describes the Accounting Page - Edit Mode parameters:

Table 7: *Accounting Page - Edit Mode Parameters*

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

RADIUS Accounting Details

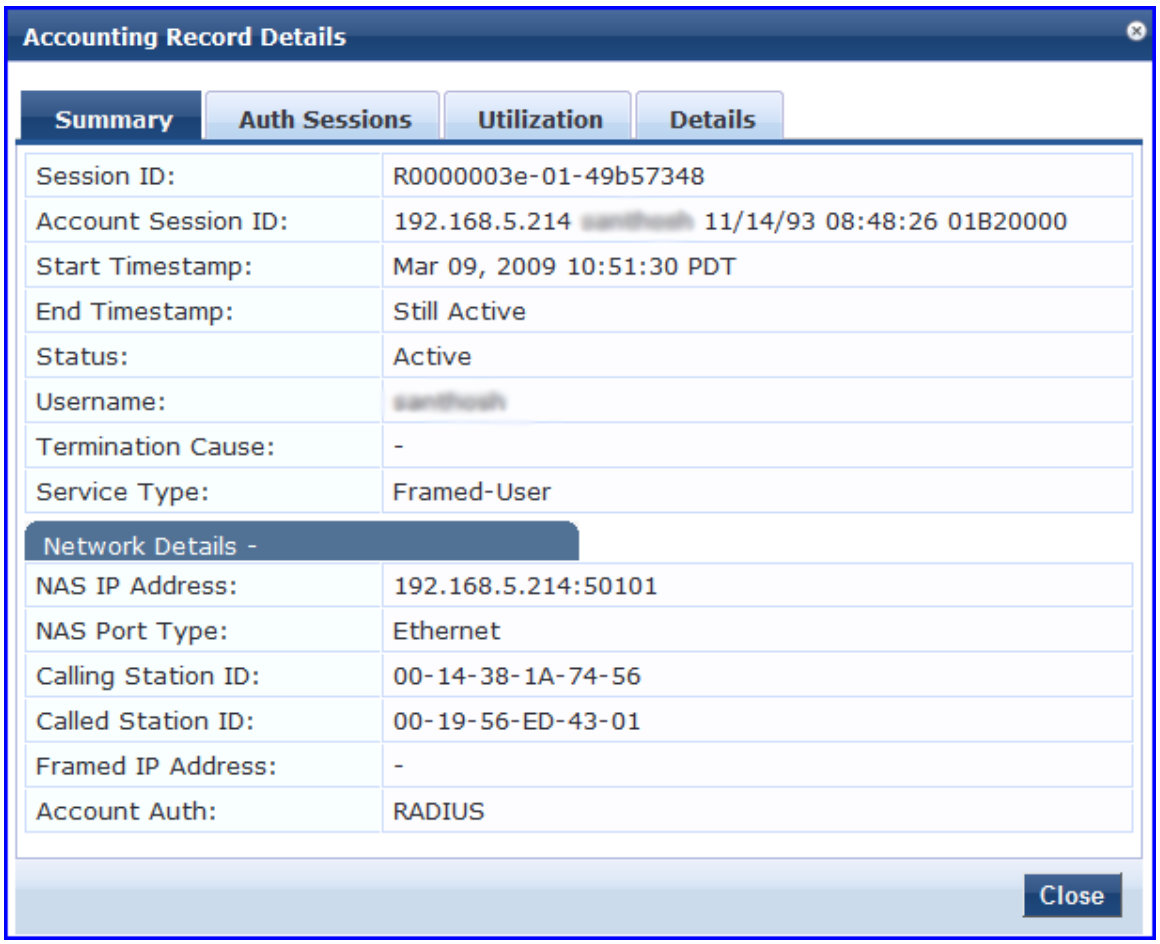
You can click any row in the Accounting table to drill down and display the corresponding **Accounting Record Details** page for the session. Refer to the following sections for more information specific types of information that can appear on each tab for the RADIUS accounting records:

- RADIUS Accounting Record Details - Summary Tab
- RADIUS Accounting Record Details - Auth Sessions Tab
- RADIUS Accounting Record Details - Utilization Tab
- RADIUS Accounting Record Details - Details Tab

RADIUS Accounting Record Details - Summary Tab

The **Accounting Record Details - Summary** tab shows a summary view of the transaction including session IDs, timestamp, and network details for the RADIUS protocol. The following figure displays the **RADIUS Accounting Record Details - Summary** tab:

Figure 18: *RADIUS Accounting Record Details Summary Tab*



The following table describes the configuration parameters on the **RADIUS Accounting Record Details - Summary** tab:

Table 8: *RADIUS Accounting Record Details Summary Tab Parameters*

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

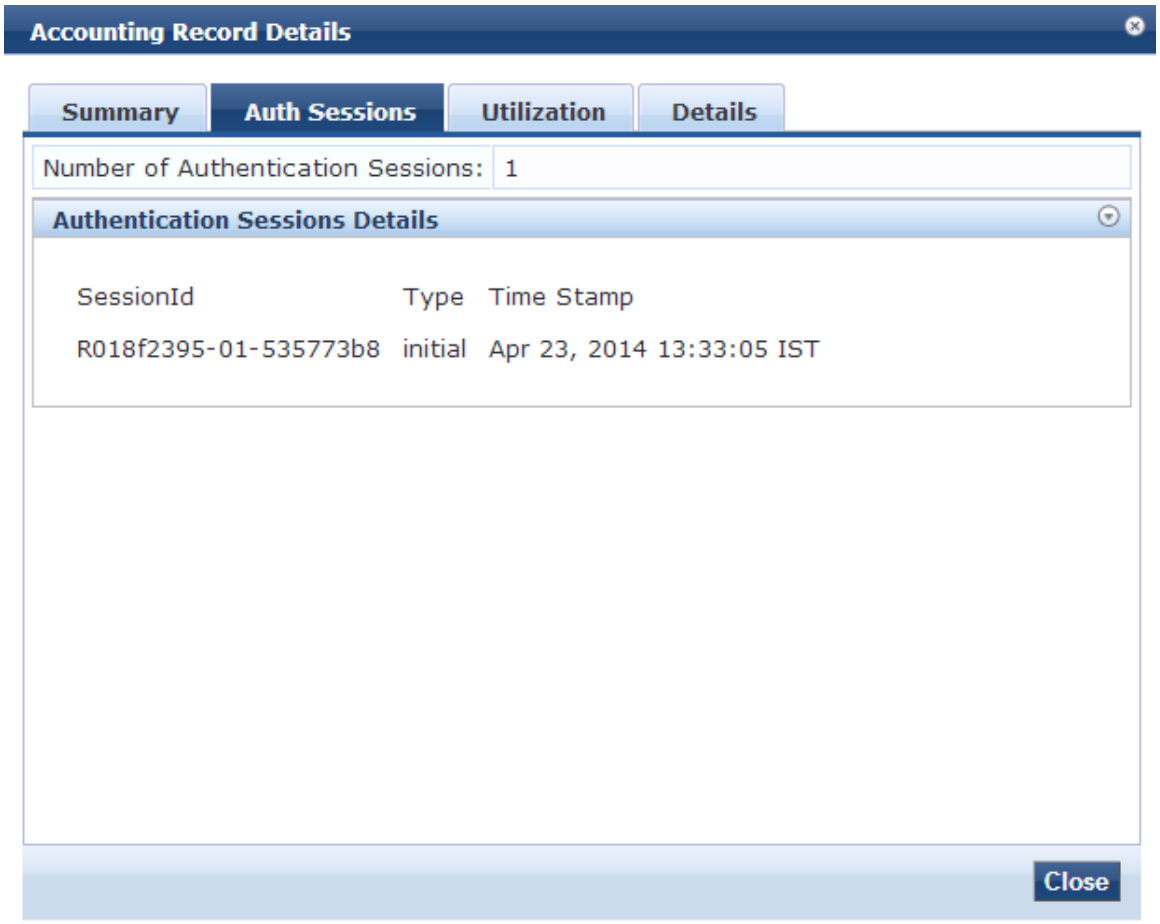
Table 8: *RADIUS Accounting Record Details Summary Tab Parameters (Continued)*

Parameter	Description
Username	Username associated with this record.
Termination Cause	Specifies the reason for termination of this session.
Service Type	Shows the value of the standard RADIUS attribute service type.
Network Details	
NAS IP Address	Shows the IP address of the network device.
NAS Port Type	Shows the access methods. For example, Ethernet, or 802.11 Wireless.
Calling Station ID	Specifies the MAC address of the client that is supported by Policy Manager.
Called Station ID	Shows the MAC Address of the network device.
Framed IP Address	Shows the IP Address of the client (if available).
Account Auth	Specifies the type of authentication. Here this specifies RADIUS authentication.

RADIUS Accounting Record Details - Auth Sessions Tab

This section describes the parameters of the **Accounting Record Details - Auth Sessions** tab for the RADIUS protocol. The following figure displays the the **Accounting Record Details- Auth Sessions** tab:

Figure 19: *RADIUS Accounting Record Details - Auth Sessions Tab*



The following table describes the **RADIUS Accounting Record Details- Auth Sessions** parameters:

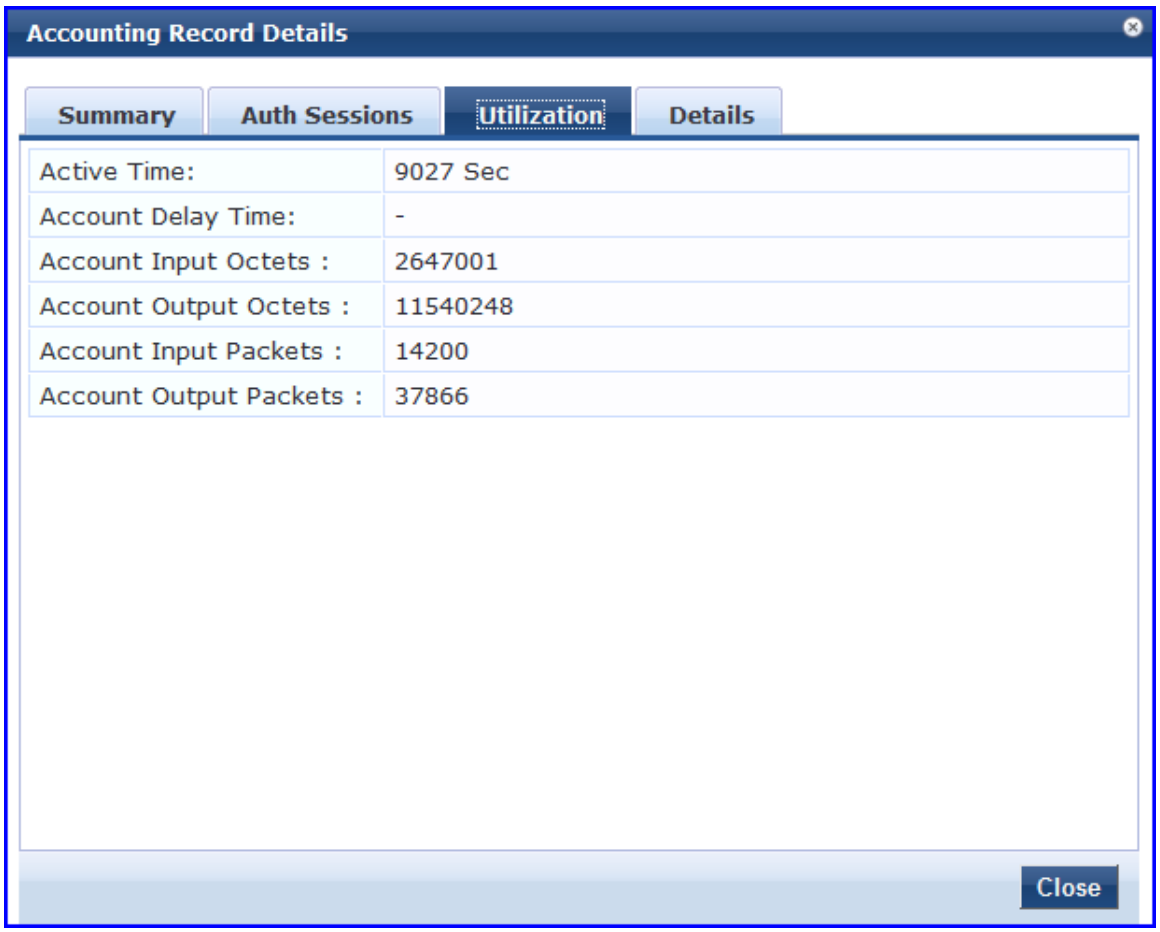
Table 9: *RADIUS Accounting Record Details Auth Sessions Tab Parameters*

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

RADIUS Accounting Record Details - Utilization Tab

This section describes the parameters of the **Accounting Record Details - Utilization** tab for the RADIUS protocol. The following figure displays the **RADIUS Accounting Record Details - Utilization** tab:

Figure 20: *RADIUS Accounting Record Details - Utilization Tab*



The following table describes the configuration parameters on the **RADIUS Accounting Record Details - Utilization** tab:

Table 10: *RADIUS Accounting Record Details - Utilization Tab Parameters*

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

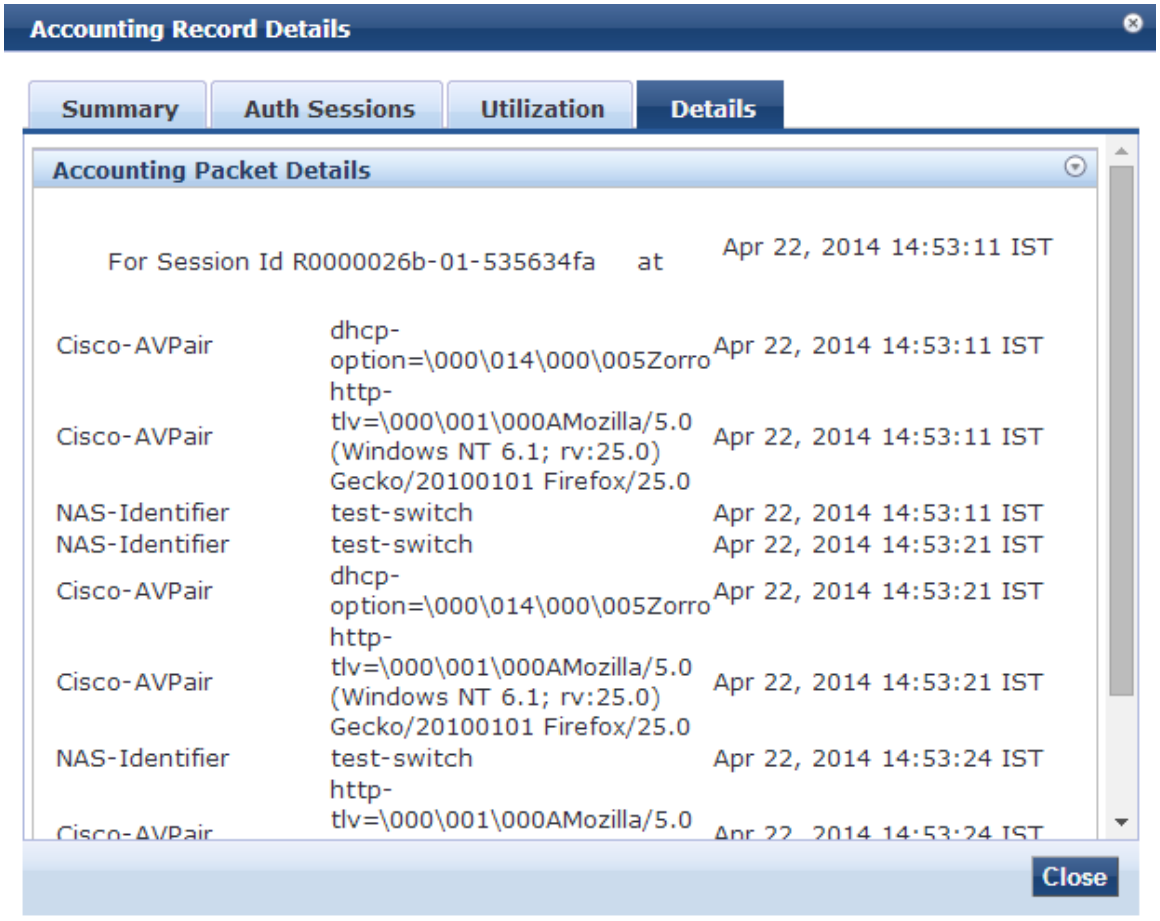
Table 10: *RADIUS Accounting Record Details - Utilization Tab Parameters (Continued)*

Parameter	Description
Account Output Octets	
Account Input Packets	Specifies the packets sent and received from the device port during the session.
Account Output Packets	

RADIUS Accounting Record Details - Details Tab

This section describes the parameters of the **Accounting Record Details - Details** tab for the RADIUS protocol. The following figure displays the example of the **RADIUS Accounting Record Details - Details** tab:

Figure 21: *RADIUS Accounting - Details Tab*



The following table describes the configuration parameters on the **RADIUS Accounting Record Details - Details** tab:

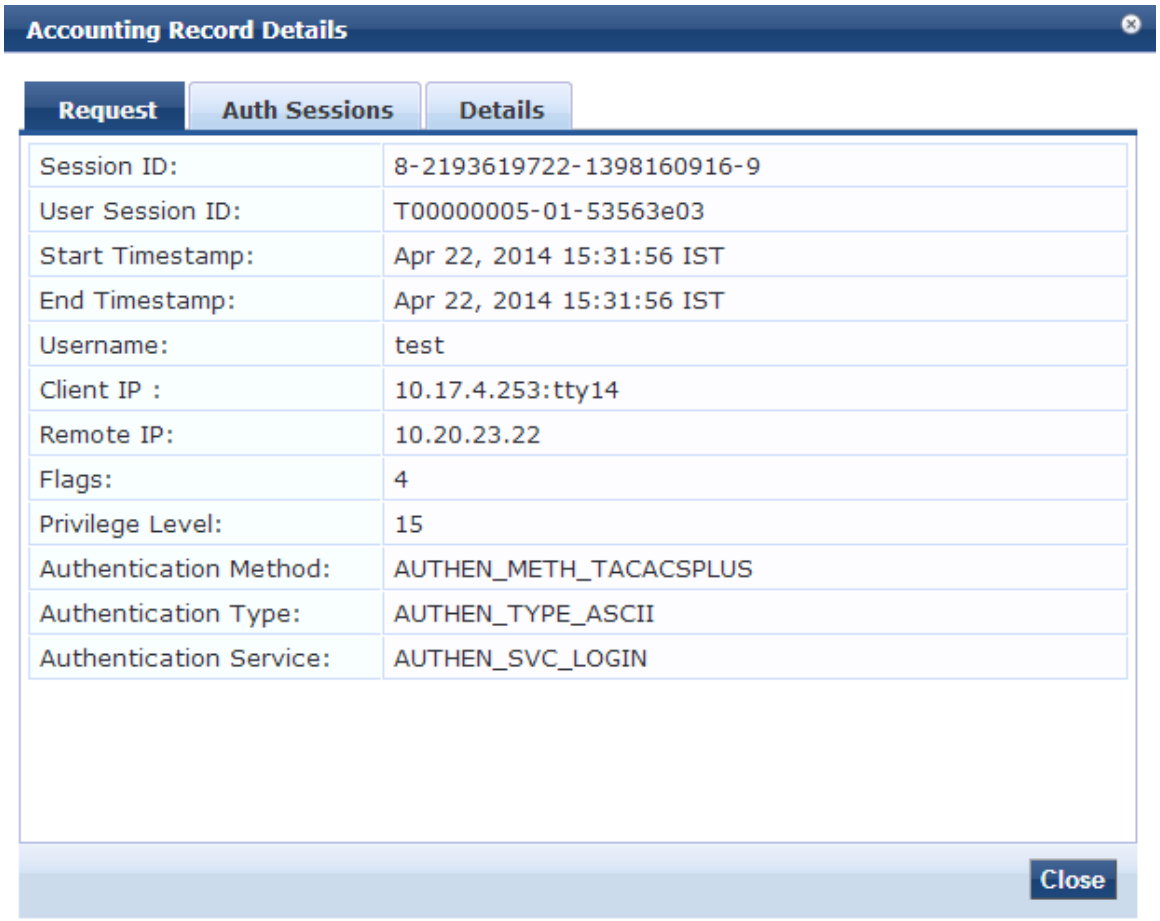
Table 11: *RADIUS Accounting Record - Details Tab Parameters*

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

TACACS+ Accounting Record Details - Request Tab

This section describes the parameters of the **Accounting Record Details - Request Sessions** tab for the TACACS+ protocol. The following figure displays the **TACACS+ Accounting Record Details - Request** tab:

Figure 22: *TACACS+ Accounting Record Details - Request Tab*



The following table describes the configuration parameters on the **TACACS+ Accounting Record - Request** tab:

Table 12: *TACACS+ Accounting Record Request Tab Parameters*

Parameter	Description
Session ID	Specifies the Session ID, a unique ID, associated with a request.
User Session ID	Specifies a session ID that correlates authentication, authorization, and accounting records.
Start and End Timestamp	Shows the start and end time of the session.
Username	Shows the username associated with this record.
Client IP	Shows the IP address and tty of the device interface.
Remote IP	Shows the IP address from which Admin is logged in.
Flags	Shows the identifier corresponding to start, stop, or update accounting record.
Privilege Level	Specifies the privilege level of the administrator. The range is from 1 (lowest) to 15 (highest).
Authentication Method	Identifies the authentication method used for the access.
Authentication Type	Identifies the authentication type used for the access.
Authentication Service	Identifies the authentication service used for the access.

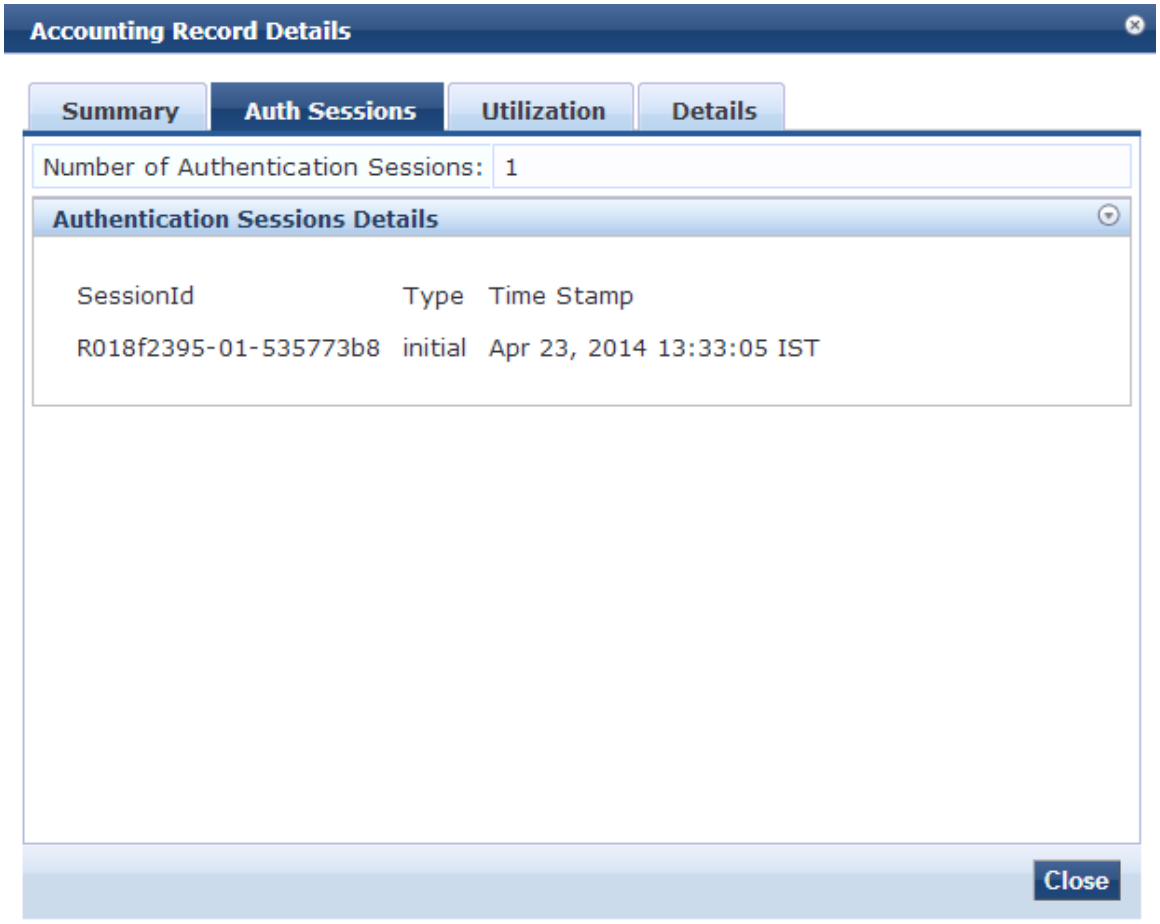
TACACS+ Accounting Details

You can click any row in the **Accounting** table to drill down and display the corresponding **Accounting Record Details** page for the session. The following sections describe the accounting record details for TACACS+ accounting records.

TACACS+ Accounting Record Details - Auth Sessions Tab

This section describes the parameters of the **Accounting Record Details - Auth Sessions** tab for the TACACS+ protocol. The following figure displays the **TACACS+ Accounting Record Details - Auth Sessions** tab:

Figure 23: *TACACS+ Accounting Record Details - Auth Sessions Tab*



The following table describes the configuration parameters on the **TACACS+ Accounting Record Details - Auth Sessions** tab:

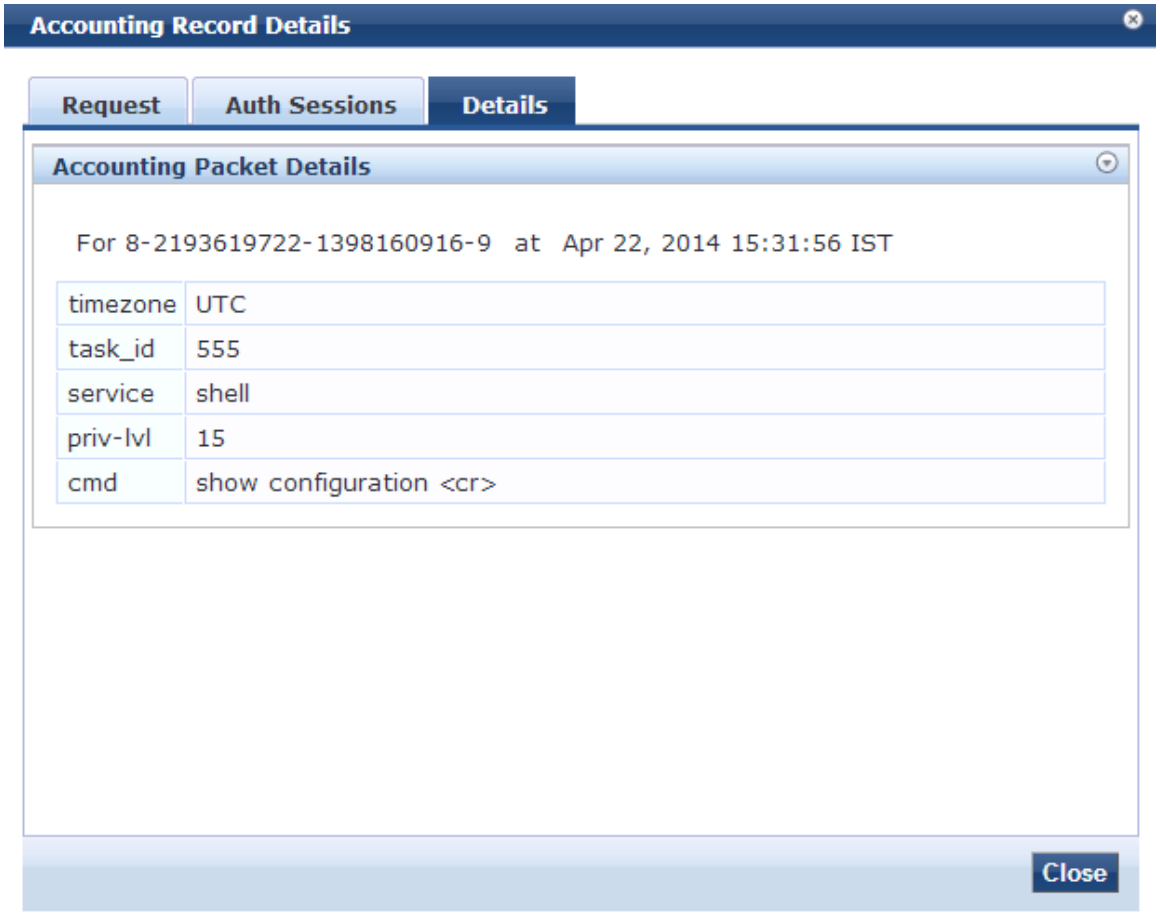
Table 13: *TACACS+ Accounting Record Details Auth Sessions Tab Parameters*

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

TACACS+ Accounting Record Details - Details Tab

This section describes the parameters of the **Accounting Record Details - Details** tab for the TACACS+ protocol. The following figure displays the **TACACS+ Accounting Record Details - Details** tab:

Figure 24: *TACACS+ Accounting Record Details - Details Tab*



The following table describes the configuration parameters on the **TACACS+ Accounting Record - Details** tab:

Table 14: *TACACS+ Accounting Record - Details Tab Parameters*

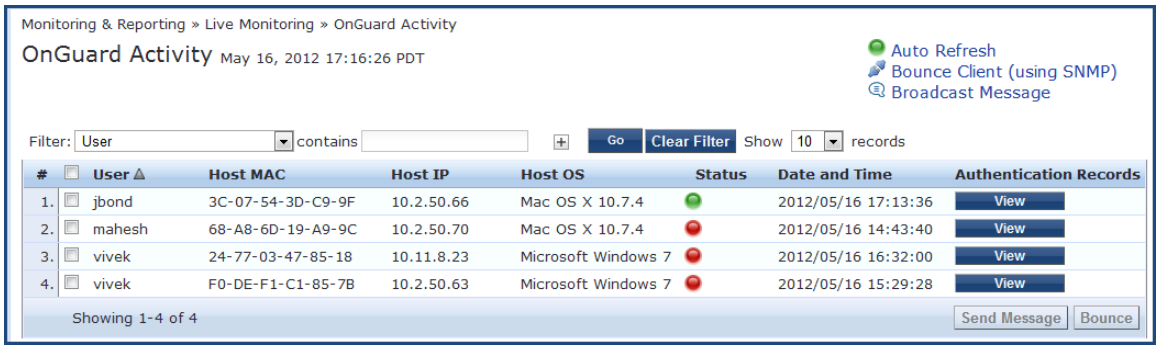
Parameter	Description
Accounting Packet Details	Shows cmd (command typed), priv-lvl (privilege level of the administrator executing the command) and service (shell) for each authorization request.

Live Monitoring: OnGuard Activity

The **OnGuard Activity** page shows the real-time status of all endpoints that have Dell W- OnGuard persistent or dissolvable agent in the **Monitoring > Live Monitoring > OnGuard Activity** page. This page also presents configuration tools to bounce an endpoint and to send unicast or broadcast messages to all endpoints running the W-OnGuard agent. The following image is an example of the **OnGuard Activity** screen:

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

Figure 25: *OnGuard Activity Page*



The following table describes the configuration parameters on the **OnGuard Activity** page:

Table 15: *OnGuard Activity Parameters*

Parameter	Description
User	Displays the name of the user.
Host MAC	Displays the MAC address of the host.
Host IP	Displays the IP address of the host.
Host OS	Displays the operating system that runs on the host.
Status	Displays the online status of the host. Green indicates online and red indicates offline.
Date and Time	Displays the date and time at which the user was created.
Authentication Records	Click the **View** button to see the **Endpoint Authentication Details** screen with the authentication records.

For additional tasks, see:

- Bouncing an Agent Using Non-SNMP on page 63
- Bouncing a Client Using SNMP on page 66
- Broadcast Message on page 67
- Send Message on page 67

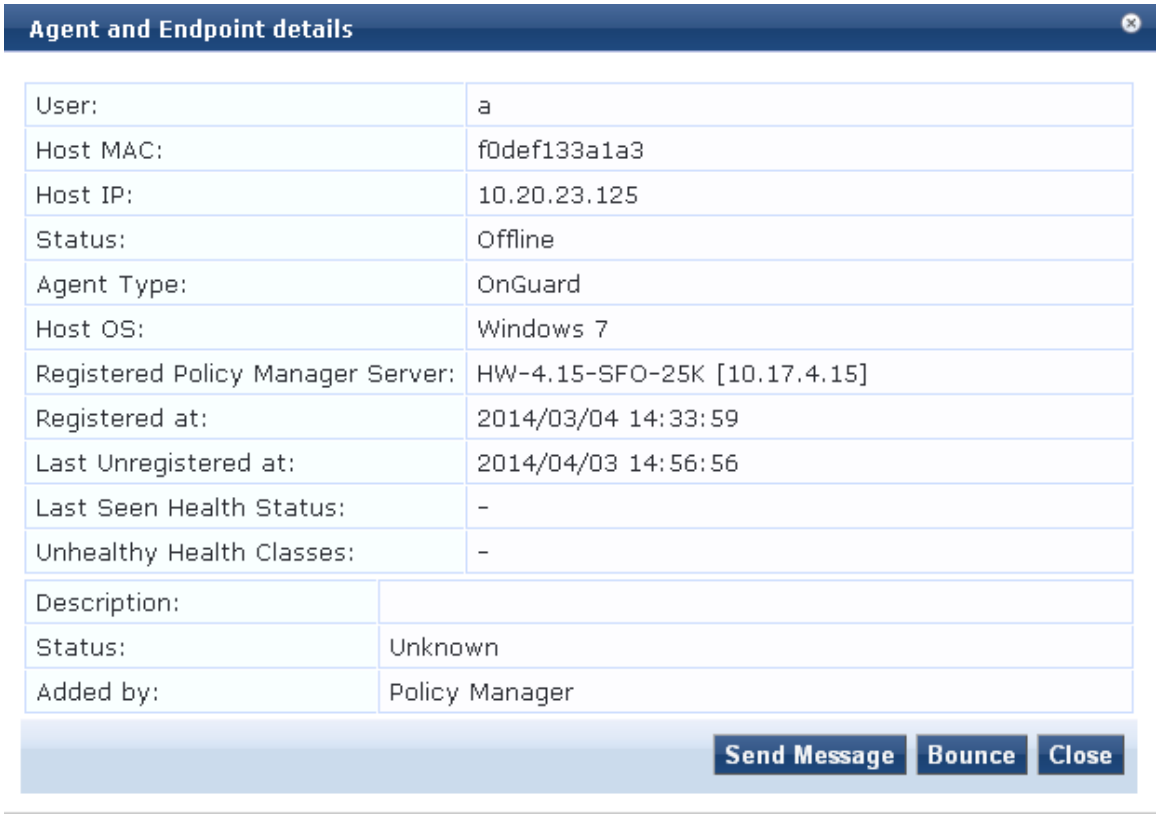
Bouncing an Agent Using Non-SNMP

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

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

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

Figure 26: *Agent and Endpoint Details*



The following table describes the configuration parameters on the **Agent and Endpoint details** page:

Table 16: *Agent and Endpoint Details Parameters*

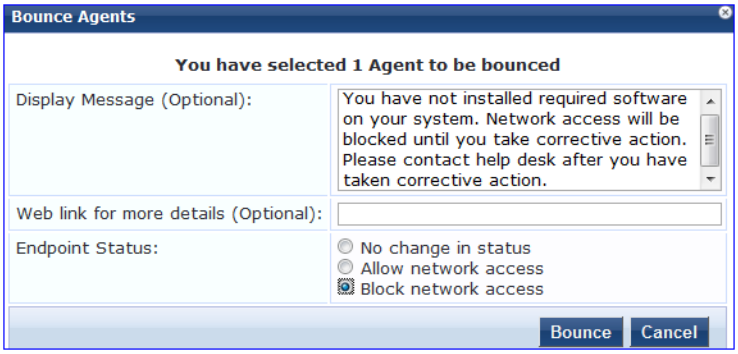
Parameter	Description
User	Displays the name of the user.
Host MAC	Displays the MAC address of the user.
Host IP	Displays the IP address of the host.
Status	Shows the online or offline status of the agent.
Agent Type	Specifies the type of the OnGuard agent.
Host OS	Displays the operating system that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

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

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

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

Figure 27: *Bounce Agents Page*



The following table describes the configuration parameters on the **Bounce Agents** page:

Table 17: *Bounce Agents Page Parameters*

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

Bouncing a Client Using SNMP

This page is used to initiate a bounce operation using SNMP with wired Ethernet switches.

Requirements

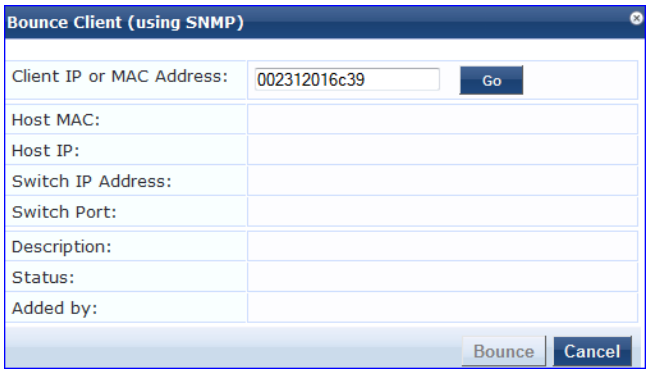
To bounce a client using SNMP successfully, the following conditions are mandatory:

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

Perform the following steps to bounce a client using SNMP:

1. Enter the client IP or MAC Address.
2. Click **Go**.
3. Click **Bounce**. The **Bounce Client (Using SNMP)** page appears.

Figure 28: *Bounce Client (Using SNMP) Page*



The following table describes the configuration parameters on the **Bounce Client (Using SNMP)** page:

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

Parameter	Description
Client IP or MAC address	Enter the Client IP or MAC address of the bounce client.
Host MAC	Displays the MAC address of the host.
Host IP	Displays the IP address of the host.
Switch IP Address	Displays the IP address of the switch.
Switch Port	Displays the port number of the switch.

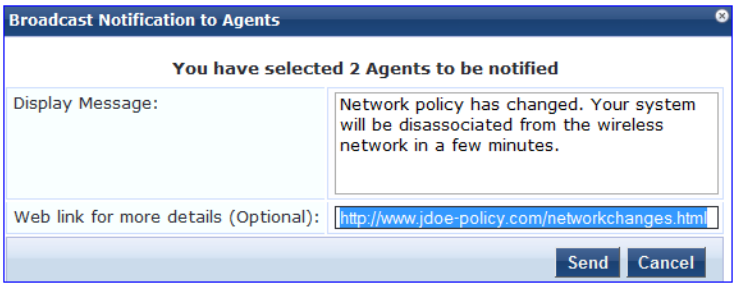
Table 18: *Bounce Client (Using SNMP) Page Parameters (Continued)*

Parameter	Description
Description	Displays the description of the client.
Status	Displays the status of the client.
Added by	Displays the name of the user who added the client.

Broadcast Message

After you click the **Broadcast Message** link on the top right of the **OnGuard Activity** page, a page appears that allows you to write and send a message to all active endpoints. The following figure is an example of the **Broadcast Notification to Agents** screen:

Figure 29: *Broadcast Notification to Agents Page*



The following table describes the configuration parameters on the **Broadcast Notification to Agents** page:

Table 19: *Broadcast Notification to Agents Page Parameters*

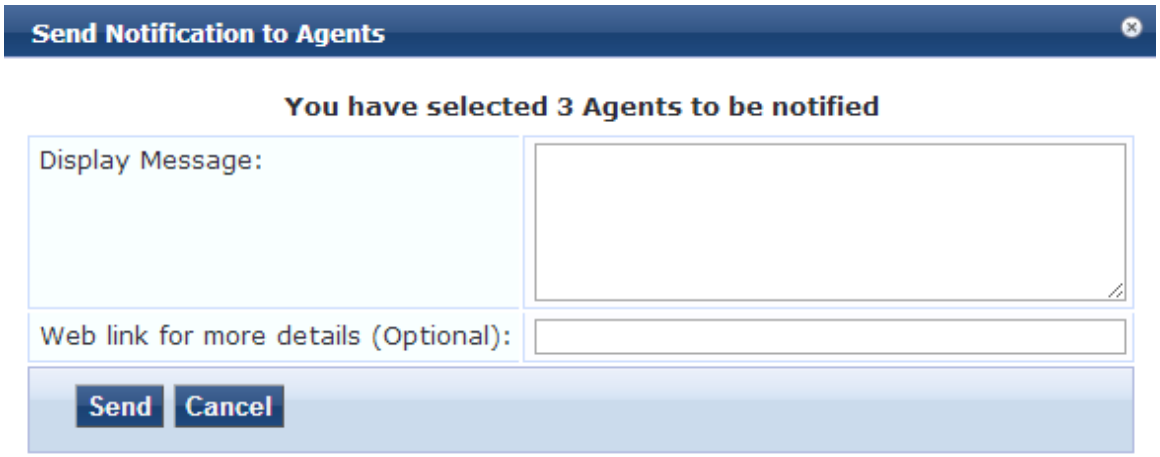
Parameter	Description
Display Message	Enter the message that needs to be sent to the active endpoints.
Web link for more details (Optional)	A clickable URL that is displayed along with the **Display Message**. This field is optional.

Send Message

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

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

Figure 30: *Send Notifications to Agents*



The following table describes the configuration parameters on the **Send Notifications to Agents** page:

Table 20: *Send Notifications to Agents Page Parameters*

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

Live Monitoring: Analysis and Trending

The **Analysis and Trending** page displays requests for the subset of components included in the selected filters over a selected time period: one month, two weeks, one week, one day, 12 hours, 6 hours, 3 hours, or one hour. The data can be aggregated by minute, hour, day, or week. The list at the end of this section shows the per-filter count for the aggregated data.

Each bar corresponding to each filter in the bar graph is clickable. Clicking a bar drills down into the Live Monitoring: Access Tracker on page 43 that shows session data for the specific time slice and for the specific requests.

Figure 31: *Analysis and Trending*

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

Component	Description
Select Server	Select a node from the cluster for which data will be displayed.
Update Now!	Click to update the display with the latest available data.
Customize This!	Click to customize the display by adding filters. You can add a maximum of 4 filters.
Toggle Chart Type	Click to toggle chart display between line and bar type.
Add new Data Filter	Click to add a data filter in the global filter list.

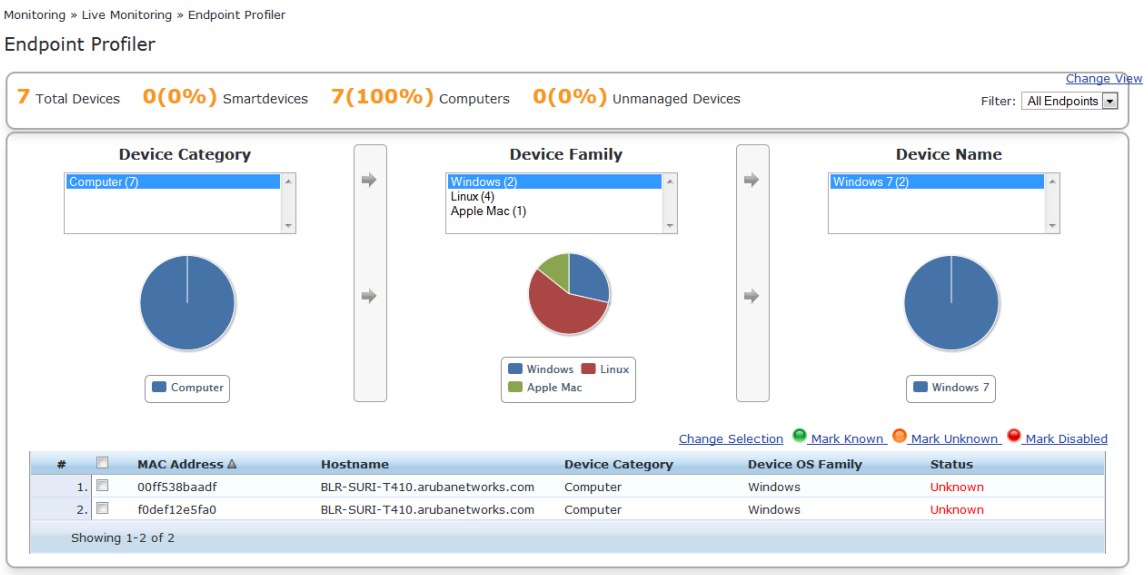
For more information on adding filters, refer to Data Filters on page 79.

Live Monitoring: Endpoint Profiler

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

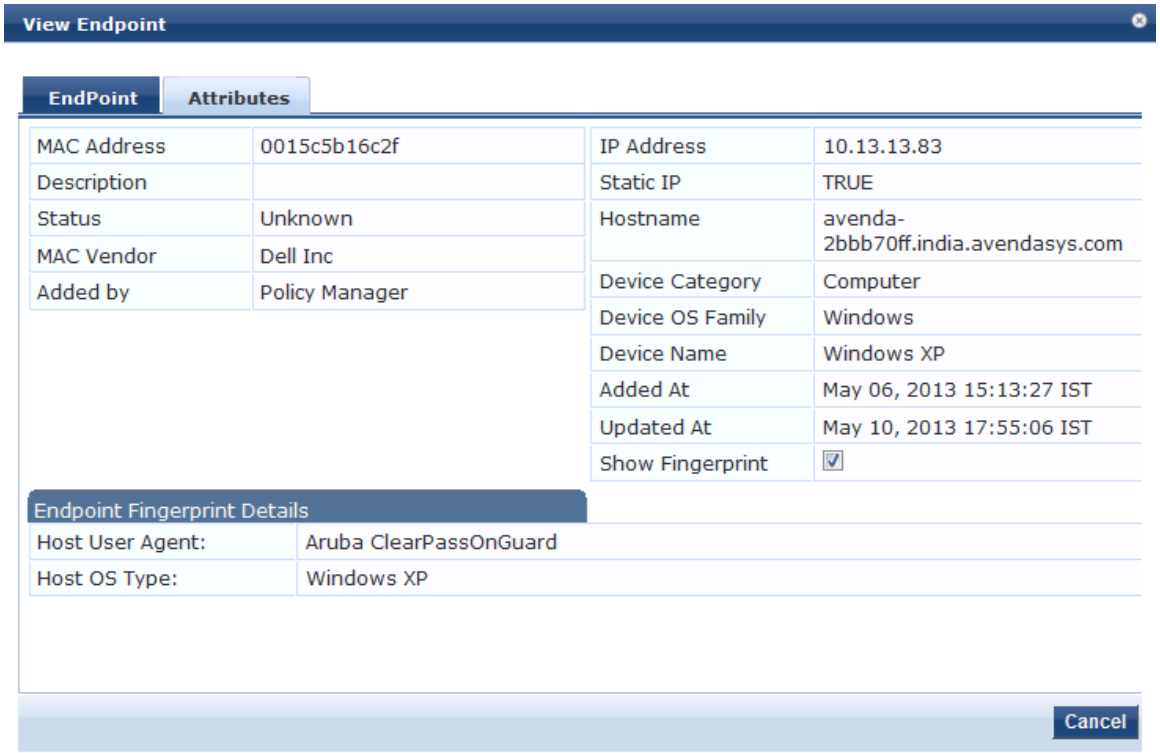
The figure below shows an example of the **Endpoint Profiler** graphs available on the **Monitoring > Live Monitoring> Endpoint Profiler** page:

Figure 32: *Endpoint Profiler*



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

Figure 33: *Endpoint Profiler Details*



Live Monitoring: System Monitor

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

NOTE

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

time in the **Last updated at** field in the **System Monitor** page.

System Monitor Tab

This tab displays charts and graphs that include information about CPU load and usage, memory usage, and disk usage.The **System Monitor** tab on the **Monitoring > Live Monitoring > System Monitor** page displays information about component usage and load.

Table 21: *System Monitor Graphs*

Graph	Description
Monitoring CPU Usage	Percentage of CPU usage based on User, System, IO Wait, and Idle time.
Monitoring CPU Usage	Percentage of CPU load in increments of 1, 5, and 15 minutes.
Monitoring Memory Usage	Percentage of free and total memory in Gigabytes.
Monitoring Memory Usage	Percentage of free and total swap memory in Gigabytes.
Monitoring Disk - Usage	Percentage of used and free disk space.
Monitoring Disk - Swap Usage	Percentage of used and total swap space.

Process Monitor Tab

This tab displays reports about a selected process. The processes that you can monitor include Policy server, TACACS server, and stats collection service. The **Process Monitor** tab on the **Monitoring > Live Monitoring > System Monitor** page displays CPU Usage and Main Memory Usage for a selected process or service. Click the **Select Process** drop-down list and select any of the following options to view CPU and Main Memory usage for that process or service:

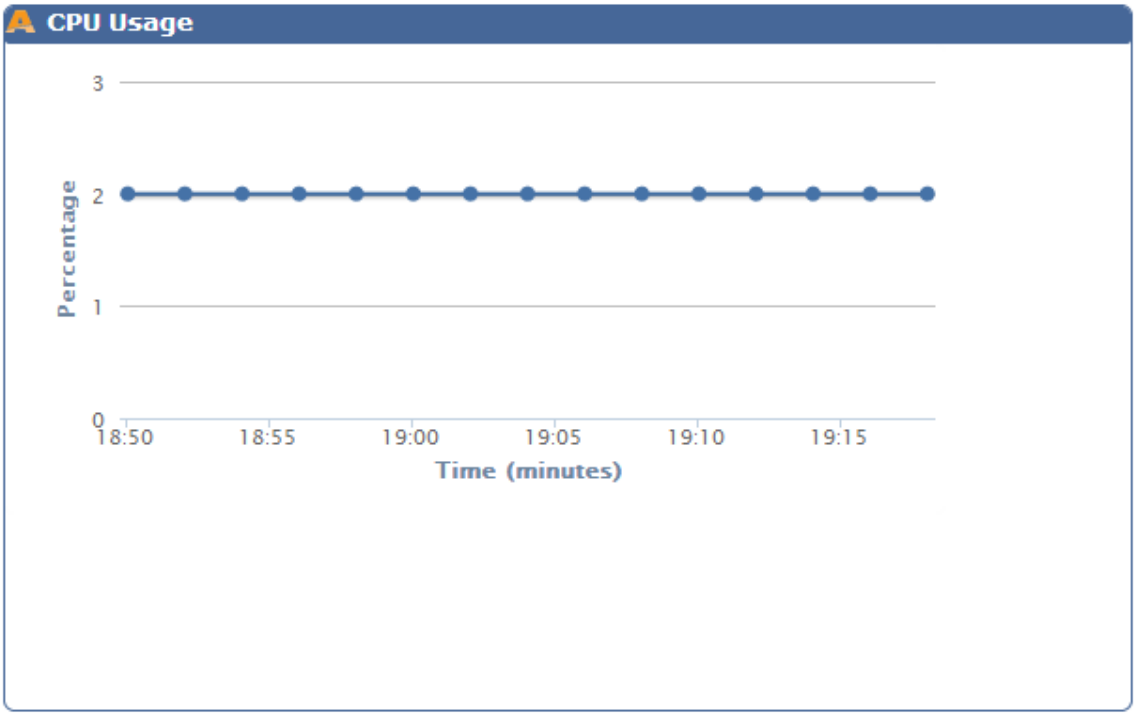
- Admin UI service
- AirGroup notification service
- Async DB write service
- Async network services
- DB change notification server
- DB replication service
- Micros Fidelio FIAS
- Multi-master cache
- Policy server
- Radius server
- Stats aggregation service
- Stats collection service
- System auxiliary services

- System monitor service
- Tacacs server
- Virtual IP service

Monitoring CPU Usage

This graph shows the CPU usage in time and percentage.

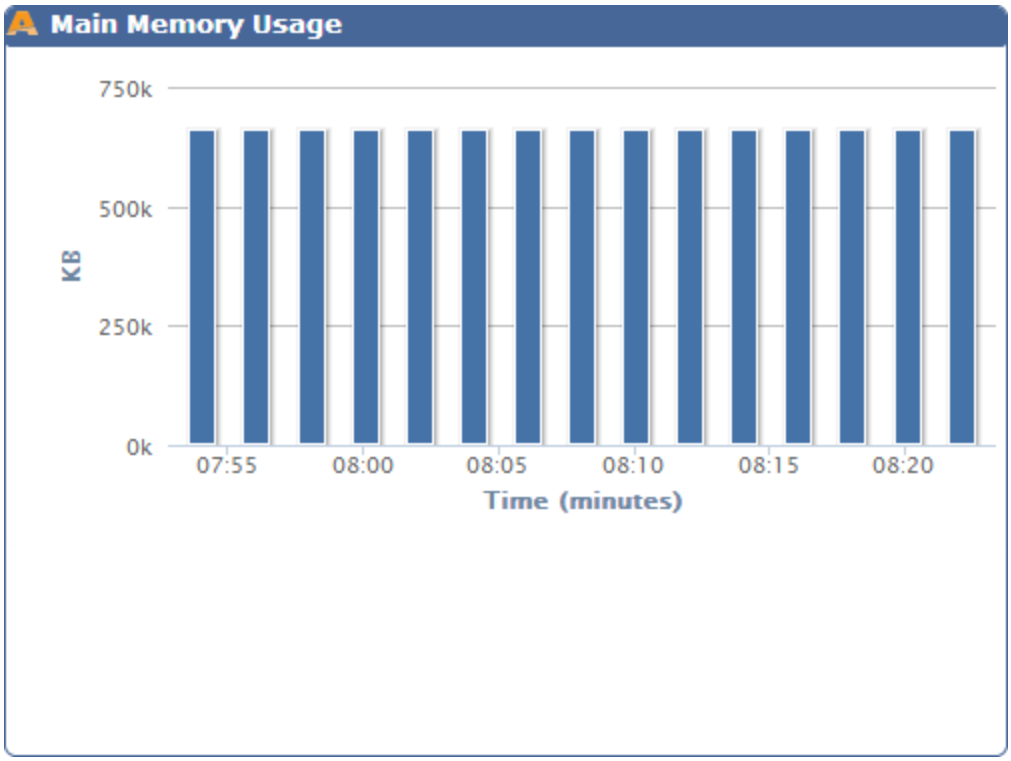
Figure 34: *CPU Usage Graph Example*



Monitoring Main Memory Usage

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

Figure 35: *Main Memory Usage Graph Example*

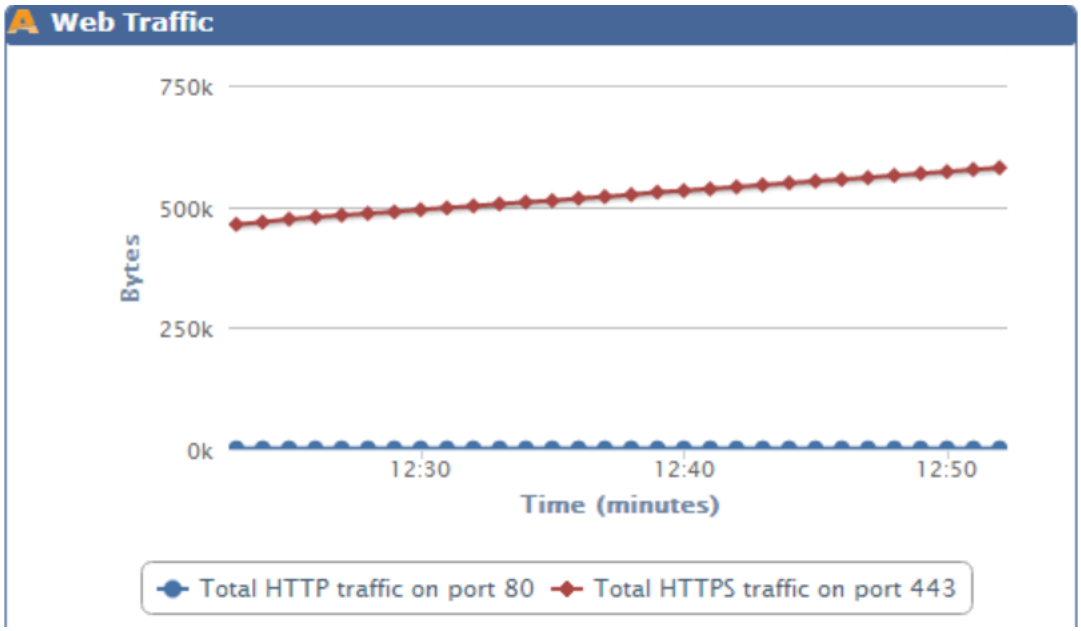


Network Tab

This tab displays a graph about any selected network parameters such as web traffic and SSH. The **Network** tab on the **Monitoring > Live Monitoring > System Monitor** page displays network activity (in bytes) for the following traffic types:

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

Figure 36: *Network Monitor Tab Graph Example - Web Traffic*



ClearPass Tab

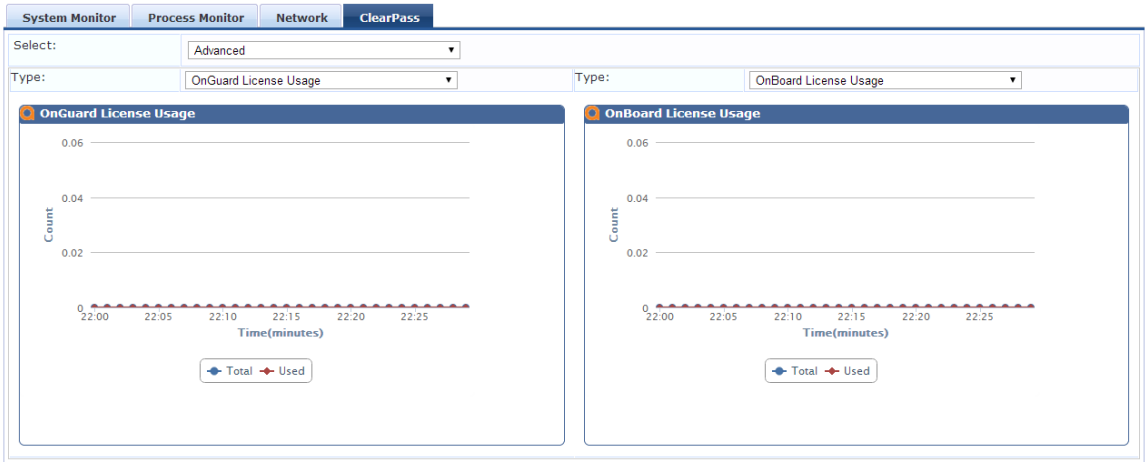
The **ClearPass** tab on the **Monitoring > Live Monitoring > System Monitor** page displays performance monitoring counters and timers for the last 30 minute of activity for the following components:

- Service Categorization
- Authentication (RADIUS, TACACS, or WebAuth)
- Authorization
- Role Mapping
- Posture Evaluation
- Audit Scan
- Enforcement
- End to End request processing (RADIUS, TACACS, or WebAuth)
- Advanced

When you select the **Advanced** component, you can view additional performance monitoring counters and timers. Select the type of performance monitoring counter by selecting the **Type** drop-down. If you do not select the performance monitoring counter from the **Type** field, the widgets will be blank.

The following figure displays the **Advanced** components:

Figure 37: *System Monitoring - ClearPass Tab*



Audit Viewer

The **Audit Viewer** table on the **Monitoring > Audit Viewer** page provides a dynamic report on actions, device name, category of policy component, user, and timestamp. Table 22 describes the information displayed in the **Audit Viewer** page.

Figure 38: *Audit Viewer Page*

The following table describes the configuration parameters on the **Audit Viewer** page:

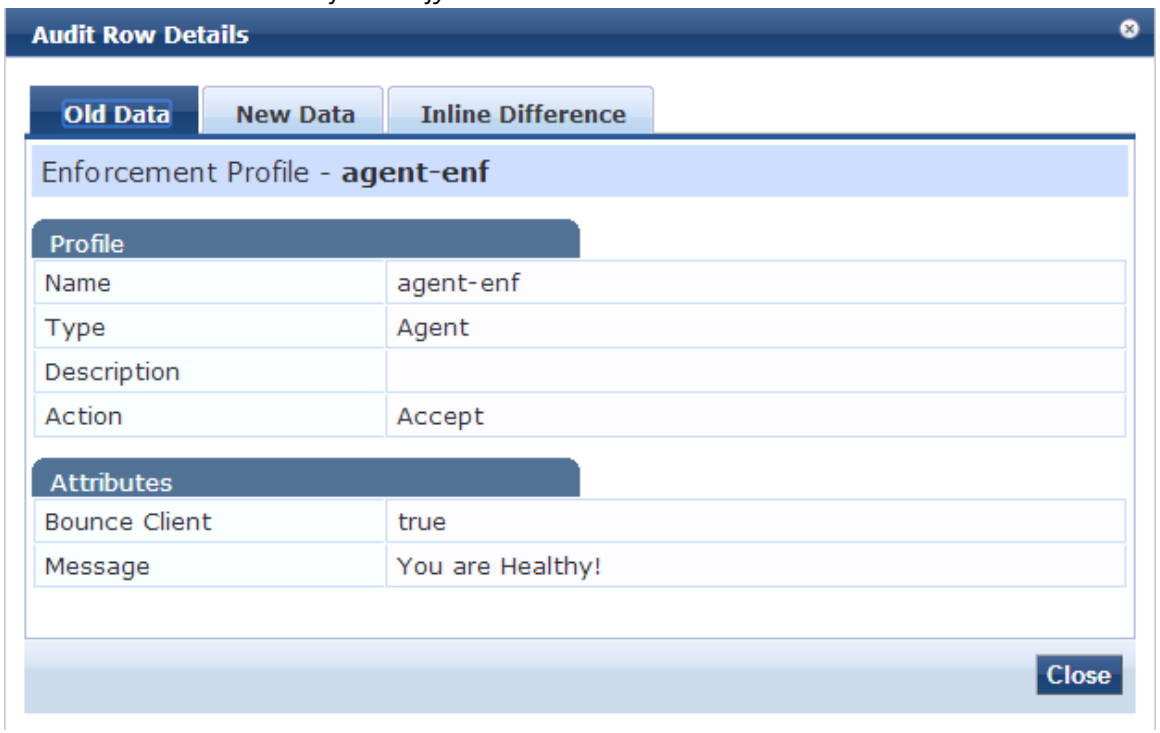
Table 22: *Audit Viewer Page Parameters*

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

Click any row in the audit viewer to display detailed information about the selected event. The content in the **Audit Row Details** window varies, depending upon type of event you select.

- **Add events**: Click a row with the **Add** action type to display additional details that are specific to the new policy component. For example, if a TACACS enforcement profile is added, the **Audit Row Details** window displays detailed information about that profile. If a policy is created, the **Audit Row Details** window displays information about the policy.
- **Modify Events**: Click a row with the **Modify** action type to display additional details information about the change, including the previous values, the latest, updated values, and the differences between the two. When you view a modify event, the **Audit Row Details** window contains the following three tabs:
  - The **Old Data** tab displays a summary of details about the original data values. The **Profile** section shows a summary of the profile values. The **Attributes** section shows data about the original attributes and values.
  - The **New Data** tab is a summary of details about the original data values. The **Profile** section shows a summary of the profile values. The **Attributes** section displays new and changed Attributes.
- **Remove Events:** Click a row with the **Remove** action type to display details about attributes that were removed.

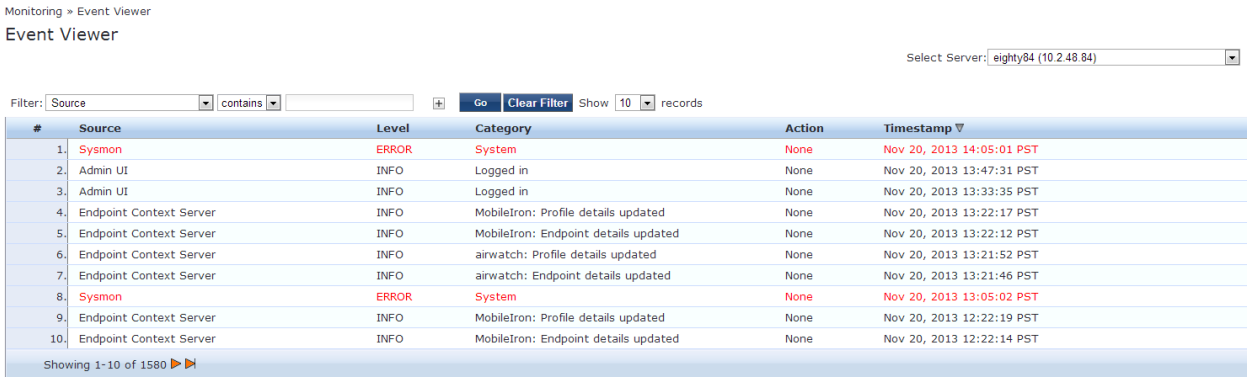
Table 23: *Audit Row Details for Modify Events*



Event Viewer

The **Event Viewer** table on the **Monitoring > Event Viewer** page provides reports about system-level events. Table 24 describes the information displayed in this table.

Figure 39: *Event Viewer Page - Default Values*



The following table describes the **Event Viewer** parameters:

Table 24: *Event Viewer Page Parameters - Default Values*

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

Creating an Event Viewer Report Using Default Values

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

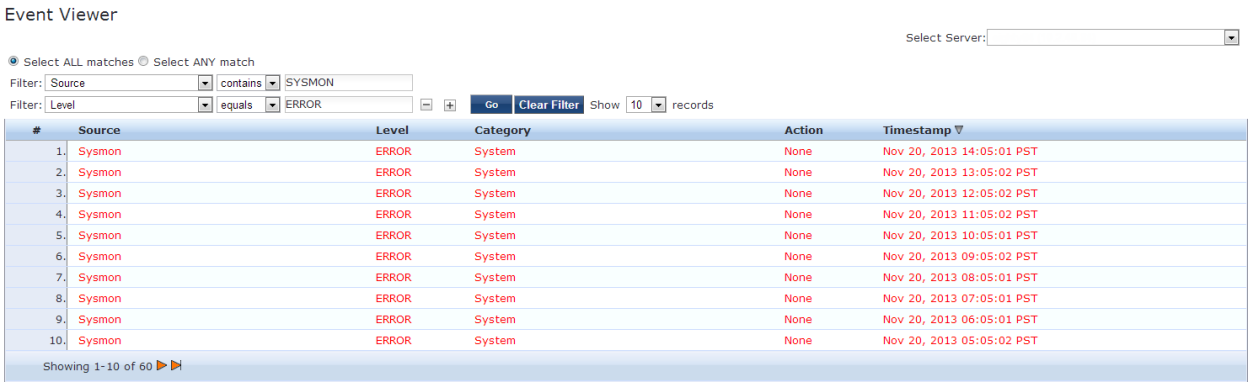
Creating an Event Viewer Report Using Custom Values

1. Click the icon. A new **Filter** field is added. You can add up to four **Filter** fields.
2. Click **Select ANY match**.
3. In the first **Filter** field, select **Level** as the **Filter** value.
4. Leave the search term set to **contains**.

5. Enter **ERROR** in the text field.
6. In the second **Filter** field, select **Source** as the **Filter** value.
7. Change the search field to **equals**.
8. Enter **SYSMON** in the text field.
9. Change the **Show records** value to 20.
10. Click **Go**.

The following figure displays the **Event Viewer** report with custom values:

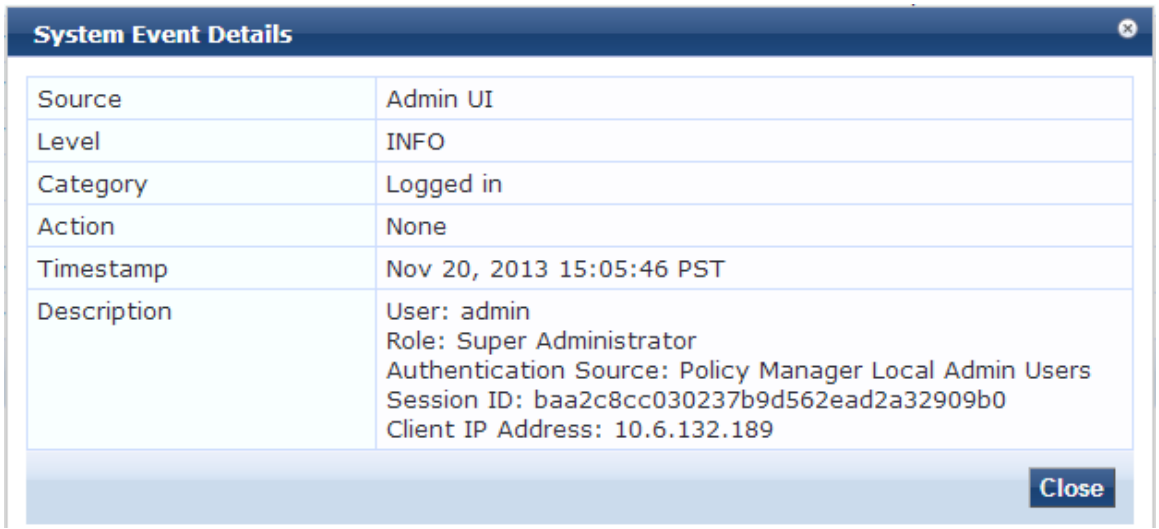
Figure 40: *Event Viewer Report Example - Custom Values*



Viewing Report Details

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

Figure 41: *System Event Details Page*



The following table describes the **System Event Details** parameters:

Table 25: *System Event Details Page Parameters*

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

Data Filters

The **Data Filters** table on the **Monitoring > Data Filters** page provides a way to filter data (limit the number of rows of data shown by defining custom criteria or rules) that is shown in the following components in Policy Manager:

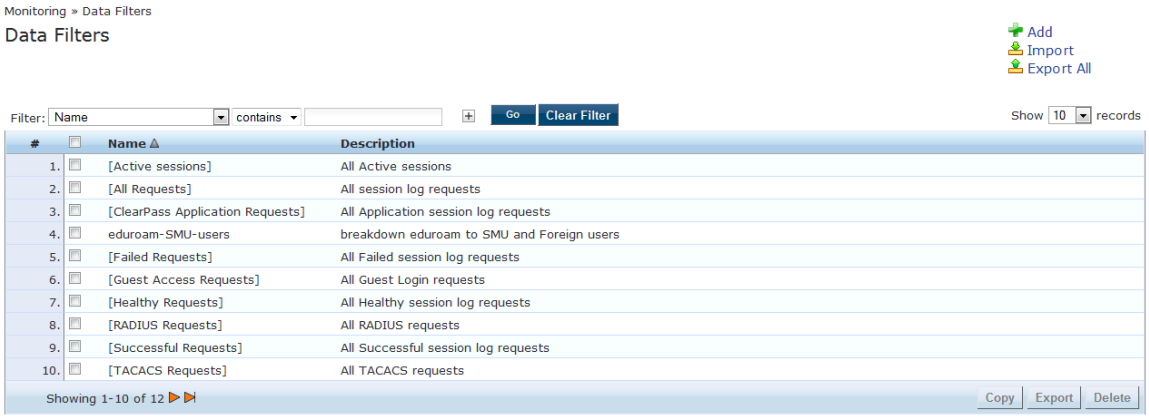
- Live Monitoring: Access Tracker on page 43
- Syslog Export Filters on page 475
- Live Monitoring: Analysis and Trending on page 68
- Live Monitoring: Accounting on page 52

Policy Manager is preconfigured with the following data filters:

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

The following figure displays the **Data Filters** page:

Figure 42: *Data Filters Page*



The following table describes the configuration parameters on the **Data Filters** page:

Table 26: *Data Filters Page Parameters*

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

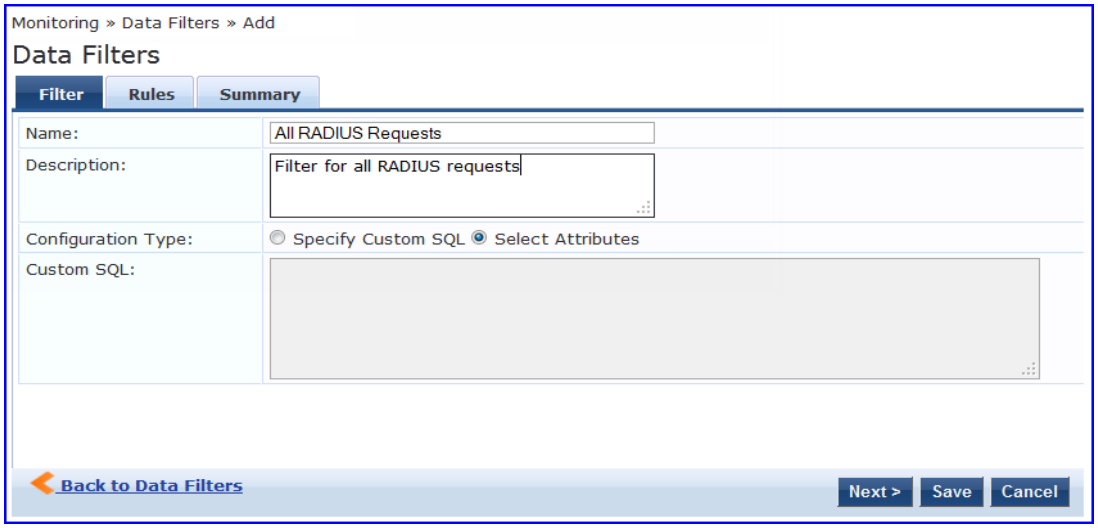
Adding a Filter

To add a filter, click the **Add** link in the top-right corner of the **Data Filters** page. Define a name and description for the filter the **Filter** tab. If you select the **Select Attributes** configuration type on the **Filter** tab, you can define and its rules in the **Rules** tab. (The **Rules** tab appears only if the **Select Attributes** option is selected.)

Filter Tab

Table 27 describes the configuration settings available on the **Filter** tab.

Figure 43: *Add Filter - Filter Tab*



The following table describes the **Filter** tab parameters:

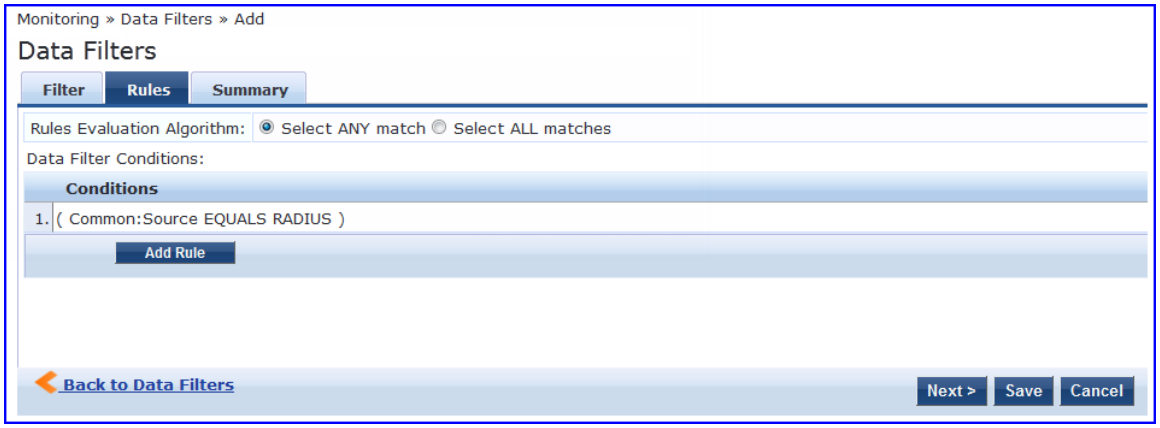
Table 27: *Add Filter - Filter Tab Parameters*

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

Rules Tab

The **Rules** tab displays only if you select the **Select Attributes** configuration type on the **Filter** tab. The configuration options in this tab are described in Table 28.

Figure 44: *Add Filter - Rules Tab*



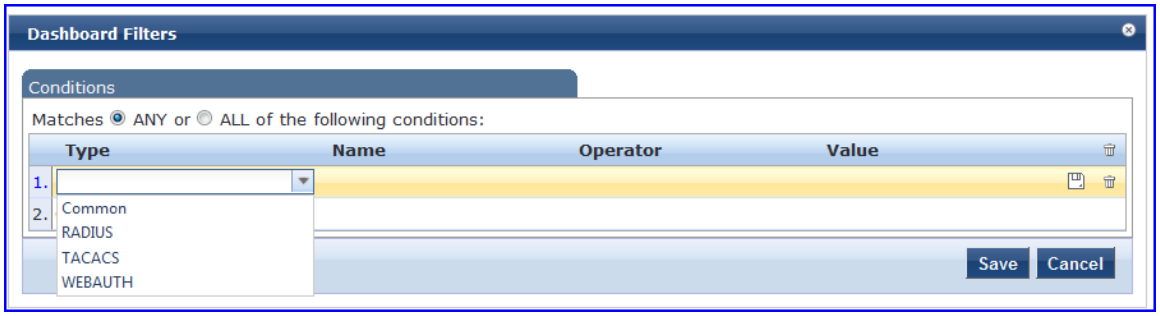
The following table describes the **Filter** tab parameters:

Table 28: *Add Filter - Rules Tab*

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

When you click on **Add Rule** or **Edit Rule**, the **Dashboard Filter** rules editorwindow appears.

Figure 45: *Dashboard Filters - Rules Editor*



The following table describes the **Dashboard Filters** parameters:

Table 29: *Dashboard Filters Configuration Parameters*

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

Blacklisted Users

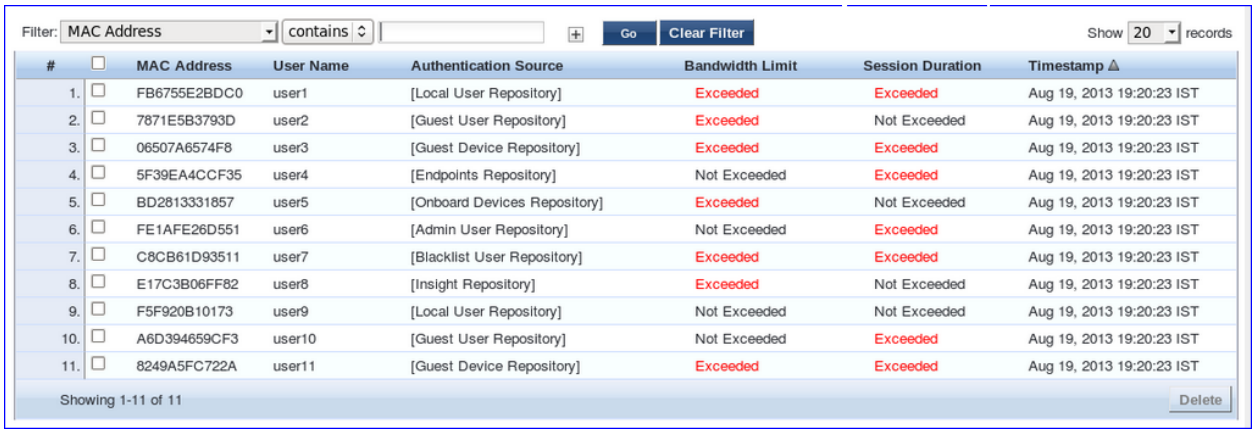
The **Blacklisted Users** table on the **Monitoring > Blacklisted Users** page lists the MAC address and user name of all blacklisted users, the authentication source for that user, and indicates whether the bandwidth

limit or session duration limits were exceeded by each blacklisted user.

To delete a user from this blacklist, select the user row and click **Delete**. After a user entry is removed from the blacklisted users table, the user is eligible to access the network again.

The following figure displays the **Blacklisted Users** page:

Figure 46: *Blacklisted Users Page*



All configuration tasks including configuring servers, authenticating user or device against an authentication source, storage of user records, configuring posture policies, posture servers, and audit servers, configuring enforcement policies, and configuring Network Access Devices (NADs) are done from the **Configuration** menus. The Policy Manager **Configuration** menu provides the following configuration categories:

- **Start Here** - The Dell Networking W-ClearPass Policy Manager**Start Here** page provides the ability to create templates for services where you can define baseline policies and require specific data, when you create services.
- **Services** - The **Services** page provides options to add, modify, and remove a service. For more information, refer to the following sections of this document:
  - Services Architecture and Flow on page 29
  - Start Here on page 87
  - Policy Manager Service Types on page 122

  This page also shows the current list and order of services that Dell Networking W-ClearPass Policy Manager follows during authentication and authorization.
- **Authentication and Authorization** - The **Authentication** page provides options to configure the following three components:
  - Authentication Method
  - Authentication Source
  - Authorization Source

  For more information on configuration, refer to the following sections of this document:
  - Adding and Modifying Authentication Methods on page 145
  - Adding and Modifying Authentication Sources on page 169
  - Configuring Authentication Components on page 1
- **Identity** - The **Identity** page provides options on the WebUI settings required to configure Dell Networking W-ClearPass Policy Manager Identity settings. For more information, refer to the following sections of this document:
  - Configuring Single Sign-On on page 211
  - Managing Local Users on page 212
  - Adding and Modifying Endpoints on page 216
  - Adding and Modifying Static Host Lists on page 223
- **Posture** - The **Posture** page provides options to configure posture policies, posture servers, and audit server. For more information, refer to the following sections of this document:
  - Posture Architecture and Flow on page 33
  - Configuring Posture Servers on page 282
  - Configuring Audit Servers on page 285
- **Enforcement** - The **Enforcement** page provides options to configure the Enforcement Profiles globally and to reference in an enforcement policy that is associated with a service. For more information, refer to the following sections of this document:
  - Enforcement Architecture and Flow on page 31

- **Network** - The **Network** page provides options to configure the Network Access Device (NAD) that sends network access requests to Policy Manager using the supported RADIUS, TACACS+, or SNMP protocol. For more information, refer to the following sections of this document:
  - Adding and Modifying Devices on page 347
  - Adding and Modifying Device Groups on page 353
  - Adding and Modifying Proxy Targets on page 356
- **Policy Simulation** - The **Policy Simulation** page provides options to configure the **Policy Simulation** utility that applies a set of request parameters as input against a given policy component. For more information, refer to the Policy Simulation section.
- **Profile Settings** - The **Profile Settings** page provides options to configure **Profile**, that is a ClearPass Policy Manager module that automatically classifies endpoints using attributes obtained from software components called **Collectors**. For more information, refer to the following sections of this document:
  - Device Profile on page 359
  - Collectors on page 359
  - Fingerprint Dictionaries on page 364
  - Profiling on page 365

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

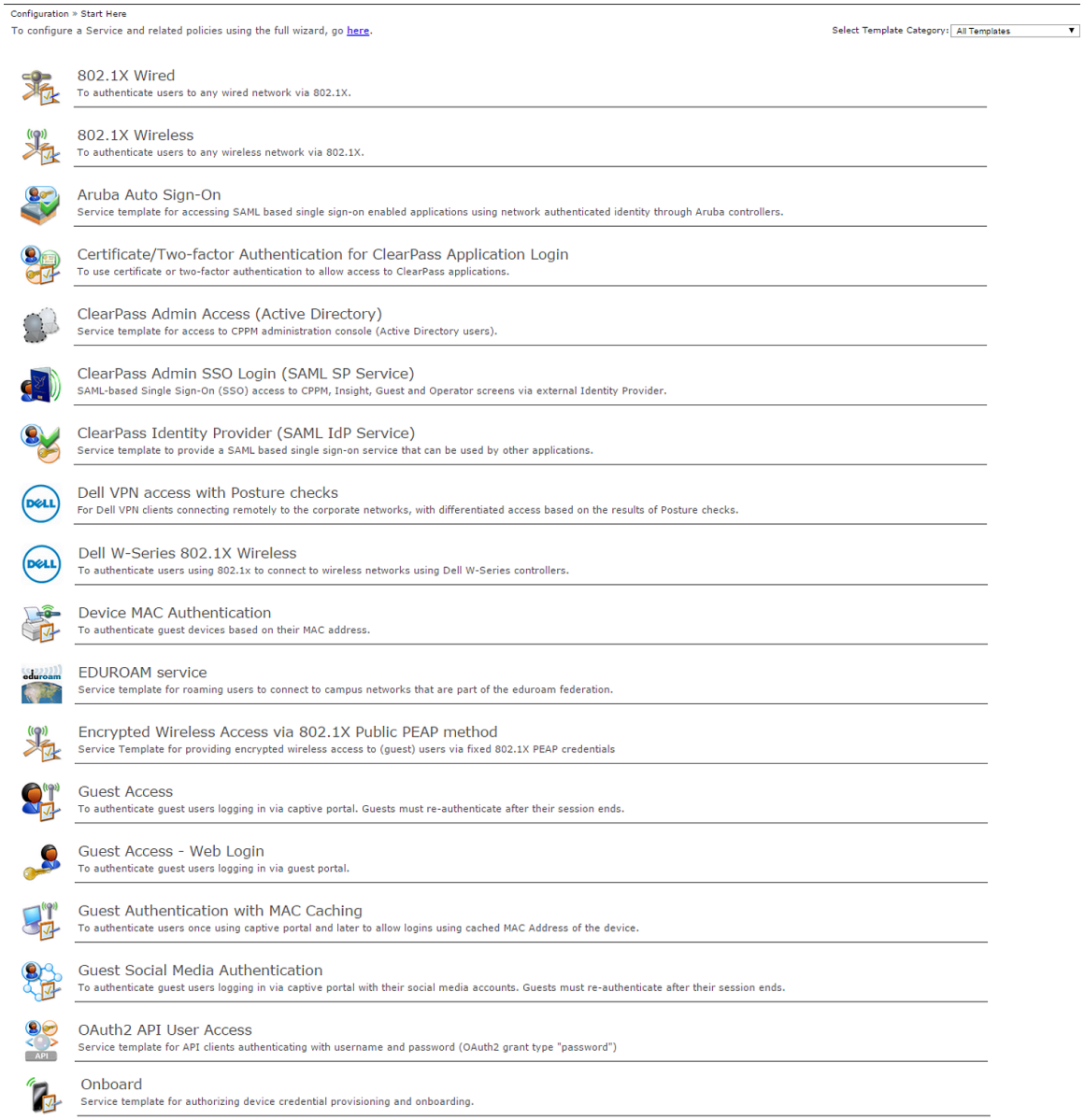
This chapter describes the following topics:

Start Here

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

The following figure displays the **Service Templates** page:

Figure 47: *Service Templates page*



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

- ClearPass Admin Access (Active Directory)
- ClearPass Admin SSO Login (SAML SP Service)
- ClearPass Identity Provider (SAML IdP Service)
- Encrypted Wireless Access via 802.1X Public PEAP method
- Guest Access
- Guest Access - Web Login
- Guest MAC Authentication
- OAuth2 API User Access

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

- MAC Authentication

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

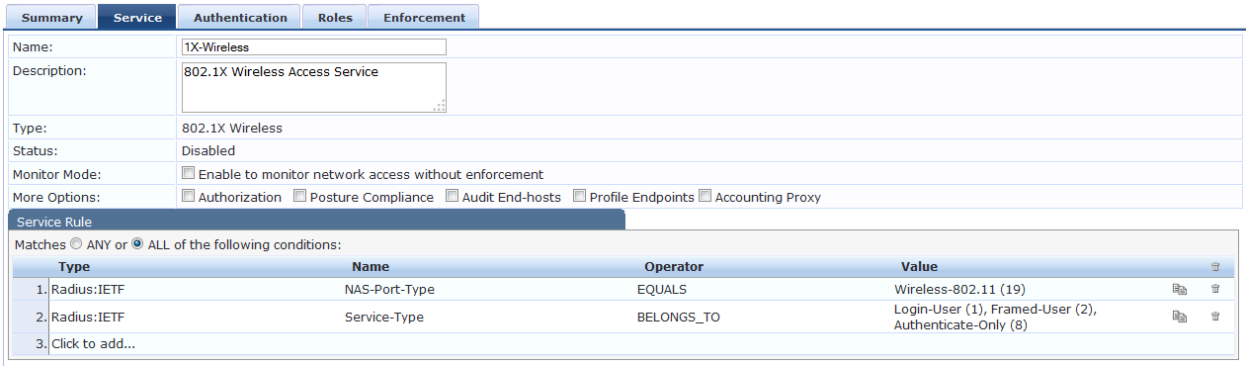
The following authentication methods are used in service templates in the **HCG** mode:

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

Viewing Existing Services

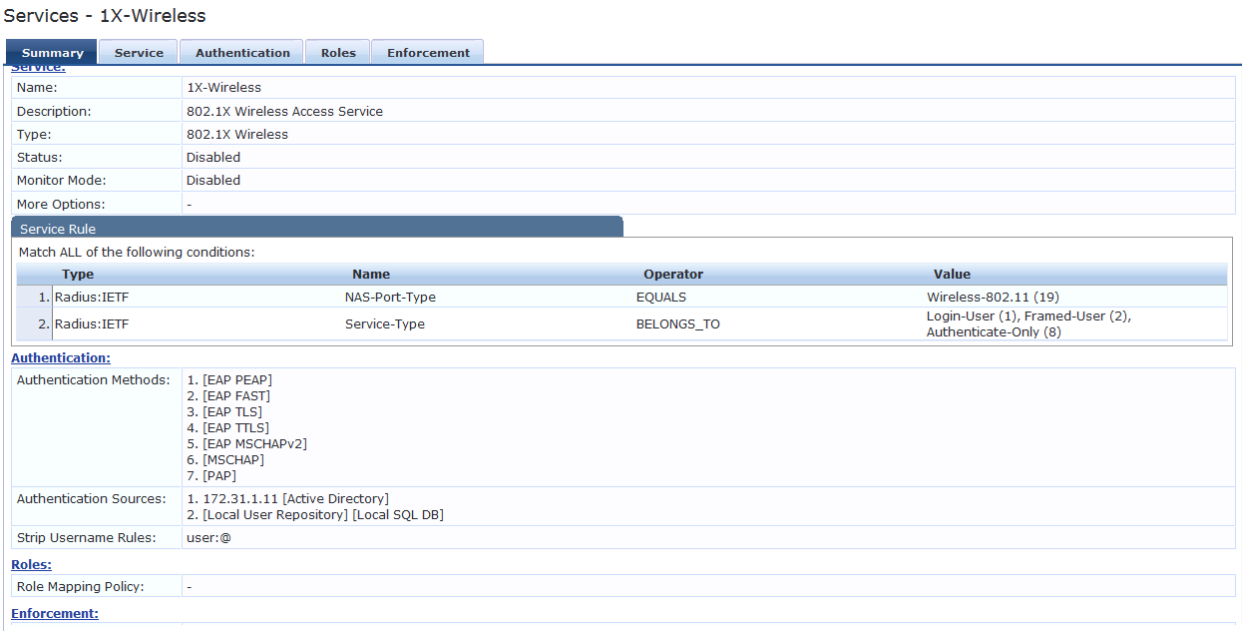
You can view all configured services in a list or drill down to individual services in the **Services** page. Click **Configuration > Services** to view a list of services that you can filter by phrase or sort by order. In the **Services** page, click the name of a **Service** to view its details. The following figure is an example of the **Services** tab with the list of services with sorting tool:

Figure 48: *List of services with sorting tool*



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

Figure 49: *Details for an individual service*



Adding and Removing Services

You can modify a list of services on the **Configuration > Services** page by creating a new service, modifying, or deleting an existing service.

- **Create a new service:** In the **Services** page, click **Add**, then follow the configuration wizard by clicking **Next** as you complete each tab. To create a service template by making a copying an existing service, select the check box by a service, then click **Copy**.
- **Modify a service:** To modify an existing service, click the check box by a service row in the page. This opens the **Services > Edit - <service_name>** form. Select the **Service** tab on this form to edit the service information.
- **Remove a service** - From the **Services** page, select the check box by a service and then click the **Delete** button. You can also disable or enable a service from the **Service** details page by clicking **Disable** or **Enable** in the lower right of page.

The following figure is an example of the **Add Service** tab. Table 30 describes the available configuration parameters on this tab. Note that the available settings will vary, depending upon the service type selected.

Figure 50: *Add Service Page (all options enabled)*

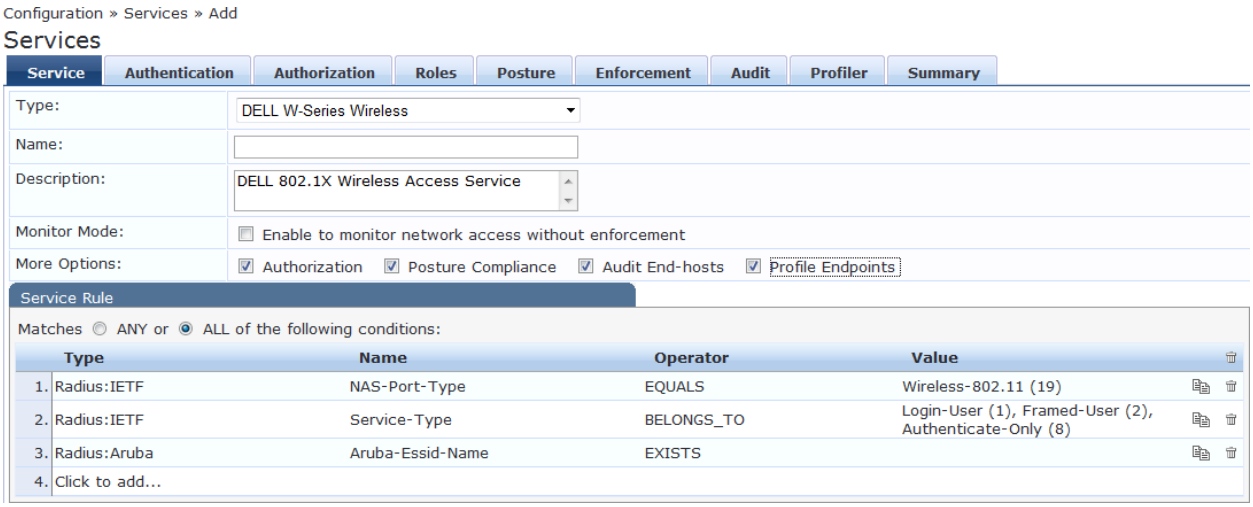


Table 30: *Service Page (General Parameters)*

Label	Description
Type	Select the desired service type from the drop-down list. When working with service rules, you can select from the following namespace dictionaries: • **Application**: The type of application for this service. • **Authentication**: The Authentication method to be used for this service. • **Connection:** Originator address (Src-IP-Address, Src-Port), Destination address (Dest-IP-Address, Dest-Port), and Protocol • **Device:** Filter the service based on a specific device type, vendor, operating system location, or controller ID. • **Date:** Time-of-Day, Day-of-Week, or Date-of-Year • **Endpoint**: Filter based on endpoint information such as enabled/disabled, device, OS, location, and more. • **Host**: Filter based on host Name, OSType, FQDN, UserAgent, CheckType, UniqueID, Agent-Type, and InstalledSHAs, • **RADIUS:** Policy Manager ships with a number of vendor-specific namespace dictionaries and distinguishes vendor-specific RADIUS namespaces with the notation *RADIUS:vendor* (sometimes with an additional suffix for a particular device). To add a dictionary for a vendor-specific RADIUS namespace, navigate to **Administration > Dictionaries > Radius > Import** (link). The notation **RADIUS:IETF** refers to the RADIUS attributes defined in RFC 2865 and associated RFCs. As the name suggests, RADIUS namespace is only available if the request type is RADIUS. • **Any other supported namespace:** See Rules Editing and Namespaces on page 601 for an exhaustive list of namespaces and their descriptions. To create new services, you can copy or import other services for use *as is* or as templates, or you can create a new service.
Name	Enter the name or label for the service you want to create.
Description	Enter a description that provides additional information to identify the service. This field is optional.
Monitor Mode	Optionally check the **Enable to monitor network access without enforcement** to

Table 30: *Service Page (General Parameters) (Continued)*

Label	Description
	allow authentication and health validation exchanges to take place between endpoint and Policy Manager, but without enforcement. In **Monitor Mode**, no enforcement profiles (and associated attributes) are sent to the network device. Policy Manager also allows *Policy Simulation* (**Monitoring > Policy Simulation**), where the administrator can test the results of a particular configuration of policy components.
More Options	Select any of the available check boxes to enable the configuration tabs for those options. The available check boxes varies based on the type of service that is selected and may include one or more of the following: • **Authorization**: Select an authorization source from the drop-down list to add the source or select the **Add new Authentication Source** link to create a new source. • **Posture Compliance:** Select a Posture Policy from the drop-down list to add the policy or create a new policy by clicking the link. Select the default Posture token. Specify whether to enable auto-remediation of non-compliant end hosts. If this is enabled, then enter the Remediation URL. You can specify the **Posture Server** from the drop-down list or add a new server by clicking the **Add new Posture Server** link. • **Audit End-hosts:** Select an **Audit Server**, either built-in or customized. Refer to Configuring Audit Servers on page 285 for audit server configuration steps. For this type of service, you can perform audit **Always**, **When posture is not available**, or **For MAC authentication requests**. You can specify to trigger an audit always, when posture is not available, or for MAC authentication requests. If **For MAC authentication requests** is specified, then you can perform an audit **For known end-hosts only** or **For unknown end hosts only**, or **For all end hosts**. Known end hosts are defined as those clients that are found in the authentication source(s) associated with this service. Performing audit on a client is an asynchronous task, which means the audit can be performed only after the MAC authentication request has been completed and the client has acquired an IP address through DHCP. Once the audit results are available, Policy Manager re-applies policies on the network deviceby one of the following ways: ▪ **No Action:** The audit does not apply policies on the network device after this audit. ▪ **Do SNMP bounce:** This option bounces the switch port or force an 802.1X re-authentication (both done using SNMP). **NOTE:** Bouncing the port triggers a new 802.1X or MAC authentication request by the client. If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager. ▪ **Trigger RADIUS CoA action:** This option sends a RADIUS CoA command to the network device by Policy Manager. • 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.

Reordering Services

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

with this request. To change the order in which service rules are processed, you can change the order of services.

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

The following figures display the **Services** page and the **Reorder Services** page. Table 31 describes the configuration settings on this page.

Figure 51: *Service Reorder Button*

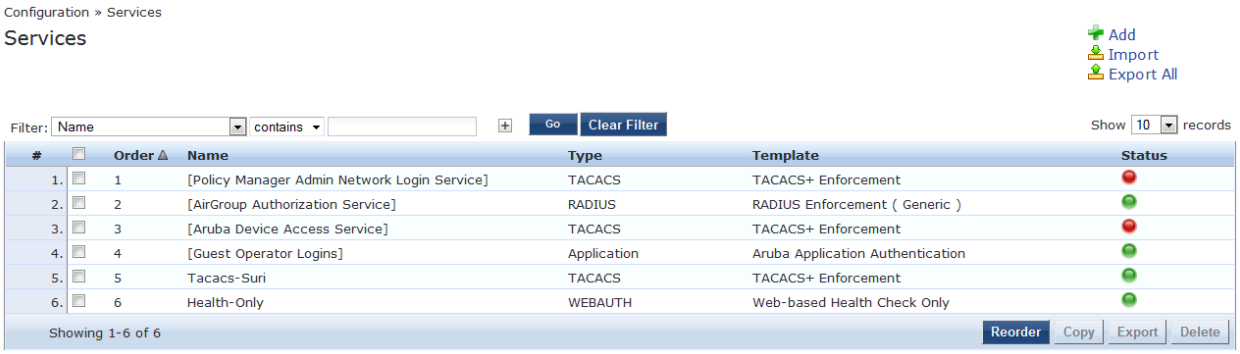
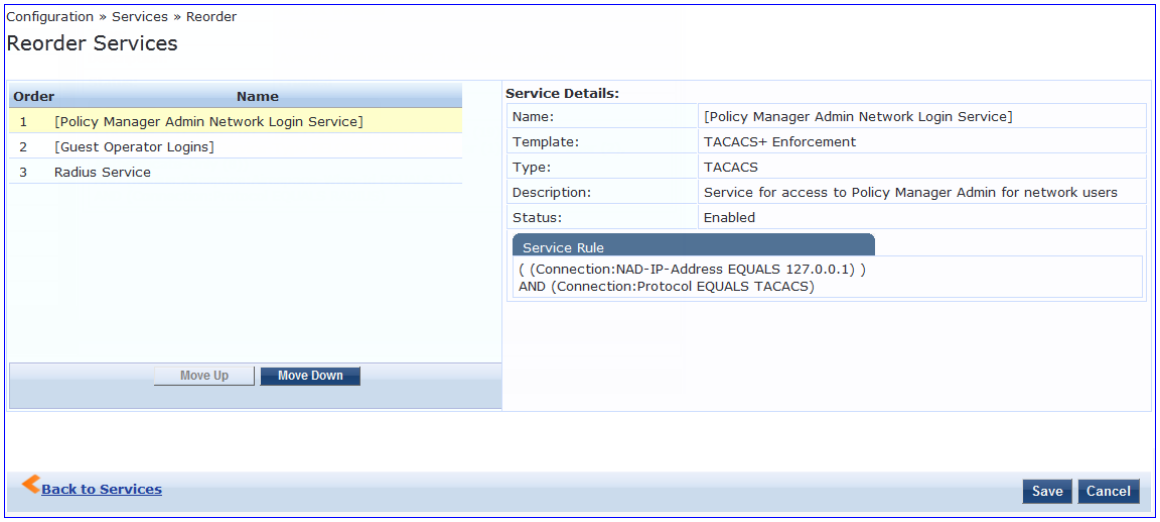


Figure 52: *Reordering Services*



The following table describes the **Reorder Services** parameters:

Table 31: *Reordering Services*

Label	Description
Name	Displays the name of the selected service.
Service Details	
Name	Shows the name of the selected service.

Table 31: *Reordering Services (Continued)*

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

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

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

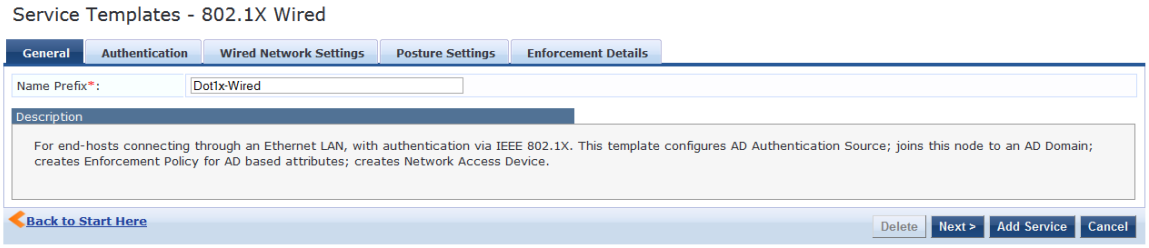
The **802.1X Wireless** template is intended for wireless end-hosts connecting through an 802.11 wireless access device or controller with authentication using IEEE 802.1X. The **802.1X Wireless** template allows configuring both identity and posture based policies.

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

NOTE

All three templates are configured using identical parameters.

Figure 53: *Service Templates - 802.1X Wired Service Template*



To add a new service for the selected service template,

1. Specify a unique **Name Prefix** (applies only to the selected template) in the **General** tab.
2. Update the required fields in the **Authentication** and **Enforcement Details** sections.
3. Click **Add Service**. An entry for the new set of configuration is created under the **Services**, **Roles**, **Role Mapping**, **Enforcement Policies** and **Profiles** menus.

NOTE

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

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

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

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

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

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

Table 32: *802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication** and **Enforcement Details** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that is appended to services using this template. Use this to identify the services that use templates.
Authentication	
Select Authentication Source	Select any available authentication source from the list, the information updated in the **Authentication** and **Enforcement Details** tabs will be auto-populated.
Active Directory Name	Enter the active directory name. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. This field is mandatory.
Identity	Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter DN of the node in your directory tree from which to start searching for records. This field is mandatory.
Enforcement Details	

Table 32: *802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters (Continued)*

Parameter	Description
Attribute Name	The attributes defined in the **Authentication Source** are listed here. Configure an optional enforcement policy based on the following attributes: • Email • Name • Phone • UserDN • Company • member of • Title For example, you can configure an enforcement policy for a contractor specifying that "If Name equals <contractor_name>, then assign the [Contractor] Role."
Attribute Value	Enter the active directory attribute value for the selected name in the **Attribute Name** field.
VLAN ID	Enter the standard RADIUS-IETF VLAN ID.
Wired Network Settings	
Select Switch	Select any switch from the drop-down list.
Device Name	Enter the name of the device.
IP Address	Enter the IP address of the device.
Vendor Name	Select the manufacturer of the wired controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated Change of Authorization (CoA) on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Wireless Network Settings	
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS	Enter the shared secret that is configured on the controller and Policy Manager to send and

Table 32: *802.1X Wired, 802.1X Wireless, and Dell W-Series 802.1X Wireless Service Template Parameters (Continued)*

Parameter	Description
Shared Secret	receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Posture Settings	
Enable Posture Checks	Select the check box to perform health checks post authentication. This enables the **Host Operating System** and **Quarantine Message** fields.
Host Operating System	Select the operating system: Windows, Linux, or Mac OS X.
Quarantine Message	Specify the quarantine message that will appear on the client.

Dell VPN Access with Posture Checks

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

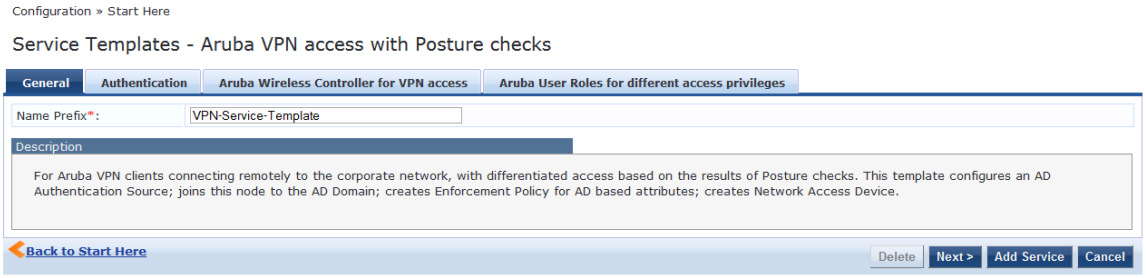
- Configures an AD authentication source
- Joins this node to the AD domain
- Creates an enforcement policy for AD-based attributes
- Creates a NAD

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

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

The following figure displays the **Dell VPN Access with Posture Checks** service template:

Figure 54: *Dell VPN access with Posture checks Service Template*



The following table describes the **Dell VPN Access with Posture Checks** service template parameters:

Table 33: *Dell VPN Access with Posture Checks Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication Dell Wireless Controller for VPN Settings** and **Dell User Roles for different access privileges** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an authentication source from the list. The information provided in the **Authentication**, **Dell Wireless Controller for VPN Settings**, and **Dell User Roles for different access privileges** sections are auto-populated.
Active Directory Name	Enter the Active Directory name.
Description	Enter a description that helps you to identify the characteristics of this template.
Server	Enter the hostname or the IP address of the Active Directory server.
Identity	Enter the Distinguished Name of the administrator account.
NETBIOS	Enter the server Active Directory domain name.
Base DN	Enter the 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 a connection.
Dell Wireless Controller for VPN Access	
Select Wireless Controller	Select a wireless controller from the drop-down list.

Table 33: *Dell VPN Access with Posture Checks Service Template Parameters (Continued)*

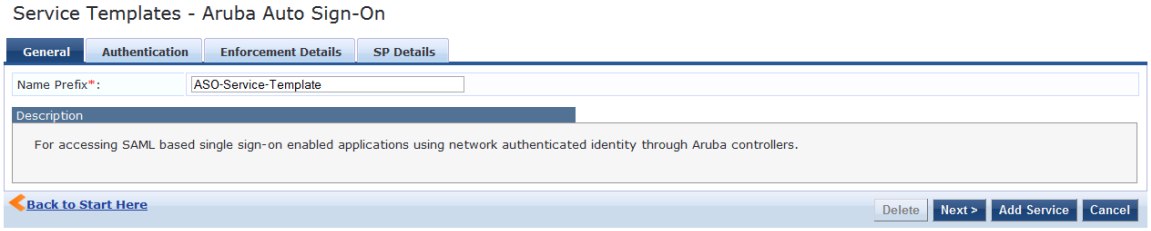
Parameter	Description
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select this option to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Dell User Roles for different access privileges - Create a new Enforcement Policy	
Initial Role (before posture checks)	Enter the initial role of the client before posture checks are performed.
Quarantined Role (failed posture checks)	Enter the role of clients that fail posture checks.
Healthy Role (passed posture checks)	Enter the role of the client after a posture check is passed and deemed healthy.

Aruba Auto Sign-On

This service template allows you to access the SAML-based single sign on enabled applications (such as Policy Manager, Guest, Onboard, and Insight) using a network authenticated (802.1X) identity through Dell controllers.

The following figure displays the **Aruba Auto Sign-On** service template :

Figure 55: *Aruba Auto Sign-On Service Template*



The following table describes the **Aruba Auto Sign-On** service template parameters:

Table 34: *ClearPass Aruba Auto Sign-On Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This field populates the pre-configured information in the **Authentication**, **SP details**, and **Enforcement Details** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select an authentication source from the list. The information provided in the **Authentication**, **Enforcement Details**, and **SP details** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the DN of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the DN of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. This value defaults to 389. This field is mandatory.
Enforcement Details	
Create new Enforcement Policy	The attributes defined in the authentication source are listed here. Configure an optional enforcement policy based on the following attributes: • Department • Email • Name • Phone • UserDN • company • memberOf • Title For example, you can configure an enforcement policy for a contractor as "If Name equals <contractor_name>, then assign the [Contractor] Role."

Table 34: *ClearPass Aruba Auto Sign-On Service Template Parameters (Continued)*

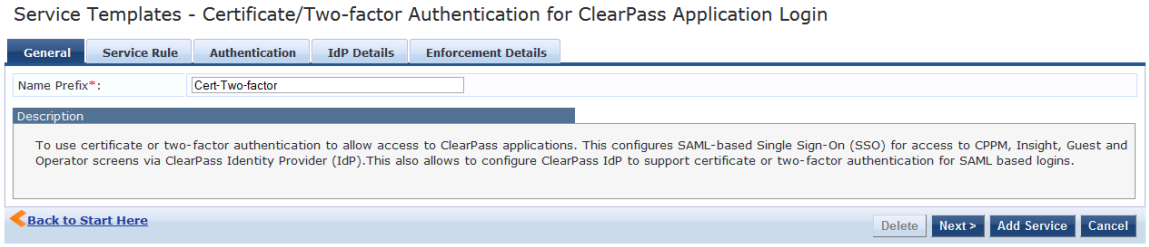
Parameter	Description
SP Details	
SP URL	Enter the Service Provider (SP) URL.
Attribute Name	Enter attribute names and assign values to those names. These name/value pairs are included in SAML responses.
Attribute Value	

Certificate/Two-factor Authentication for ClearPass Application Login

This template is designed to allow the administrators and operators to log in to CPPM using smart card and TLS certificates. Ensure that the services are configured using **Certificate/Two-factor Authentication for ClearPass Application Login** service template to log in using smart card and TLS certificates.

The following figure displays the **Certificate/Two-factor Authentication for ClearPass Application Login** service template:

Figure 56: *Certificate/Two-factor Authentication Service Template*



The following table describes the **Certificate/Two-factor Authentication for ClearPass Application Login** service template parameters:

Table 35: *ClearPass Certificate/Two-factor Authentication Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This field populates the pre-configured information in the **Authentication**, **SP details**, and **Enforcement Details** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Application	Select the application for which SAML-based Single Sign-On (SSO) should be enabled from the following options: Policy Manager, Guest, Insight, and Onboard.
Authentication	

Table 35: *ClearPass Certificate/Two-factor Authentication Service Template Parameters (Continued)*

Parameter	Description
Select Authentication Source	Select an authentication source from the list. The information provided in the **Authentication**, **Enforcement Details**, and **SP details** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. The default value is value defaults to 389. This field is mandatory.
Identity	Enter the DN of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the DN of the administrator account. This field is mandatory.
IdP Details	
Page Name	Select the Web Login pages from the drop-down list. To create a new Web Login page, click the **Add new Guest Web Login page** link. This opens the ClearPass Guest application in which you can create a new **Guest Web Login** page. Select **Single Sign On -SAML Identity Provider** in the **Vendor Settings** field in the **Web Login** page (**ClearPass Guest** > **Configuration** > **Pages** > **Web Logins**) to log in using smart card and TLS certificates. When you select Optional - Request a client certificate from the user, but allow none from the **Client Certificate** field, user need to provide certificate, username, and password. When you select **Required - Require a client certificate from the user** from the **Client Certificate** field, user need to provide only certificates for authentication. This enables the **Authentication** field with the following drop-down options: • **Certificate only - No username or password required -** Need only certificate authentication. • **Credentials - Also require a username and password** - Need username and password
Enforcement Details	

Table 35: *ClearPass Certificate/Two-factor Authentication Service Template Parameters (Continued)*

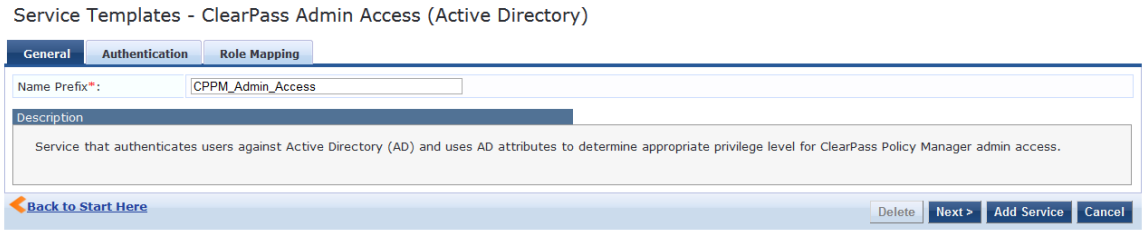
Parameter	Description
Certificate Attribute - Super Admin Condition	Select the certificate attribute from the drop-down list. Enter the value in the **Super Admin Condition** field that matches the **Certificate Attribute** value to provide the super administrator access.
Certificate Attribute - Read Only Admin Condition	Select the certificate attribute from the drop-down list. Enter the value in the **Read Only Admin Condition** field that matches the **Certificate Attribute** value to provide the Read Only administrator access.
Certificate Attribute - Help Desk Admin Condition	Select the certificate attribute from the drop-down list. Enter the value in the **Help Desk Admin Condition** field that matches the **Certificate Attribute** value to provide the help desk administrator access.

ClearPass Admin Access

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

The following figure displays the **ClearPass Admin Access** service template:

Figure 57: *ClearPass Admin Access Service Template*



The following table describes the **ClearPass Admin Access** service template parameters:

Table 36: *ClearPass Admin Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication** and **Role Mapping** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication	Select an authentication source from the list. The information updated in the **Authentication** and **Role Mapping** tabs are auto-populated.

Table 36: *ClearPass Admin Access Service Template Parameters (Continued)*

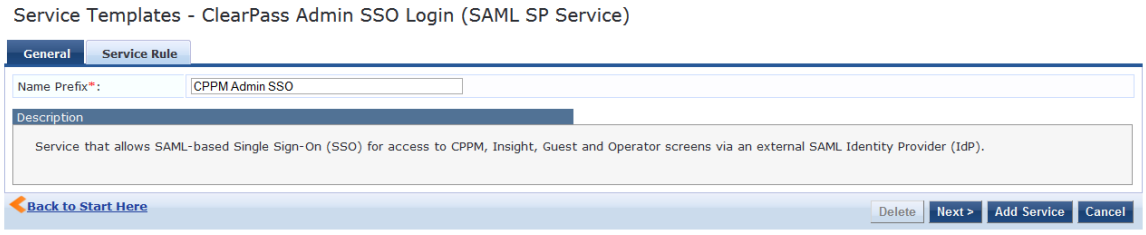
Parameter	Description
Source	
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the DN of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the DN of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. This field is mandatory.
Role Mapping	
Attribute Name	Select the active directory attribute.
Super Admin Condition	Defines the various privilege levels.
Read Only Admin Condition	
Help Desk Condition	

ClearPass Admin SSO Login (SAML SP Service)

This application service template allows Security Asserting Markup Language (SAML) based Single Sign-On (SSO) authenticated users to access Policy Manager, Guest, Insight, and Operator pages.

The following figure displays the **ClearPass Admin SSO Login** service template:

Figure 58: *ClearPass Admin SSO Login (SAML SP Service) Service Template*



The following table describes the **ClearPass Admin SSO Login** service template parameters:

Table 37: ClearPass *Admin SSO Login Service Template Parameters*

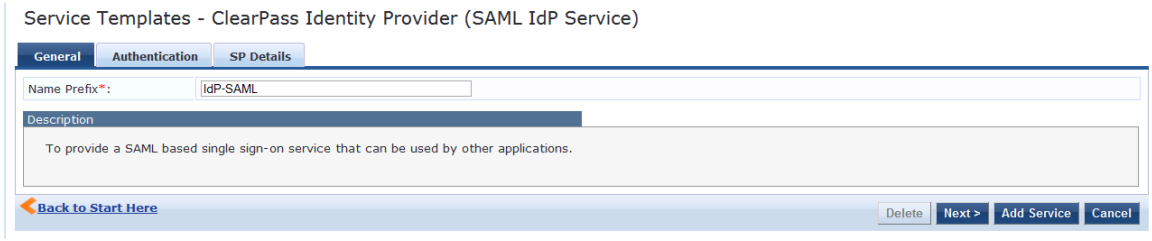
Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Service Rule** tab. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use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

ClearPass Identity Provider (SAML IdP Service)

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

The following figure displays the **ClearPass Identity Provider (SAML IdP Service)** service template:

Figure 59: *Identity Provider (SAML IdP Service)*



The following table describes the **ClearPass Identity Provider (SAML IdP Service)** service template parameters:

Table 38: *ClearPass Identity Provider (SAML IdP Service) Service Template Parameters*

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

Table 38: *ClearPass Identity Provider (SAML IdP Service) Service Template Parameters (Continued)*

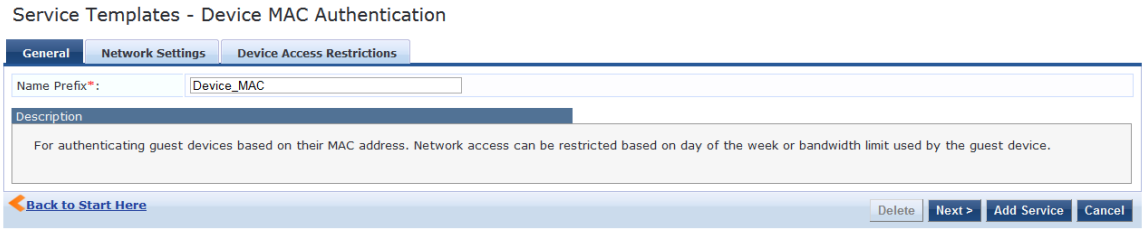
Parameter	Description
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address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

Device Mac Authentication

This template is designed for authenticating guest devices based on their MAC address. You can limit the network access for guest devices that do not have user directly associated with them for a specific duration in days or the bandwidth limit.

The following figure displays the **Device Mac Authentication** service template:

Figure 60: *Device Mac Authentication Service Template*



The following table describes the parameters used in the **Device Mac Authentication** service template:

Table 39: *Device Mac Authentication Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication** and **SP Details** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Network Settings	
Select Device	Select a pre-configured device from the drop-down list. To create a new device, leave this field blank and enter the remaining fields.
Device Name	The name of the device is populated automatically based on the device selected from the **Select Device** field. If you create a new device, enter the name of the device.
IP Address	The IP address of the device is populated automatically based on the device selected from the **Select Device** field. If you create a new device, enter the name of the device.
Vendor Name	The name of the manufacturer of the device is populated automatically based on the device selected from the **Select Device** field. If you create a new device, enter the name of the manufacturer of the device.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated Change of Authorization (CoA) on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Device Access Restrictions	
Days allowed for access	Select the days on which network access is allowed.
Maximum bandwidth allowed per device	Enter a number to set an upper limit for the amount of data in megabytes to which a device is allowed per day. A value of 0 (zero), the default, means no limit is set.

EDUROAM Service

This template is designed for the following scenarios:

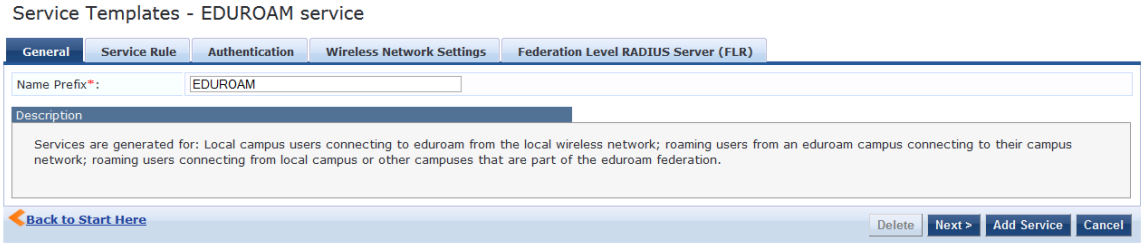
- Local campus users connecting to eduroam from the local wireless network.
- Roaming users from an eduroam campus connecting to their campus network.
- Roaming users connecting from local campus or other campuses that are part of the eduroam federation.

NOTE

You cannot view the **EDUROAM** service template if the **HCG** mode is enabled in the cluster.

The following figure displays the **EDUROAM** service template:

Figure 61: *EDUROAM Service Template*



The following table describes the parameters used in the **EDUROAM** service template:

Table 40: *EDUROAM Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Authentication, Service Rule, Wireless,** and**Federation Level Radius Server (FLR) tabs**. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Enter domain details	Enter the domain name of the network. For example, @edunet.ucla.com. This field is mandatory.
Select Vendor	Select the vendor of the network device. This field is mandatory.
Authentication	
Select Active Directory	Select an authentication source from the list, the information updated in the **Authentication**, **Wireless**, and **Federation Level Radius Server (FLR)** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the DN of the administrator account. This field is mandatory.
NETBIOS	Enter the server Active Directory domain name. This field is mandatory.

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

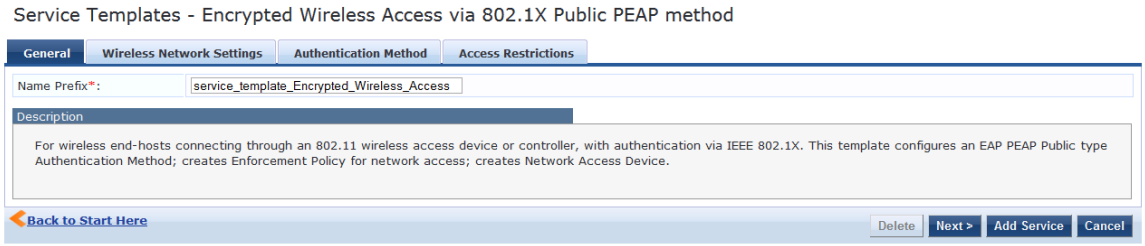
Parameter	Description
Base DN	Enter the DN of the administrator account. This field is mandatory.
Password	Enter the account password. This field is mandatory.
Port	Enter the TCP port where the server is listening for a connection. This field is mandatory.
Wireless Network Settings	
Select wireless controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Federation Level RADIUS Server (FLR)	
Host Name	Enter the hostname of the federation RADIUS server.
IP Address	Enter the IP address of the federation RADIUS server.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
RADIUS Authentication Port	Enter a port number here.
RADIUS Accounting Port	Enter a port number here.

Encrypted Wireless Access via 802.1X Public PEAP method

This template is designed for providing encrypted wireless access to users using fixed 802.1X PEAP credentials. This template configures an **EAP PEAP Public** type authentication method and creates enforcement policy for network access.

The following figure displays the **Encrypted Wireless Access via 802.1X Public PEAP method** service template:

Figure 62: *Encrypted Wireless Access via 802.1X Public PEAP method Service Template*



The following table describes the parameters used in the **Encrypted Wireless Access via 802.1X Public PEAP method** service template:

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

Parameter	Description
General	
Name Prefix	Enter a prefix that you want to append to services using this template. You can use this to identify services that use templates.
Wireless Network Settings	
Select wireless controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the IP address of the wireless controller.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Authentication Method	
Public Username	Enter public username for EAP PEAP Public type authentication method.

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

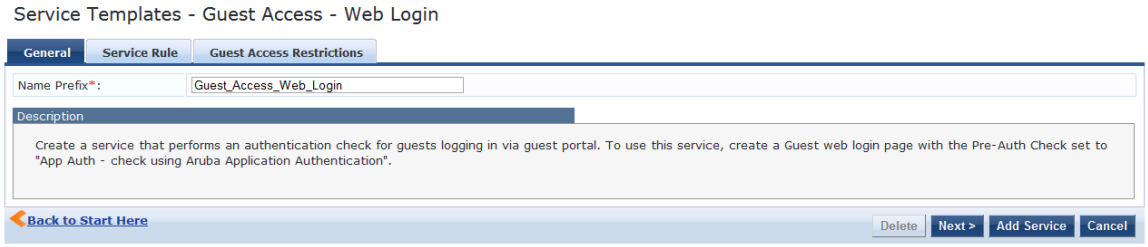
Parameter	Description
Public Password	Enter password for EAP PEAP Public type authentication method.
Access Restrictions	
Days allowed for access	Select the days on which network access is allowed.

Guest Access Web Login

This service authenticates guests logging in using the Guest portal. To use this service, create a **Guest Web Login** page that sets the **Pre-Auth Check** option to **AppAuth - Check** using **Dell Application Authentication**.

The following figure displays the **Guest Access Web Login** service template:

Figure 63: *Guest Access Web Login Service Template*



The following table describes the **Guest Access Web Login** service template parameters:

Table 42: *Guest Web Login Service Template Parameters*

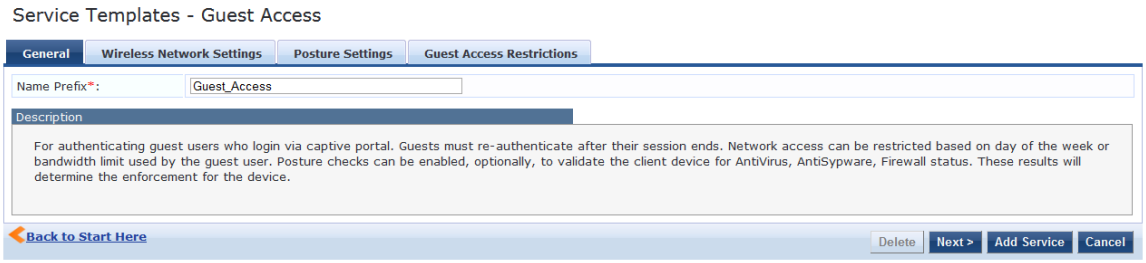
Parameter	Description
General	
Select Prefix	Select any one prefix from the existing list of prefixes. This populates the pre-configured information in the **Service Rule** and **Guest Web Login** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append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

Guest Access

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

The following figure displays the **Guest Access** service template:

Figure 64: *Guest Access Service Template*



The following table describes the parameters used in the **Guest Access** service template:

Table 43: *Guest Access Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select any one prefix from the existing list of prefixes. This populates the pre-configured information in the **Wireless Network Settings** and **Guest Access Restrictions** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Wireless Network Settings	
Wireless SSID for Guest access	Enter the SSID value here.
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.

Table 43: *Guest Access Service Template Parameters (Continued)*

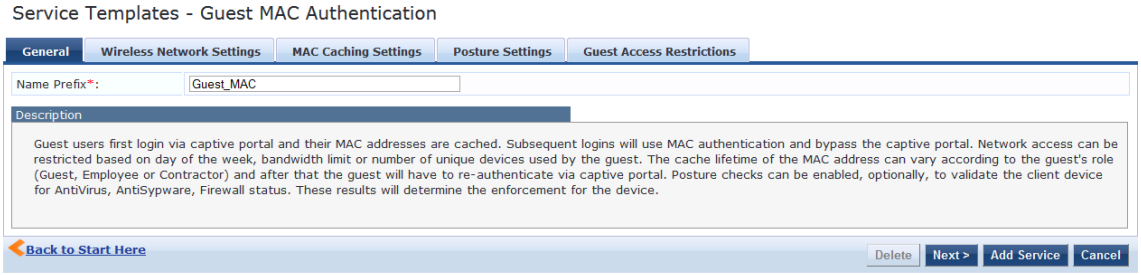
Parameter	Description
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.
Posture Settings	
Enable Posture Checks	Select the check box to perform health checks post authentication. This enables the **Host Operating System** and **Quarantine Message** fields.
Host Operating System	Select the operating system: Windows, Linux, or Mac OS X.
Quarantine Message	Specify the quarantine message that will appear on the client.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

Guest MAC Authentication

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

The following figure displays the **Guest MAC Authentication** service template:

Figure 65: *Guest MAC Authentication Service Template*



The following table describes the **Guest MAC Authentication** service template parameters:

Table 44: *Guest MAC Authentication Service Template Parameters*

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

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

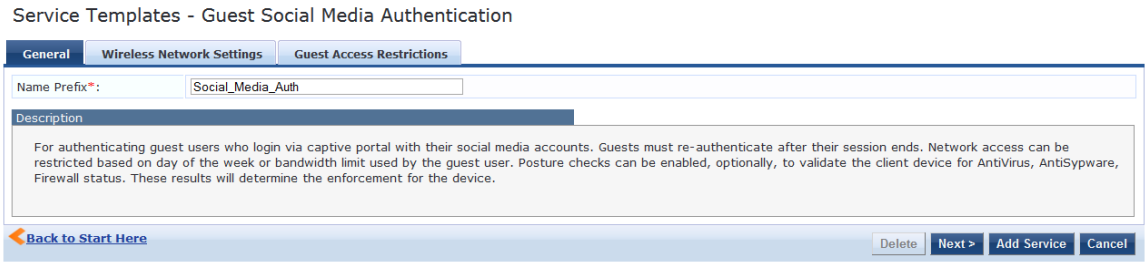
Parameter	Description
Checks	**Operating System** and **Quarantine Message** fields.
Host Operating System	Select the operating system: Windows, Linux, or Mac OS X.
Quarantine Message	Specify the quarantine message that will appear on the client.
Initial Role/VLAN	Enter the initial role of the client before posture checks are performed.
Quarantine Role/VLAN	Enter the role of clients that fail posture checks.
Guest Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum number of devices allowed per user	Enter a number to define how many devices users can connect to the network.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

Guest Social Media Authentication

This template is designed for authenticating guest users logging in through captive portal with their social media accounts such as Google, Facebook, LinkedIn, and Twitter. Guests must re-authenticate after the session ends.

The following figure displays the **Guest Social Media Authentication** service template:

Figure 66: *Guest Social Media Authentication Service Template*



The following table describes the **Guest Social Media Authentication** service template parameters:

Table 45: *Guest Social Media Service Template Parameters*

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

Table 45: *Guest Social Media Service Template Parameters (Continued)*

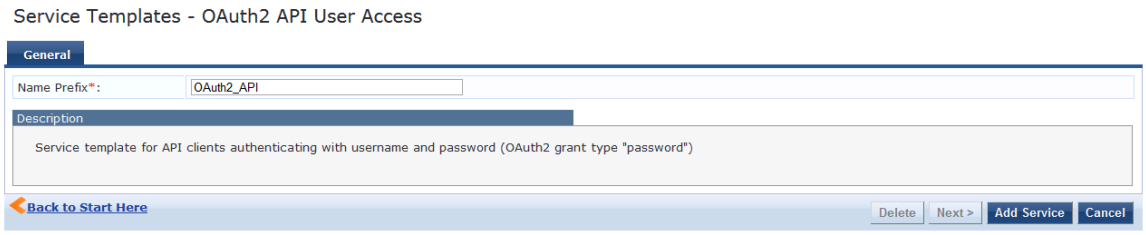
Parameter	Description
Social login Provider	Select the social media network options: Google, Facebook, LinkedIn, and Twitter.
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

OAuth2 API User Access

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

The following figure displays the **OAuth2 API User Access** service template:

Figure 67: *OAuth2 API User Access Service Template*



The following table describes the **OAuth2 API User Access** service template parameters:

Table 46: *OAuth2 API User Access Service Template Parameters*

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

Onboard

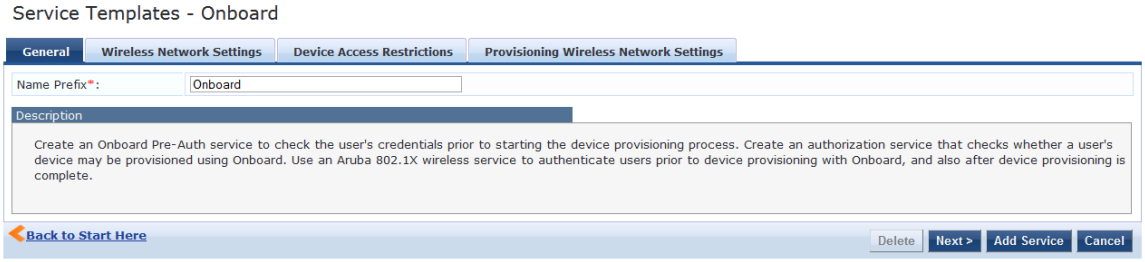
This template is designed for configuration that allows to perform checks before allowing Onboard provisioning for Bring Your Own Device (BYOD) use-cases. This service creates an Onboard Pre-Auth service to check the user's credentials before starting the device provisioning process. This also creates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

NOTE

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

The following figure displays the **Onboard Authorization** service template:

Figure 68: *Onboard Authorization Service Template*



The following table describes the **Onboard Authorization** service template parameters:

Table 47: *Onboard Authorization Service Template Parameters*

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

Table 47: *Onboard Authorization Service Template Parameters (Continued)*

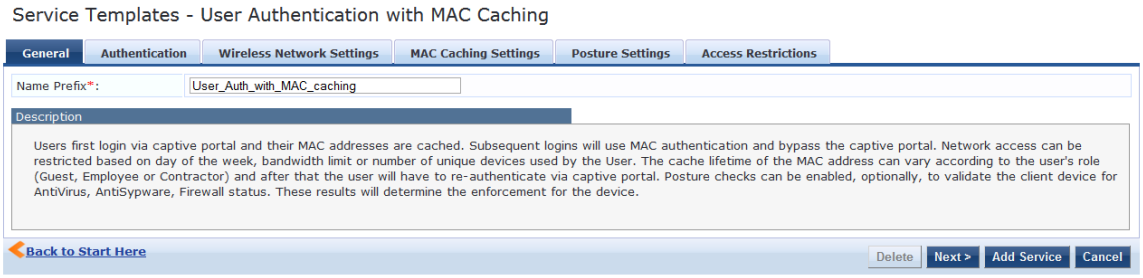
Parameter	Description
Device Access Restrictions	
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Provisioning Wireless Network Settings	
Wireless SSID for Onboard Provisioning	Enter the SSID of your network.
Add new Onboard Network settings	Click the **Add new Onboard Network settings** link to launch the Web UI to modify the Onboard Network settings.

User Authentication with MAC Caching

This template is designed for authenticating users once using captive portal and later to allow log-ins using cached MAC Address of the device. Users first log-in using captive portal and their MAC addresses are cached. Subsequent log-ins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit, or number of unique devices used by the user. The cache lifetime of the MAC address can vary according to the user's role such as Guest, Employee, or Contractor and after that the user will have to re-authenticate through captive portal. Posture checks can be enabled, optionally, to validate the client device for AntiVirus, AntiSypware, Firewall status. These results will determine the enforcement for the device.

The following figure displays the **User Authentication with MAC Caching** service template:

Figure 69: *User Authentication with MAC Caching Service Template*



The following table describes the **User Authentication with MAC Caching** service template parameters:

Table 48: *User Authentication with MAC Caching Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the pre-configured information in the **Wireless Network Settings, MAC Caching Settings,** and **Guest Access restrictions** tabs. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication	
Select Authentication Source	Select the authentication source from the drop-down list. Select Create a new Active Directory option to select a new authentication source.
Wireless Network Settings	
Wireless SSID	Enter the SSID name of your network.
Select wireless controller	Select the wireless controller from the drop-down list if you already configured.
Wireless controller name	Enter the name of the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.

Table 48: *User Authentication with MAC Caching Service Template Parameters (Continued)*

Parameter	Description
MAC Caching Settings	
Cache duration for Employee	Enter the duration from the options: One day, One week, One month, or Six months to which the MAC account will remain valid for the **Employee** role. After this the guest must re-authenticate using captive portal.
Cache duration for Guest	Enter the duration from the options: Account Expiry Time, One day, One week, One month, or Six months to which the MAC account will remain valid for the **Guest** role. After this the guest must re-authenticate using captive portal. **NOTE:** You must enter cache duration for at least one role.
Cache duration for Contractor role	Enter the duration from the options: Account Expiry Time, One day, One week, One month, or Six months to which the MAC account will remain valid for the **Contractor** role. After this the guest must re-authenticate using captive portal.
Posture Settings	
Enable Posture Checks	Select the check box to perform health checks post authentication.
Host Operating System	Select the type of the host operating system: Windows, Linux, or Mac OS X.
Quarantine Message	Specify the quarantine message that will appear on the client.
Initial Role/VLAN	Enter the initial role of the client before posture checks are performed.
Quarantine Role/VLAN	Enter the role of clients that fail posture checks.
Access Restrictions	
Guest Role/VLAN	Enter the Guest role to which the access to be restricted.
Employee Role/VLAN	Enter the Employee role to which the access to be restricted.
Contractor Role/VLAN	Enter the Contractor role to which the access to be restricted.
Captive Portal Role/VLAN	Enter the Captive Portal role to which the access to be restricted.
Days allowed for access	Select the duration in number of days to enable on which the guest users are allowed network access.
Maximum number of devices allowed per user	Enter a number to define how many devices users can connect to the network.
Maximum bandwidth allowed per user	Enter a number to set an upper limit for the amount of data in megabytes to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

Policy Manager Service Types

The following service types are available in Policy Manager:

Dell 802.1X Wireless

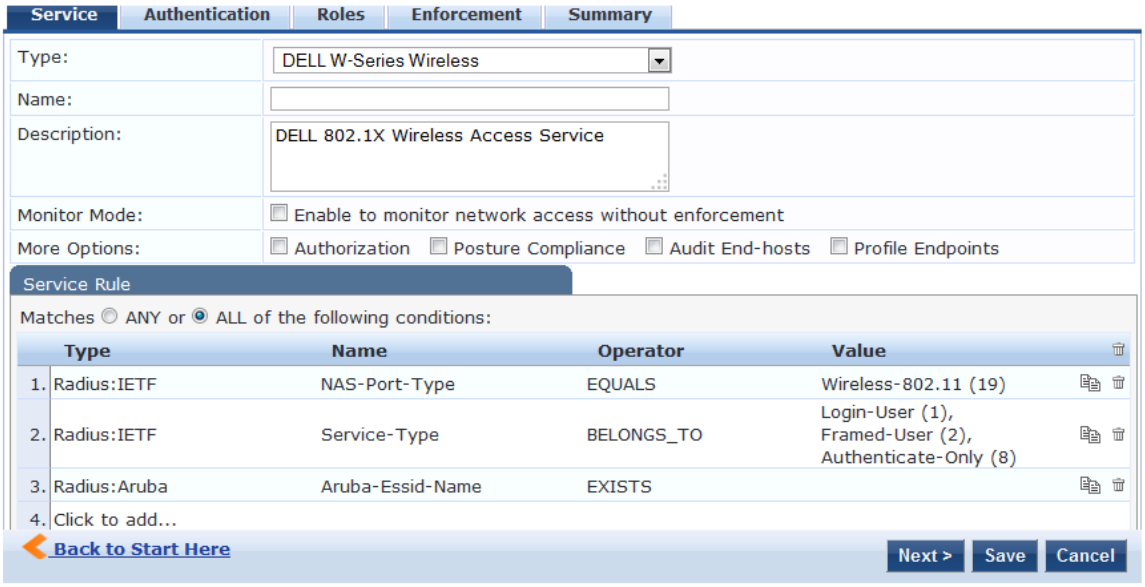
Configure this service for wireless hosts by connecting through a Dell 802.1X wireless access device or controller with authentication using IEEE 802.1X. Service rules are customized for a typical Dell W-Series Controller deployment. By default, the Dell W-Series 802.1X service includes a rule that specifies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

The following are the default configuration tabs available in the **Add Service (Configuration > Services > Add)** page:

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

The following figure displays the **Dell 802.1X Wireless** service configuration fields:

Figure 70: *Dell 802.1X Wireless Service*

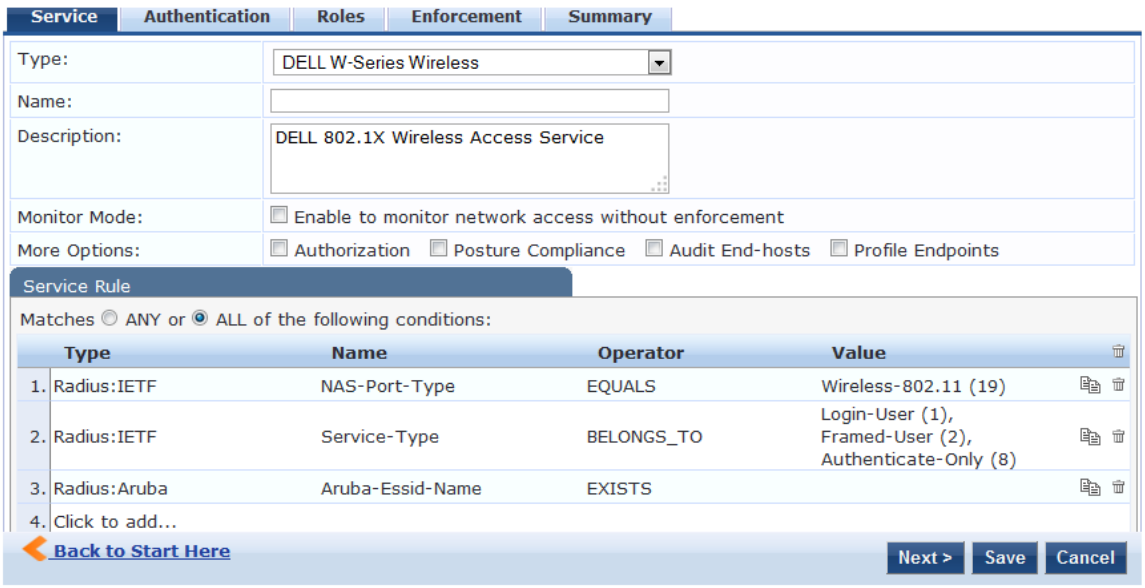


Service Tab

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

The following figure displays the **Service** tab:

Figure 71: *Dell 802.1X Wireless Service - Service Tab*



The following table displays the **Service** tab parameters:

Table 49: *Dell 802.1X Wireless Service - Service Tab Parameters*

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

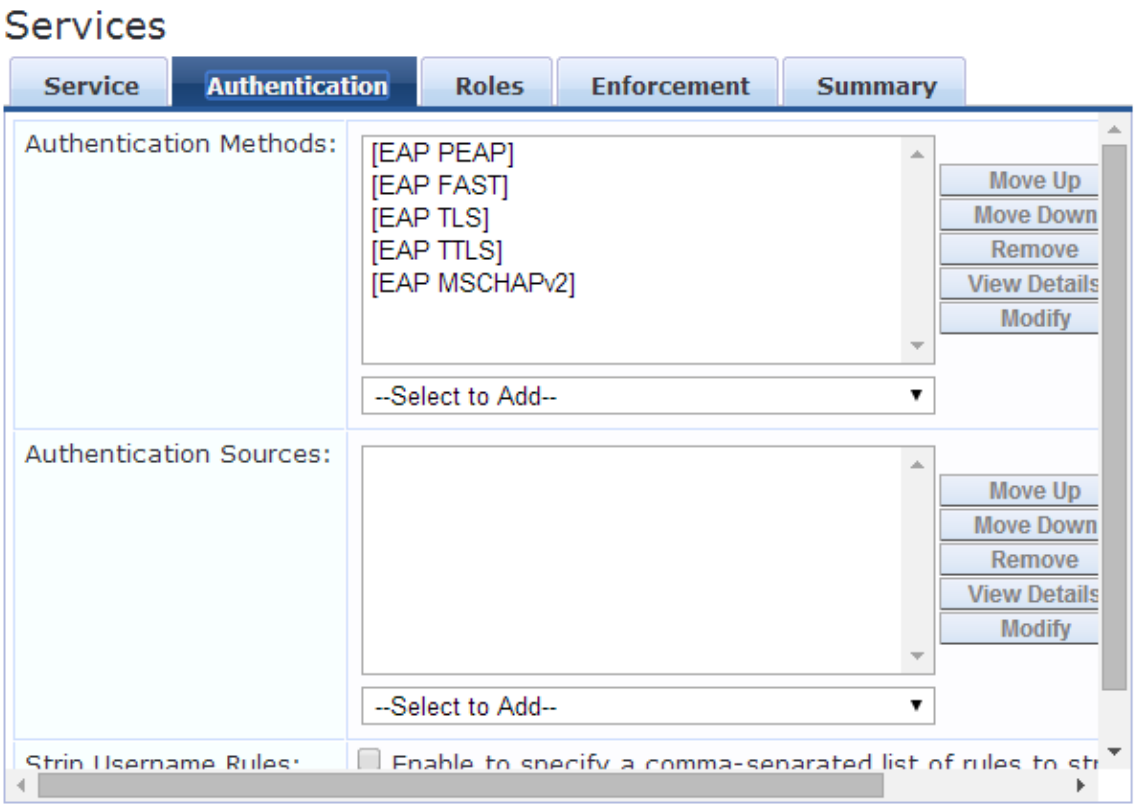
Service rules define a set of criteria that supplicants must match to trigger the service. Some service templates have one or more rules pre-defined. Click on a service rule to modify its options.

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

Authentication Tab

The **Authentication** tab contains options for configuring authentication methods and authentication sources. The following figure displays the **Authentication** tab:

Figure 72: *Dell 802.1X Wireless Service - Authentication Tab*



The following table displays the **Authentication** tab parameters:

Table 50: *Dell 802.1X Wireless Service - Authentication Tab Parameters*

Parameter	Description
Authentication Methods	Select authentication methods using the **Select to Add** field used for this service depend on the 802.1X supplicants and the type of authentication methods you choose to deploy. Policy Manager automatically selects the appropriate method for authentication, when a user attempts to connect. The common types, which are automatically selected include the following examples: • EAP PEAP • EAP FAST • EAP TLS • EAP TTLS The **EAP-MD5** authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** mode. The order of authentication is significant, when a client tries to perform an 802.1X authentication. Policy Manager proposes the first authentication method configured. However, the client can accept the authentication method proposed by Policy Manager and continue authentication or send a Negative-Acknowledgment (NAK) and propose a different authentication method. If the newly proposed authentication method is also configured, then the authentication proceeds, otherwise authentication fails. If most of the clients in the network use a specific authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged. For more information, see the following: • Adding and Modifying Authentication Methods on page 145 • Adding and Modifying Authentication Sources on page 169.
Authentication Sources	Specify the authentication sources using the **Select to Add** field. This can be one or more instances of the following examples: • Active Directory • LDAP Directory • SQL DB • Token Server • Policy Manager local DB
Strip Username Rules	Select the check box to pre-process the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

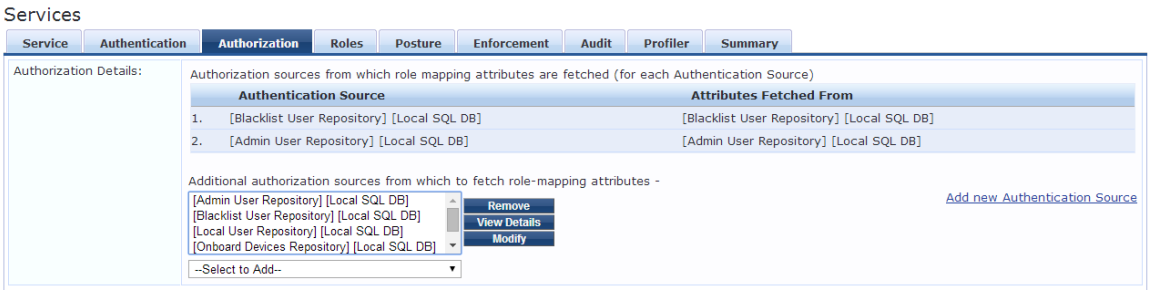
Authorization Tab

Use the **Authorization** tab to select the authorization sources for this service. The **Authorization** tab is not displayed by default. To access this tab, select the **Authorization** check box from **More Options** on the **Services** tab. Policy Manager fetches role mapping attributes from the authorization sources associated with the service, regardless of which authentication source was used to authenticate the user. For a given service, role mapping attributes are fetched from the following authorization sources:

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

The following figure displays the **Authorization** tab:

Figure 73: *Dell 802.1X Wireless Service - Authorization Tab*



The following table displays the **Authorization** tab parameters:

Table 51: *Dell 802.1X Wireless Service - Authorization Tab Parameters*

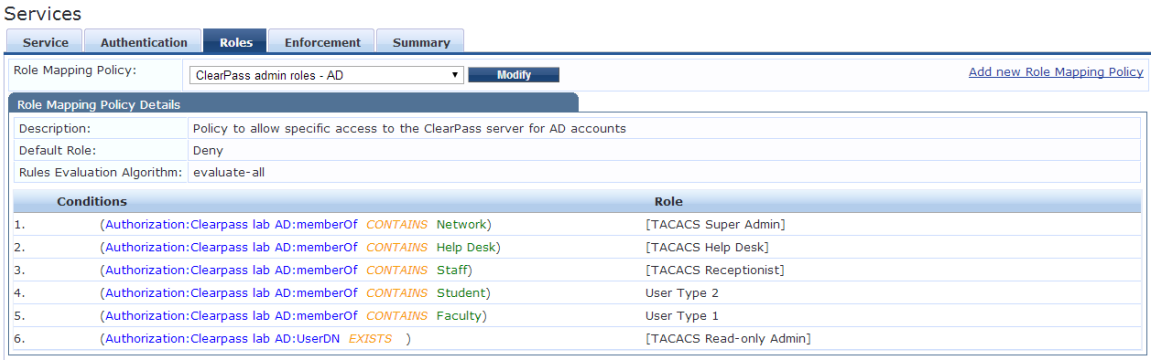
Parameter	Description
Authentication Source	Displays the authorization sources from which role mapping attributes are fetched for each authentication source.
Attributes Fetched From	Displays the source of attributes.
Additional authorization sources from which to fetch role-mapping attributes	Select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

For more information on configuring authorization sources, see Adding and Modifying Authentication Methods on page 145.

Roles Tab

Use the **Roles** tab to associate a role mapping policy with this service. The following figure displays the **Dell 802.1X Wireless Service - Roles** tab:

Figure 74: *Dell 802.1X Wireless Service - Roles Tab*



The following table displays the **Roles** tab parameters:

Table 52: *Dell 802.1X Wireless Service - Roles Tab Parameters*

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

For information on configuring role mapping policies, see Configuring a Role and Role Mapping Policy on page 224.

Posture Tab

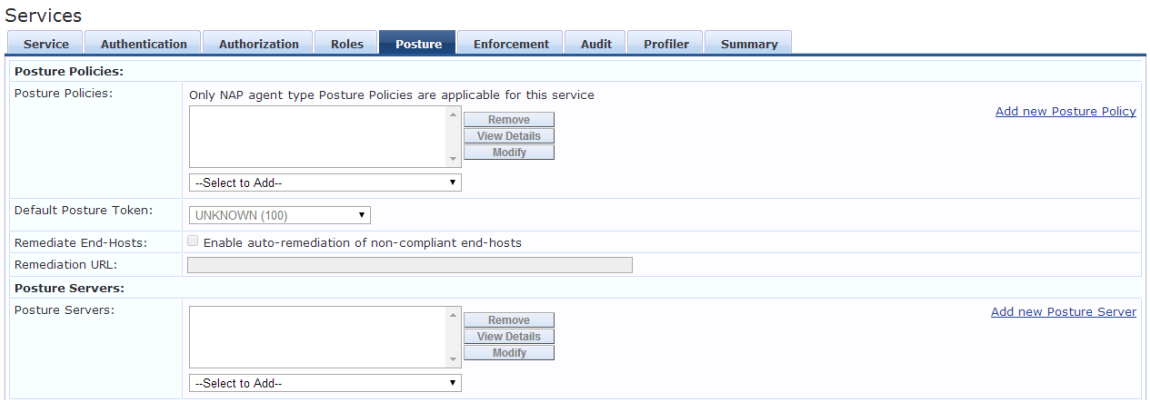
The **Posture** tab is not enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box from the **More Options** field on the **Service** tab. You can enable the posture checking for this kind of service, if you deploy any of the following:

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

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

The following figure displays the **Posture** tab:

Figure 75: *Dell 802.1X Wireless Service - Posture Tab*



The following table displays the **Posture** tab parameters:

Table 53: *Dell 802.1X Wireless Service - Posture Tab Parameters*

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

For more information on configuring posture polices and posture servers, see

- Configuring Posture Policy Agents and Hosts on page 230
- Configuring Posture Servers on page 282

Enforcement Tab

Use this tab to select an enforcement policy for a service. The following figure displays the **Enforcement** tab:

Figure 76: *Dell 802.1X Wireless Service - Enforcement Tab*

The following table displays the **Enforcement** tab parameters:

Table 54: *Dell 802.1X Wireless Service - Enforcement Tab Parameters*

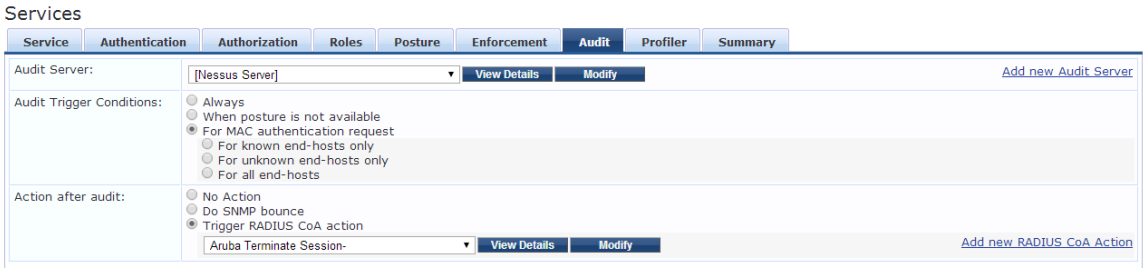
Parameter	Description
Use Cached Results	Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	Select the pre-configured enforcement policy from the drop-down list. This is mandatory. If you do not have any pre-configured enforcement policies, click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

For more information, see Configuring Enforcement Policies on page 1.

Audit Tab

Use the **Audit** tab to enable the Audit checking for this service. Select the **Audit End-hosts** check box from the **More Options** field on the **Service** tab to enable the **Audit** tab. The following figure displays the **Audit** tab:

Figure 77: *Dell 8021X Wireless Service - Audit Tab*



The following table displays the **Audit** tab parameters:

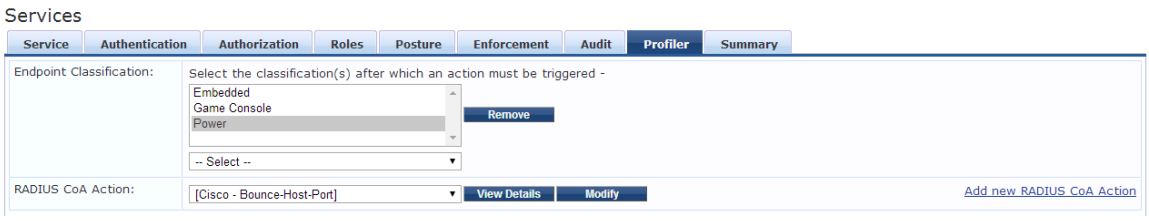
Table 55: *Dell 802.1X Wireless Service - Audit Tab Parameters*

Parameter	Description
Audit Server	Select the audit server from the following options: • **Nessus Server** - Interfaces with Policy Manager primarily to perform vulnerability scanning • **Nmap Audit** - Performs specific audit functions You can click the **View Details** button to view the **Policy Manager Entity Details** pop-up with the summary of audit server details. Click the **Modify** button to view the **Summary** tab with audit server details.
Audit Trigger Conditions	Select an audit trigger condition. Known end hosts are the clients that are found in the authentication source(s) associated with this service.
Action after audit	Specifies the audit that can be performed only after the MAC authentication request is completed and the client has acquired an IP address through DHCP. Once the audit results are available, Policy Manager re-applies policies on the network device in one of the following ways: • **No Action** - The audit does not apply policies on the network device after completing this audit. • **Do SNMP bounce** - This option bounces the switch port or forces an 802.1X re-authentication (both done using SNMP). Bouncing the port triggers a new 802.1X or MAC authentication request by the client. If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager. • **Trigger RADIUS CoA action** - This option sends a RADIUS CoA command from Policy Manager to the network device.

Profiler Tab

The **Profiler** tab is not displayed by default. To access this tab, select the **Profile Endpoints** check box from the **More Options** field on the **Services** tab. The following figure displays the **Profiler** tab:

Figure 78: *Dell 802.1X Wireless Service - Profiler Tab*



The following table displays the **Profiler** tab parameters:

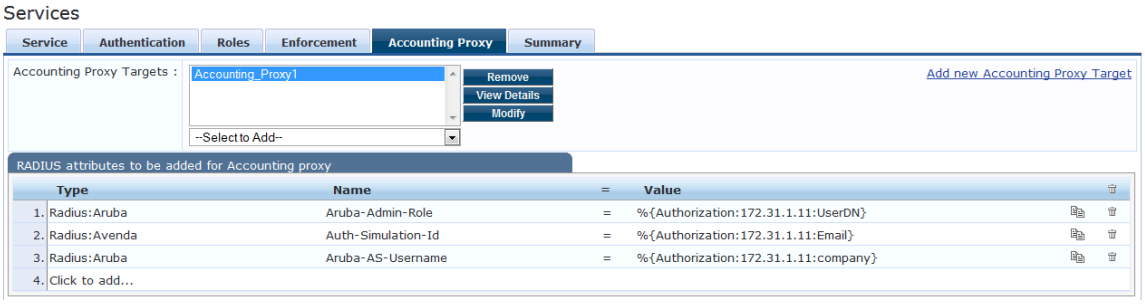
Table 56: *Dell 802.1X Wireless Service - Profiler Tab Parameters*

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

Accounting Proxy Tab

Use the **Accounting Proxy** tab to broadcast the RADIUS accounting packets to all the proxy targets. You can configure the proxy targets to which RADIUS server should be forwarded and attributes to be added in the accounting. This enables the external security solutions (For example, CheckPoint, Fortinet, or Bluecoat) to use the RADIUS account event to detect when a user connects and disconnects to the server configuration. The following figure displays the **Accounting Proxy** tab:

Figure 79: *802.1X Wireless - Accounting Proxy Tab*



The following table describes the **Accounting Proxy** parameters:

Table 57: *Dell 802.1X Wireless Service - Accounting Proxy Tab Parameters*

Parameter	Description
Accounting Proxy Targets	Specify the proxy targets to which RADIUS server should be forwarded and attributes to be added in the accounting. Select the accounting proxy target from the **Select to Add** drop-down list.
Add new Accounting Proxy Target	Click this link to add a new accounting proxy target.
RADIUS attributes to be added for Accounting proxy	

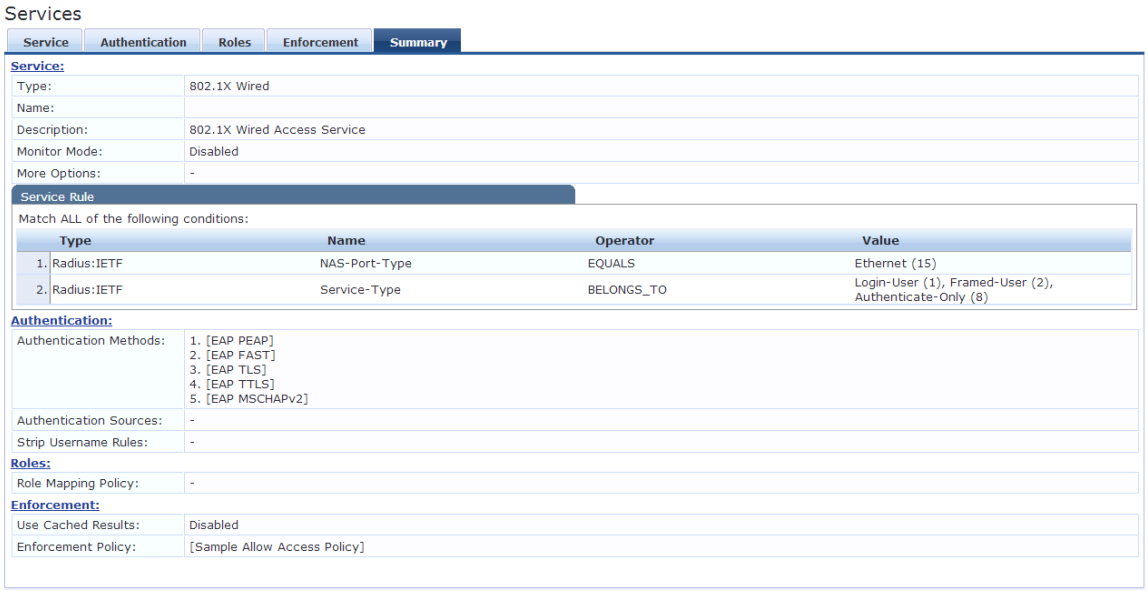
Table 57: *Dell 802.1X Wireless Service - Accounting Proxy Tab Parameters (Continued)*

Parameter	Description
Type	Select the RADIUS attribute type from the drop-down list.
Name	Select the name of the RADIUS attribute from the drop-down list.
Value	Select the value: parameter, static, or role from the drop-down list. The values displayed here is depend on the name of the RADIUS attribute selected.

Summary Tab

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

Figure 80: *Dell 802.1X Wireless Service - Summary Tab*



802.1X Wireless

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

- Service
- Authentication
- Roles
- Enforcement

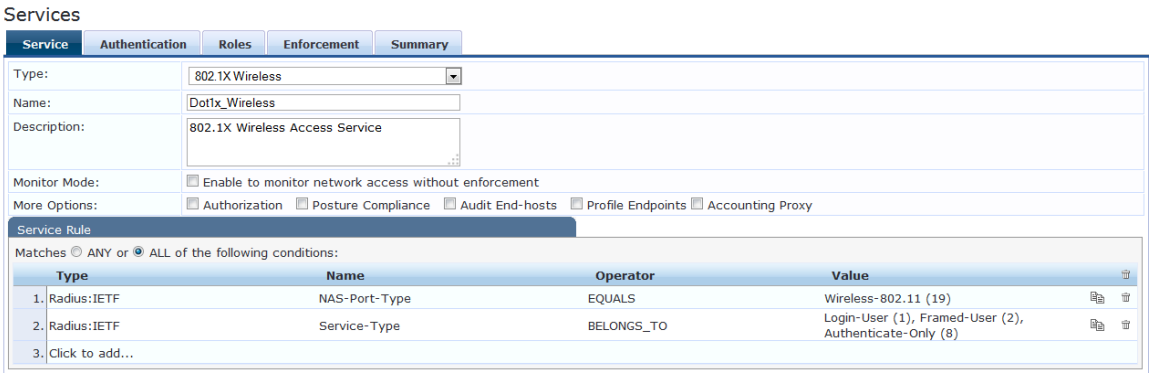
You can also select the following additional tabs by checking the **More Options** field to access these configuration tabs:

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

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

The following figure displays the **802.1X Wireless** service configuration page:

Figure 81: *802.1X Wireless Service*



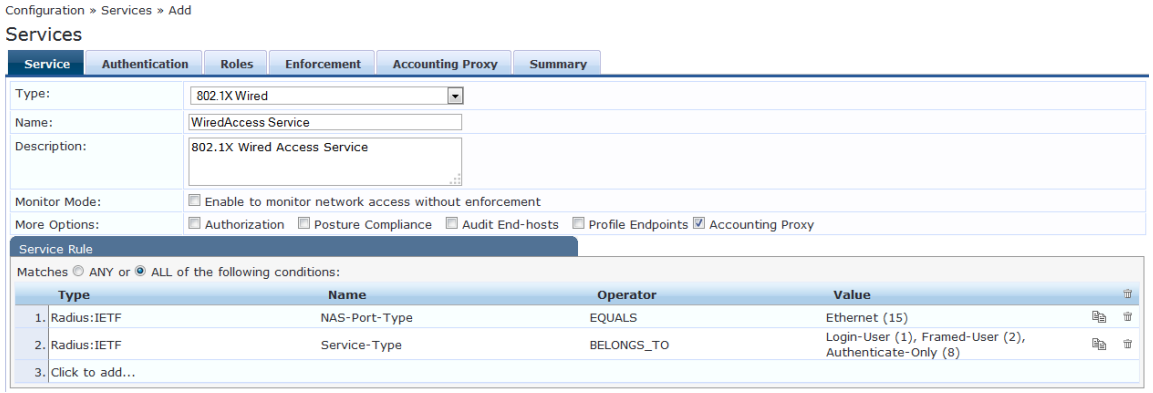
If you want to administer the same set of policies for wired and wireless access, you can combine the service rules to define a single service. The other option is to keep two services for wired and wireless access, but re-use the policy components (authentication methods, authentication source, authorization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

Configuring the 802.1X Wireless service for wireless clients connecting through an 802.11 wireless access device is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see Dell 802.1X Wireless on page 122

802.1X Wired

Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X. Except for the NAS-Port-Type service rule value (which is Ethernet for 802.1X Wired and Wireless 802.11 for 802.1X Wireless), configuration for the rest of the tabs is similar to the Dell 802.1X Wireless service. For more information, see Dell 802.1X Wireless on page 122. The following figure displays the **802.1X Wired** service page:

Figure 82: *802.1X Wired Service*



MAC Authentication

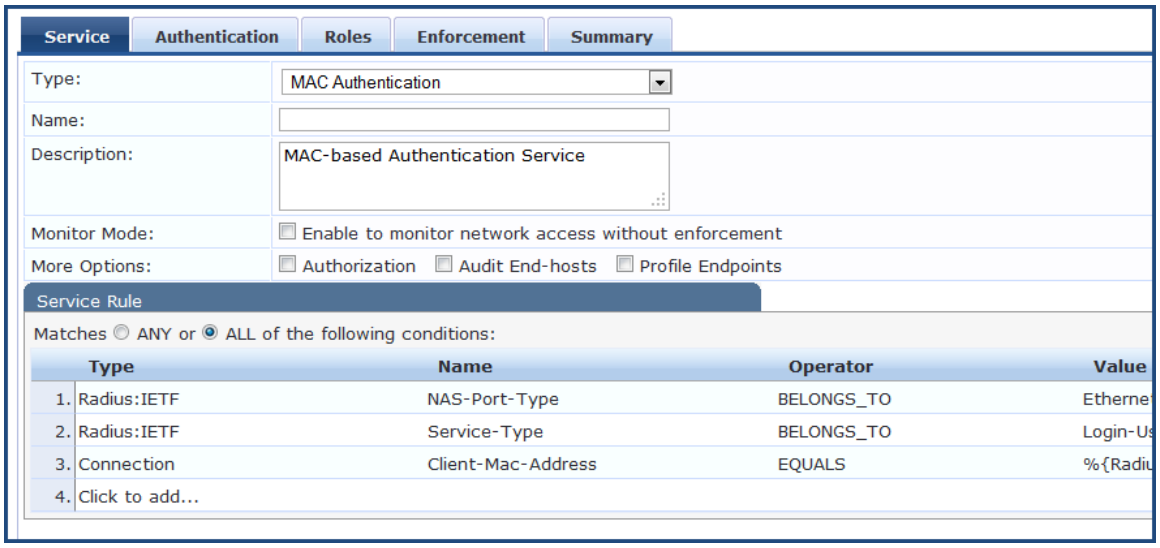
MAC-based authentication service is used for clients without an 802.1X supplicant or a posture agent (printers, other embedded devices, and computers owned by guests or contractors). The network access device sends a

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.

You cannot configure posture for this type of service.

The following figure displays the **MAC Authentication** service:

Figure 83: *MAC Authentication Service*



The **Posture** tab is not available for the MAC-based authentication service. Configuration for the rest of the tabs is similar to the **Dell 802.1X Wireless** service. For more information on configuration tabs, See Dell 802.1X Wireless on page 122 for details.

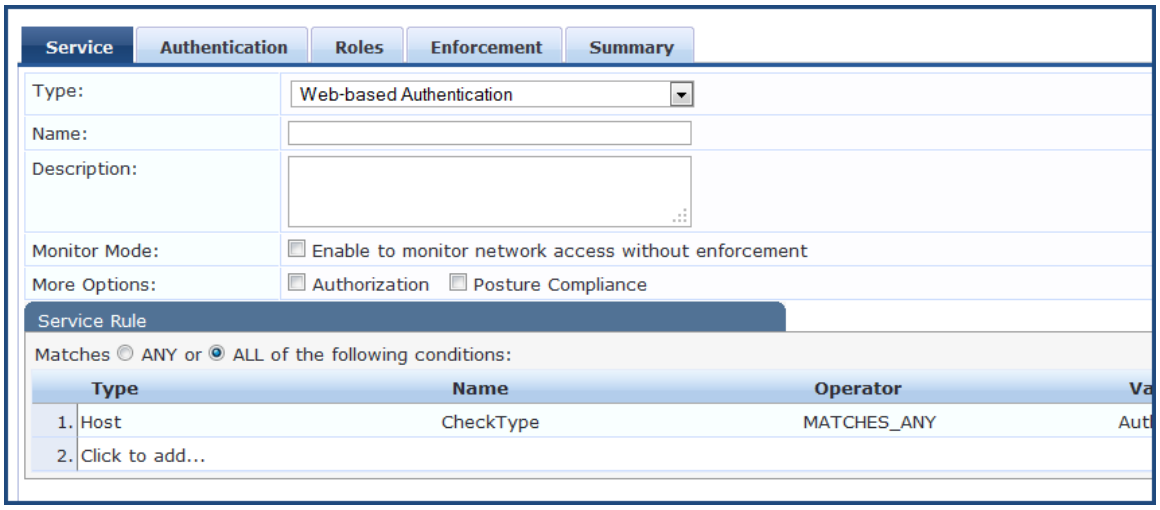
Web-based Authentication

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

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

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

Figure 84: *Web-based Authentication Service*



NOTE

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

Configuring the **Web-based Authentication** service for guests or agentless hosts is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see Dell 802.1X Wireless on page 122.

Web-based Health Check Only

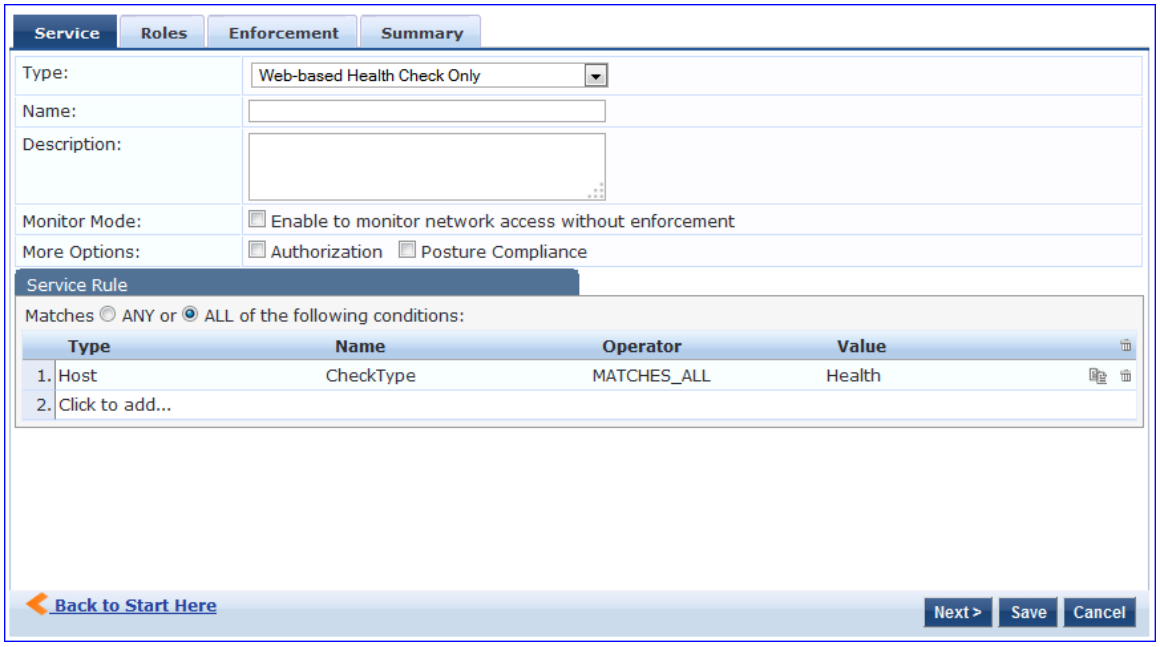
This type of service is the same as the **Web-based Authentication** service except that there is no authentication performed; only health check is done. The internal service rule **Connection:Protocol EQUALS WebAuth** categorizes requests into this type of service. The external service rule **Host:CheckType EQUALS Health** is automatically added when you select this type of service. For more information, see Web-based Authentication on page 135.

NOTE

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

The following figure displays the **Web-Based Health Check Only** service:

Figure 85: *Web-Based Health Check Only Service*

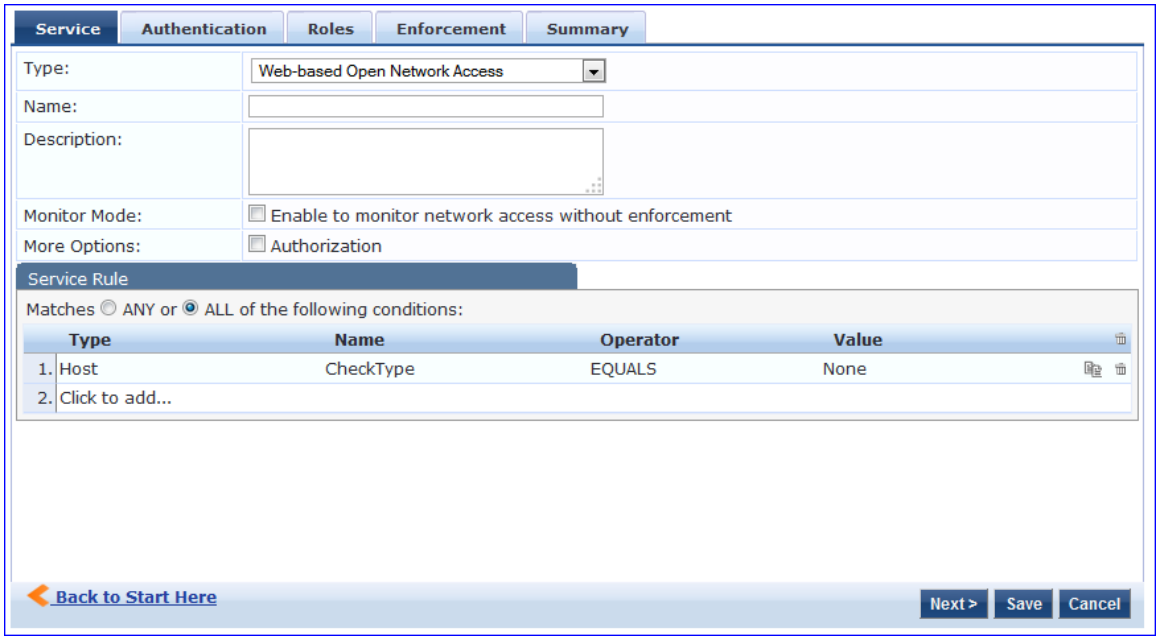


For more information on configuration tabs, see Dell 802.1X Wireless on page 122

Web-based Open Network Access

Configuration for this service is the same as **Web-based Authentication** service except that a health check is not performed on the endpoints. A **Terms of Service** page (as configured on the **Dell Networking W-ClearPass Policy Manager Guest Portal** page) is presented to the user. Network access is granted, when you click **Submit Action**. The **Posture** option is not available for the **Web-based Authentication** service. For more information, see Web-based Authentication on page 135. The following figure displays the **Web-based Open Network** service page:

Figure 86: *Web-based Open Network Access Service*

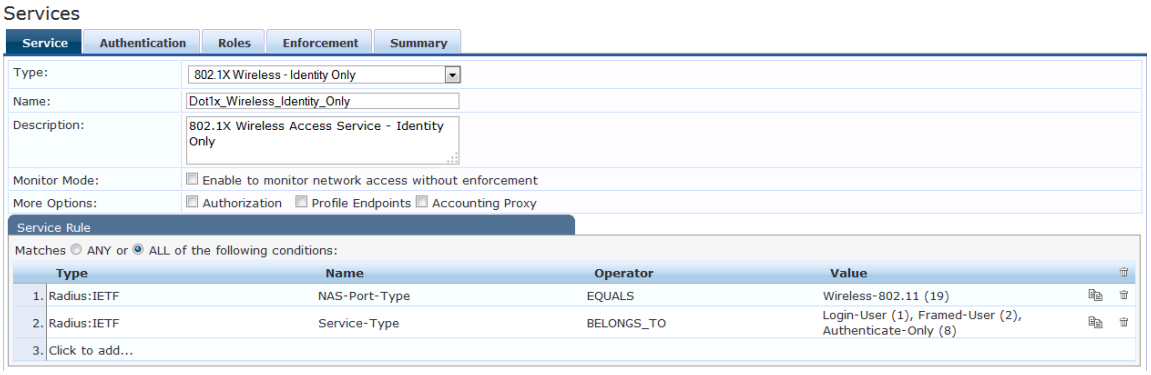


For more information on configuration tabs, see Dell 802.1X Wireless on page 122.

802.1X Wireless - Identity Only

Configuration for this type of service is the same as the **Dell 802.1X Wireless** service except that **Posture** and **Audit** policies are not configurable, when you use this template. For more information, see 802.1X Wireless on page 133. The following figure displays the **802.1X Wireless - Identity Only** service:

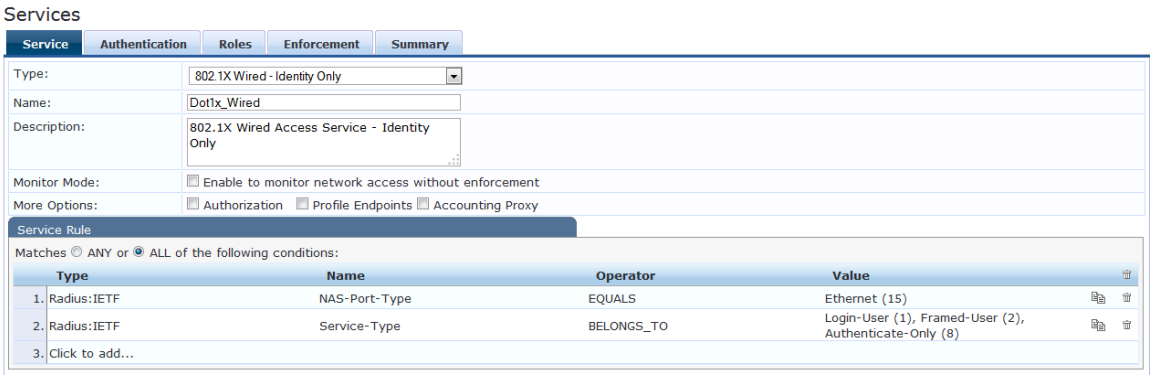
Figure 87: *802.1X Wireless - Identity Only Service*



802.1X Wired - Identity Only

Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X. Configuration for the **802.1X Wired - Identity Only** service is same as the **802.1X Wired** service except that **Posture** and **Audit** policies are not configurable, when you use this template. For more information, see 802.1X Wired on page 134. The following figure displays the **802.1X Wired - Identity Only** service:

Figure 88: *802.1X Wired - Identity Only Service*



RADIUS Enforcement (Generic)

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

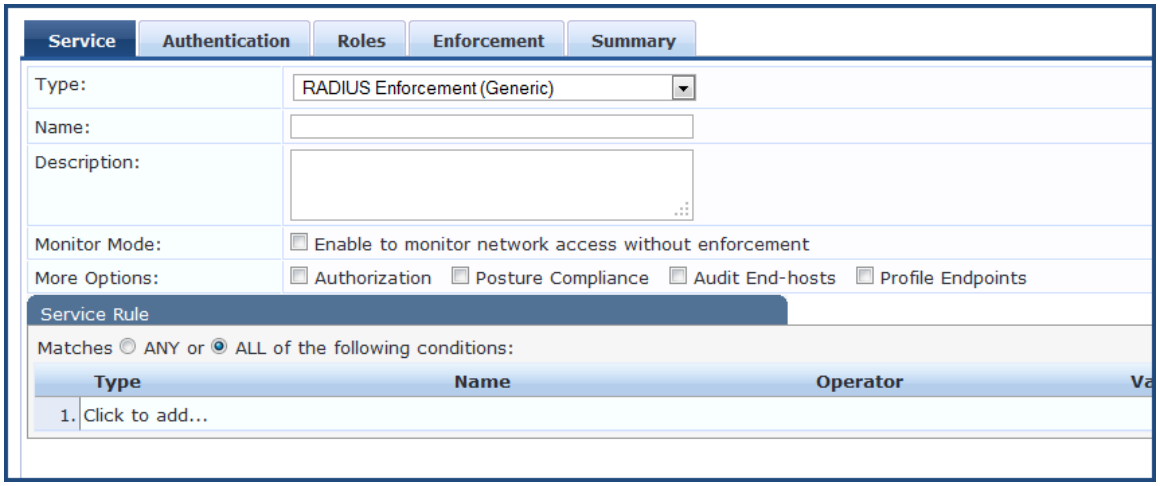
The **[AirGroup Authorization Service]** service is the only **RADIUS Enforcement (Generic)** service that is available by default.

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

There are no default rules associated with this service type. Rules can be added to handle any type of standard or vendor-specific RADIUS attributes (any attribute that is loaded through the pre-packaged vendor-specific or

standard RADIUS dictionaries, or through other dictionaries imported into Policy Manager). The following figure displays the **RADIUS Enforcement (Generic)** service:

Figure 89: *RADIUS Enforcement (Generic) Service*



Configuring a service for RADIUS requests is similar to configuring the **Dell 802.1X Wireless** service. For more information on configuration tabs, see Dell 802.1X Wireless on page 122.

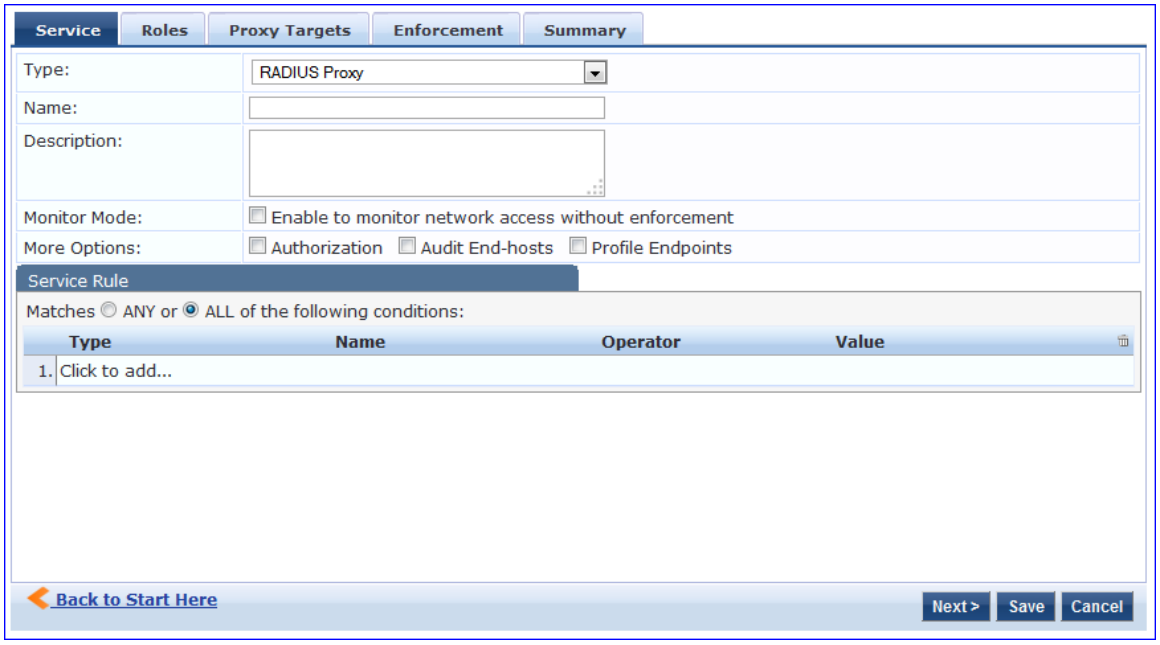
RADIUS Proxy

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

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

The following figure displays the **RADIUS Proxy** service:

Figure 90: *RADIUS Proxy Service*

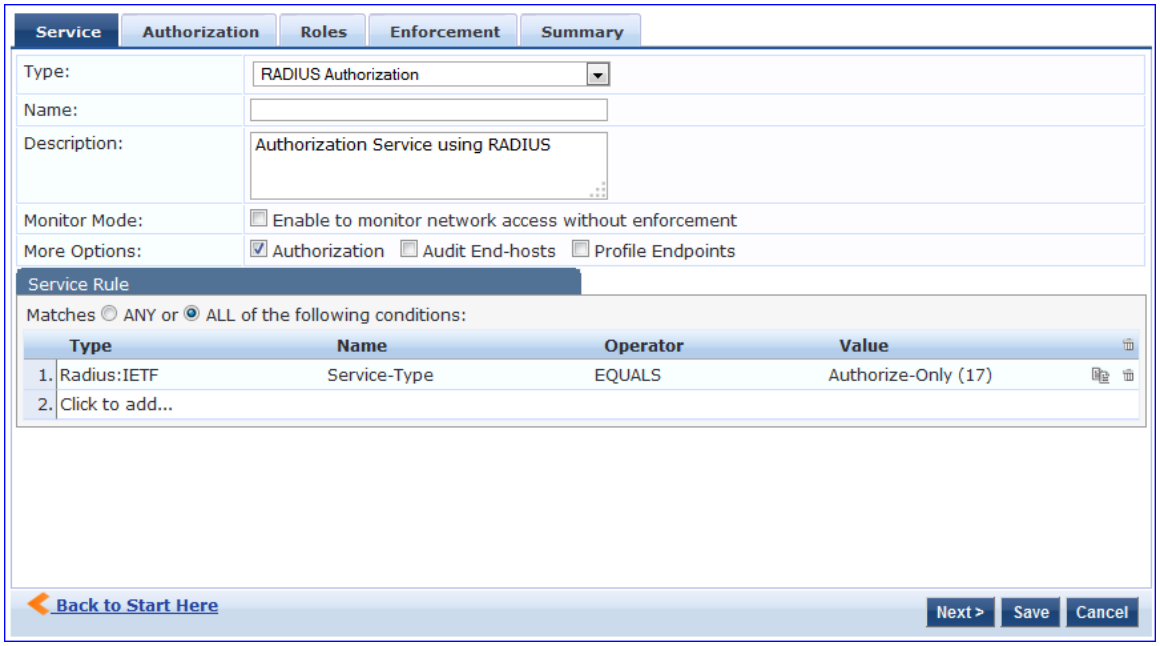


For more information, see RADIUS Enforcement (Generic) on page 138.

RADIUS Authorization

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

Figure 91: *RADIUS Authorization Service*



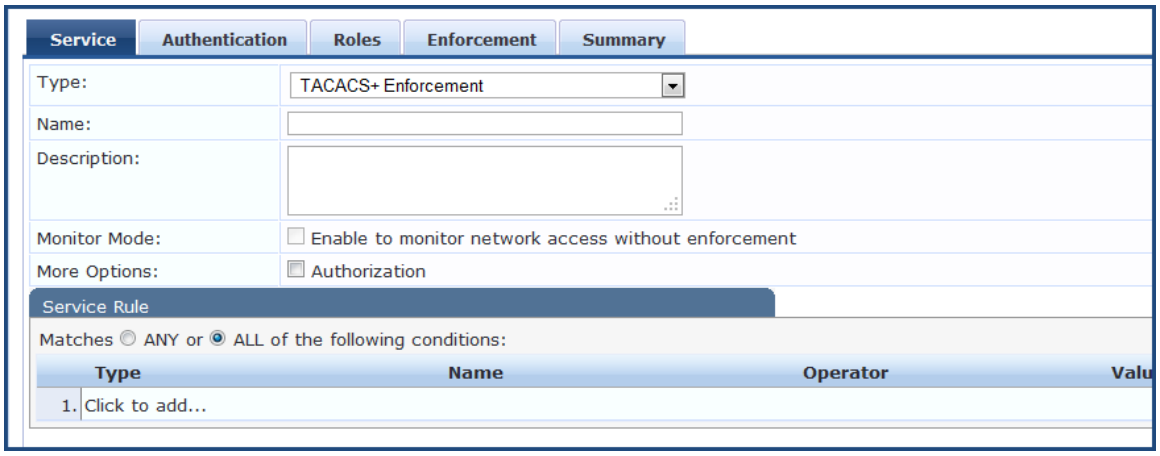
Configuration for this service is the same as the **RADIUS Enforcement (Generic)** service except that you do not configure authentication or posture with this service type. Refer to RADIUS Enforcement (Generic) on page 138 for more information.

TACACS+ Enforcement

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

The result of evaluating a TACACS+ enforcement policy is one or more TACACS+ enforcement profiles. For more information on TACACS+ enforcement profiles, see TACACS+ Based Enforcement on page 341 for more information. The following figure displays the **TACACS+ Enforcement** service:

Figure 92: *TACACS+ Enforcement Service*

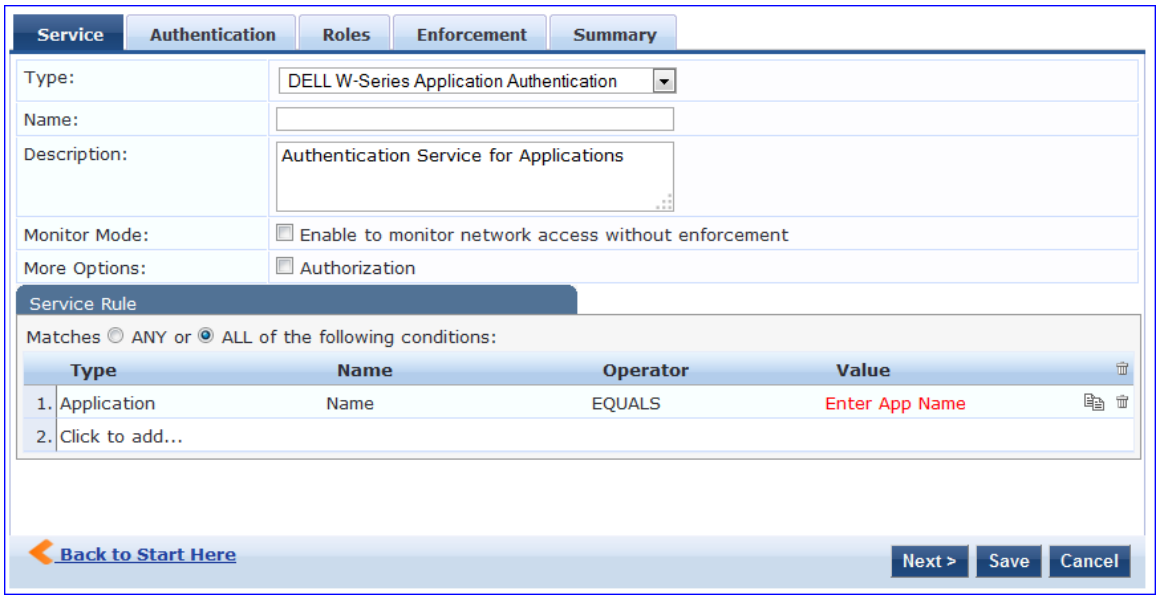


Configuring the **TACACS+ Enforcement** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 122.

Dell W-Series Application Authentication

This type of service provides authentication and authorization to users of Dell applications: W-Series ClearPass Guest and W-Series ClearPass Insight. You can send Generic Application Enforcement on page 329 to these or other generic applications for authenticating and authorizing the users. The following figure displays the **Dell W-Series Application Authentication** service:

Figure 93: *Dell W-Series Application Authentication*

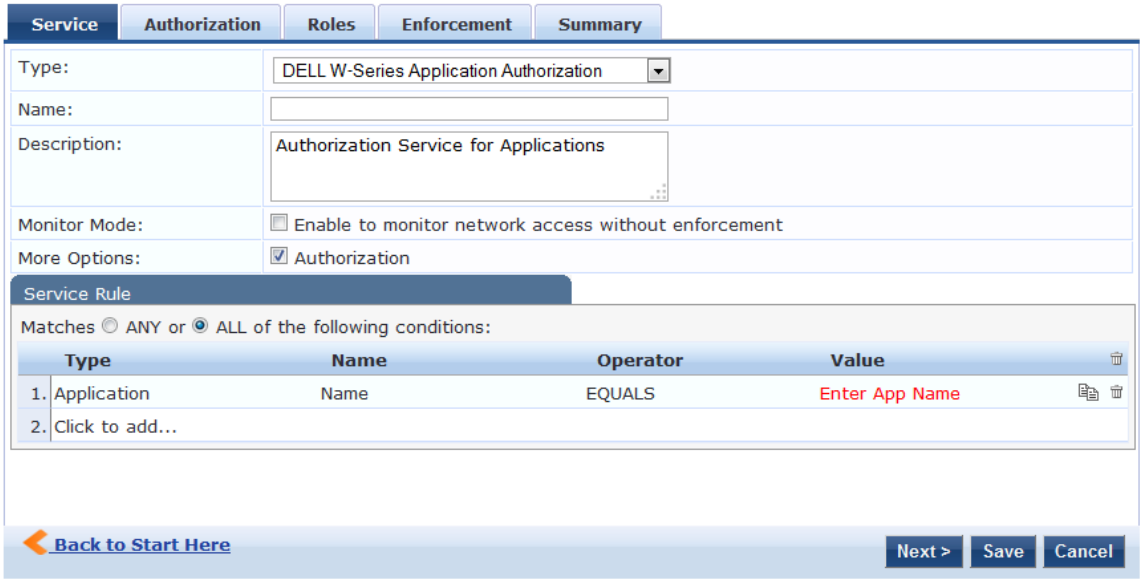


Configuring the **Dell W-Series Application Authentication** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 122.

Dell W-Series Application Authorization

This type of service provides authorization for users of Dell applications: W-Series ClearPass Guest and W-Series ClearPass Insight. Generic Application Enforcement on page 329 can be sent to these or other generic applications for authorizing the users. The following figure displays the **Dell W-Series Application Authorization** service:

Figure 94: *Dell W-Series Application Authorization*



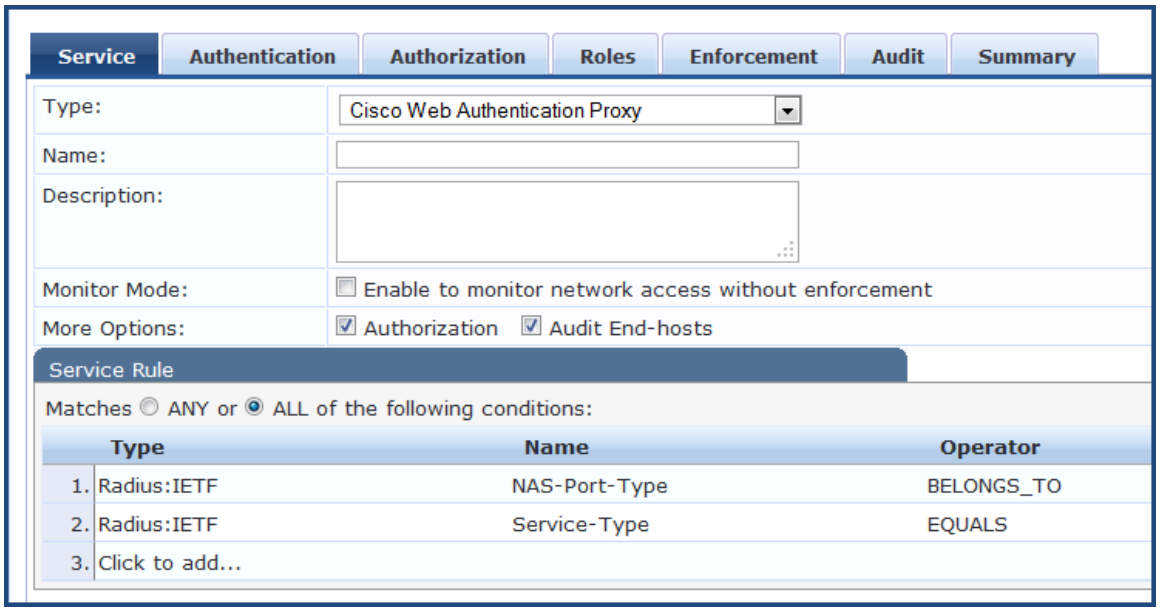
Configuring the Dell W-Series Application Authorization service is similar to configuring the Dell 802.1X Wireless service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 122.

Cisco Web Authentication Proxy

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

The following figure displays the **Cisco Web Authentication Proxy** service:

Figure 95: *Cisco Web Authentication Proxy Service*



Configuring the **Cisco Web Authentication Proxy** service is similar to configuring the **Dell 802.1X Wireless** service except that the **Posture Compliance** and **Profile Endpoints** options are not available. For more information on configuration tabs, see Dell 802.1X Wireless on page 122.

As a first step in the service-based processing, Policy Manager uses an authentication method to authenticate the user or device against an authentication source. After the user or device is authenticated, Policy Manager fetches attributes for role mapping policies from the authorization sources associated with this authentication source. For a general overview of Policy Manager authentication and authorization, see Authentication and Authorization Architecture and Flow on page 30

For more information, see:

- Supported Authentication Methods on page 145
- Adding and Modifying Authentication Methods on page 145
- Adding and Modifying Authentication Sources on page 169
- Configuring Authentication Components on page 1

Supported Authentication Methods

Policy Manager supports the following authentication methods:

- Tunneled EAP authentication
  - EAP Protected EAP (EAP-PEAP)
  - EAP Flexible Authentication Secure Tunnel (EAP-FAST)
  - EAP Transport Layer Security (EAP-TLS)
  - EAP Tunneled TLS (EAP-TTLS)
- Non-tunneled authentication
  - EAP Message Digest 5 (EAP-MD5) - Dell Networking W-ClearPass Policy Manager does not support EAP-MD5 in the **FIPS** mode
  - EAP Microsoft Challenge Handshake Authentication Protocol version 2 (EAP- MSCHAPv2)
  - EAP Generic Token Card (EAP-GTC)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
  - Microsoft CHAP version 1 and 2
  - MAC authentication method (MAC-AUTH)
- Authorize authentication

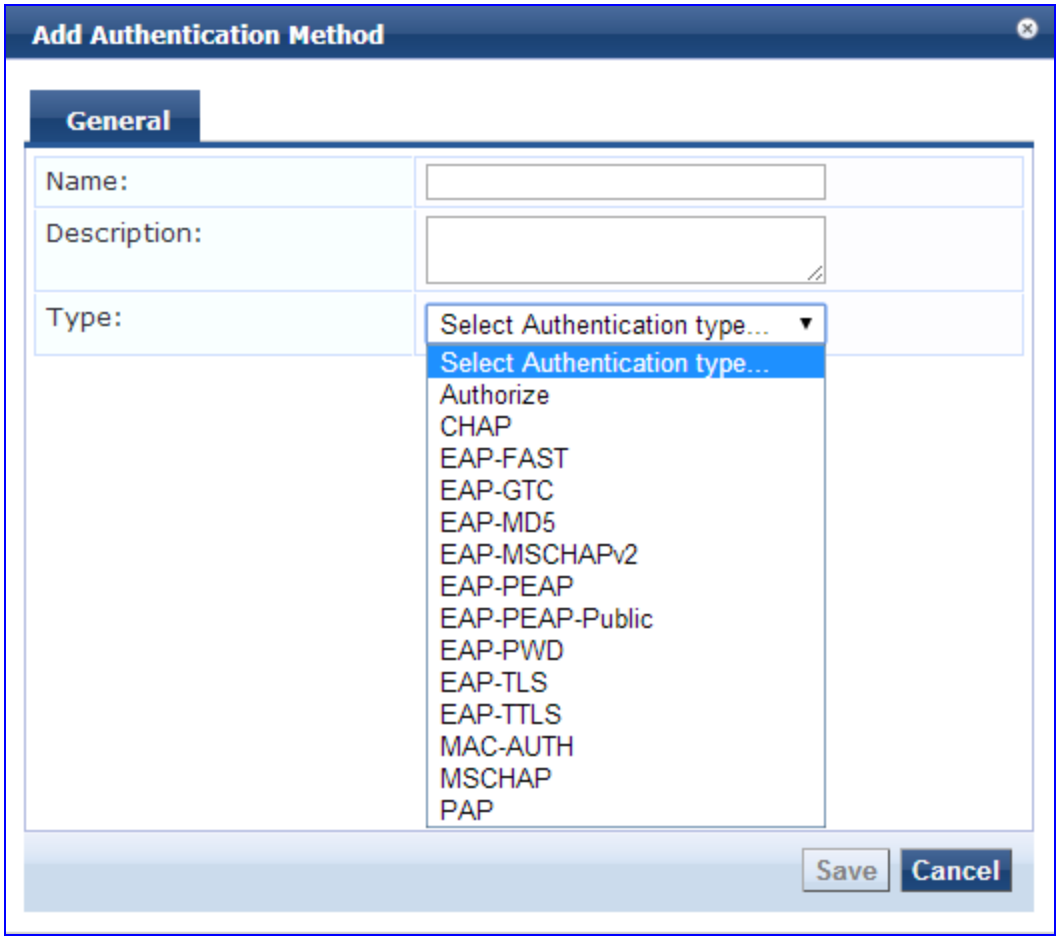
The MAC_AUTH authentication type must be used exclusively in a MAC-based authentication service. When the MAC_AUTH method is selected, Policy Manager makes internal checks to verify that the request is a **MAC_ Authentication** request and not a spoofed request. In tunneled EAP methods, authentication and posture credential exchanges occur inside a protected outer tunnel.

Adding and Modifying Authentication Methods

From the **Services** (**Configuration > Services**) page, you can configure authentication for a new service (using the **Add Service** wizard) or modify an existing authentication method directly (**Configuration > Authentication > Methods**, then click any row in the **Authentication Methods** page). When you click **Add** from any of these locations, Policy Manager displays the **Add Authentication Method** popup.

The following figure displays the **Add Authentication Method** page:

Figure 96: *Add Authentication Method Page*



NOTE

The EAP-MD5 authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS (**Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab) mode.

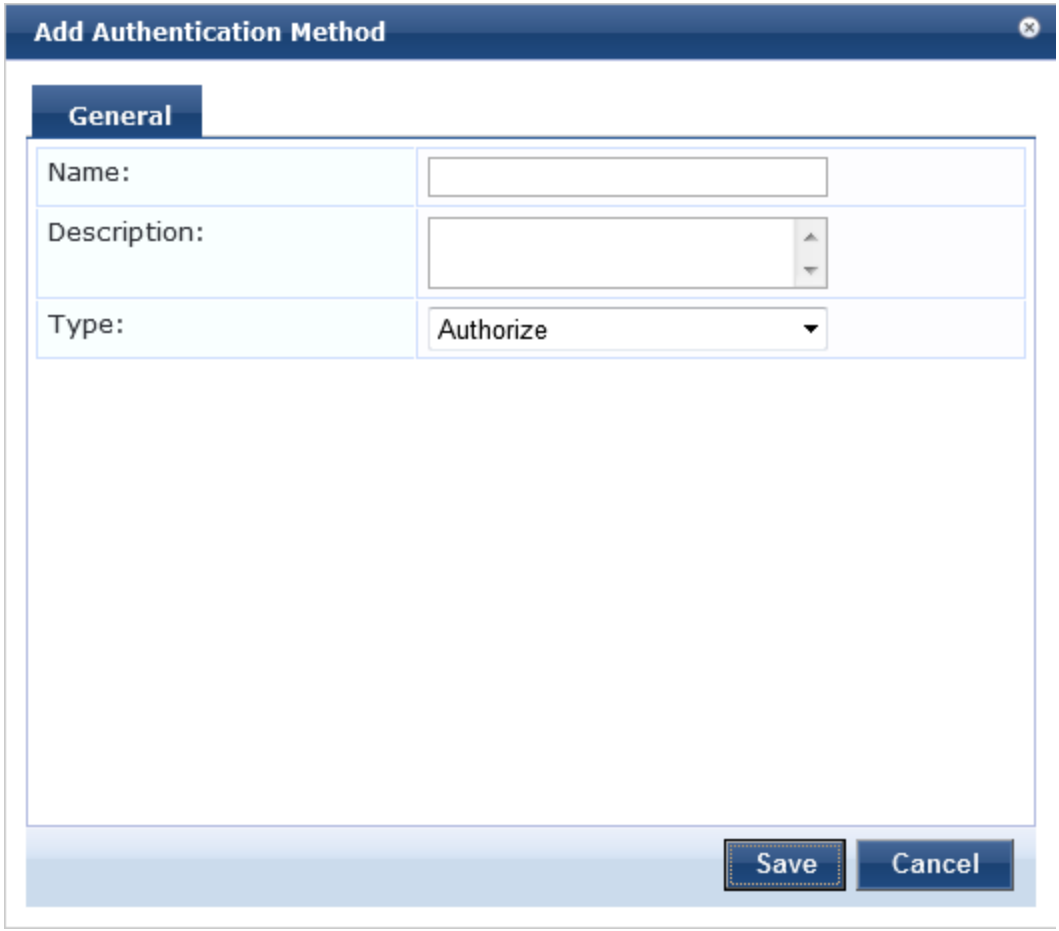
You can configure the following authentication methods:

- Authorize Authentication Method on page 147
- CHAP and EAP-MD5 on page 147
- EAP-FAST on page 148
- EAP-GTC on page 152
- EAP-MSCHAPv2 on page 154
- EAP-PEAP on page 154
- EAP-PEAP-Public on page 157
- EAP-PWD on page 160
- EAP-TLS on page 161
- EAP-TTLS on page 163
- MAC-AUTH on page 166
- MSCHAP on page 166
- PAP on page 167

Authorize Authentication Method

This is an authorization-only method that you can add with a custom name. The **General** tab labels the authentication method and defines session details. The following figure displays the **Authorization - General** tab:

Figure 97: *Add Authentication - General Tab*



The following table describes the **Authorize General** parameters:

Table 58: *Authorize General Tab Parameters*

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

CHAP and EAP-MD5

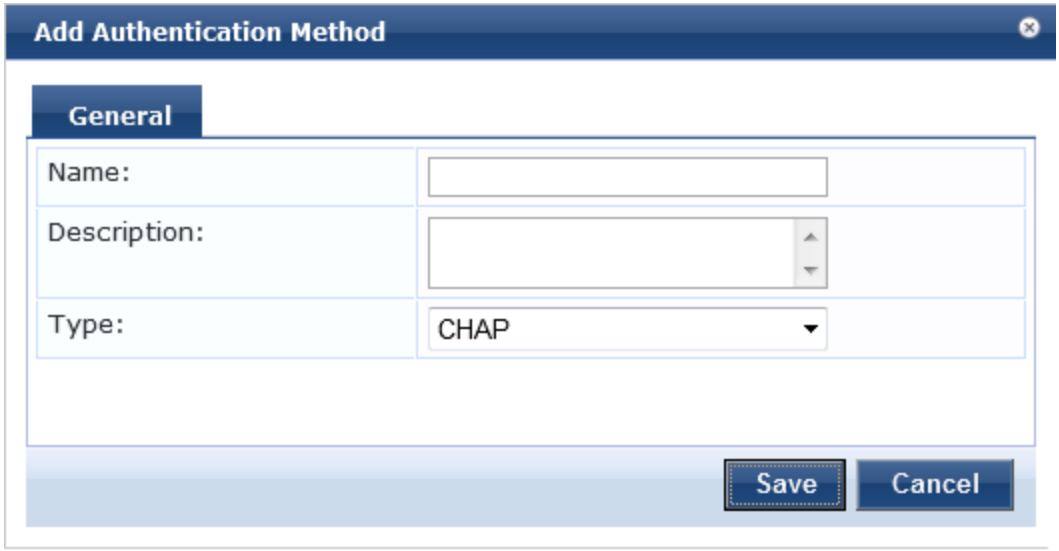
Policy Manager is packaged with **CHAP** and **EAP-MD5** authentication methods. You can create one or more instances of CHAP and EAP-MD5 authentication methods by assigning a customized name to each one. These methods can also be associated to a service as authentication methods.

NOTE

The EAP-MD5 authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS (**Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab) mode.

The following figure is an example of the **General** tab for the **CHAP** authentication method:

Figure 98: *General Tab (CHAP)*



The following table describes the **CHAP and EAP-MD5 - General** parameters:

Table 59: *CHAP and EAP-MD5 - General Tab Parameters*

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

EAP-FAST

EAP-Flexible Authentication through Secure Tunneling (EAP-FAST) is an authentication method that encrypts EAP transactions within a TLS tunnel. The EAP-FAST method contains the following four tabs:

- General Tab on page 148
- Inner Methods Tab on page 150
- PACs Tab on page 151
- PAC Provisioning Tab on page 151

NOTE

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

General Tab

The **General** tab labels the authentication method and defines session details. The following figure displays the **EAP-FAST - General** tab:

Figure 99: *EAP-FAST - General Tab*

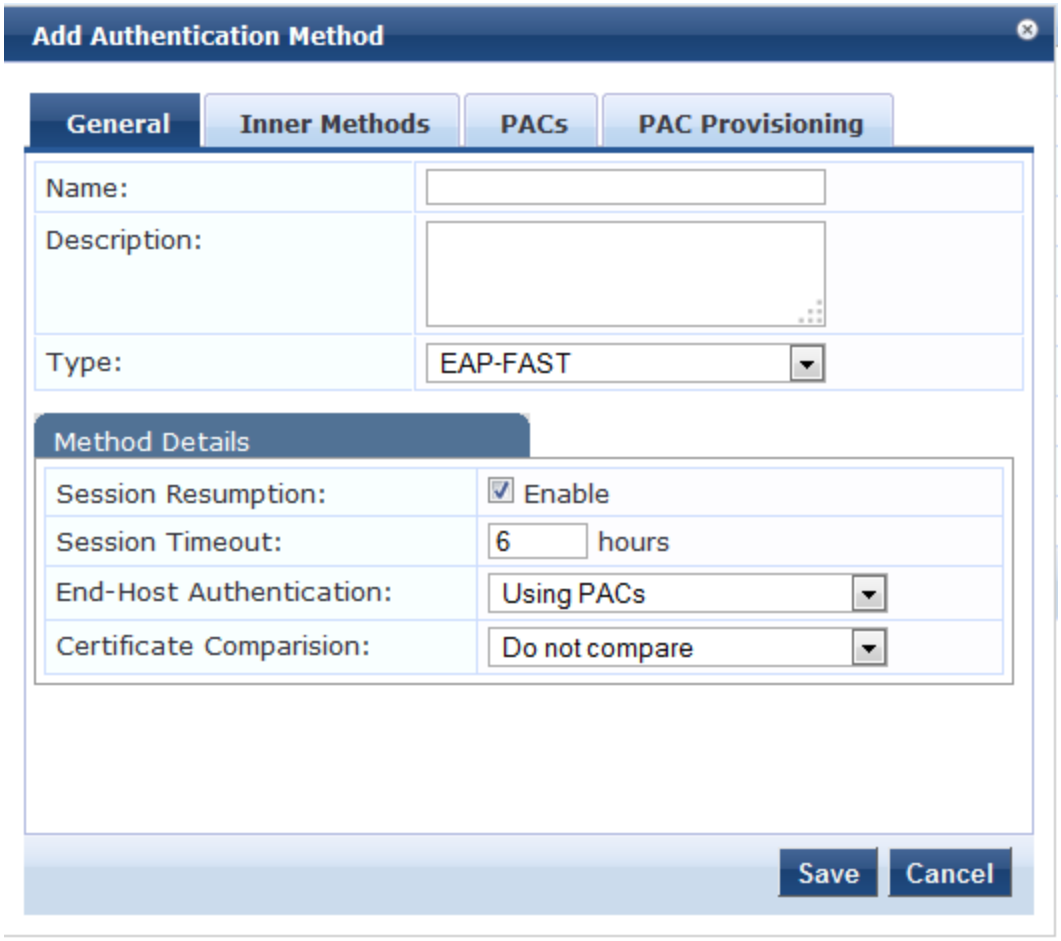


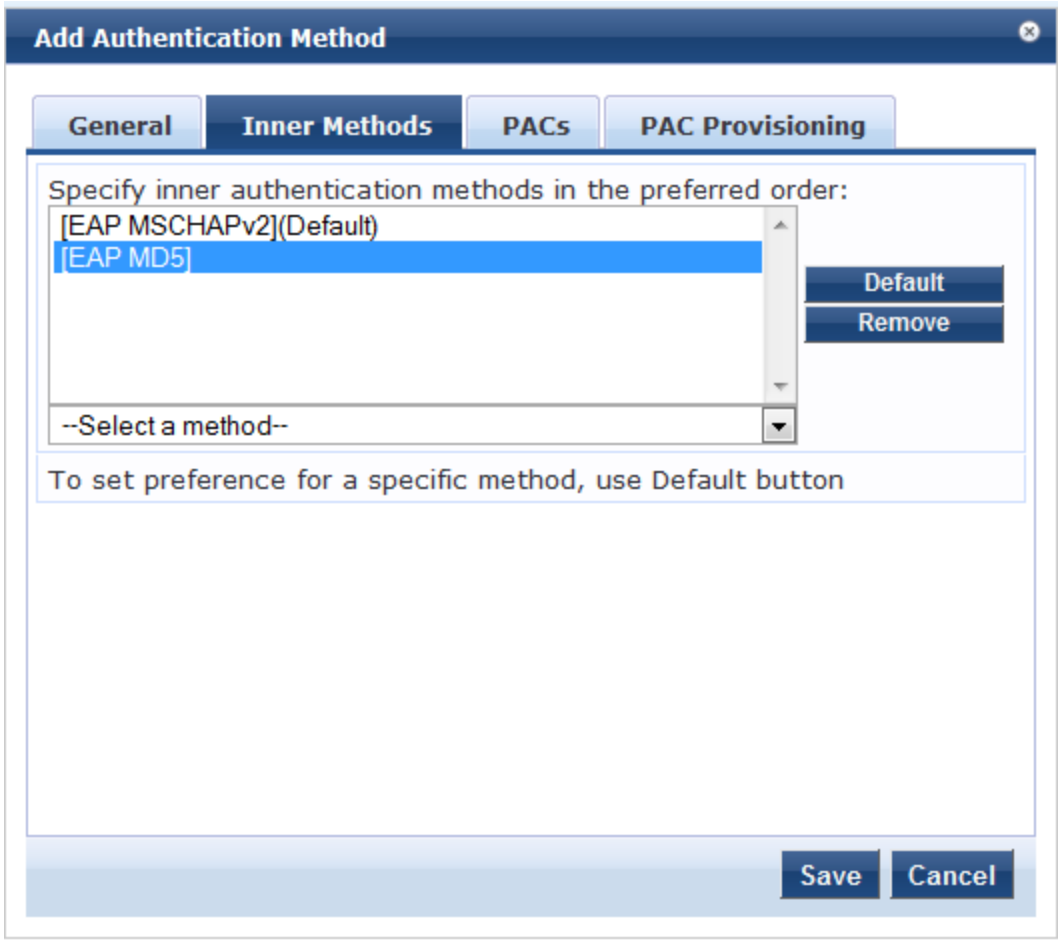
Table 60: *EAP_FAST - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **EAP_FAST**.
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. By default, this option is enabled.
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, then the cached sessions are not purged.
Fast Reconnect	Enable this check box to allow fast reconnect. When **Fast Reconnect** is enabled, the inner method of the server-authenticated outer tunnel is also bypassed. This makes the process of re-authentication faster. For the fast reconnect to work, **session resumption** must be enabled.

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-FAST** method. The following figure displays the **EAP-FAST - Inner Methods** tab:

Figure 100: *EAP-FAST Add Authentication Method - Inner Methods Tab*



NOTE

The EAP-MD5 authentication method is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS (**Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab) mode.

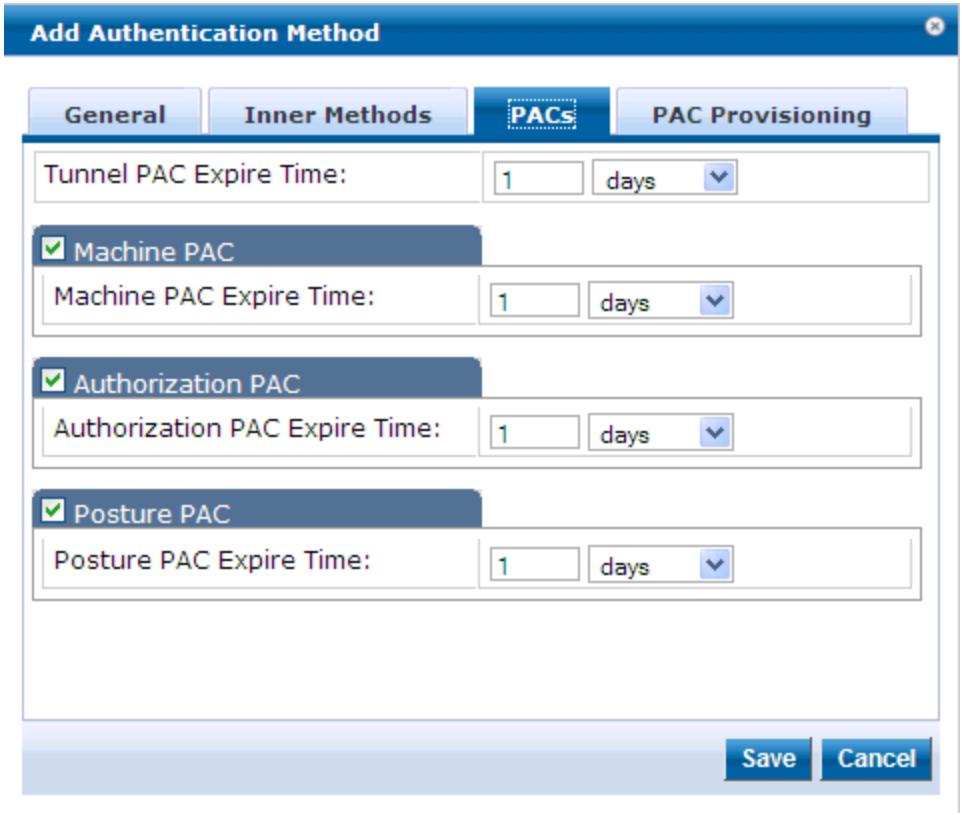
Table 61: *EAP-FAST - Inner Methods Tab Parameters*

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

PACs Tab

The **PACs** tab enables or disables Protected Access Credential (PAC) types. The following figure displays the **EAP-FAST - PACs** tab:

Figure 101: *EAP_FAST PACs Tab*



PAC Provisioning Tab

The **PAC Provisioning** tab controls anonymous and authenticated modes. The following figure displays the **EAP-FAST PAC - Provisioning** tab:

Figure 102: *EAP_FAST PAC Provisioning Tab*

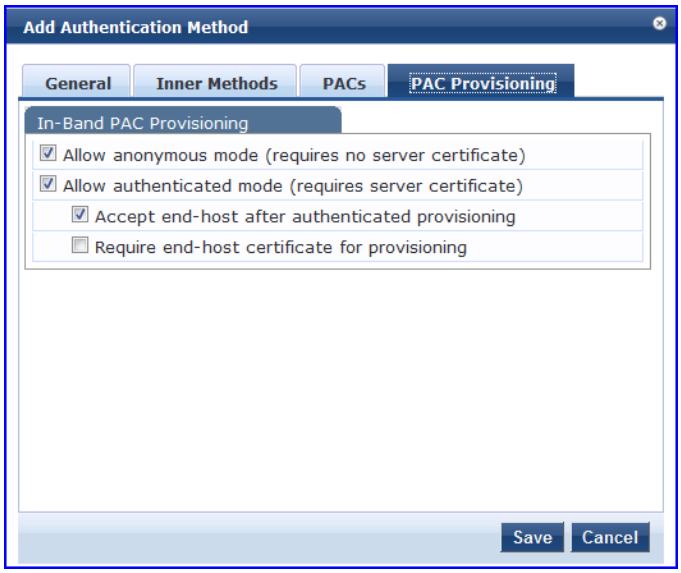


Table 62: *EAP_FAST PAC Provisioning Tab Parameters*

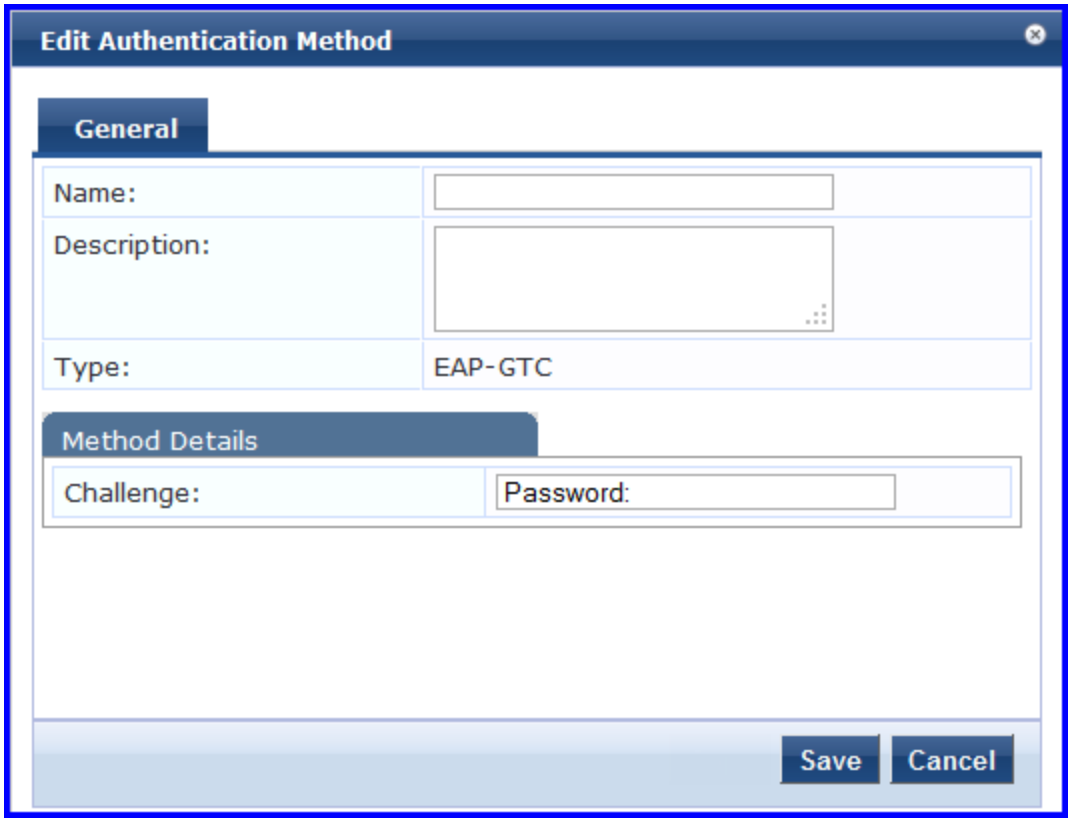
Parameter	Description	Considerations
In-Band PAC Provisioning		
Allow anonymous mode	When in anonymous mode, phase 0 of EAP_FAST provisioning establishes an outer tunnel without end-host/Policy Manager authentication (not as secure as the authenticated mode). After an outer tunnel is established, end-host and Policy Manager perform mutual authentication using MSCHAPv2, then Policy Manager provisions the end-host with an appropriate PAC (tunnel or machine).	Authenticated mode is more secure than anonymous provisioning mode. After the server is authenticated, the phase 0 tunnel is established. The end-host and Policy Manager perform mutual authentication and provision on the end-host with an appropriate PAC (tunnel or machine): • If both anonymous and authenticated provisioning modes are enabled and the end-host sends a cipher suite that supports server authentication, Policy Manager picks the authenticated provisioning mode. • If the appropriate cipher suite is supported by the end-host, Policy Manager performs anonymous provisioning.
Allow authenticated mode	Enable to allow authenticated mode provisioning. When **Allow authenticated mode** is in phase 0, Policy Manager establishes the outer tunnel inside a server-authenticated tunnel. The end-host authenticates the server by validating the Policy Manager certificate.	
Accept end-host after authenticated provisioning	After the authenticated provisioning mode is complete and the end-host is provisioned with a PAC, Policy Manager rejects end-host authentication; the end-host subsequently re-authenticates using the newly provisioned PAC. When this field is enabled, Policy Manager accepts the end-host authentication in the provisioning mode itself; the end-host does not have to re-authenticate.	None.
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 this field is enabled, the server can require the end-host to send a certificate inside the tunnel for the purpose of authenticating the end-host.	None.

EAP-GTC

EAP-Generic Token Card (GTC) enables the exchange of clear-text authentication credentials across the network. EAP-GTC is used inside a TLS tunnel created by TTLS or PEAP to provide server authentication in wireless environments. The EAP-GTC method contains the **General** tab that labels the authentication method and defines session details.

The following figure displays the **EAP-GTC - General** tab:

Figure 103: *EAP-GTC - General Tab*



The following figure displays the **EAP-GTC General** parameters:

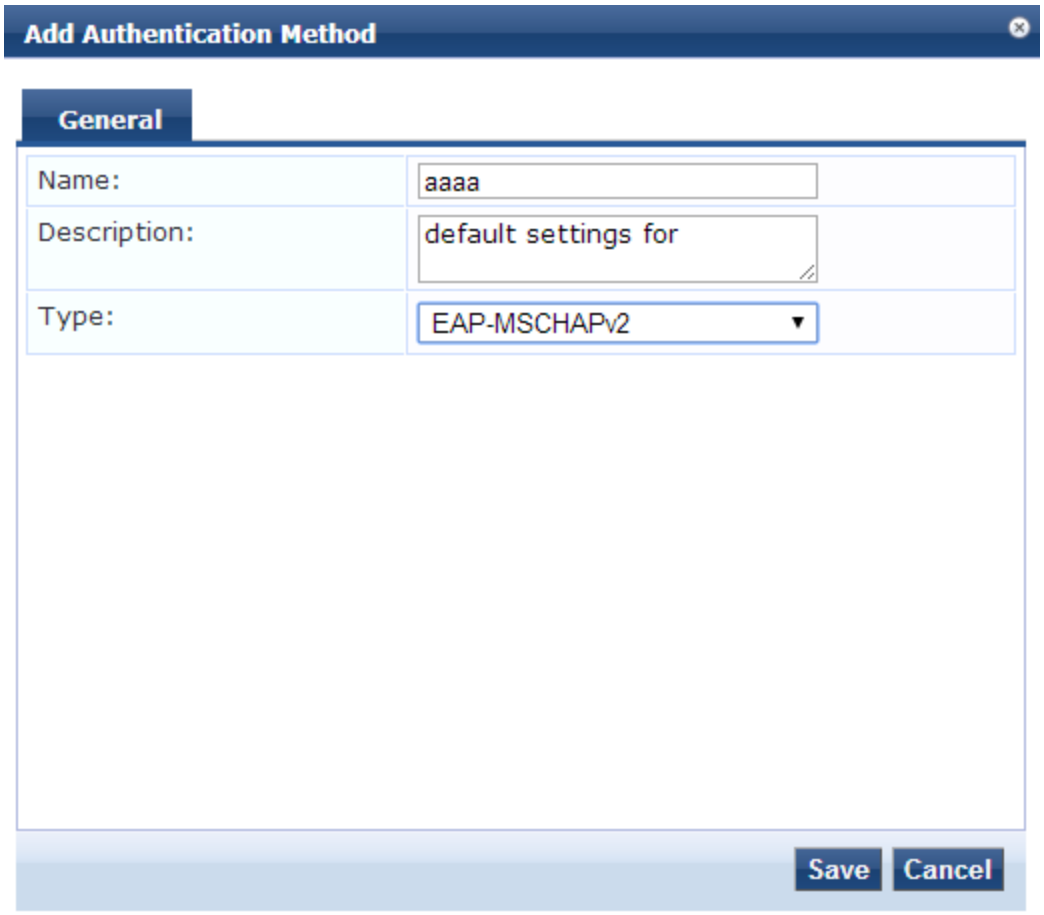
Table 63: *EAP-GTC General Tab Parameters*

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

EAP-MSCHAPv2

The **EAP-MSCHAPv2** method contains the **General** tab that labels the method and defines session details. The following figure is an example of the **EAP-MSCHAPv2 - General** tab:

Figure 104: *EAP-MSCHAPv2 - General Tab*



The following table describes the **EAP-MSCHAPv2 - General** parameters:

Table 64: *EAP-MSCHAPv2 - General Tab Parameters*

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

EAP-PEAP

EAP-Protected Extensible Authentication Protocol (EAP-PEAP) is a protocol that creates an encrypted (and more secure) channel before the password-based authentication occurs. PEAP is an 802.1X authentication method that uses server-side public key certificate to establish a secure tunnel in which the client authenticates with server. The PEAP authentication creates an encrypted SSL/TLS tunnel between client and authentication server. The exchange of information is encrypted and stored in the tunnel ensuring that the user credentials are kept secure.

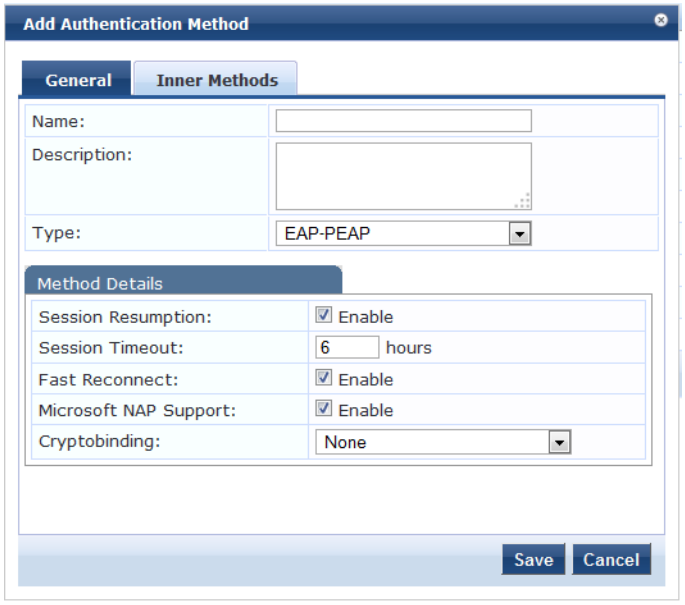
The **EAP-PEAP** authentication method contains the following two tabs:

- General Tab on page 155
- Inner Methods Tab on page 156

General Tab

The **General** tab labels the authentication method and defines session details. The following figure is an example of the **EAP-PEAP General** tab:

Figure 105: *EAP-PEAP - General Tab*



The following table describes the **EAP-PEAP - General** parameters:

Table 65: *EAP-PEAP - General Tab Parameters*

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

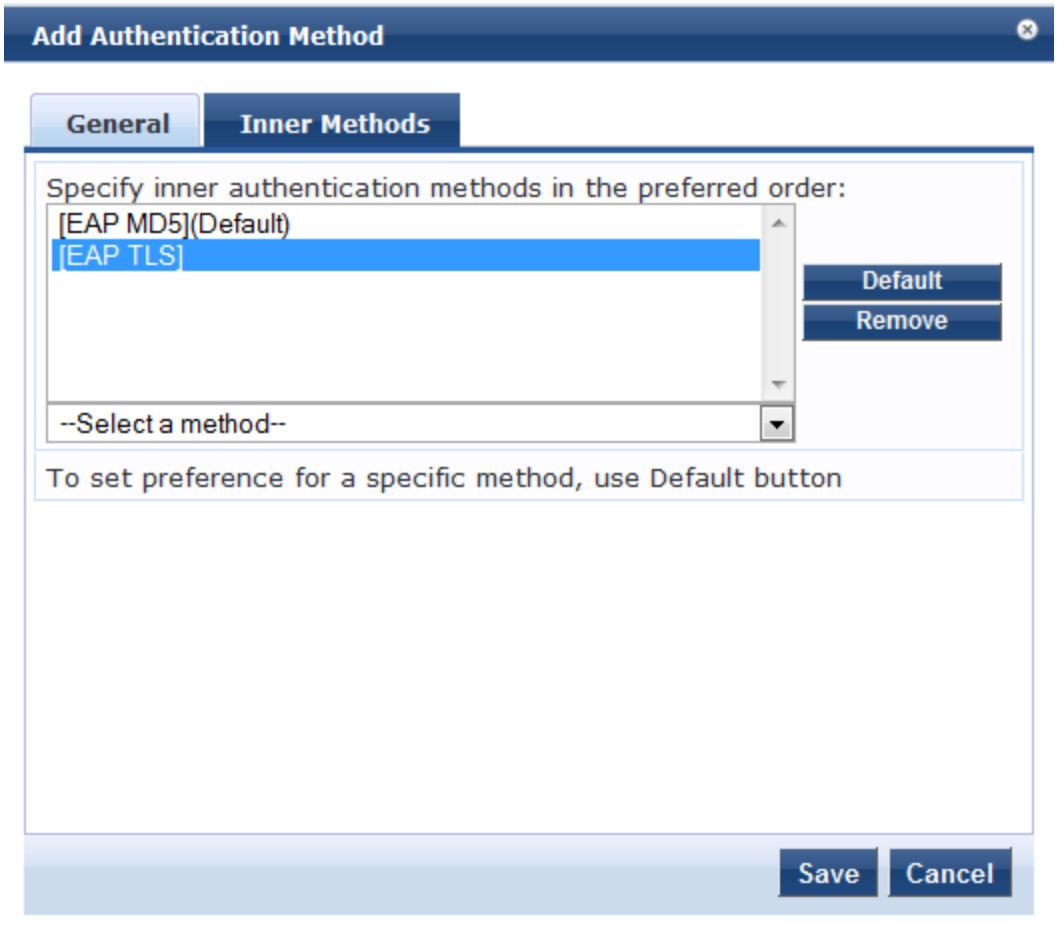
Table 65: *EAP-PEAP - General Tab Parameters (Continued)*

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

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-PEAP** authentication method. The following figure is an example of the **EAP-PEAP - Inner Methods** tab:

Figure 106: *EAP-PEAP - Inner Methods Tab*



NOTE

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

The following table describes the **EAP-PEAP Inner Methods** parameters:

Table 66: *EAP-PEAP Inner Methods Tab Parameters*

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

EAP-PEAP-Public

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

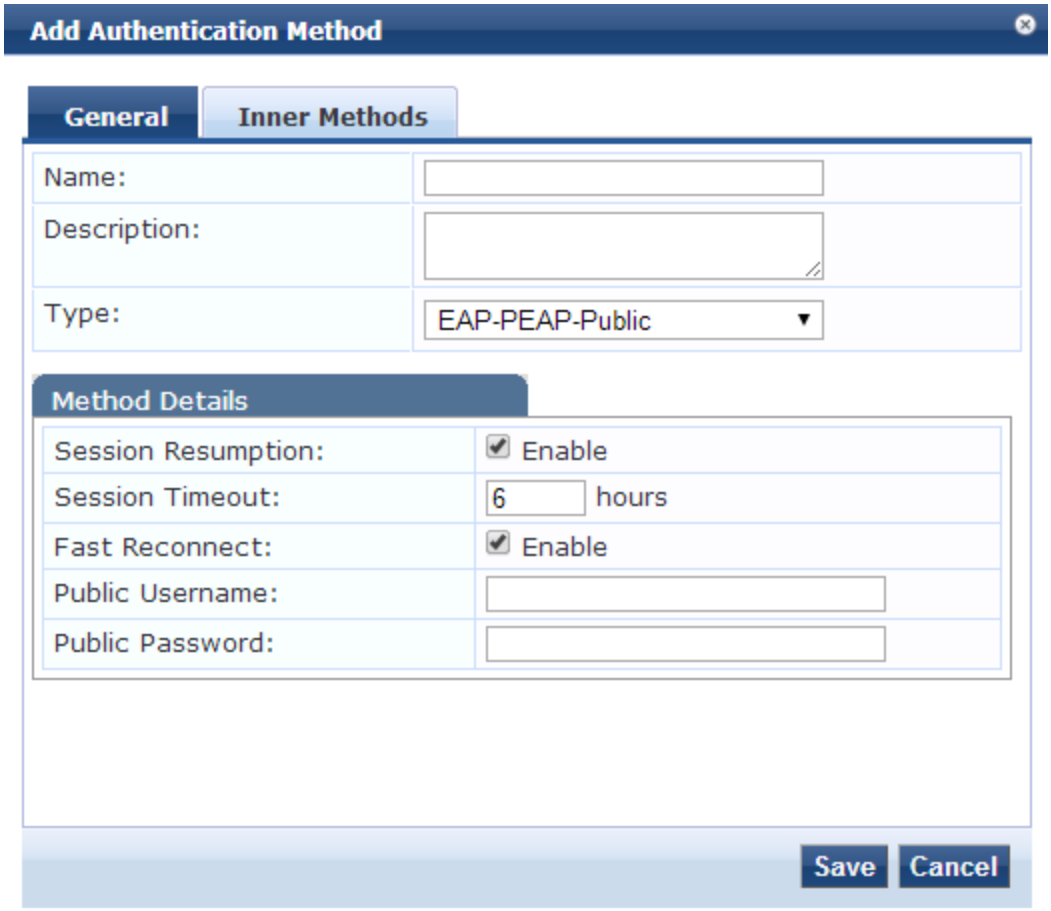
The **EAP-PEAP-Public** method contains the following two tabs:

- General on page 158
- Inner Methods on page 159

General

The **General** tab labels the authentication method and defines session details. The following figure is an example of the **EAP-PEAP-Public - General** tab:

Figure 107: *EAP-PEAP-Public - General Tab*



The following table describes the **EAP-PEAP-Public - General** parameters:

Table 67: *EAP-PEAP-Public - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select **EAP-PEAP-Public.**
Session Resumption	Caches EAP-PEAP-Public sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval. By default, this option is enabled.
Session Timeout	Caches EAP-PEAP-Public sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval in hours. If session timeout value is set to 0, the cached sessions are not purged. The default session timeout is 6 hours.

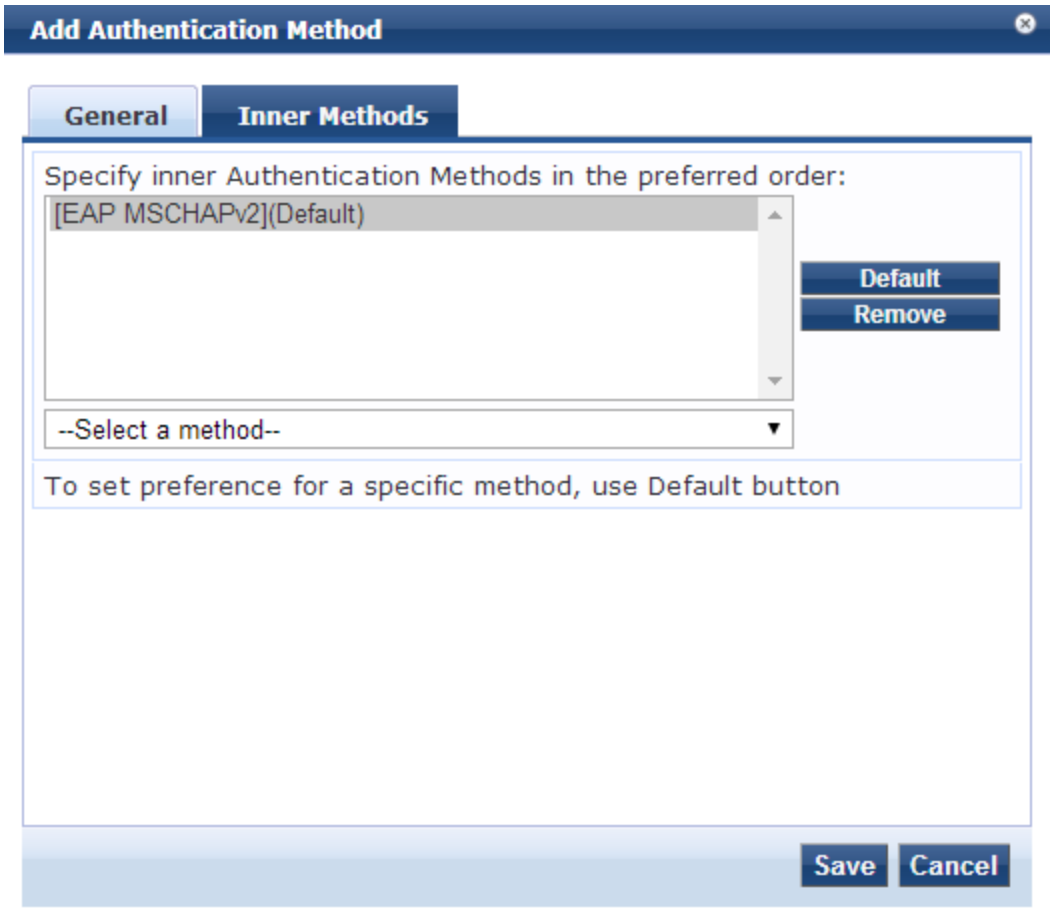
Table 67: *EAP-PEAP-Public - General Tab Parameters (Continued)*

Parameter	Description
Fast Reconnect	Enable this check box to allow fast reconnect. When fast reconnect is enabled, the inner method that happens inside the server authenticated outer tunnel is also bypassed. This makes the process of re-authentication faster. For the fast reconnect to work, session resumption must be enabled.
Public Username	Enter the Guest username. In this context, enter 'public'.
Public Password	Enter the Guest password. In this context, enter 'public'.

Inner Methods

The **Inner Methods** tab controls the inner methods for the **EAP-PEAP-Public** authentication method. The following figure is an example of the **EAP-PEAP-Public - Inner Methods** tab:

Figure 108: *EAP-PEAP-Public - Inner Methods Tab*



NOTE

The EAP-MD5 authentication method is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS (**Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab) mode.

Table 68: *EAP-PEAP-Public Inner Methods Tab Parameters*

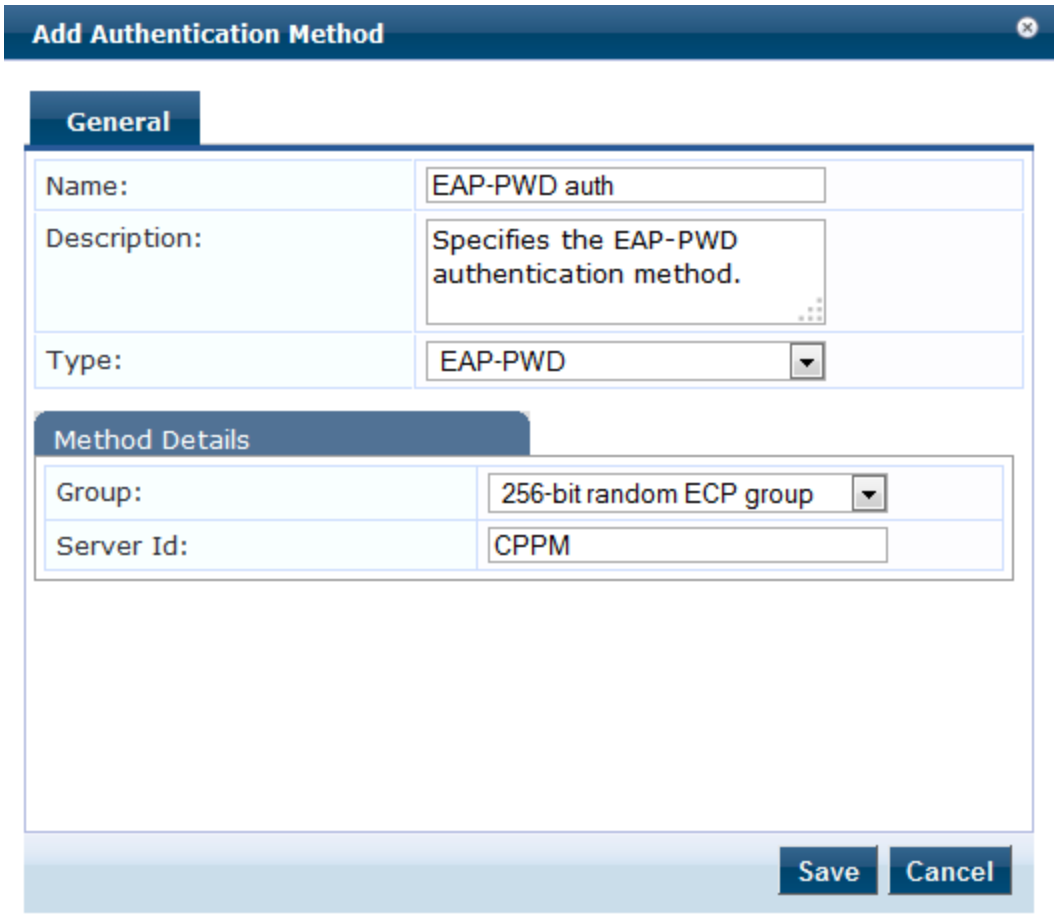
Parameter	Description
Specify inner authentication methods in the preferred order	Select the inner authentication method available from the drop-down list. In this context, only the EAP-MSCHAPv2 method is available. The following functions are available in this tab: • To append an inner method to the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

EAP-PWD

EAP-PWD is an EAP authentication method, which uses a shared password for authentication. EAP-PWD addresses the problem of password-based authenticated key exchange using a possibly weak password for authentication to derive an authenticated and cryptographically strong shared secret. The **EAP-PWD** method contains the **General** tab that labels the authentication method and defines session details.

The following figure displays the **EAP-PWD - General** tab:

Figure 109: *EAP-PWD - General Tab*



The following table describes the **EAP-PWD - General** parameters:

Table 69: *EAP-PWD - General Tab Parameters*

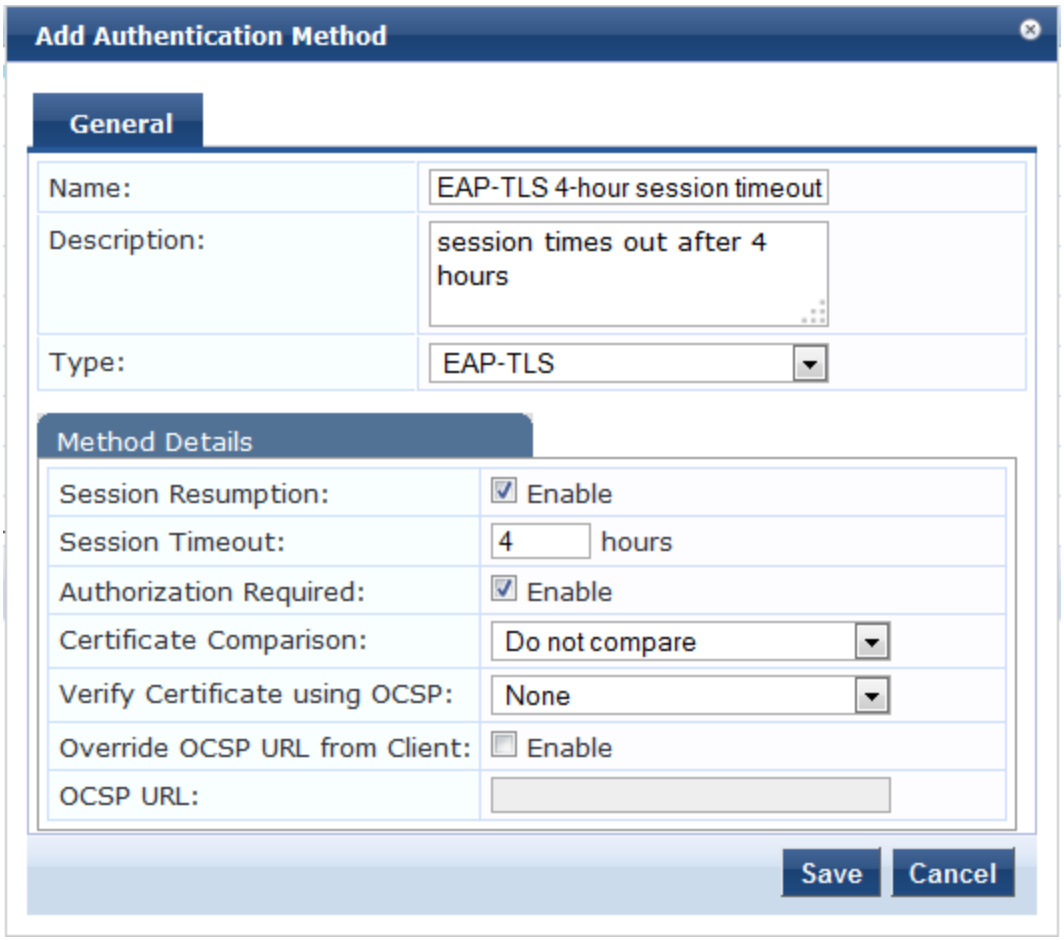
Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select **EAP-PWD.**
Method Details	
Group	Select the group from the drop-down list. Each party to the exchange derives ephemeral keys with respect to a particular set of domain parameters, that is a 'group'. A group can be based on Finite Field Cryptography (FFC) or Elliptic Curve Cryptography (ECC).
Server Id	Specify the string that identifies the server to the peer.

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) requires an exchange of proof of identities through public key cryptography (such as digital certificates). EAP-TLS secures this exchange with an encrypted TLS tunnel which helps to resist dictionary or other attacks. The **EAP-TLS** authentication method contains the **General** tab that labels and defines session details.

The following figure displays the **EAP-TLS - General** tab:

Figure 110: *EAP-TLS - General Tab*



The following table describes the **EAP_TLS - General** parameters:

Table 70: *EAP_TLS - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Specify the type of authentication. In this context, select **EAP_TLS**.
Session Resumption	Caches EAP-TLS sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.
Session Timeout	Specifies the duration in hours for the cached EAP-TLS sessions to be retained.
Authorization Required	Check **Enable** to specify whether to perform an authorization check.
Certificate Comparison	Specify the type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate:

Table 70: *EAP_TLS - General Tab Parameters (Continued)*

Parameter	Description
	• To skip the certificate comparison, choose **Do not compare.** • To compare specific attributes, choose **Compare Common Name (CN)**, **Compare Subject Alternate Name (SAN)**, or **Compare CN or SAN**. • To perform a binary comparison of the stored (in the client record in Active Directory or another LDAP-compliant directory) and presented certificates, choose **Compare Binary**.
Verify Certificate using OCSP	Select **Optional** or **Required** if the certificate to be verified by the Online Certificate Status Protocol (OCSP). Select **None** to not to verify the certificate.
Override OCSP URL from the Client	Select this option to use a different URL for OCSP. After this option is enabled, you can enter a new URL in the **OCSP URL** field.
OCSP URL	If the **Override OCSP URL from the Client** field is enabled, then enter the replacement URL.

EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) is designed to provide authentication that is similar to EAP-TLS, but each user does not require a certificate be issued. The certificates are issued only to authentication servers.

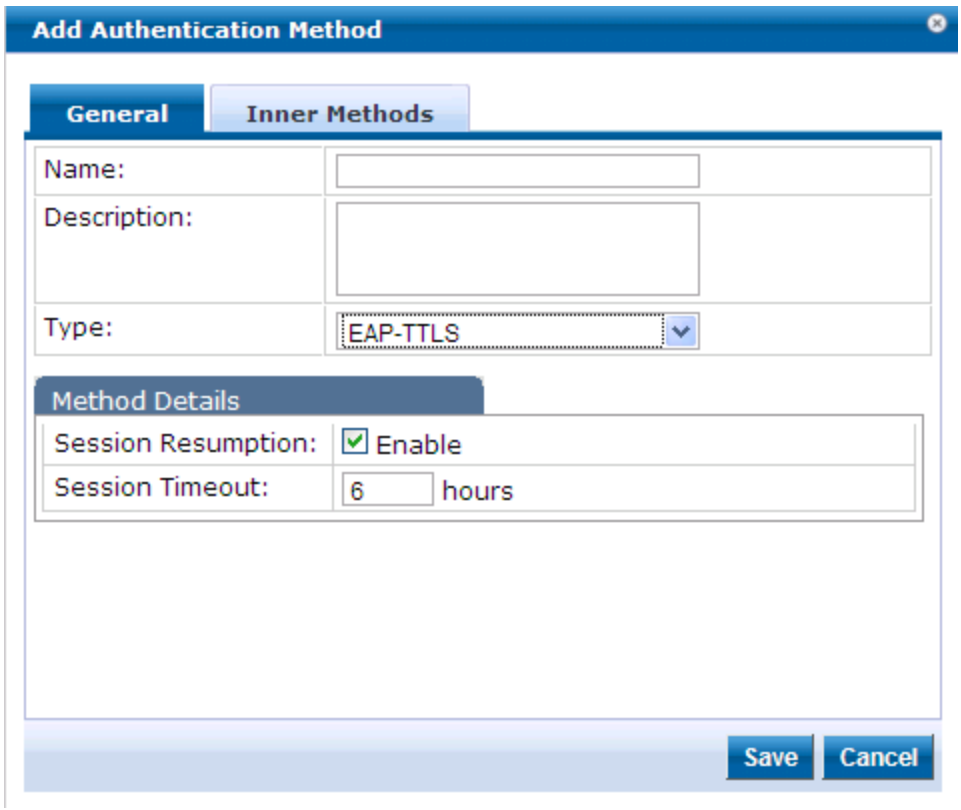
The **EAP-TTLS** method contains the following two tabs:

- General Tab on page 164
- Inner Methods Tab on page 165

General Tab

The **General** tab labels the method and defines session details. The following figure is an example of the **EAP-TTLS - General** tab:

Figure 111: *EAP-TTLS - General Tab*



The following table describes the **EAP-TTLS - General** parameters:

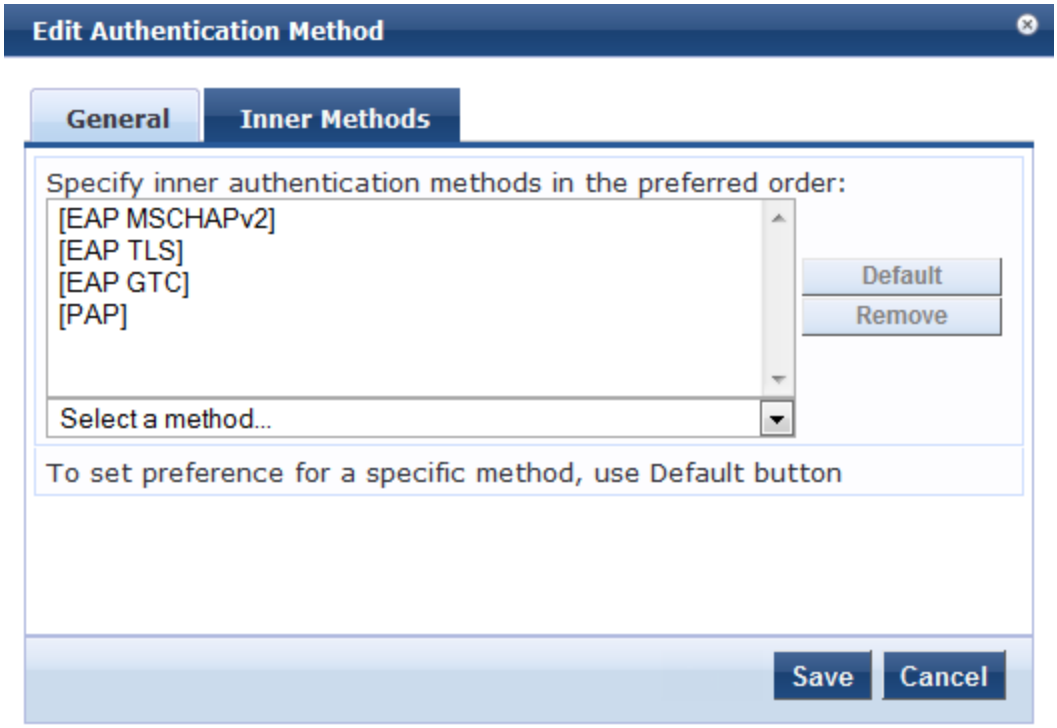
Table 71: *EAP-TTLS - General Tab Parameters*

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

Inner Methods Tab

The **Inner Methods** tab controls the inner methods for the **EAP-TTLS** method. The following figure is an example of the **EAP-TTLS - Inner Methods** tab:

Figure 112: *EAP_TTLS - Inner Methods Tab*



The following table describes the **EAP-TTLS - Inner Methods** parameters:

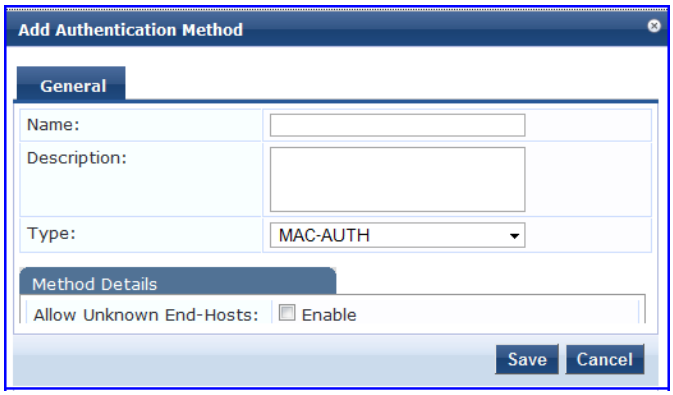
Table 72: *EAP-TTLS - Inner Methods Tab Parameters*

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

MAC-AUTH

The MAC-AUTH method contains the **General** tab that labels the authentication method and defines session details. The following figure is an example of the **MAC-AUTH - General** tab:

Figure 113: *MAC-AUTH - General Tab*



The following table describes the **MAC-Auth - General** parameters:

Table 73: *MAC-Auth - General Tab Parameters*

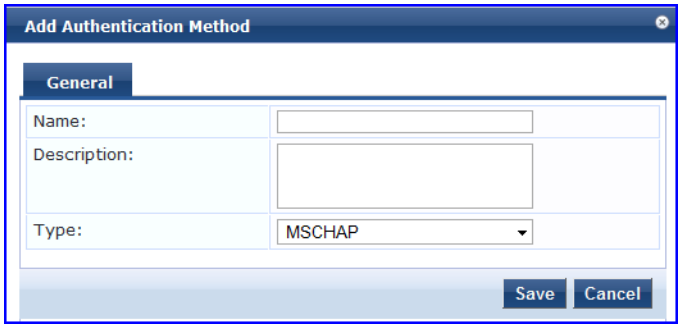
Parameter	Description
General	
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **MAC-AUTH.**
Method Details	
Allow Unknown End-Hosts	Enables further policy processing of MAC authentication requests of unknown clients. If this is not enabled, Policy Manager automatically rejects a request whose MAC address is not in a configured authentication source. This setting is enabled, for example, when you want Policy Manager to trigger an audit for an unknown client. By selecting this check box and enabling audit (See Configuring Audit Servers on page 285), you can trigger an audit of an unknown client.

MSCHAP

The MS-CHAP authentication method authenticates remote Windows-based workstations, integrating the functionality to which LAN-based users are accustomed with the hashing algorithms used on Windows networks. MS-CHAP uses a challenge-response mechanism to authenticate connections without sending any passwords. The MSCHAP method contains the **General** tab that labels the authentication method and defines session details.

The following figure is an example of the **MSCHAP - General** tab:

Figure 114: *MSCHAP - General Tab*



The following table describes the **MSCHAP - General** parameters:

Table 74: *MSCHAP - General Tab Parameters*

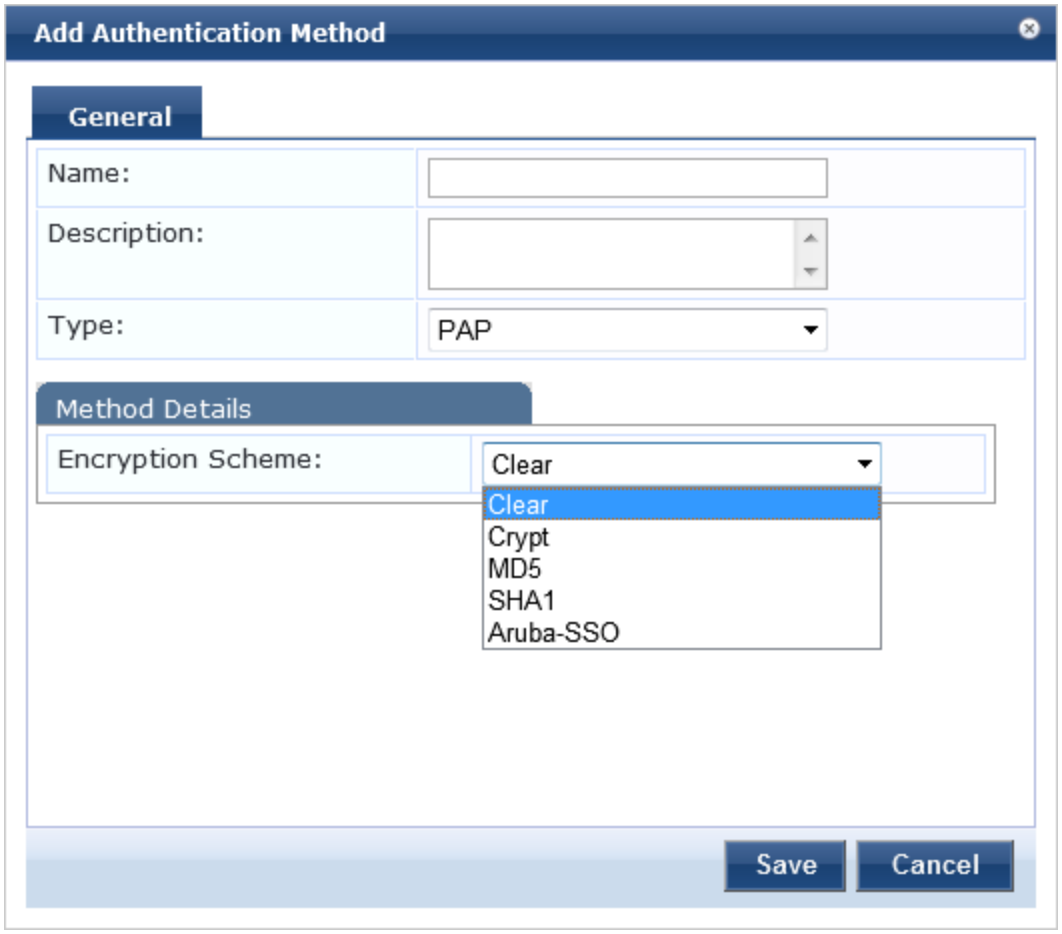
Parameter	Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	Select the type of authentication. In this context, select **MSCHAP**.

PAP

Password Authentication Protocol (PAP) is an authentication protocol in which the user name and password is sent to the remote access server in unencrypted form. The PAP method contains the **General** tab that labels the authentication method and defines session details.

The following figure is an example of the **PAP - General** tab:

Figure 115: *PAP - General Tab*



The following table describes the **PAP - General** parameters:

Table 75: *PAP - General Tab Parameters*

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

Table 75: *PAP - General Tab Parameters (Continued)*

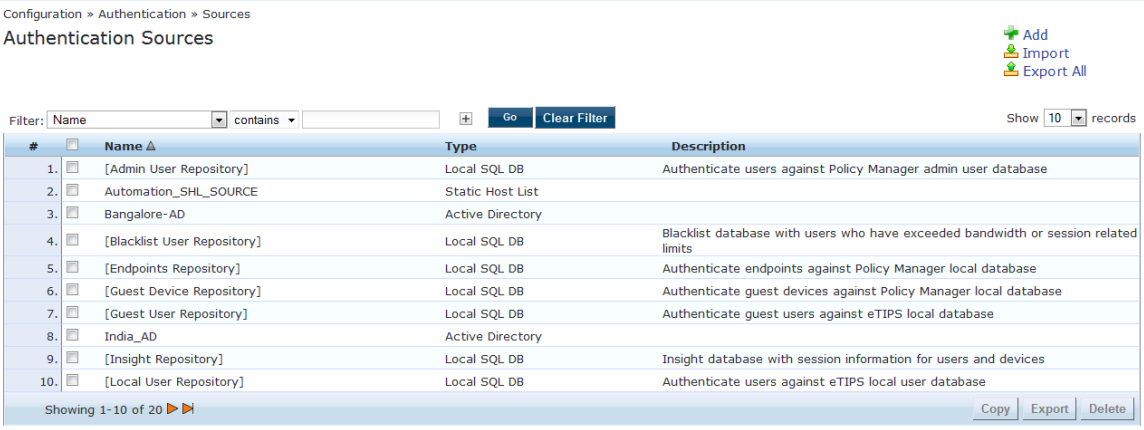
Parameter	Description
Method Details	
Encryption Scheme	Select the PAP authentication encryption scheme from the drop-down list. The following encryption schemes are supported: • Clear • Crypt • MD5 • SHA1 • SHA256 • NT Hash • LM Hash • Aruba-SSO **NOTE:** The MD5 encryption scheme is not supported if you use Dell Networking W-ClearPass Policy Manager in the FIPS (**Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab) mode.

Adding and Modifying Authentication Sources

Policy Manager supports multiple authentication sources. Navigate to the **Configuration > Services** page to configure an authentication source for a new service using the **Add Service** wizard. Alternatively, navigate to **Configuration > Authentication > Sources** to modify an existing authentication source.

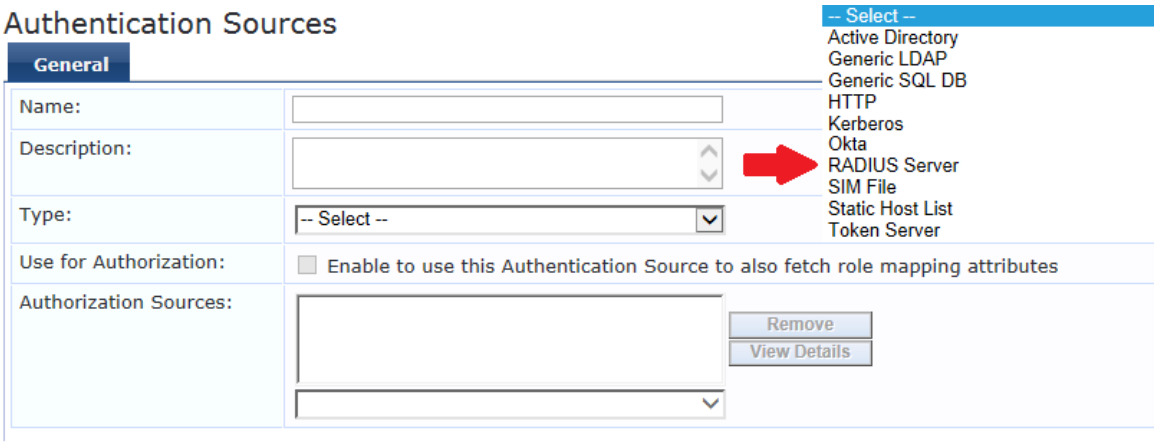
The following figure displays the **Authentication Sources** page:

Figure 116: *Authentication Sources Page*



After clicking **Add Authentication Source** from either of these locations, Policy Manager displays the **Add** page. Different tabs and fields appear, depending on the **Authentication Source** selected.

Figure 117: *Add Authentication Source Page*



You can configure the following authentication sources:

- Generic LDAP and Active Directory
- Generic SQL DB
- HTTP
- Kerberos
- Okta
- RADIUS Server
- Static Host List
- Token Server

Generic LDAP and Active Directory

Policy Manager can perform NTLM/MSCHAPv2, PAP/GTC, and certificate-based authentications against Microsoft Active Directory and against any LDAP-compliant directory. For example, Novell eDirectory, OpenLDAP, or Sun Directory Server. Both LDAP and Active Directory based server configurations are similar. You can retrieve role mapping attributes by using filters. For more information, see Adding and Modifying Role Mapping Policies on page 225.

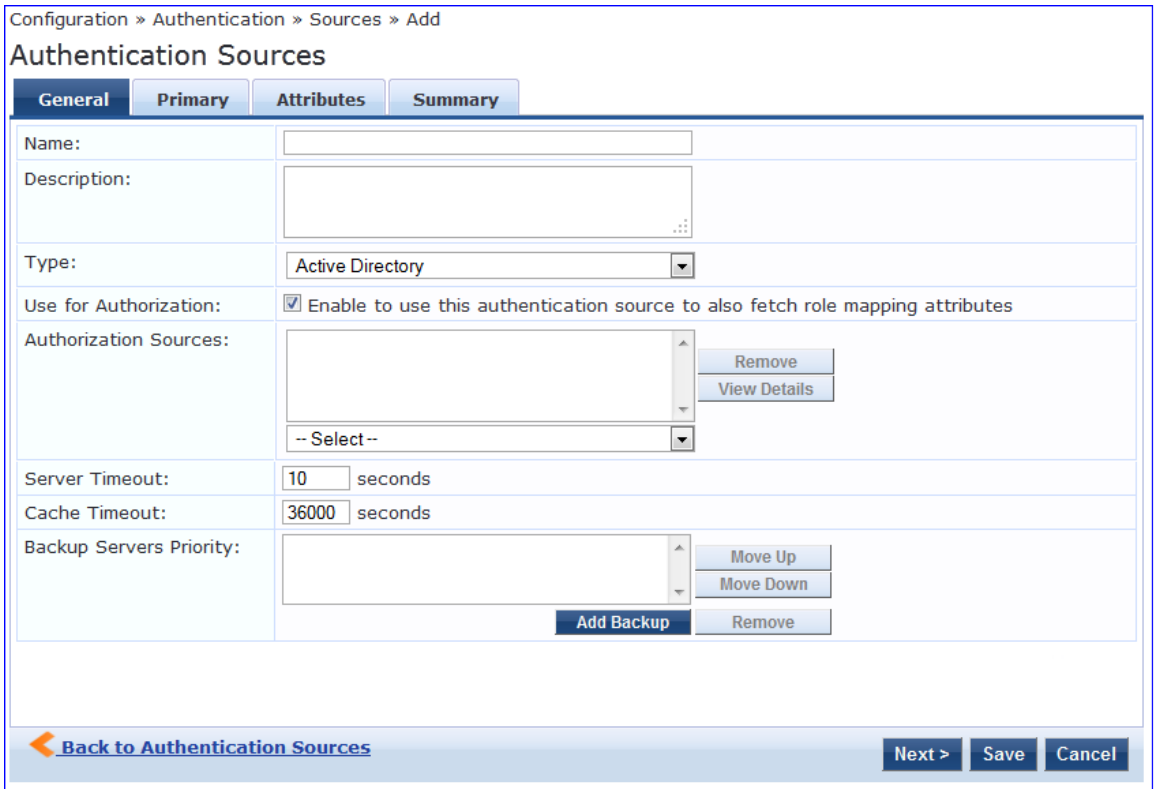
Use the following tabs to configure Generic LDAP and Active Directory authentication sources on the **Configuration > Authentication > Sources >Add** page:

- General Tab on page 170
- Primary Tab on page 172
- Attributes Tab on page 174
- Summary Tab on page 183

General Tab

The **General** tab labels the authentication source and defines session details. The following image is an example of the **Active Directory - General** tab:

Figure 118: *Generic LDAP or Active Directory - General Tab*



The following table describes the **Generic LDAP or Active Directory - General** parameters:

Table 76: *Generic LDAP or Active Directory - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of authentication source. In this context, select **General LDAP** or **Active Directory.**
Use for Authorization	Enable this check box instruct Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This box is checked (enabled) by default.
Authorization Sources	Specifies additional sources from which role mapping attributes to be fetched. Select a previously configured authentication source from the drop-down list and click **Add** to add authentication source to the list of authorization sources. Click **Remove** to remove the authentication source from the list. If Policy Manager authenticates the user or device from this authentication source, then also fetches role mapping attributes from these additional authorization sources **NOTE:** As described in Services on page 87, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes regardless of which authentication source the user or device was authenticated against.

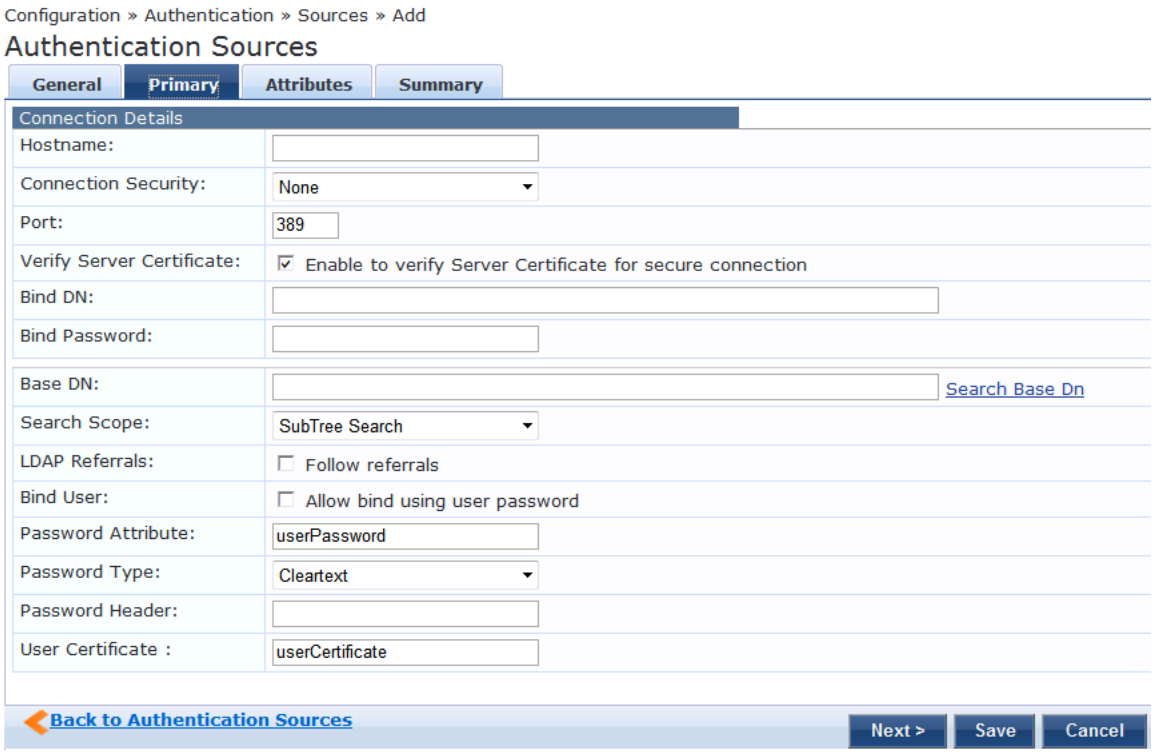
Table 76: *Generic LDAP or Active Directory - General Tab Parameters (Continued)*

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

Primary Tab

The **Primary** tab defines the settings for the primary server. The following image is an example of the **Generic Active Directory - Primary** tab:

Figure 119: *Generic LDAP or Active Directory - Primary Tab*



The following table describes the **Generic LDAP or Active Directory - Primary** parameters:

Table 77: *Generic LDAP or Active Directory - Primary Tab Parameters*

Parameter	Description
Hostname	Specify the hostname or the IP address of the LDAP or Active Directory server.
Connection Security	• Select **None** for default non-secure connection (usually port 389). • Select **StartTLS** for secure connection that is negotiated over the standard LDAP port. This is the preferred way to connect to an LDAP directory securely. • Select **LDAP over SSL** or **AD over SSL** to choose the legacy way of securely connecting to an LDAP directory. Port 636 must be used for this type of connection.
Port	Specifies the TCP port at which the LDAP or Active Directory server is listening for connections. The default TCP port for LDAP connections is 389 and the default port for LDAP over SSL is 636.
Verify Server Certificate	Select this checkbox to verify the server certificate as part of authentication.
Bind DN	Specify the DN of the administrator account. Policy Manager uses this account to access all other records in the directory. **NOTE:** For Active Directory, the bind DN can also be in the administrator@domain format (for example, administrator@acme.com).
Bind Password	Specify the password for the administrator DN entered in the **Bind DN** field.
NetBIOS Domain Name	Specify the Active Directory domain name for this server. Policy Manager prepends this name to the user ID to authenticate users found in this Active Directory. **NOTE:** This setting is available only for Active Directory.
Base DN	Enter the DN of the node in your directory tree from which to start searching for records. After entering the values for the fields described above, click **Search Base DN** to browse the directory hierarchy. The LDAP browser opens. You can navigate to the DN that you want to use as the base DN. Click on any node in the tree structure that is displayed to select it as a base DN. Note that the base DN is displayed at the top of the LDAP browser. **NOTE:** This is also a method to test the connectivity to your LDAP or AD directory. If the values entered for the primary server attributes are correct, you can browse the directory hierarchy by clicking **Search Base Dn**.
Search Scope	Select the scope of the search you want to perform, starting at the base DN. • **Base Object Search** allows you to search at the level specified by the base DN. • **One Level Search** allows you to search up to one level lesser to the immediate children of the base DN. • **Subtree Search** allows you to search the entire subtree under the base DN (including at the base DN level).
LDAP Referral	Enable this check box to automatically follow referrals returned by your directory server in search results. Refer to your directory documentation for more information on referrals.

Table 77: *Generic LDAP or Active Directory - Primary Tab Parameters (Continued)*

Parameter	Description
Bind User	Enable this checkbox to authenticate users by performing a bind operation on the directory using the credentials (user name and password) obtained during authentication. For clients to be authenticated by using the LDAP bind method, Policy Manager must receive the password in cleartext.
Password Attribute (Available only for **Generic LDAP**)	Enter the name of the attribute in the user record from which user password can be retrieved. This is not available for Active Directory.
Password Type (Available only for **Generic LDAP**)	Specify whether the password type is Cleartext, NT Hash, or LM Hash.
Password Header (Available only for **Generic LDAP**)	Specifies the Oracle's LDAP implementation that prepends a header to a hashed password string. If using Oracle LDAP, enter the header in this field to correctly identify and read the password .
User Certificate	Enter the name of the attribute in the user record from which user certificate can be retrieved.
Always use NETBIOS name	Check this option to always use NETBIOS name instead of the domain part in username for authentication. **NOTE:** This field is available only if you select **Active Directory** as an authentication source.

Attributes Tab

The **Attributes** tab defines the Active Directory or LDAP Directory query filters and the attributes to be fetched by using those filters. The following images are the examples of the **Active Directory - Attributes** tab and the **Generic LDAP Directory - Attributes** tab:

Figure 120: *Active Directory Attributes Tab (with Default Data)*

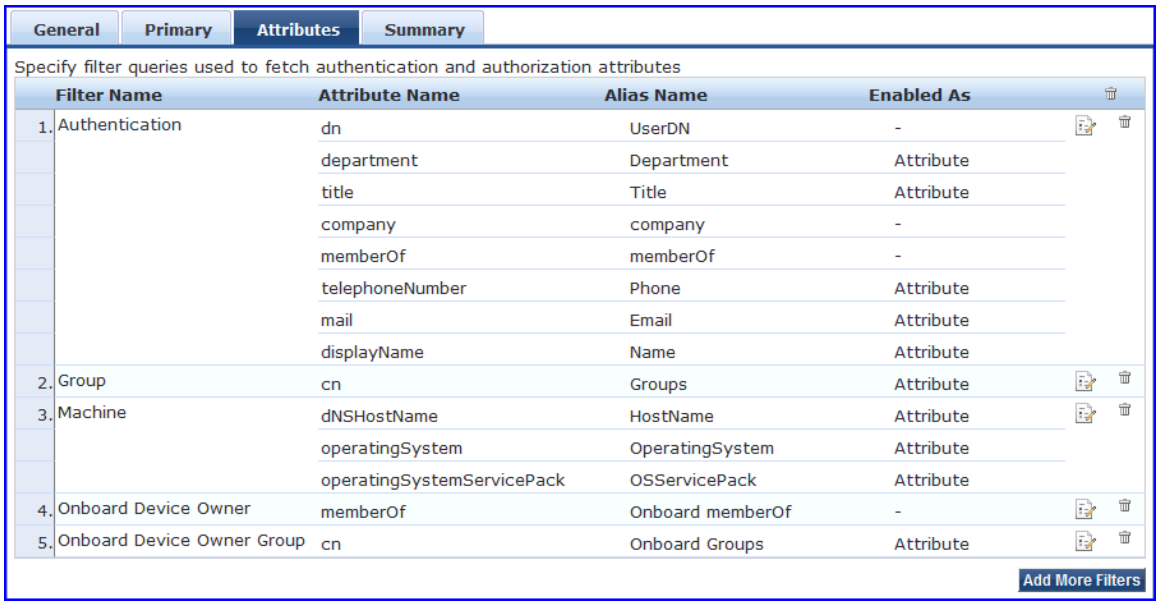


Figure 121: *Generic LDAP Directory - Attributes Tab*

The following table describes the **AD/LDAP Attributes Tab - Filter Listing Screen** parameters:

Table 78: *AD/LDAP Attributes Tab - Filter Listing Screen Parameters*

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

The following table describes the available directories:

Table 79: *AD/LDAP Default Filters*

Directory	Default Filters

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

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

Table 79: *AD/LDAP Default Filters (Continued)*

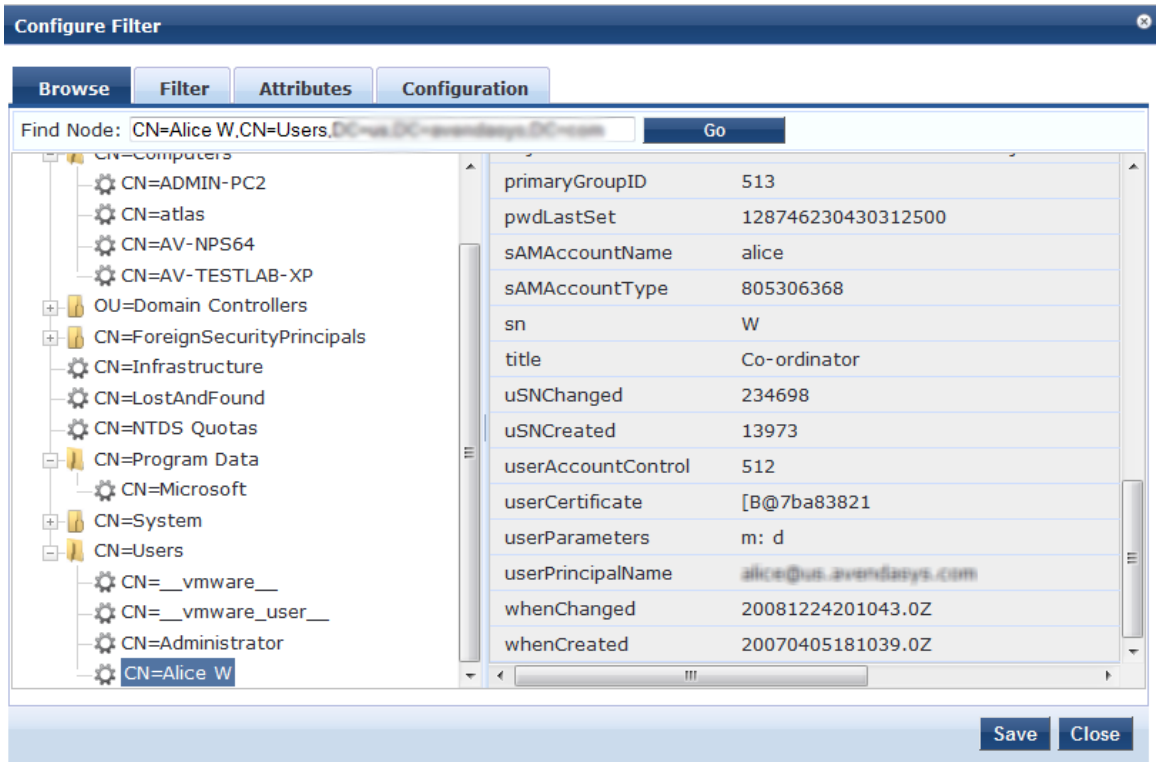
Directory	Default Filters
	▪ This query fetches all group records (of objectClass groupOfNames), where the member field contains the DN of the user record (UserDN, which is populated after the authentication filter query is executed. The attribute fetched with this filter query is cn, which is the name of the group (this is aliased to a more readable name: groupName)).
Add More Filters	Click this button to open the **Authentication Sources > Add** page to open the **Configure Filter** page. From this page, you can define a filter query and the related attributes to be fetched.

Browse Tab

The **Browse** tab shows an LDAP browser from which you can browse the nodes in the LDAP or AD directory, starting at the base DN. This is presented in the read-only mode. Selecting a leaf node (a node that has no children) displays the attributes associated with that node.

The following image is an example of the **AD/LDAP Configure Filter - Browse** tab:

Figure 122: *AD/LDAP Configure Filter - Browse Tab*



The following table describes the **AD/LDAP Configure Filter Page - Browse** tab parameters:

Table 80: *AD/LDAP Configure Filter Page - Browse Tab Parameters*

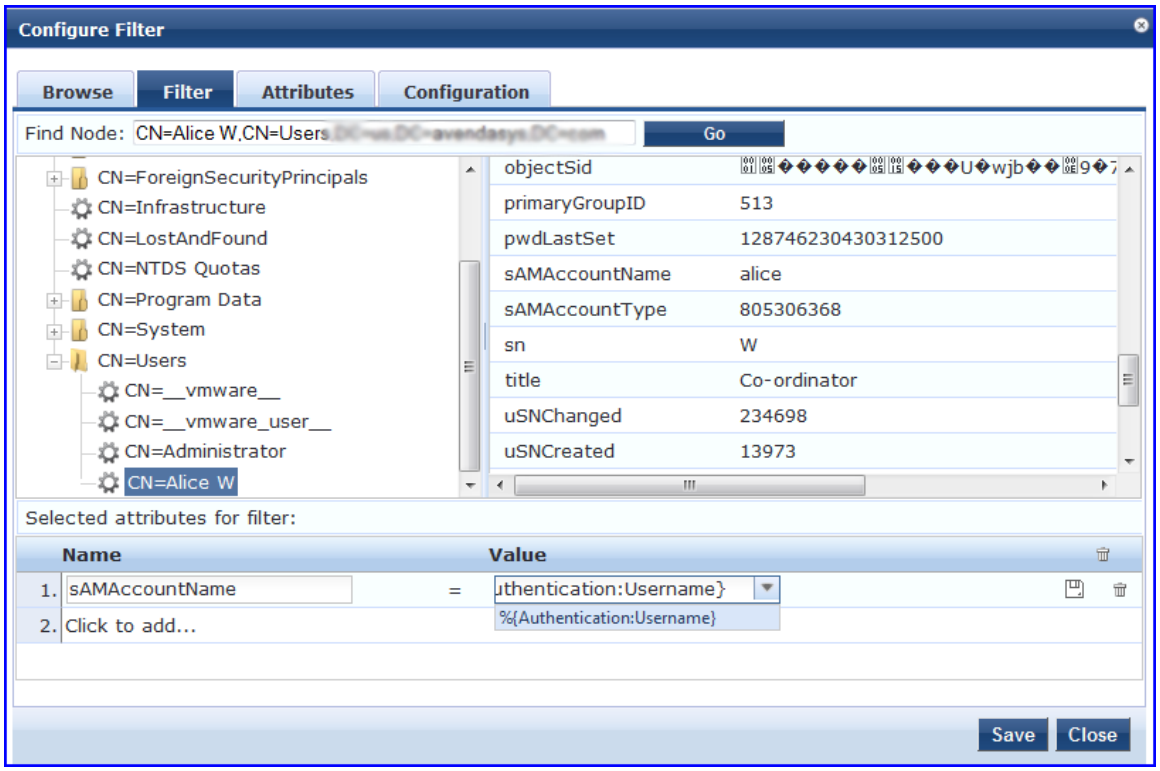
Navigation	Description
Find Node	Find the node by entering the DN and clicking the **Go** button.

Filter Tab

The **Filter** tab provides an LDAP browser interface to define the filter search query. You can define the attributes used in the filter query using this interface.

The following image is an example of the **AD/LDAP Create Filter Page - Filter** tab:

Figure 123: *AD/LDAP Create Filter Page - Filter Tab*



NOTE

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

NOTE

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

The following table describes the **Configure Filter Page - Filter** tab parameters:

Table 81: *Configure Filter Page - Filter Tab Parameters*

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

Creating Filters

The goal of filter creation is to help Policy Manager to understand how to find a user or device connecting to the network in LDAP or Active Directory.Use the following steps to create a filter:

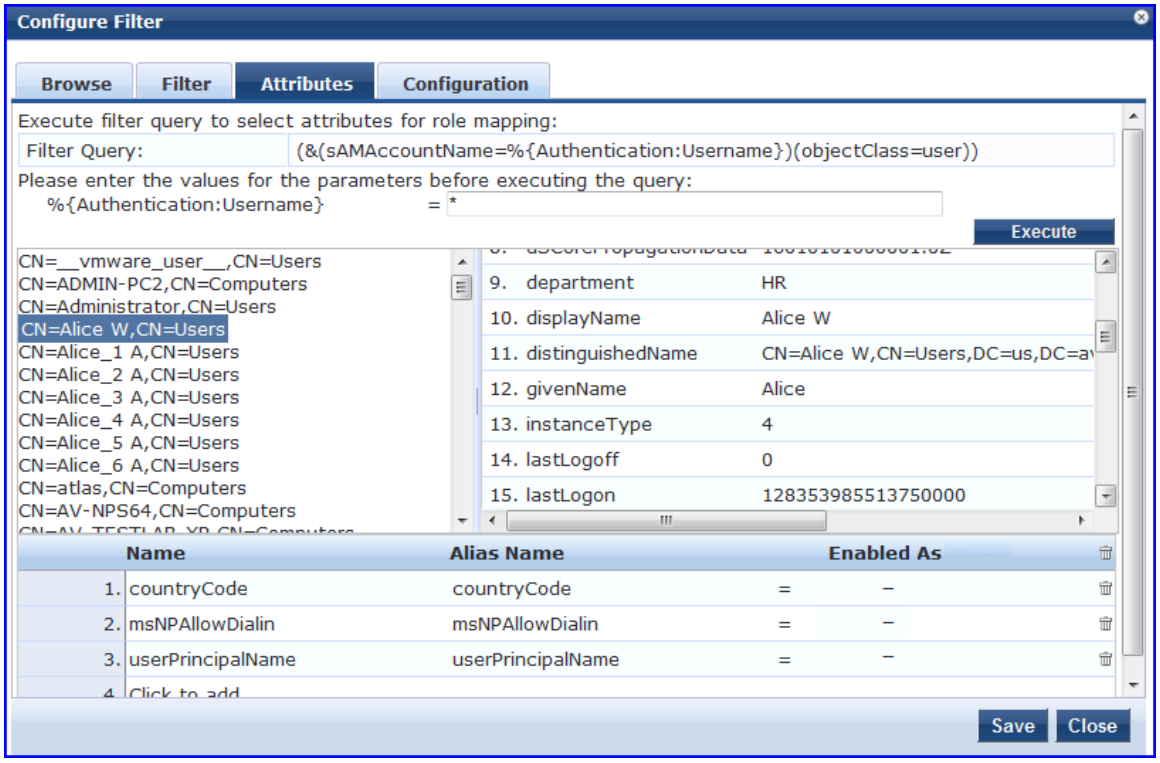
1. From the **Filter** tab, click on a node that you want to extract user or device information from. For example, browse the **Users** container in Active Directory and select the node for a user (Alice, for example). On the right hand side, you can view the attributes associated with that user.
2.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

Attributes Tab

The **Attributes** tab defines the attributes to be fetched from Active Directory or LDAP directory. Each attribute can also be enabled as a role, which means the value fetched for this attribute can be used directly in enforcement policies. For more information, see Configuring Enforcement Policies on page 1.

The following figure displays the **AD/LDAP Configure Filter - Attributes** tab:

Figure 124: *AD/LDAP Configure Filter - Attributes Tab*



The following table describes the **AD/LDAP Configure Filter Page - Attributes** tab parameters:

Table 82: *AD/LDAP Configure Filter Page - Attributes Tab Parameters*

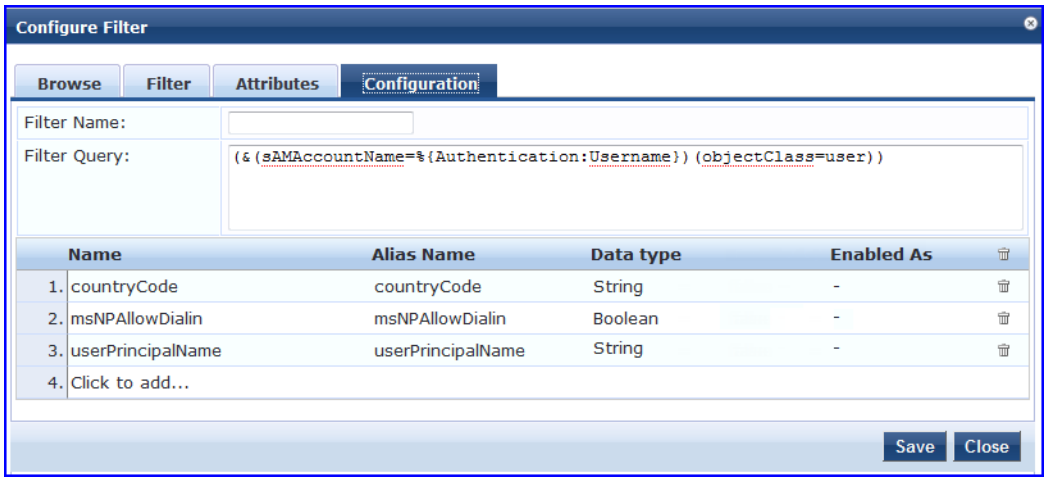
Parameter	Description
Enter values for parameters	Policy Manager parses the filter query (created in the **Filter** tab and shown at the top of the **Attributes** tab) and prompts to enter the values for all dynamic session parameters in the query. For example, if you have **%{Authentication:Username}**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

Configuration Tab

The **Configuration** tab shows the filter and attributes configured in the **Filter** and **Attributes** tabs respectively. From this tab, you can also manually edit the filter query and attributes to be fetched.

The following figure displays the **Configure Filter - Configuration** tab:

Figure 125: *Configure Filter Popup - Configuration Tab*



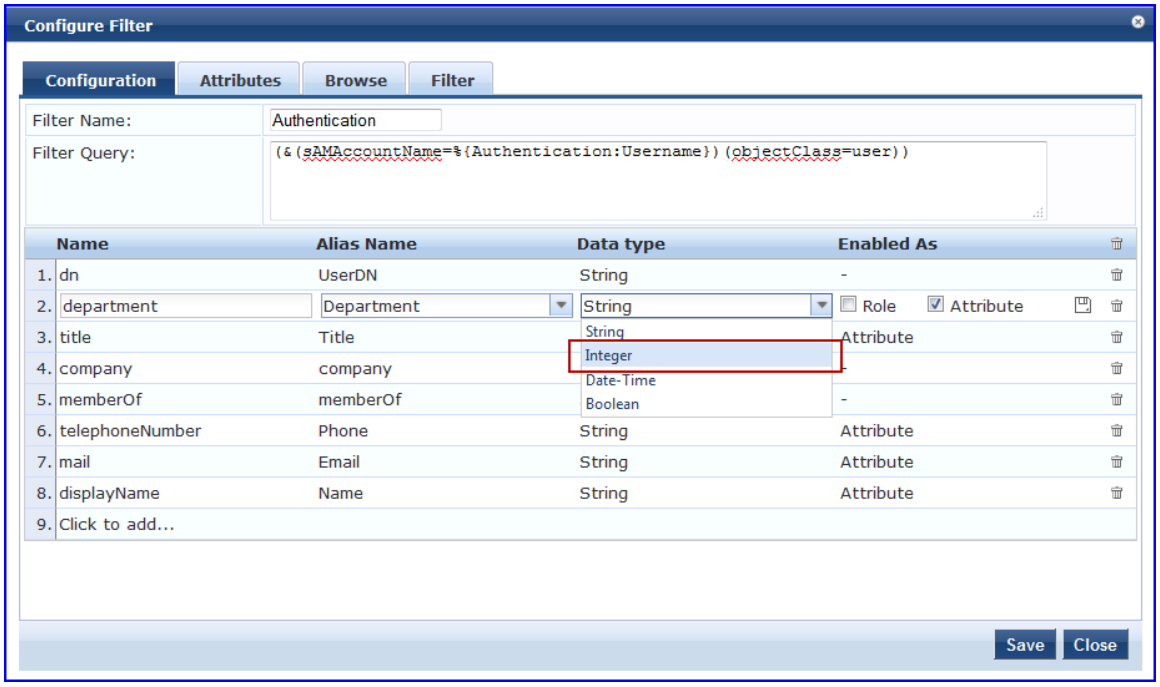
Modify Default Filters

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

NOTE

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

Figure 126: *Modify Default Filters - Configuration Tab*

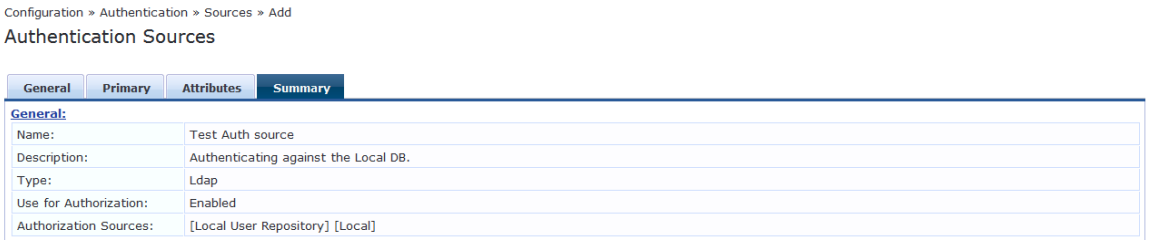


The attributes that are defined for the authentication source display as attributes in role mapping policy rules editor under the authorization source namespace. Then, on the **Role Mappings - Rules Editor** page, the operator values that display are based on the **Data type** specified here. For example,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

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure is an example of the **Generic LDAP - Summary** tab:

Figure 127: *Generic LDAP - Summary Tab*



Generic SQL DB

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

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

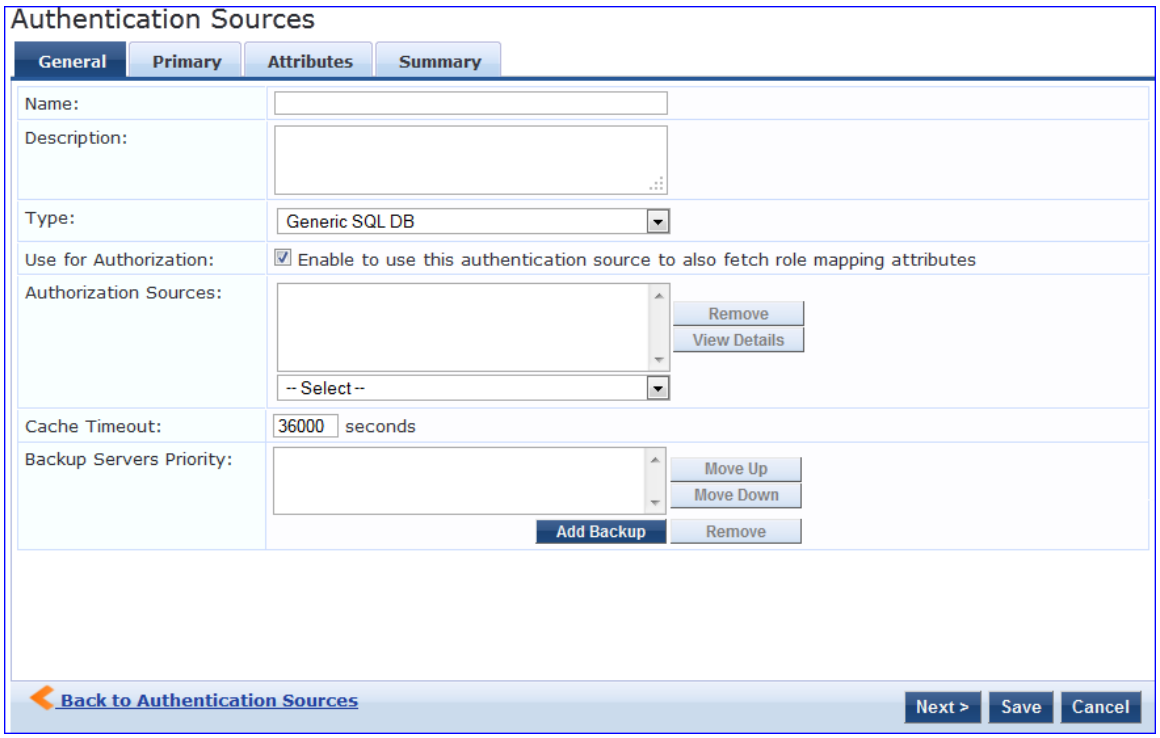
- General Tab on page 184
- Primary Tab on page 185
- Attributes Tab on page 186
- Summary Tab on page 188

The **Configuration > Authentication > Sources > Add** page includes two configuration options for managing existing Generic SQL DB authentication source. The **Clear Cache** option on the main page clears the attributes cached by Policy Manager for all entities that authorize against this serve, and the **Copy** option creates a copy of this authentication/authorization source.

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **Generic SQL DB - General** tab:

Figure 128: *Generic SQL DB - General Tab*



The following table describes the **General SQL DB - General** parameters:

Table 83: *General SQL DB - General Tab Parameters*

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

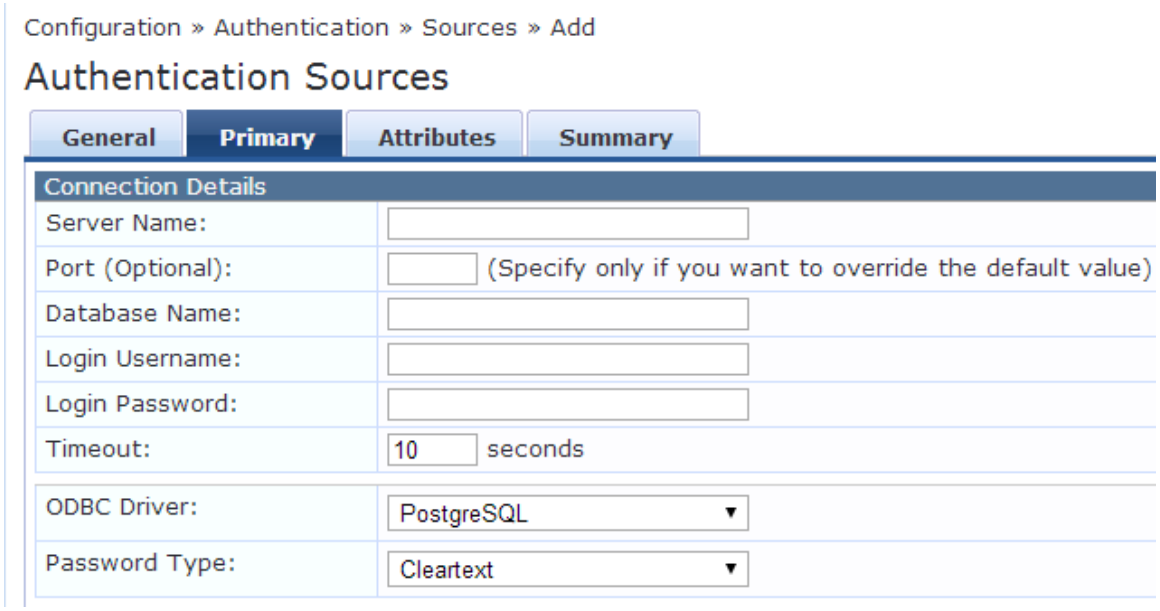
Table 83: *General SQL DB - General Tab Parameters (Continued)*

Parameter	Description
Authorization Sources	Specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop-down list and click **Add** to add to the list of authorization sources. Click **Remove** to remove the authorization source from the list. If Policy Manager authenticates the user or device from this authentication source, then Policy Manager also fetches role mapping attributes from these additional authorization sources. **NOTE:** As described in Services on page 87, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the time period for which the attributes are cached.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **General SQL DB - Primary** tab:

Figure 129: *General SQL DB - Primary Tab*



The following table describes the **Generic SQL DB - Primary** parameters:

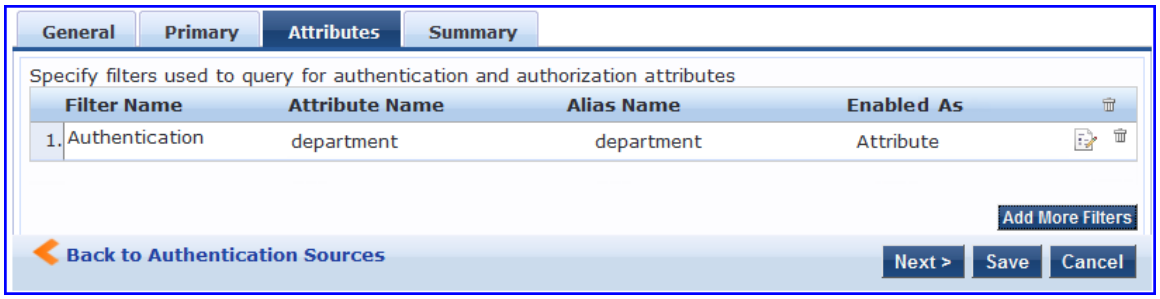
Table 84: *Generic SQL DB - Primary Tab Parameters*

Parameter	Description
Server Name	Enter the hostname or IP address of the database server.
Port (Optional)	Specify a port value to override the default port.
Database Name	Enter the name of the database from which records can be retrieved.
Login Username	Enter the name of the user used to log into the database. This account must have read access to all the attributes that need to be retrieved by the specified filters.
Password	Enter the password for the user account entered in the **Login Username** field.
Timeout	Enter the duration in seconds that Policy Manager waits before attempting to fail over from primary to backup servers (in the order in which they are configured).
ODBC Driver	Select the ODBC driver (Postgres, Oracle11g, or MSSQL) to connect to the database. MySQL is supported in versions 6.0 and later. Dell does not ship MySQL drivers by default. If you require MySQL, contact Dell support at dell.com/support to get the required patch. This patch does not persist across upgrades. If you are using MySQL, you should contact support before upgrading. If you connect to a Microsoft SQL server using Integrated Authentication, the login username in the authentication source, formatted as either domain/username or UPN (User Principal Name), the backslash (\ ) and at-sign (@) characters in addition to the hyphen and underscore characters are supported.
Password Type	Specify how the user password is stored in the database: • Cleartext : Password is stored as clear, unencrypted text. • NT Hash: Password is stored with an NT hash using MD4. • LM Hash : Password is stored with a LAN Manager Hash using DES. • SHA: Password is stored with a Secure Hash Algorighm (SHA) hash. • SHA256: Password is stored with an SHA-256 hash function.

Attributes Tab

The **Attributes** tab defines the SQL DB query filters and the attributes to be fetched by using those filters. The following figure displays the **Generic SQL DB - Attributes** tab:

Figure 130: *Generic SQL DB - Attributes Tab*



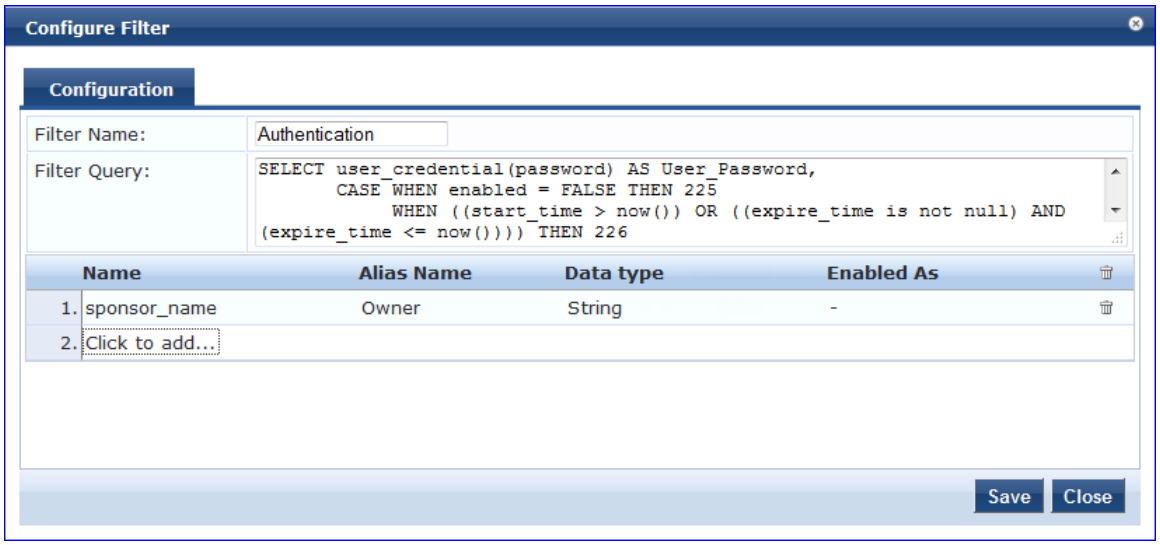
The following table describes the **Generic SQL DB - Attributes (Filter List)** parameters:

Table 85: *Generic SQL DB - Attributes Tab (Filter List) Parameters*

Tab	Parameter/Description
Filter Name	Specifies the name of the filter.
Attribute Name	Specifies the name of the SQL DB attributes defined for this filter.
Alias Name	Specifies an alias name for each attribute name selected for the filter.
Enabled As	Indicates whether the filter is enabled as a role or attribute type. This can also be blank.
Add More Filters	Click this button to open the **Configure Filter** page. Use this page to define a filter query and the related attributes to be fetched from the SQL DB store. Figure 131 displays the **Generic SQL DB - Configure Filter** page.

The following figure displays the **Generic SQL DB - Configure Filter** page:

Figure 131: *Generic SQL DB - Configure Filter Page*



The following table describes the **Generic SQL DB - Configure Filter** parameters:

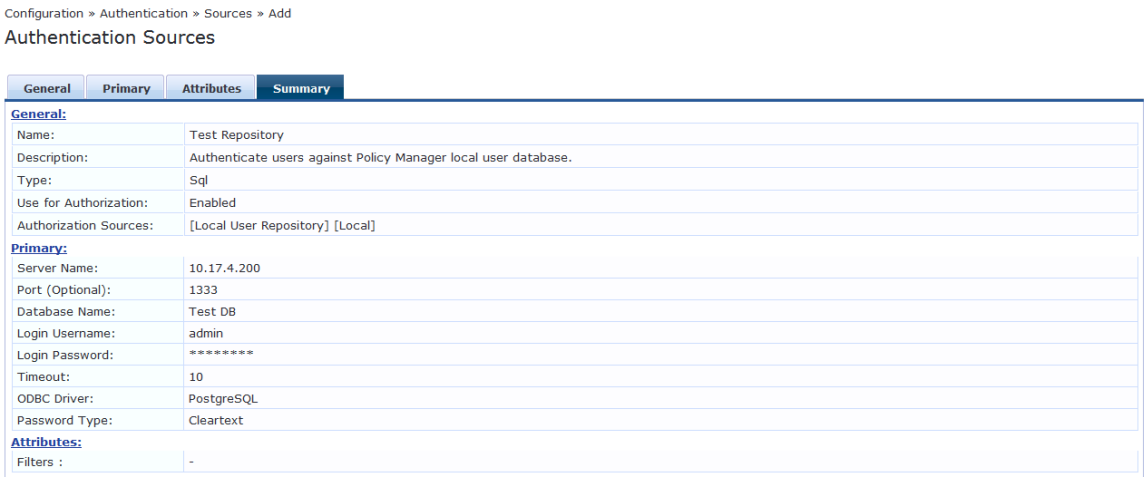
Table 86: *Generic SQL DB Configure Filter Page Parameters*

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

Summary Tab

Use the **Summary** tab to view the parameters configured in the **General**, **Primary**, and **Attributes** tabs. The following figure displays the **Generic SQL DB - Summary** tab:

Figure 132: *Generic SQL DB - Summary Tab*



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 is secure and can be trusted.

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

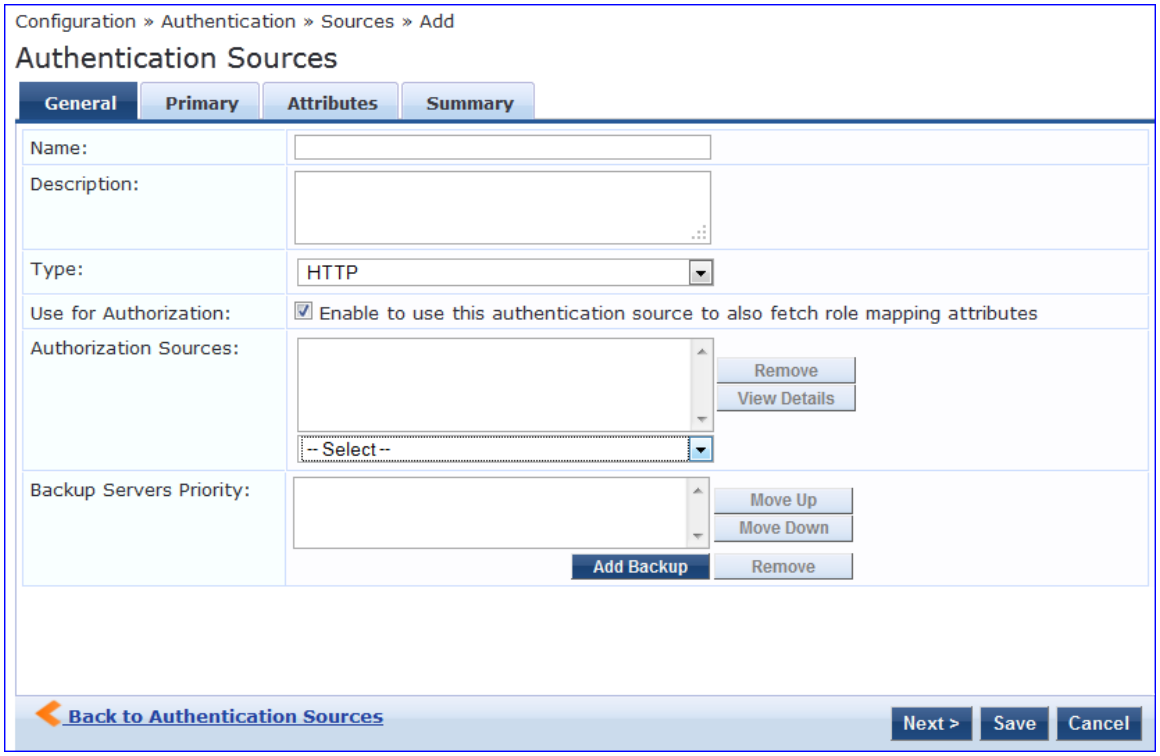
- General Tab on page 189
- Primary Tab on page 190
- Attributes Tab on page 191

- Summary Tab on page 193

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **HTTP - General** tab:

Figure 133: *HTTP - General Tab*



The following table describes the **HTTP - General** tab parameters:

Table 87: *HTTP - General Tab Parameters*

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

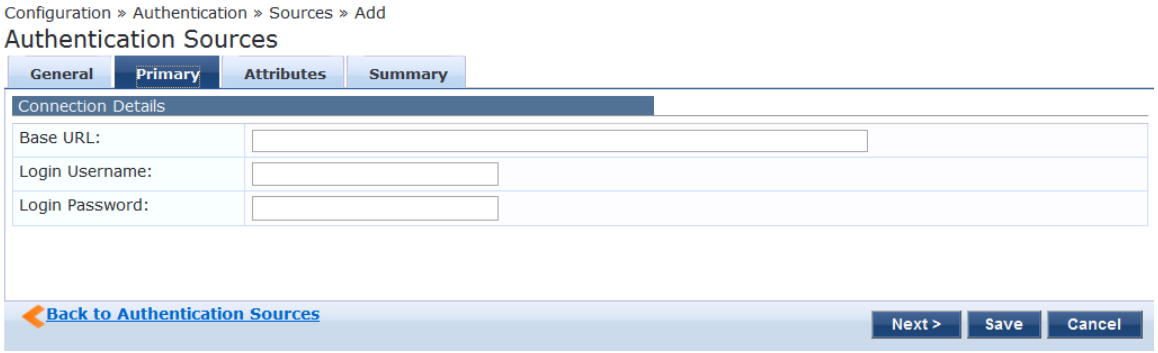
Table 87: *HTTP - General Tab Parameters (Continued)*

Parameter	Description
Use for Authorization	Enable this option to request Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This check box is enabled by default.
Authorization Sources	Specify additional sources from which to fetch role mapping attributes. Select a previously configured authentication source from the drop-down list and click **Add** to add it to the list of authorization sources. Click **Remove** to remove the selected additional resource from the list. If Policy Manager authenticates the user or device from this authentication source, then also fetches role mapping attributes from these additional authorization sources. **NOTE:** As described in Services on page 87, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields applicable for primary server specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **HTTP - Primary** tab:

Figure 134: *HTTP - Primary Tab*



The following table describes the **HTTP - Primary** tab parameters:

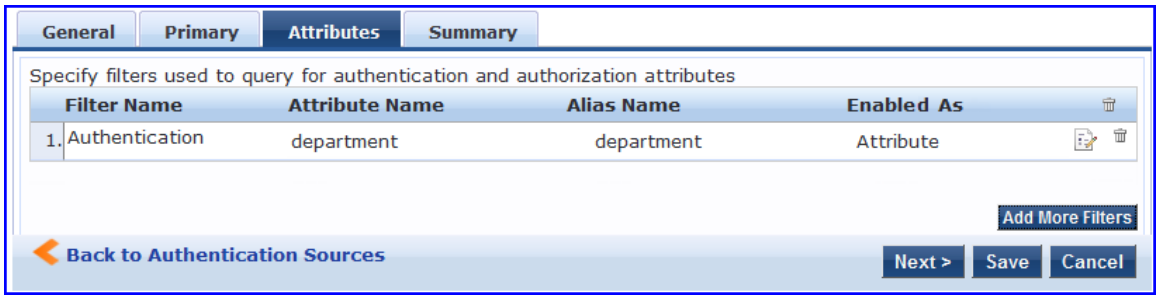
Table 88: *HTTP - Primary Tab Parameters*

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

Attributes Tab

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

Figure 135: *HTTP - Attributes Tab*



The following table describes the **HTTP - Attributes** tab parameters:

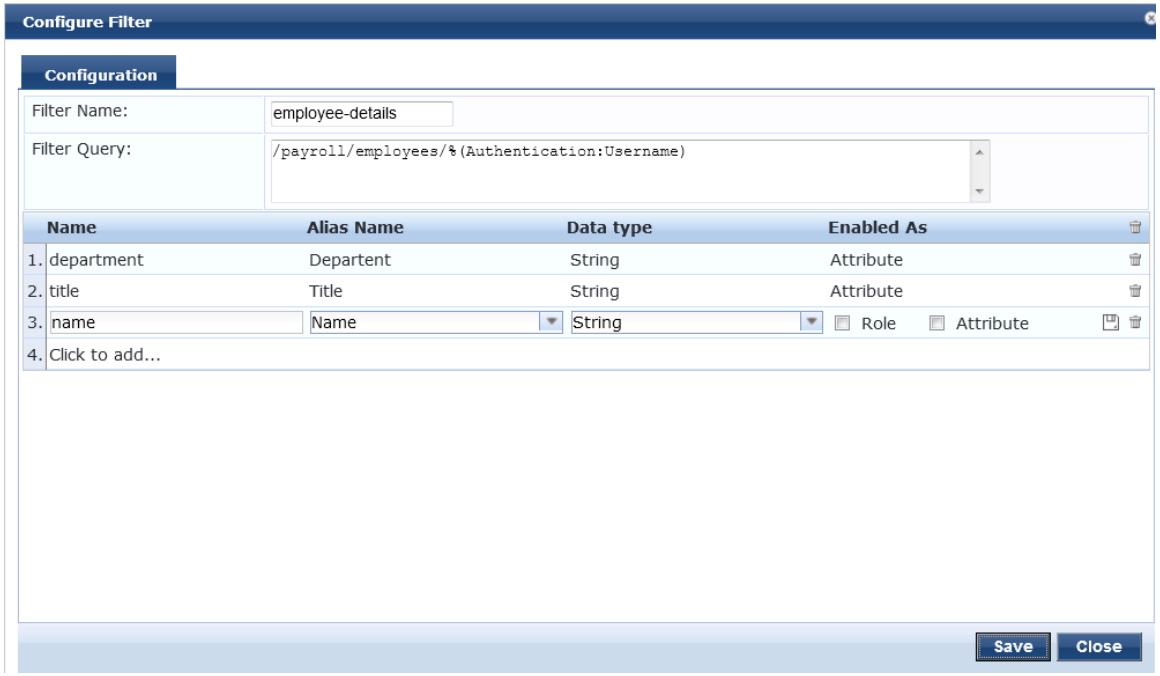
Table 89: *HTTP - Attributes tab (Filter List) Parameters*

Parameter	Description
Filter Name	Displays the name of the filter.
Attribute Name	Specifies the name of the SQL DB attributes defined for this filter.
Alias Name	Specifies the name of an alias name for each attribute name selected for the filter.
Enabled As	Indicates whether an attribute is enabled as a role.
Add More Filters	Opens the **Configure Filter** page. For more information, see Add More Filters on page 192.

Add More Filters

The **Configure Filter** page defines a filter query and the related attributes to be fetched from the SQL DB store. The following figure displays the **HTTP Filter Configure** page:

Figure 136: *HTTP Filter Configure Page*



The following table describes the **HTTP Configure - Filter** parameters:

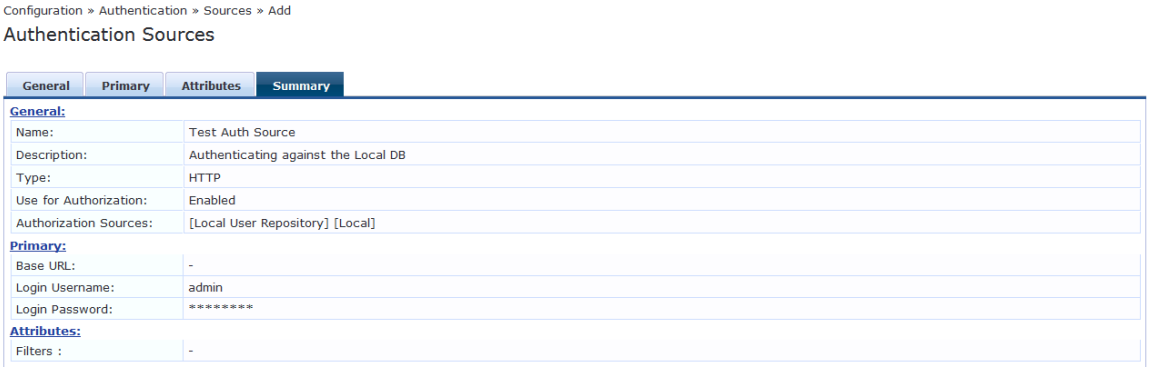
Table 90: *HTTP Configure Filter Page Parameters*

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

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure is an example of the **HTTP - Summary** tab:

Figure 137: *HTTP - Summary Tab*



Kerberos

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

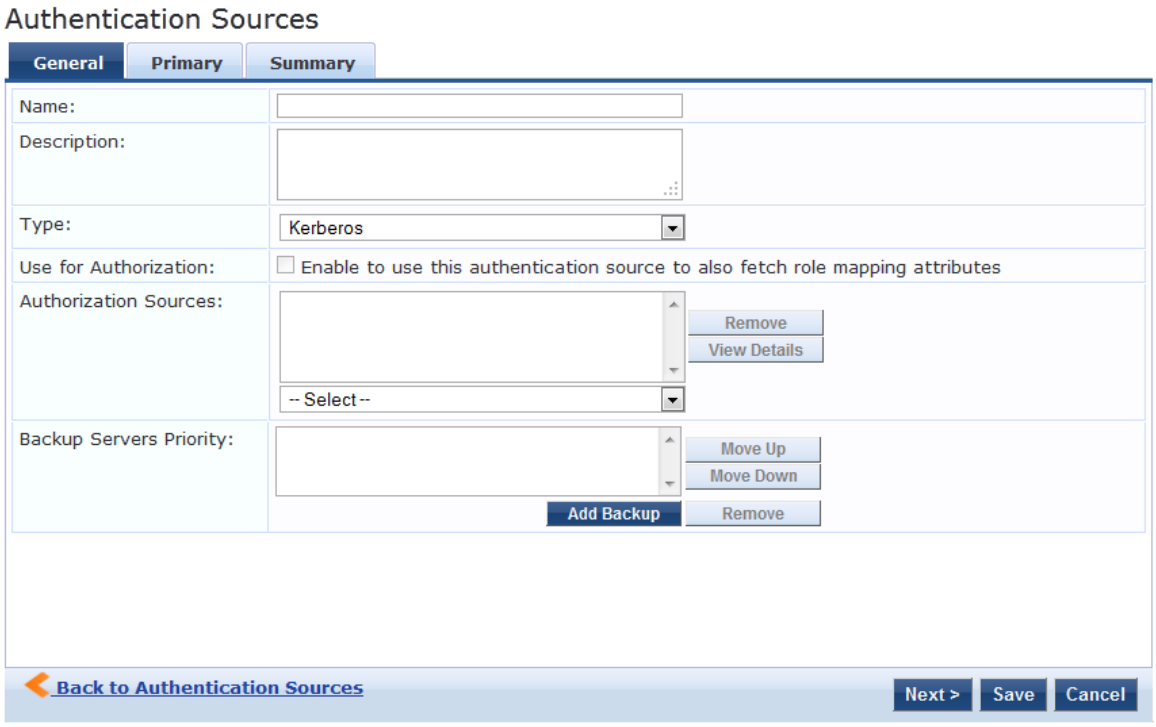
You can configure Kerberos authentication sources using the following tabs:

- General Tab on page 194
- Primary Tab on page 195
- Summary Tab on page 196

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **Kerberos - General** tab:

Figure 138: *Kerberos - General Tab*



The following table describes the **Kerberos - General** parameters:

Table 91: *Kerberos - General Tab Parameters*

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

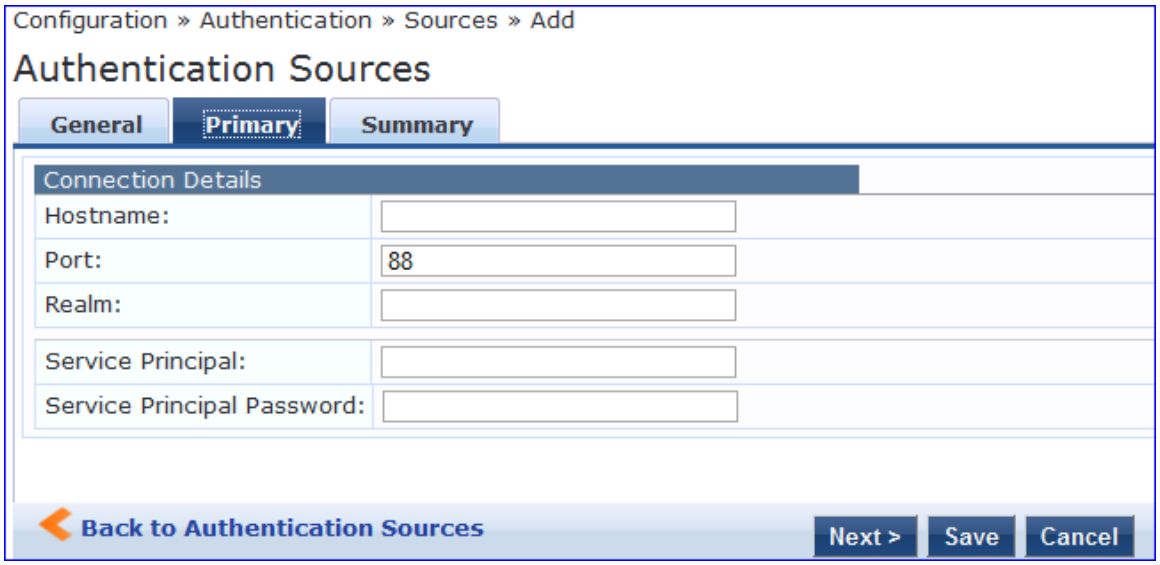
Table 91: *Kerberos - General Tab Parameters (Continued)*

Parameter	Description
Use for Authorization	Disable in this context.
Authorization Sources	Specify one or more authorization sources from which role mapping attributes to be fetched. Select a previously configured authentication source from the drop-down list and click **Add** to add it to the list of authorization sources. Click **Remove** to remove the selected authentication source from the list. **NOTE:** As described in Services on page 87, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Backup Servers	To add a backup kerberos server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields applicable for primary server specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **Kerberos - Primary** tab:

Figure 139: *Kerberos - Primary Tab*



The following table describes the **Kerberos - Primary** parameters:

Table 92: *Kerberos - Primary Tab Parameters*

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

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure displays the **Kerberos - Summary** tab:

Figure 140: *Kerberos - Summary Tab*

Okta

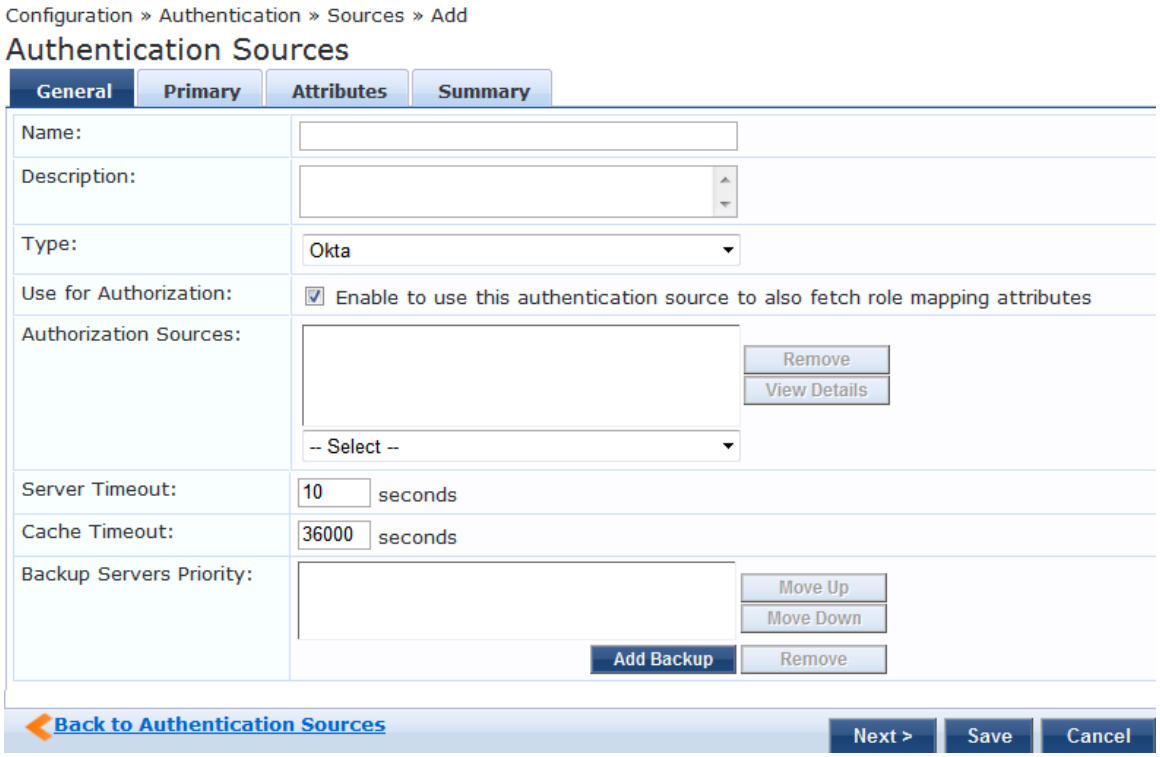
You can use Okta as an authentication source only for servers of the type Dell Application Authentication. Configure Okta authentication sources on the following tabs:

- General Tab on page 197
- Primary Tab on page 198
- Attributes Tab on page 199
- Summary Tab on page 201

General Tab

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

Figure 141: *Okta - General Tab*



The following table describes the **Okta - General** parameters:

Table 93: *Okta - General Tab Parameters*

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

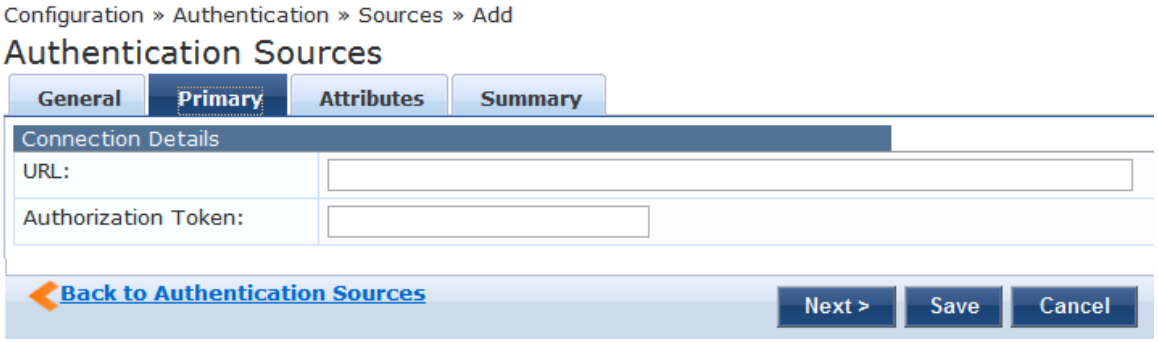
Table 93: *Okta - General Tab Parameters (Continued)*

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

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **Okta - Primary** tab:

Figure 142: *Okta - Primary Tab*



The following table describes the **Okta - Primary** parameters:

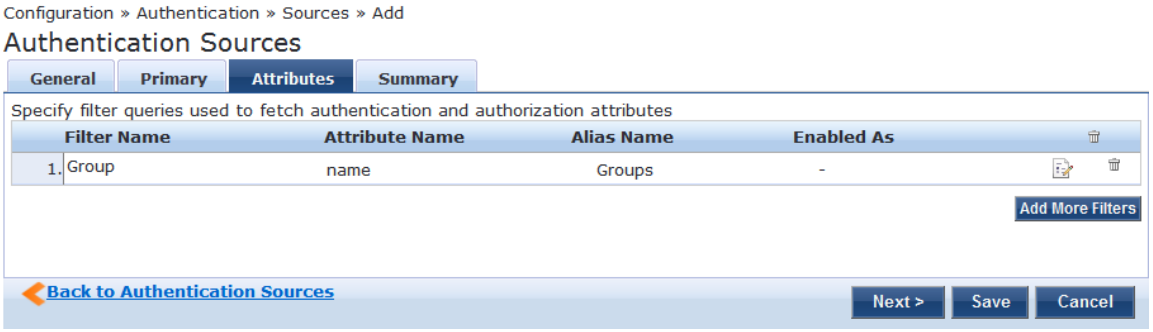
Table 94: *Okta - Primary Tab Parameters*

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

Attributes Tab

The **Attributes** tab defines the Okta query filters and the attributes to be fetched by using those filters. The following figure displays the **Okta - Attributes** tab:

Figure 143: *Okta - Attributes Tab*



The following table describes the **Okta - Attributes** parameters:

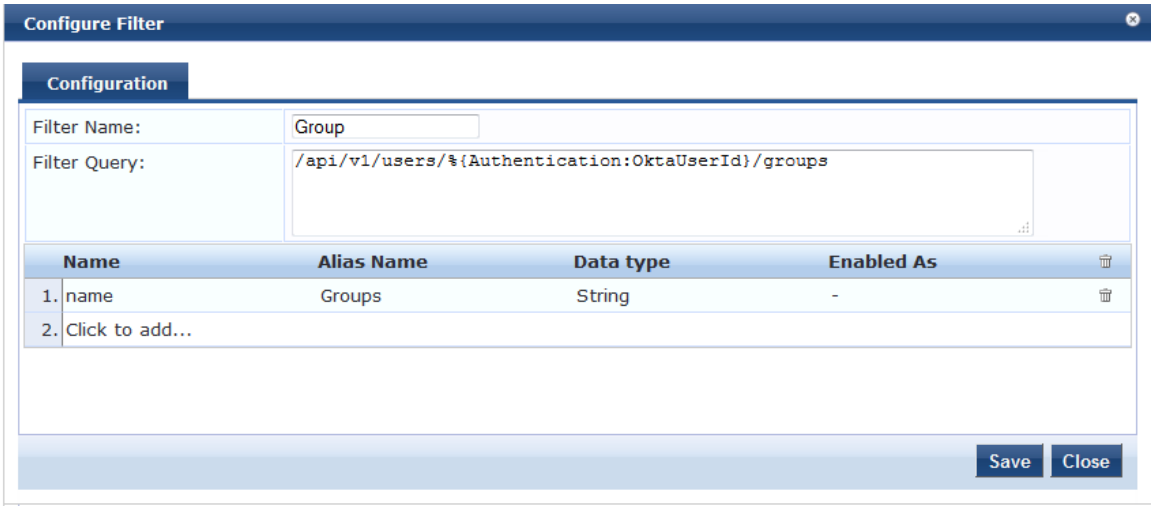
Table 95: *Okta - Attributes Tab Parameters*

Parameter	Description
Filter Name	Displays the name of the filter. You can configure only **Group** for Okta.
Attribute Name	Specifies the name of the LDAP/AD attributes defined for this filter.
Alias Name	Specifies the alias name for each attribute name selected for the filter.
Enable As	Specifies whether value to be used directly as a role or attribute in an enforcement policy. This bypasses the step of assigning a role in Policy Manager through a role mapping policy.
Add More Filters	Click this button to open the **Configure Filter** page. Refer to Add More Filters on page 200.

Add More Filters

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

Figure 144: *Okta - Configure Filter Page*



The following table describes the **Okta Configure Filter** parameters:

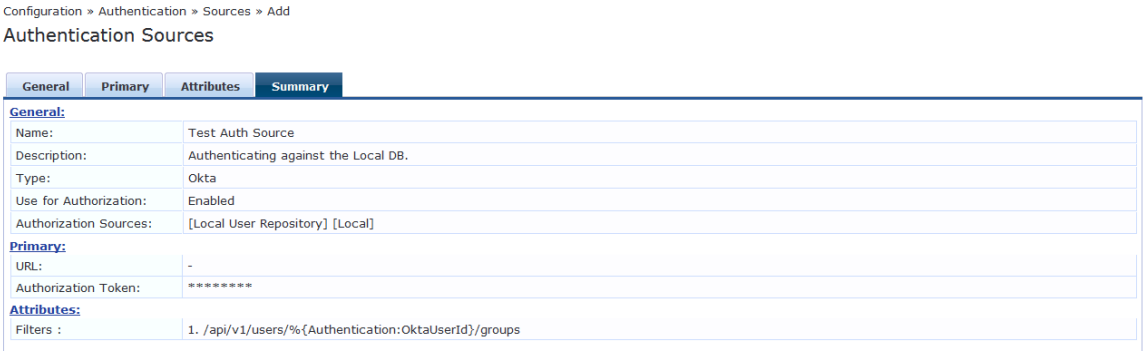
Table 96: *Okta Configure Filter Page*

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

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure displays the **Okta - Summary** tab:

Figure 145: *Okta - Summary Tab*



RADIUS Server

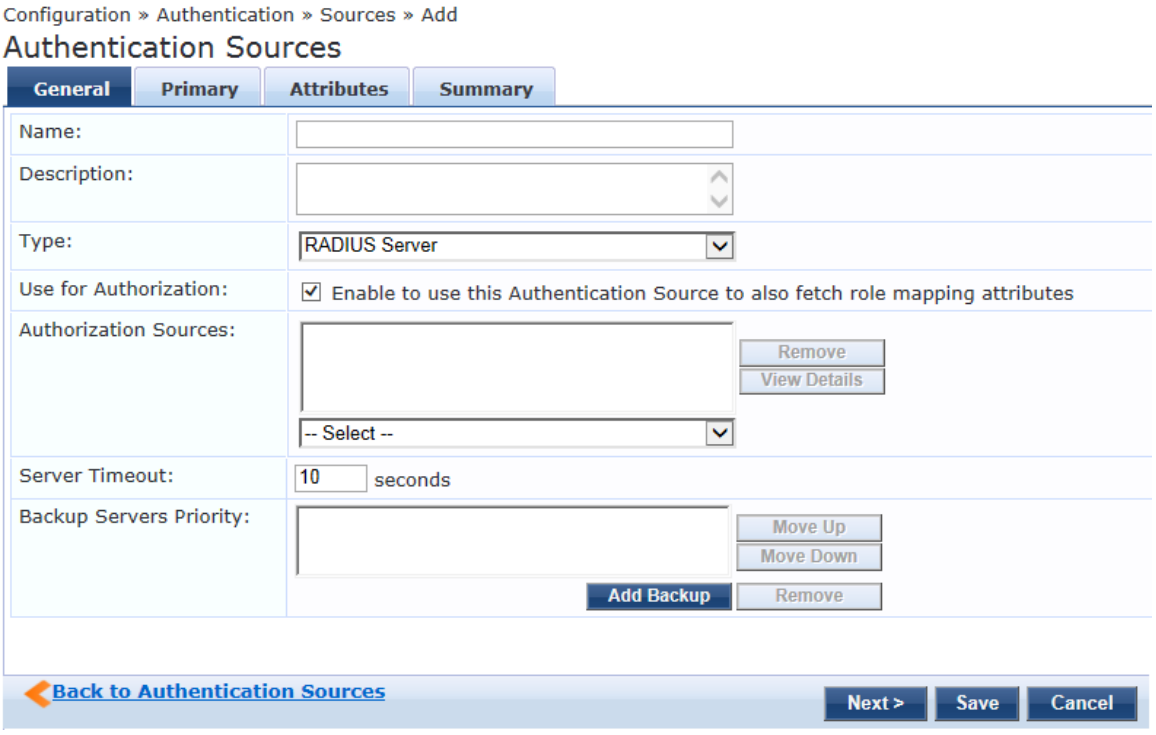
You can use the **RADIUS Server** as an authentication source to allow ClearPass to query a third-party **RADIUS Serve**r for authentication. Configure **RADIUS Server** authentication sources on the following tabs:

- General Tab on page 201
- Primary Tab on page 202
- Attributes Tab on page 203
- Summary Tab on page 204

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **RADIUS Server - General** tab:

Figure 146: *RADIUS Server - General Tab*



The following table describes the **Radius Server - General** parameters:

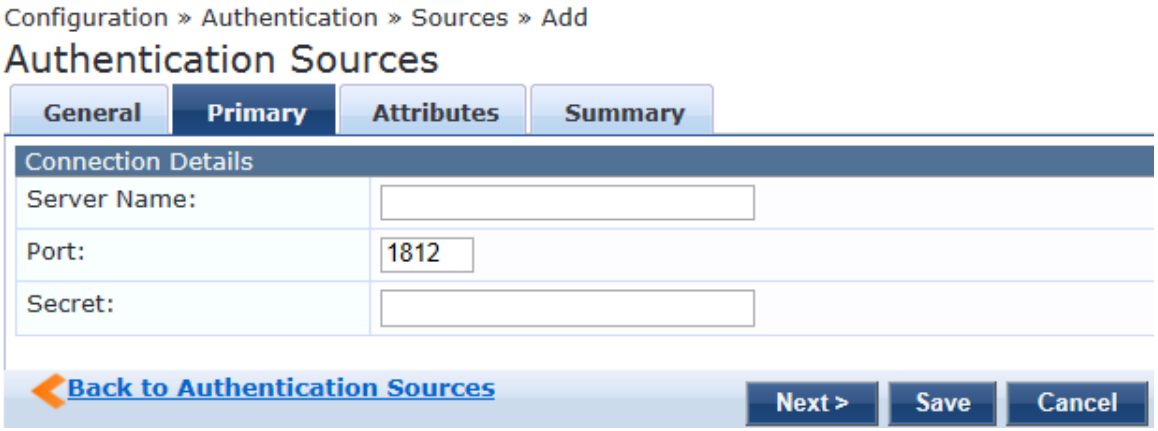
Table 97: *Radius Server - General Tab Parameters*

Parameter	Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	Select the type of source. In this context, select **RADIUS Server**.
Use for Authorization	Enable this check box to request Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source. If a user or device successfully authenticates against this authentication source, then Policy Manager also fetches role mapping attributes from the same source if the **Use for Authorization** field is enabled. This check box is enabled by default.
Server Timeout	Specify the duration in number of seconds that Policy Manager waits before considering this server unreachable. If multiple backup servers are available, then this value indicates the duration in number of seconds that Policy Manager waits before attempting to fail over from the primary to the backup servers in the order in which they are configured.
Backup Servers Priority	Click **Add Backup** to add a backup server. From the **Backup 1** tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **RADIUS Server - Primary** tab:

Figure 147: *RADIUS Server - Primary Tab*



The following table describes the **Radius Server - Primary** parameters:

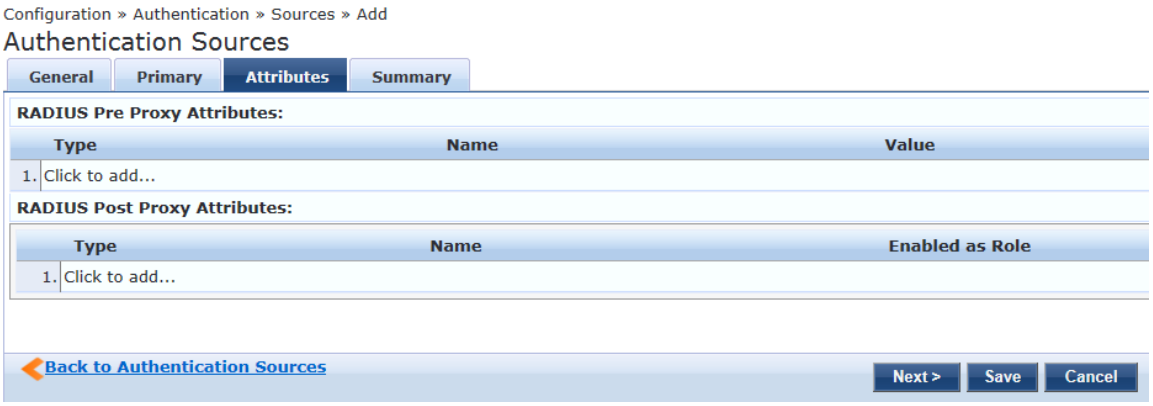
Table 98: *RADIUS Server - Primary Tab Parameters*

Parameter	Description
Connection Details	
Server Names	Enter the name of the RADIUS Server.
Port	The default port number is 1812. You may enter a different port number if required.
Secret	Enter the secret key for authentication.

Attributes Tab

The **Attributes** tab defines the Okta query filters and the attributes to be fetched by using those filters. The following figure displays the **RADIUS Server - Attributes** tab:

Figure 148: *RADIUS Server - Attributes Tab*



The following table describes the **RADIUS Server - Attributes** parameters:

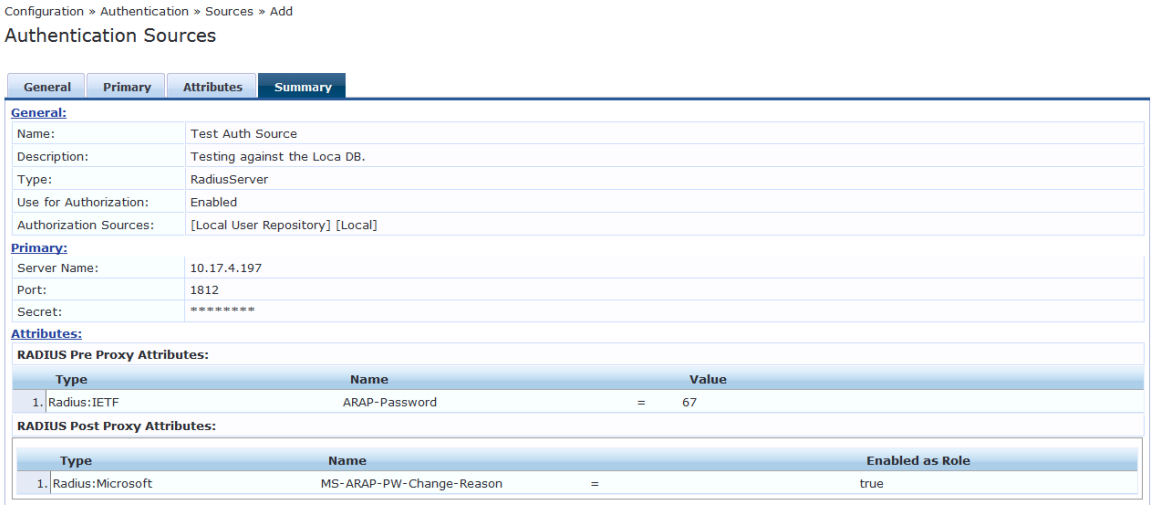
Table 99: *RADIUS Server - Attributes Tab Parameters*

Parameter	Description
RADIUS Pre-Proxy attributes	The following attributes that can be set prior to the proxy authentication: • **Type** - Select a type from the drop-down. • **Name** - Select a name from the drop-down. • **Value** - Enter a value in the text box. Save the changes by clicking the **Save** icon that appears at the end of the row.
RADIUS Post-Proxy attributes	The attributes for the post-proxy authentication are identical except that these can be set after the proxy authentication. • **Type** - Select a type from the drop-down. • **Name** - Select a name from the drop-down. • **Value** - Enter a value in the text box. Save the changes by clicking the **Save** icon that appears at the end of the row.

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure displays the **RADIUS Server - Summary** tab:

Figure 149: *RADIUS Server - Summary Tab*



Static Host List

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

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

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

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

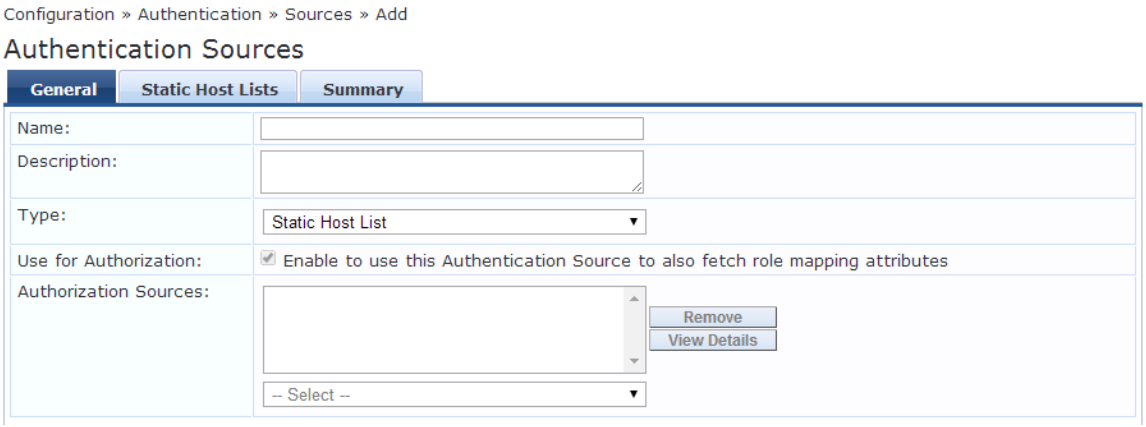
Configure primary and backup servers, session details, and the list of static hosts for **Static Host List** authentication sources on the following tabs:

- General Tab on page 205
- Static Host Lists Tab on page 205
- Summary Tab on page 206

General Tab

The **General** tab labels the authentication source. The following figure displays the **Static Host List - General** tab:

Figure 150: *Static Host List - General Tab*



The following table describes the **Static Host List - General** parameters:

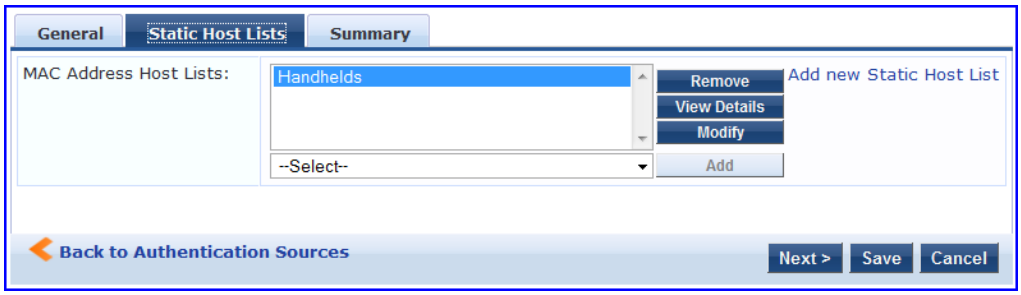
Table 100: *Static Host List - General Tab Parameters*

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

Static Host Lists Tab

The **Static Hosts List** tab defines the list of static hosts to be included as part of an authorization source. The following figure displays the **Static Host List - Static Host Lists** tab:

Figure 151: *Static Host List - Static Host Lists Tab*



The following table describes the **Static Host List - Static Host Lists** parameters:

Table 101: *Static Hosts List - Static Host Lists Tab Parameters*

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

NOTE

Only static host lists of type MAC Address List or MAC Address Regular Expression can be configured as authentication sources. Refer to Adding and Modifying Static Host Lists on page 223 for more information.

Summary Tab

You can use the **Summary** tab to view configured parameters. The following figure displays the **Static Hosts List - Summary** tab:

Figure 152: *Static Hosts List - Summary Tab*

Token Server

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

Pair this source type with an authorization source (identity store) containing user records. When using a token server as an authentication source, use the administrative interface to optionally configure a separate authorization server. Policy Manager can also use the RADIUS attributes returned from a token server to create role mapping policies. For more information, see Namespaces on page 601.

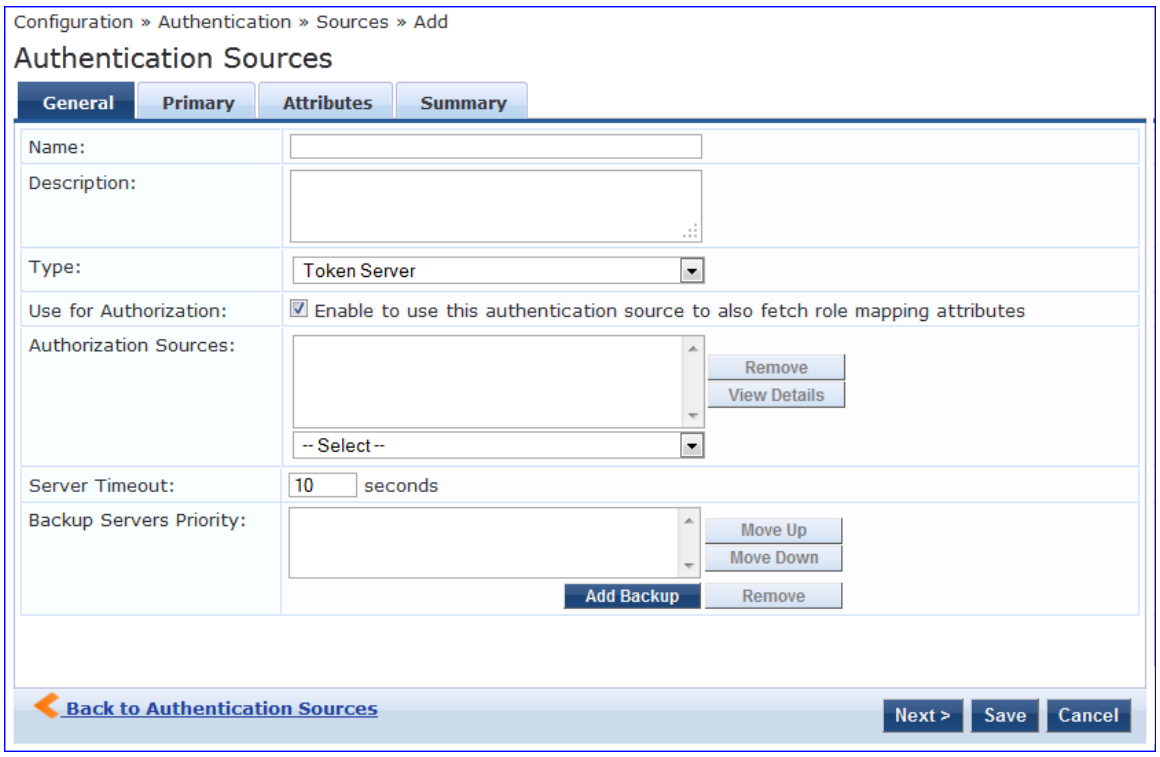
You configure primary and backup servers, session details, and the filter query and role mapping attributes to fetch for token server authentication sources on the following tabs:

- General Tab on page 207
- Primary Tab on page 208
- Attributes Tab on page 208
- Summary Tab on page 209

General Tab

The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details. The following figure displays the **Token Server - General** tab:

Figure 153: *Token Server - General Tab*



The following table describes the **Token Server - General** parameters:

Table 102: *Token Server - General Tab Parameters*

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

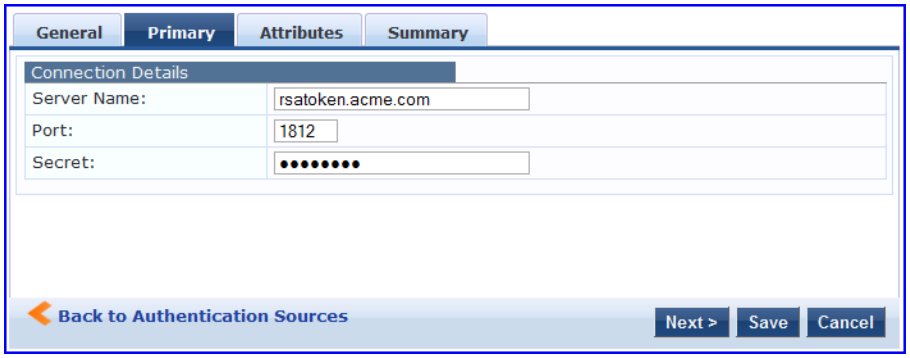
Table 102: *Token Server - General Tab Parameters (Continued)*

Parameter	Description
	NOTE: As described in Services on page 87, you can specify additional authorization sources at the service level. Policy Manager fetches role mapping attributes irrespective of which authentication source the user or device was authenticated against.
Server Timeout	Specify the duration in seconds that Policy Manager waits before attempting to fail over from primary to backup servers (in the order in which they are configured).
Backup Servers Priority	To add a backup server, click **Add Backup**. From the **Backup 1** tab, you can specify connection details for a backup server (same fields as for primary server that are specified below). To remove a backup server, select the server name and click **Remove**. Select **Move Up** or **Move Down** to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

Primary Tab

The **Primary** tab defines the settings for the primary server. The following figure displays the **Token Server - Primary** tab:

Figure 154: *Token Server - Primary Tab*



The following table describes the **Token Server - Primary** parameters:

Table 103: *Token Server - Primary Tab Parameters*

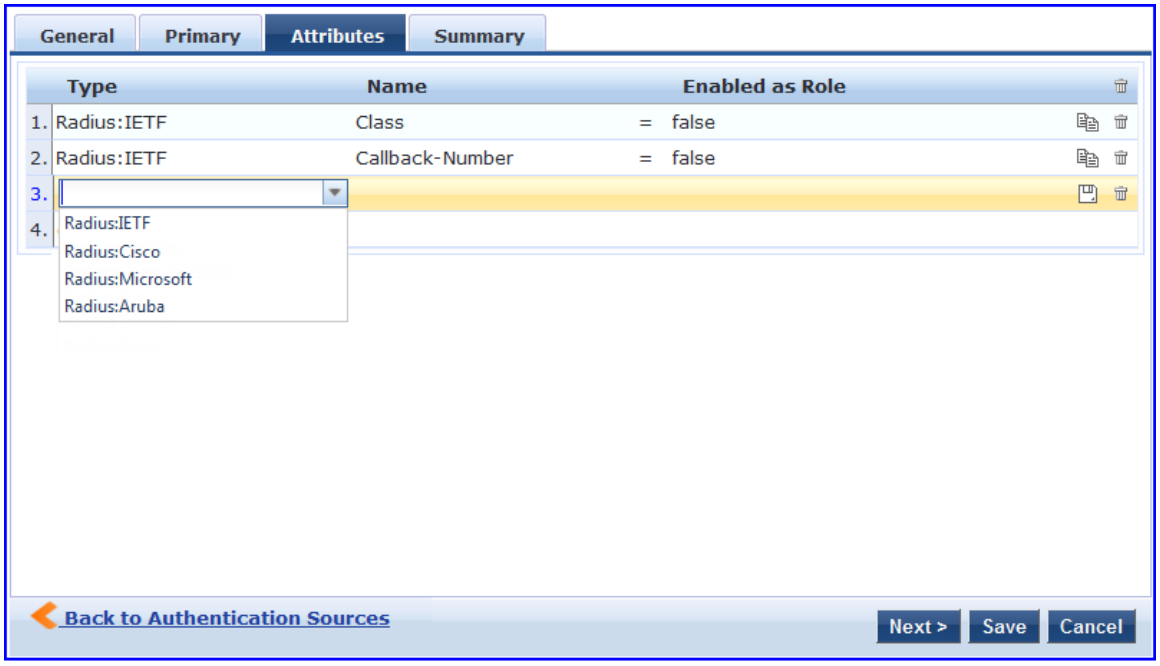
Parameter	Description
Server Name	Displays the host name or the IP address of the token server,
Port	Specifies the UDP port at which the token server listens for RADIUS connections. The default port is 1812.
Secret	Specify the RADIUS shared secret to connect to the token server.

Attributes Tab

The **Attributes** tab defines the RADIUS attributes to be fetched from the token server. These attributes can be used in role mapping policies. Policy Manager loads all RADIUS vendor dictionaries in the **Type** drop-down list with attributes.

The following figure is an example of the **Token Server - Attributes** tab:

Figure 155: *Token Server - Attributes Tab*



See Configuring a Role and Role Mapping Policy on page 224 for more information. The following table describes the **Token Server - Attribute** parameters:

Table 104: *Token Server - Attribute Tab Parameters*

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

Summary Tab

The **Summary** tab provides the summarized view of the parameters configured in the **General**, **Primary**, and **Attributes** tab. The following figure displays the **Summary** tab:

Figure 156: *Token Servers - Summary Tab*

The internal Policy Manager database supports storage of user records, when a particular class of users is not present in a central user repository (for example, neither Active Directory nor any other database).

To authenticate local users from a particular service, include local user repository among authentication sources.

For details on the WebUI settings required to configure Dell Networking W-ClearPass Policy Manager identify settings, refer to the following sections of this document:

- Configuring Single Sign-On on page 211
- Managing Local Users on page 212
- Adding and Modifying Endpoints on page 216
- Adding and Modifying Static Host Lists on page 223

Configuring Single Sign-On

The Single Sign-On (SSO) settings on the **Configuration > Identity > Single Sign-On** page allows ClearPass users that have signed in Dell Networking W-ClearPass Policy Manager to access the Onboard, Guest, and Insight applications and Policy Manager administration settings without re-authenticating. ClearPass provides SSO support using the Security Assertion Markup Language (SAML).

The single-sign on section of the Dell Networking W-ClearPass Policy Manager UI contains two tabs:

- SAML Service Provider (SP) Configuration on page 211
- Identity Provider (IdP) Configuration on page 212

SAML Service Provider (SP) Configuration

Select the application(s) you want users to access with single sign-on, and create trusted relationships between a Service Provider (SP) and Identity Provider (IdP) by providing the Identity Provider (IdP) URL and IdP certificate.

The following table describes the **Configuration > Identity > Single Sign-On>SAML SP Configuration** tab parameters**:**

Table 105: *SAML Service Provider Configuration Settings*

Parameter	Description
Identity Provider (IdP) URL	Enter the URL of the identity provider.
Enable SSO For	Select **Onboard**, **Guest** or **Insight** to enable single-sign on access to these applications. Select **Policy Manager** to enable single-sign on access to Policy Manager administration settings.
Select Certificate	Select the Identity Provider (IdP) certificate to use for single-sign on. When you select a certificate, the UI tab displays the following information about the certificate: • Subject DN

Table 105: *SAML Service Provider Configuration Settings (Continued)*

Parameter	Description
	• Issuer DN • Issue Date/Time • Expiry Date/Time • Validity Status • Signature Algorithm • Public Key Format • Serial Number • Enabled This field only displays certificates that are enabled in the certificate trust list. See also Certificate Trust List on page 535
CPPM Service Provider (SP) Metadata	• SP Metadata: Click **Download** to download and view an XML file containing metadata for the Service Provider Uniform Resource Identifier (URI). • Metadata URI : View the Uniform Resource Identifier (URI) for the SP metadata resource.

Identity Provider (IdP) Configuration

The following table describes the **Configuration > Identity > Single Sign-On>SAML IdP Configuration** tab:

Table 106: *SAML Identity Provider Configuration Settings*

Parameter	Description
IdP Portal Name	Enter the name of the identity provider portal. Click **Download** to download and view an XML file containing metadata for the Identity Provider Uniform Resource Identifier (URI).
IdP Metadata URI	View the Uniform Resource Identifier (URI) for the IdP metadata resource.
Service Provider (SP) Metadata	If you upload metadata for an SAML Service Providers, ClearPass can upload the SP metadata for validation during the single-sign on process 1. Click Add SP Metadata. 2. Enter the name of the service provider. 3. Upload the service provider metadata file. For information on obtaining a service provider metadata file, see CPPM Service Provider (SP) Metadata on page 212
CPPM Service Provider (SP) Metadata	• SP Metadata section: Click **Download** to download and view an XML file containing metadata for the Service Provider Uniform Resource Identifier (URI). • The Metadata URI : View the location of this metadata file.

Managing Local Users

Policy Manager lists all local users in the **Configuration > Identity > Local Users** page. You can also add, import, export, and set password policies for the local users using the links provided at the top-right corner of the **Local Users** page.

The following figure displays the **Local Users** page:

Figure 157: *Local Users Listing*

Adding a Local User

To add a local user in the **Local Users** table:

1. Click **Add** link at the top-right corner the page. The **Add Local User** window is displayed.
2. In the **User ID** and **Name** fields, specify a user ID and name for the local user.
3. In the **Password** and **Verify Password** fields, specify a password for the local user.
4. Select the **Enable User** check box to enable the user account. Otherwise, the user account is disabled.
5. Select a static role to be assigned to the user from the **Role** drop-down list.
6. Under the **Attributes** tab, click the **Click to add...** row to add attributes for the local users. A new row is created with a drop-down list in the **Attribute** column. This field is optional. By default, the drop-down list contains the following attributes:
   - Phone
   - Email
   - Sponsor
   - Title
   - Department
   - Designation

   a. Select an attribute from the drop-down list or enter any string to add a custom attribute in the **Attribute** column.

If you add a new custom attribute, it is available for selection in the **Attribute** drop-down list for all local users.

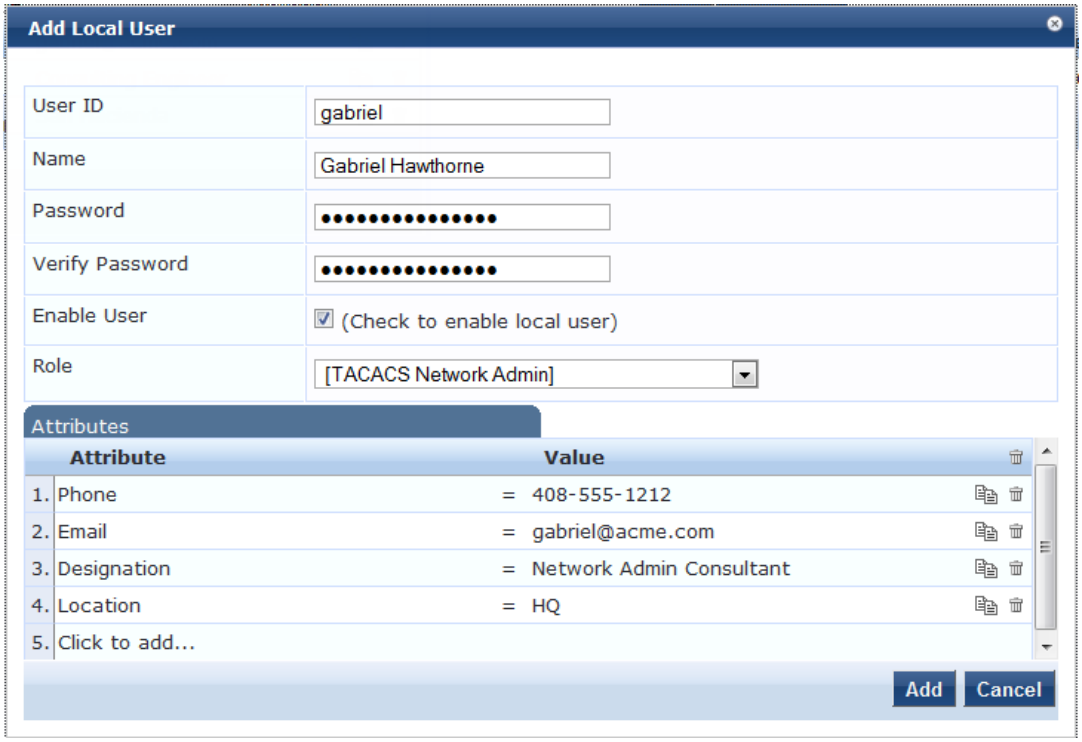
   b. In the **Value** column, enter a value for the attribute specified in the corresponding row.

All attributes entered for a local user are available in the role mapping rules editor under the **LocalUser** namespace.

7. Click **Add**.

The following figure displays the **Add Local User** page:

Figure 158: *Add Local User*

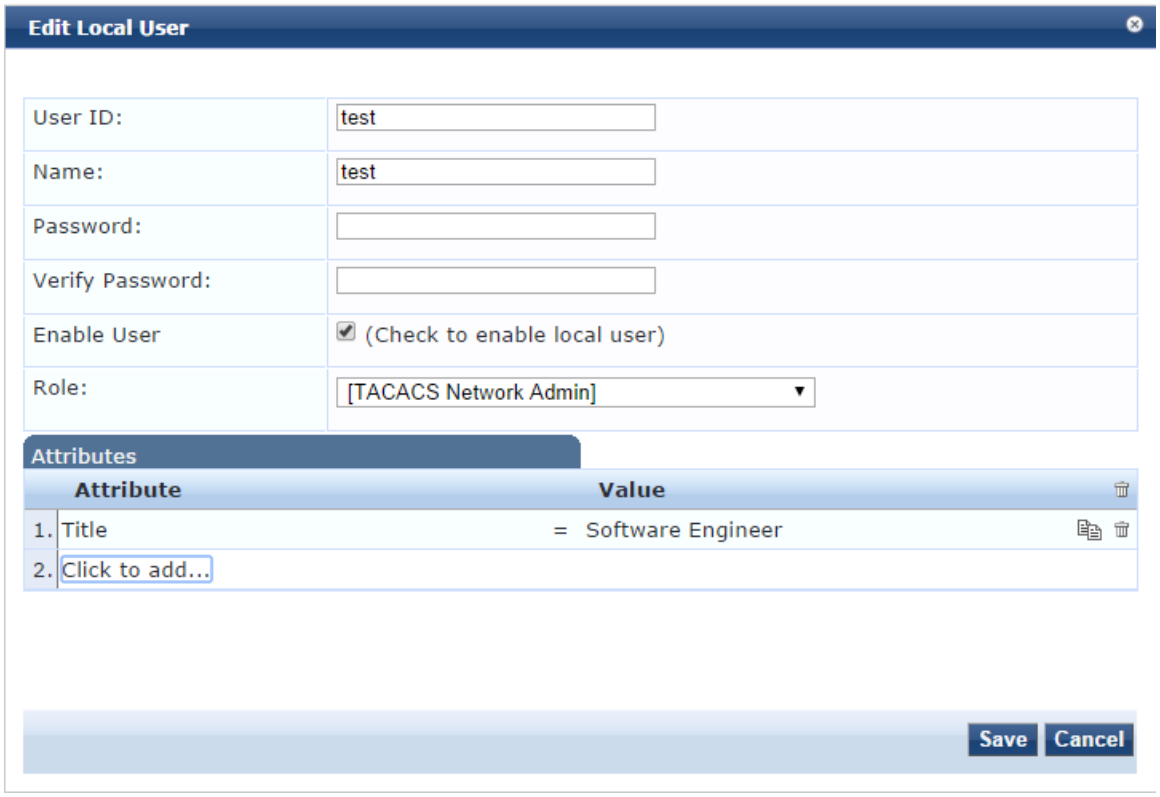


Modifying a Local User Account

To modify a local user account in the **Local Users** table:

1. Click the **User ID** row that you want to edit. The **Edit Local User** window is displayed.
2. Modify any values in the **Edit Local User** window. For more information on editing the fields, see Adding a Local User on page 213.
3. Click **Save**.

Figure 159: *Modify Local User*



Importing and Exporting Local Users

You can import or export the admin user accounts by using the **Import** and **Export All** links at the top-right corner of the **Local Users** page. You can also export specific user accounts by using the **Export** button that appears after selecting one or more user accounts from the list. For more information on importing and exporting local users, see Importing on page 35 and Exporting on page 36.

NOTE

The passwords of the local user accounts are not stored in cleartext when exported to an XML file.

Setting Password Policy for Local Users

To set password policies for the local users:

1. Click the **Password Policy** link from the upper right portion of the page. The **Password Policy** window is displayed.
2. Specify the minimum length required for the password in the **Minimum Length** field.
3. Select the complexity setting from the **Complexity** drop-down list. The complexity settings can be one of the following:
   - No password complexity requirement
   - At least one uppercase and one lowercase letter
   - At least one digit
   - At lease one letter and one digit
   - At least one of each: uppercase letter, lowercase letter, digit
   - At least one symbol
   - At least one of each: uppercase letter, lowercase letter, digit, and symbol

4. Specify the characters not to be allowed in the password in the **Disallowed Characters** field.
5. Specify the words not to be allowed in the password in the **Disallowed Words (CSV)** field.
6. Select any additional checks, if required. The options are:
   - May not contain User ID or its characters in reversed order
   - May not contain repeated character four or more times consecutively
7. Set the password expiry time for the local users. The allowed range is 0–500 days. The default value is 0.

NOTE

If the value is set to 0, the password never expires. For any other value, the local users are forced to reset the expired password when they log in to the UI. The Policy Manager UI alerts the users five days before the password expires.

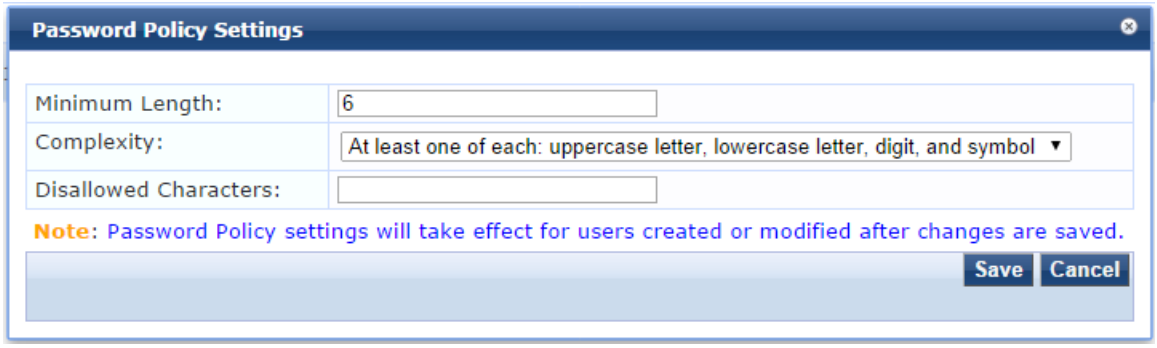
8. Click **Save**.

NOTE

Password Policy settings are effective only for the users created or modified after the changes are saved.

The following figure displays the **Password Policy Settings** window:

Figure 160: *Set (Local User) Password Policy*



Adding and Modifying Endpoints

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

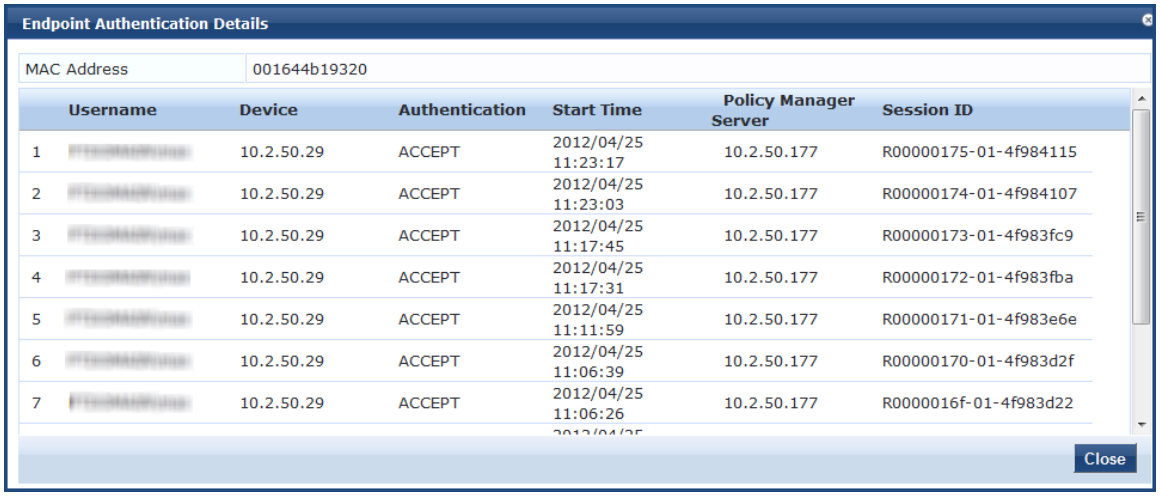
Figure 161: *Endpoints Listing*

Table 107: *Endpoint Page Parameters*

Parameter	Description
MAC Address	Displays the MAC address of the endpoint.
Hostname	Specifies the hostname of the policy server.
Device Category	Specifies the built-in category of the profiled device belongs to. For example, Smartdevices, Access Points, Computer, VOIP phone, and so on.
Device OS Family	Specifies the operating system that the device is configured with. For example, when the category is Computer, ClearPass Policy Manager shows a **Device OS Family** of Windows, Linux, or Mac OS X.
Status	Displays the status of the endpoint.
Profiled	Displays whether the device is profiled or not.

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

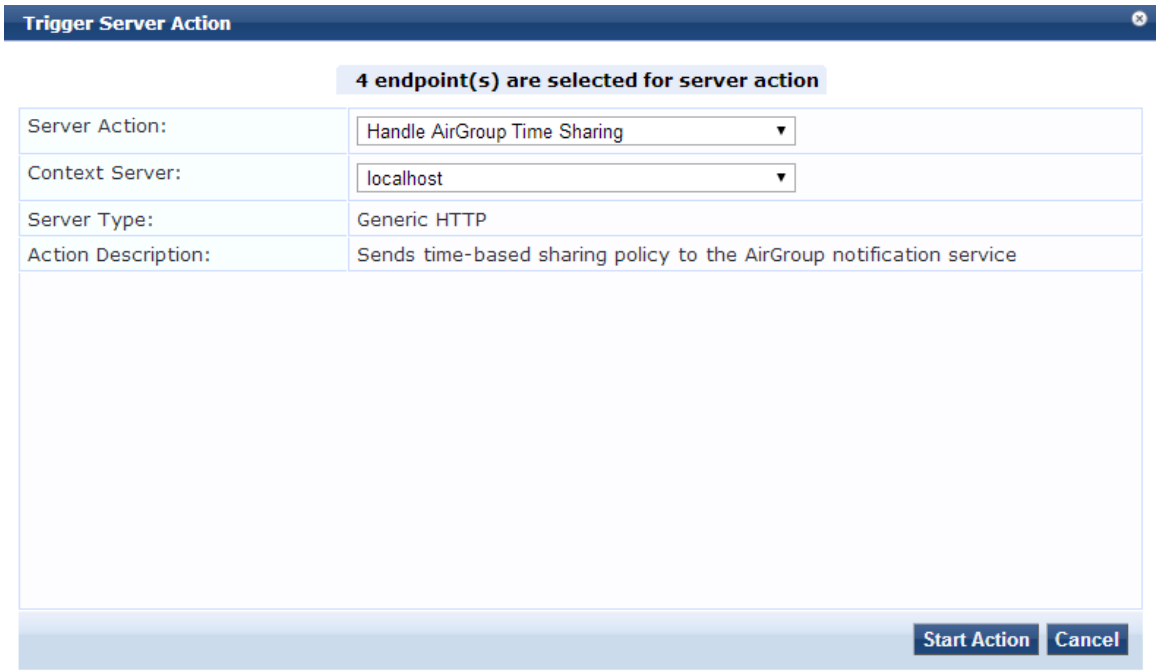
Figure 162: *Endpoint Authentication Details*



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

The following figure displays the **Trigger Server Action** page:

Figure 163: *Endpoints - Trigger Server Action Page*



The following figure displays the **Trigger Server Action** page parameters:

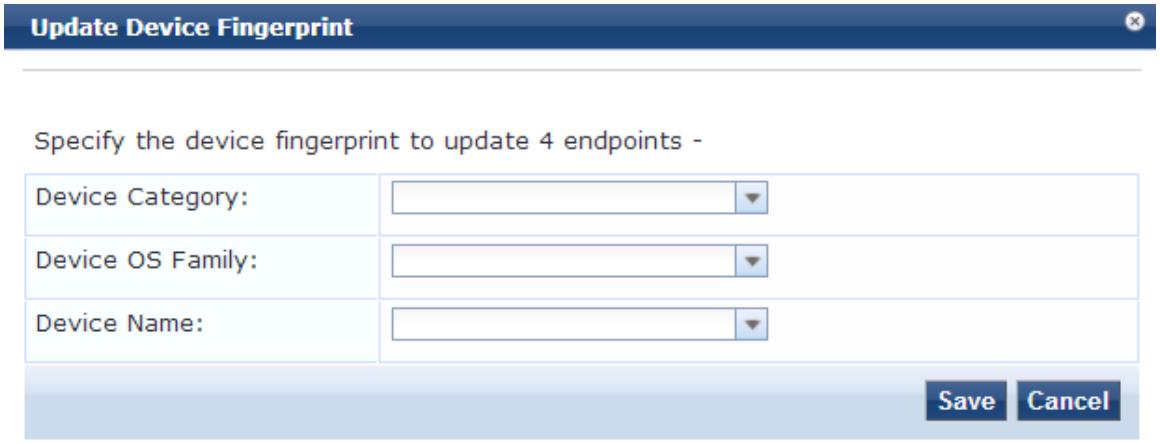
Table 108: *Trigger Server Action Page Parameters*

Parameter	Description
Server Action	Select the server action from the drop-down list. The list includes the following options: • Check Point Login • Check Point Logout • Fortinet Login • Fortinet Logout • Handle AirGroup Time Sharing • Nmap Scan • SNMP Scan
Context Server	Enter a valid server name. You can enter an IP address or domain name.
Server Type	Specifies the server type configured when the server action was configured.
Action Description	Specifies the description of the action. For example, the description can be "Delete all information stored" if the configured action is **Remote Wipe**.

Select an endpoint by clicking the check box and click the **Update Fingerprint** button from the **Endpoints** page to update device fingerprints from a hosted portal.

The following figure displays the **Update Device Fingerprint** page:

Figure 164: *Update Device Fingerprint*



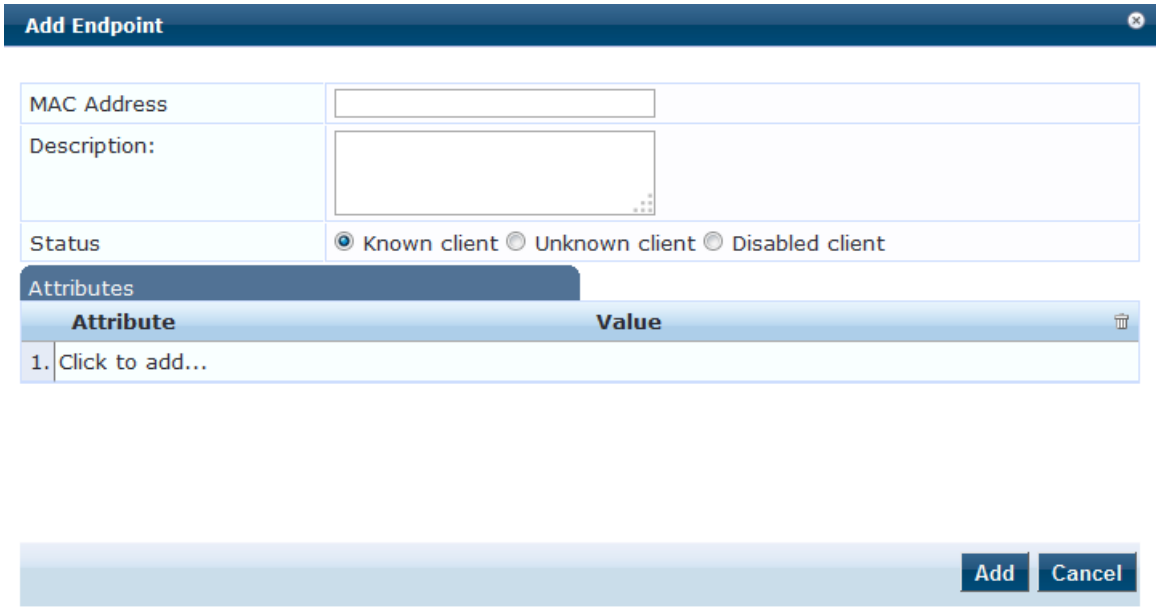
The following table describes the **Update Device Fingerprint** page:

Table 109: *Update Device Fingerprint parameters*

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

Click **Add** to view the **Add Endpoint** page to manually add an endpoint. The following figure displays the **Add Endpoint** page.

Figure 165: *Add Endpoint Page*



The following table describes the **Add Endpoint** page parameters:

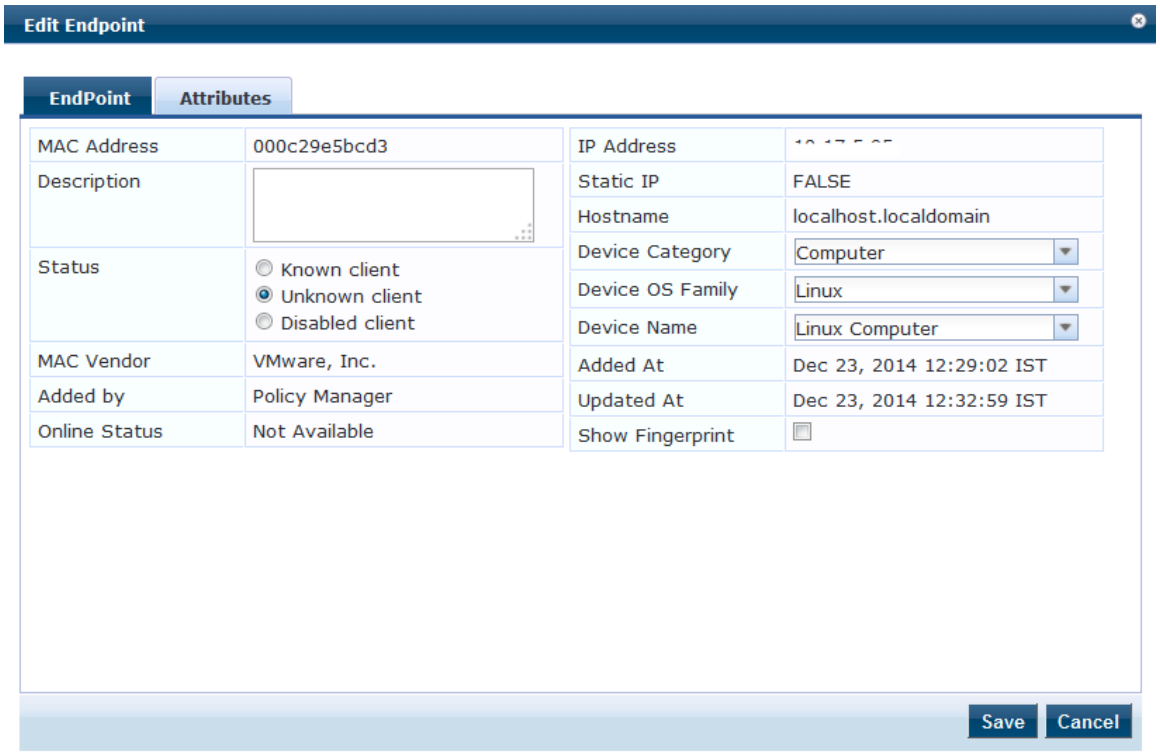
Table 110: *Add Endpoint Page Parameters*

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

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

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

Figure 166: *Edit Endpoint Page*



The following table describes the **Edit Endpoint** page parameters:

Table 111: *Edit Endpoint Page Parameters*

Parameter	Description
MAC Address	Displays the MAC address of the endpoint.
Description	Specifies the description that provides additional information about the endpoint.
Status	Mark the status as **Known client**, **Unknown client**, or **Disabled client**. The **Known** and **Unknown** status can be used in role mapping rules using the Authentication:MacAuth attribute. You can use the **Disabled client** status to block access to a specific endpoint. This status is automatically set when an endpoint is blocked from the **Endpoint Activity** table (in the **Live Monitoring** section).
MAC Vendor	Displays the MAC OUI (Organizationally Unique Identifier) information for all endpoints even when no other profiling information is available for an endpoint.
Added by	Displays the name of the ClearPass server that added the endpoint.
Online Status	Displays the online status of the endpoint.
IP Address	Displays the IP address that is associated with the endpoint.
Static IP	Specifies the static IP of the endpoint. You can select TRUE or FALSE. The default options is FALSE.

Table 111: *Edit Endpoint Page Parameters (Continued)*

Parameter	Description
Hostname	Enter the hostname or the IP address of the endpoint.
Device Category	Specifies the built-in category of the endpoint belongs to. For example, SmartDevices, Access Points, Computer, VOIP phone, and so on.
Device OS Family	Specifies the operating system that the endpoint is configured with. For example, when the category is Computer, ClearPass Policy Manager shows a Device OS Family of Windows, Linux, or Mac OS X.
Device Name	Enter the name of the device. You can select the name of the device from the built-in list.
Added At	Displays the time at which the endpoint was added.
Updated At	Displays the time at which the endpoint was updated.
Show Fingerprint	Select this option to view the endpoint fingerprint details.
Endpoint Fingerprint Details	
Host User Agent	Displays the host user agent of the endpoint. For example, Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident/6.0).
Host OS Type	Displays the type of the host operating system. For example, Windows 8.
Device Category	Displays the category of the device. For example, Computer.
Device Family	Displays the operating system family of the endpoint. For example, Windows.
Device Name	Displays the name of the device.

Additional Available Tasks

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

Adding and Modifying Static Host Lists

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

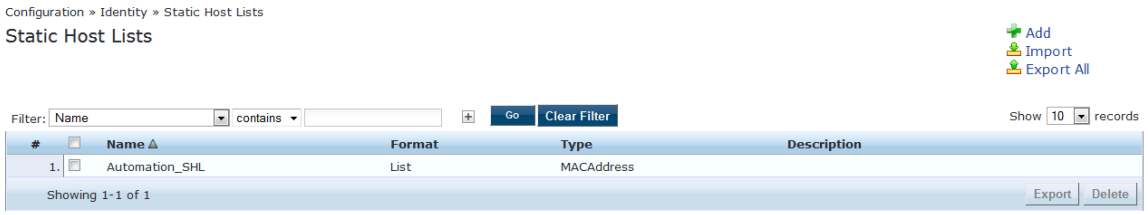
- In service and role-mapping rules as a component.
- For non-responsive services on the network (for example, printers or scanners), as an authentication source.

NOTE

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

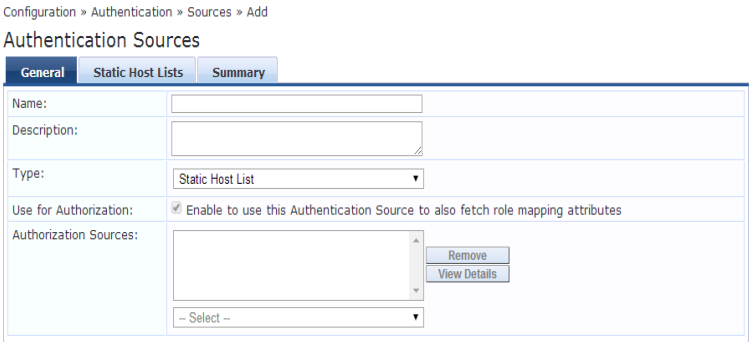
The following figure displays the **Static Host Lists** page:

Figure 167: *Static Host Lists Page*



To add a static host list, go to the **Configuration > Identity > Static Host Lists** page and click the **Add** link. The **Add Static Host List** pop-up opens. For more information, see the and Table 112:

Figure 168: *Add Static Host List Page*



The following table describes the **Static Host Lists** page parameters:

Table 112: *Add Static Host List Page Parameters*

Parameter	Description
Name	Enter the name of the static host list.
Description	Enter the description that provides additional information about the static host list.
Host Format	Select a format for expression of the address: **subnet, IP address**, or **regular expression**.

Table 112: *Add Static Host List Page Parameters (Continued)*

Parameter	Description
Host Type	Select a host type: **IP Address** or **MAC Address** (radio buttons).
List	Use the **Add Host** and **Remove Host** widgets to maintain membership in the current Static Host List.

Additional Available Tasks

- To edit a static host list from the **Static Host Lists** listing page, click on the name to display the **Edit Static Host List** pop-up.
- To delete a static host List from the **Static Host Lists** listing page, select a static host list using check box and click the **Delete** button.
- To export a static host list, in the **Static Host Lists** listing page, select a static host list using check box and click the **Export** button.
- To export all static host lists, in the **Static Host Lists** listing page, click the **Export All** link.
- To import static host lists, in the **Static Host Lists** listing page, click the **Import** link

Configuring a Role and Role Mapping Policy

After authenticating a request, a Policy Manager service invokes its role mapping policy, resulting in assignment of a role(s) to the client. This role becomes the identity component of enforcement policy decisions.

A service can be configured without a role mapping policy, but only one role mapping policy can be configured for each service.

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

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

Additional roles are available with AirGroup and Onboard licenses.

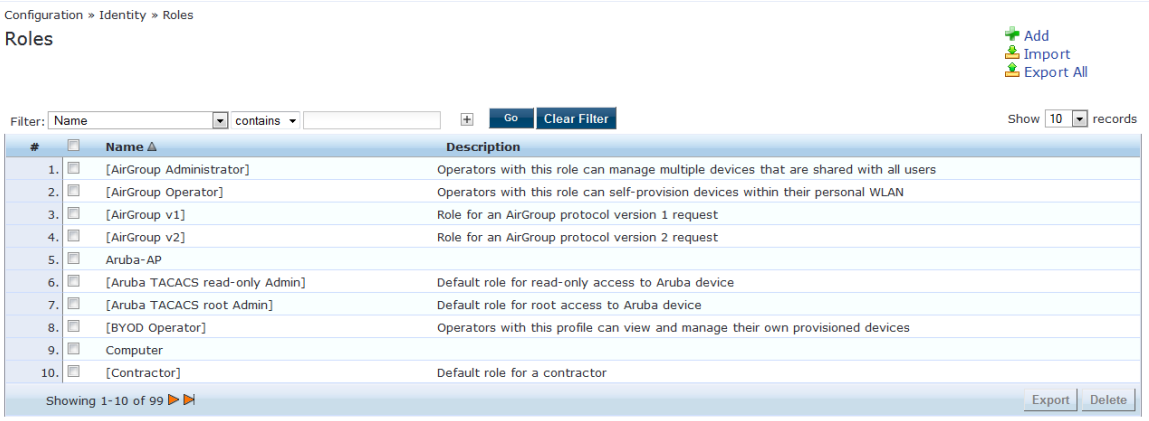
For additional tasks, see the following:

- Adding and Modifying Role Mapping Policies on page 225
- Adding and Modifying Roles on page 225

Adding and Modifying Roles

Policy Manager lists all available roles in the **Configuration > Identity > Roles** page. The following figure displays the **Roles** page:

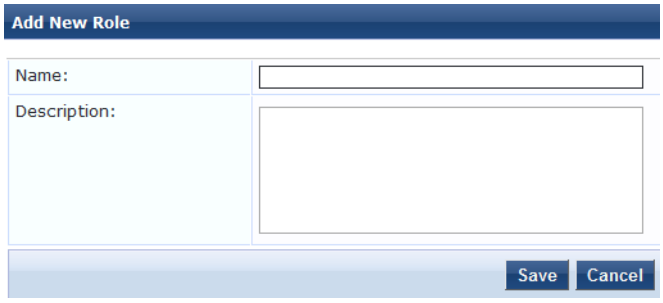
Figure 169: *Roles Page*



You can configure a role from within a role mapping policy (**Add New Role**), or independently from the **Configuration > Identity > Roles > Add** page. 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** pop-up. The following figure displays the **Add New Role** page:

Figure 170: *Add New Role Page*



The following table describes the **Add New Role** parameters:

Table 113: *Add New Role Page Parameters*

Parameter	Description
Name	Enter the name of the role.
Description	Enter the description that provides additional information about the new role.

Adding and Modifying Role Mapping Policies

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

The following figure displays the **Role Mappings** page:

Figure 171: *Role Mappings Page*

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

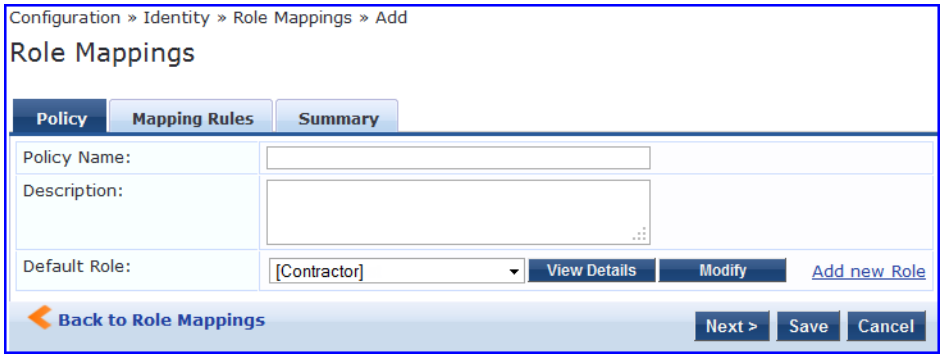
- Policy Tab on page 226
- Mapping Rules Tab on page 227

Policy Tab

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

The following figure displays the **Role Mappings - Policy** tab:

Figure 172: *Role Mappings - Policy Tab*



The following figure displays the **Role Mappings - Policy** tab parameters:

Table 114: *Role Mappings - Policy Tab Parameters*

Parameter	Description
Policy Name	Enter the name of the role mapping policy.
Description	Enter the description that provides additional information about the role mapping policy.
Default Role	Select the role to which Policy Manager will default when the role mapping policy does not produce

Table 114: *Role Mappings - Policy Tab Parameters (Continued)*

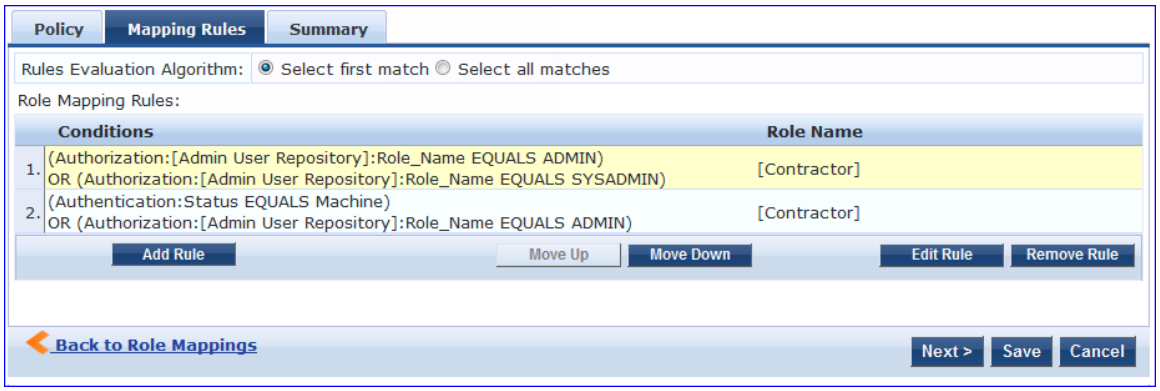
Parameter	Description
	a match.
View Details	Click on **View Details** to view the details of the default role.
Modify	Click on **Modify** to modify the default role.
Add new Role	Click on **Add new Role** to add a new role.

Mapping Rules Tab

The **Mapping Rules** tab selects the evaluation algorithm to add, edit, remove, 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** or **Remove Rule** button.

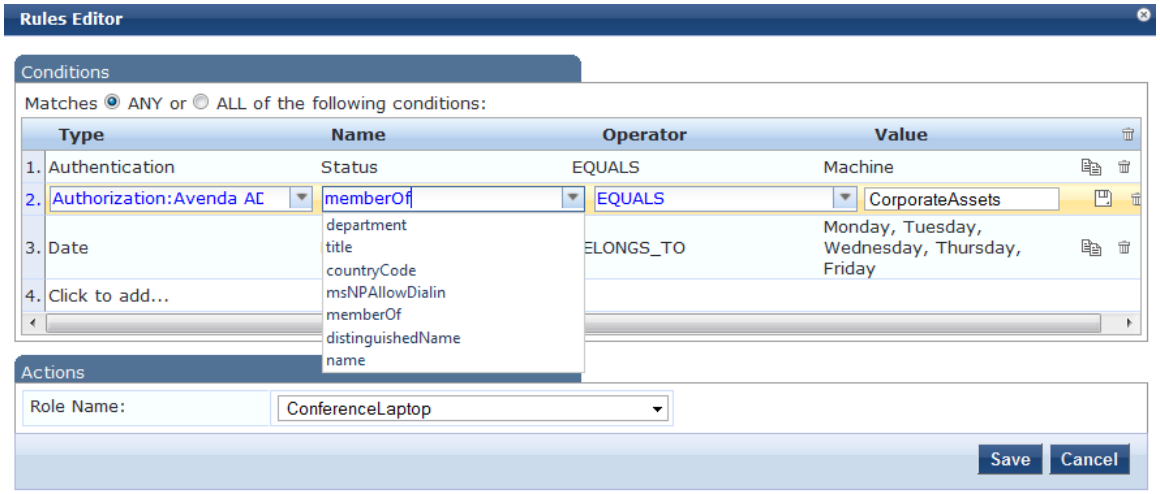
The following figure displays the **Role Mapping - Mapping Rules** tab:

Figure 173: *Role Mapping - Mapping Rules Tab*



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

Figure 174: *Rules Editor Page*



The following table describes the **Role Mappings Page - Rules Editor** page parameters:

Table 115: *Role Mappings Page - Rules Editor Page Parameters*

Parameter	Description
Type	The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on context. (Refer to Namespaces on page 601.) In the role mapping context, Policy Manager allows attributes from following namespaces: • Application • Application:ClearPass • Authentication • Authorization • Authorization:<authorization_source_instance> - Policy Manager shows each instance of the authorization source for which attributes have been configured to be fetched. (See Adding and Modifying Authentication Sources on page 169). Only those attributes that have been configured to be fetched are shown in the attributes drop-down list. • Certificate • Connection • Date • Device • Endpoint • GuestUser • Host • LocalUser • Onboard • TACACS • RADIUS - All enabled RADIUS vendor dictionaries.
Name	Displays the drop-down list of attributes present in the selected namespace.
Operator	Displays the drop-down list of context-appropriate (with respect to the attribute data type) operators. Operators have the obvious meaning; for stated definitions of operator meaning, refer to Operators on page 612.
Value	Depending on attribute data type, this may be a free-form (one or many line) edit box, a drop-down list, or a time/date widget.

The operator values that display for each type and name are based on the data type specified for the authentication source (from the **Configuration > Authentication > Sources** page). If, for example, you modify the UserDN Data type on the authentication sources page to be an integer rather than a string, then the list of operator values here will populate with values that are specific to integers.

After you save your role mapping configuration, it appears in the **Mapping Rules** list. In this interface, you can select a rule, and then use the various widgets to move up, move down, edit the rule, or remove the rule.

Dell Networking W-ClearPass Policy Manager evaluates the health of the clients that request access using posture policies, posture servers, and an audit server. These methods all return Posture Tokens (For example, Healthy and Quarantine) for use by Policy Manager as input for into an enforcement policy. One or more posture methods can be associated with a service.

This chapter describes the following topics:

Posture Methods

Dell Networking W-ClearPass Policy Manager can forward all or part of the posture data received from the client to a posture server. Policy Manager supports redundant posture severs, ensuring posture evaluations in the event of a server failure. NMAP or Nessus audit servers provide posture checking for unmanageable devices, such as devices lacking adequate posture agents or supplicants. For more information on posture servers or audit servers, see Configuring Posture Servers on page 282 and Configuring Audit Servers on page 285.

The **Posture Policies** table on the **Configuration > Posture > Posture Policies** page displays a list of all existing posture policies. The following figure displays the **Posture Policies** page:

Figure 175: *Posture Policies Page*

From the **Posture Policies** page, you can create a new policy or edit an existing policy. To create a new policy. click the **Add** link at the top-right corner of the **Posture Policies** page. To edit an existing policy, click the name of any policy in the **Posture Policies** page.

For more information, refer to the following topics:

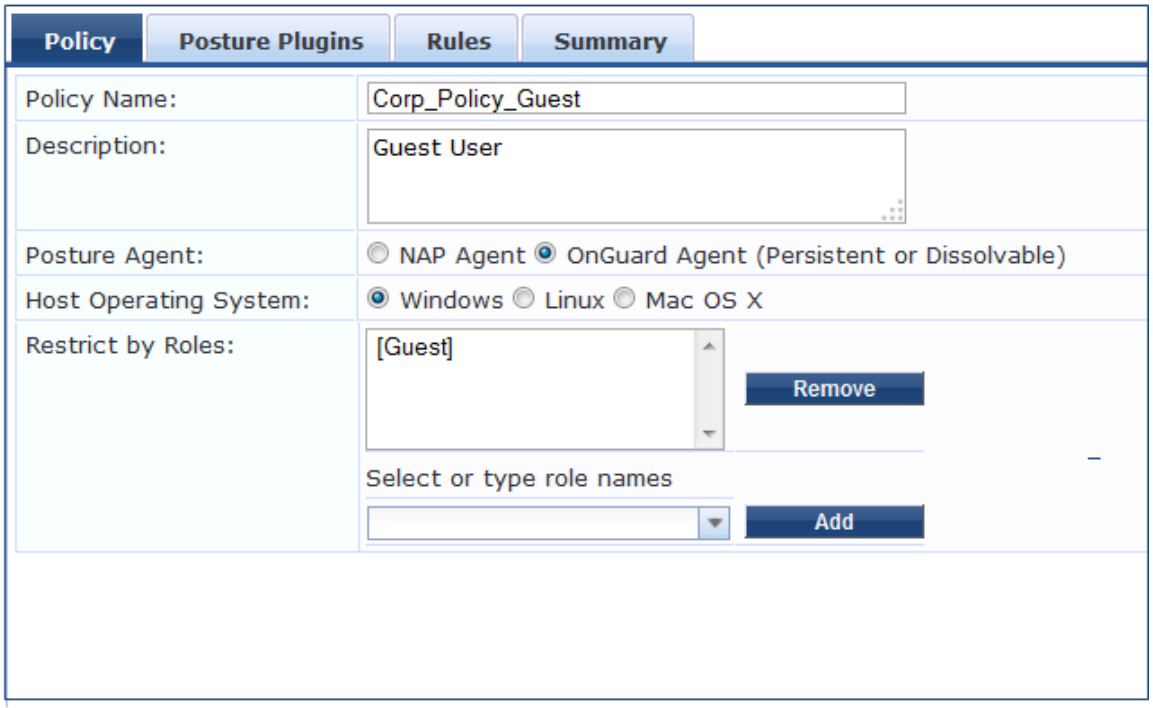
- Configuring Posture Policy Agents and Hosts on page 230
- Configuring Posture Policy Plug-ins on page 235
- Configuring Posture Policy Rules on page 279

Configuring Posture Policy Agents and Hosts

Navigate to the **Policy** tab on the **Configuration > Posture > Posture Policies > Add** page to configure the policy name and description, select a posture agent and host operating system, and specify role restrictions.

The following figure displays the **Policy** tab:

Figure 176: *Policy Tab - Policies Page*



The following table describes the **Policy** tab parameters:

Table 116: *Policy Tab Parameters*

Feature	Description
Policy Name	Enter the name assigned to the policy by the Dell Networking W-ClearPass Policy Manager administrator.
Description	Specify the description that provides additional information about the posture policy.
Posture Agent	Select the posture agent type. For for information on these agents, see NAP Agent on page 230 and OnGuard Agent (Persistent or Dissolvable) on page 232.
Host Operating System	Specify whether the host is using a Window, Linux, or MAC OS X operating system.
Restrict by Roles	Apply the posture policy to the selected roles.

NAP Agent

If you select the **Posture Agent: NAP Agent** in the **Policy** tab, you can configure the following posture plug-ins:

Table 117: *NAP Agent Posture Plug-ins for Windows Operating System*

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

Table 118: *NAP Agent Posture Plug-ins for Linux Operating Systems*

LINUX Operating Systems						
Plug-in Name	**Description**	**CentOS**	**Fedora**	**RedHat Enterprise Linux**	**SUSE Linux Enterprise**	**Ubuntu**
ClearPass Linux Universal System Health Validator	Services, which allows you to enable or disable health checks, set auto remediation checks, select or insert available services, and set which services to run and which to stop.	yes	yes	yes	yes	yes

OnGuard Agent (Persistent or Dissolvable)

Select **OnGuard Agent (Persistent or Dissolvable)** from the **Posture Agent** field (**Configuration** > **Posture** > **Posture Policies** > **Add**) for use in the following scenarios:

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

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

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

Supported Operating System Versions								
Posture Plug-in Name	**Description**	**Windows 2003**	**Windows 8**	**Windows 7**	**Windows Vista**	**Windows XP Service Pack 3**	**Windows Server 2008**	**Windows Server 2008R2**
ClearPassWindows Universal System Health Validator	The configurable parameter categories for this validator are Services, Processes, Registry Keys, AntiVirus, AntiSpyware, Firewall, Peer To Peer, Patch Management, Windows HotFixes, USB Devices, Virtual Machines, Network Connections, Disk Encryption, and Installed Applications.	yes	yes	yes	yes	yes	yes	yes
Windows System Health Validator	The configurable parameter categories for this validator allow you to configure client computers that can connect to your	yes	yes	yes	yes	yes	yes	yes

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

Supported Operating System Versions								
	network, and clients that are restricted from your network. Access is determined by a check of the service pack level. You can determine the service pack level.							
Windows Security Health Validator	The configurable parameter categories for this validator allow you to configure parameters that permit or deny client computers access to your network, subject to checks of the client's system for Firewall, Virus Protection, Spyware Protection, Automatic Updates, and Security Updates*.	no	yes	yes	yes	yes	no	no
* If you configure the posture plug-in for Windows XP, spyware protection is disabled.								

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

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

Table 121: *OnGuard Agent (Persistent or Dissolvable) Posture Plug-ins for Linux*

Name of the Plug-in	Description
ClearPass Linux Universal System Health Validator	The configurable parameter categories for this validator are: • Services • AntiVirus

Configuring Posture Policy Plug-ins

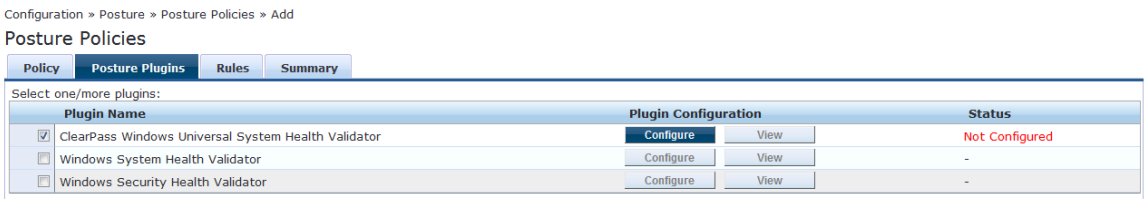
The **Posture Plugins** tab of the **Posture Policies** page allows you to configure plug-ins for the posture policy. The plug-ins available on this tab vary, depending upon whether the policy is using a network access protection (NAP) agent or the OnGuard agent plug-in. To configure posture policy plug-ins, navigate to **Configuration > Posture > Posture Policies > Add**, and click the **Posture Plugins** tab on the **Posture Policies** window.

You can configure the following posture plug-ins in the **Posture Policies** page:

- ClearPass Windows Universal System Health Validator
- Windows System Health Validator
- Windows Security Health validator

Select the check box of the specific plug-in and Click **Configure** button to view the configuration options. The following figure displays the **Posture Policies** page:

Figure 177: *Posture Policies Page*



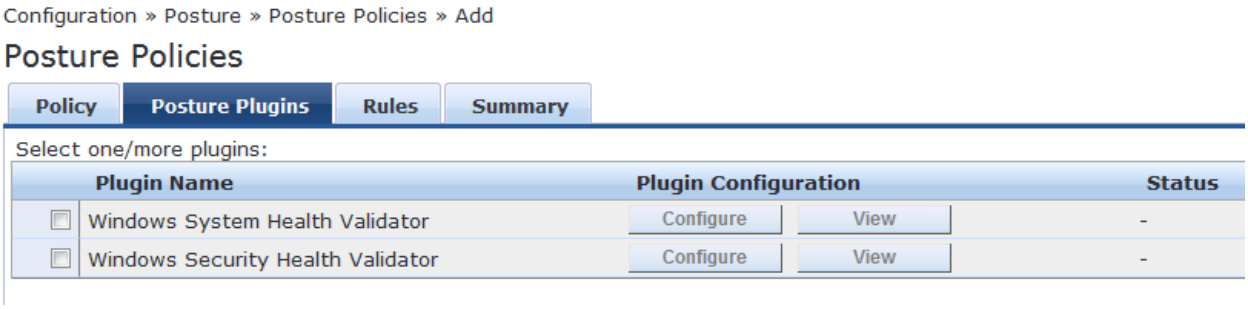
Configuring NAP Agent Plugins

If your posture policy is using a NAP agent, the **Posture Plugins** tab allows you to configure the following plug-in types:

- Windows System Health Validator - NAP Agent on page 236
- Windows Security Health Validator - NAP Agent on page 237

The following figure displays the **NAP Agent - Posture Plugins** tab:

Figure 178: *NAP Agent - Posture Plugins Options*



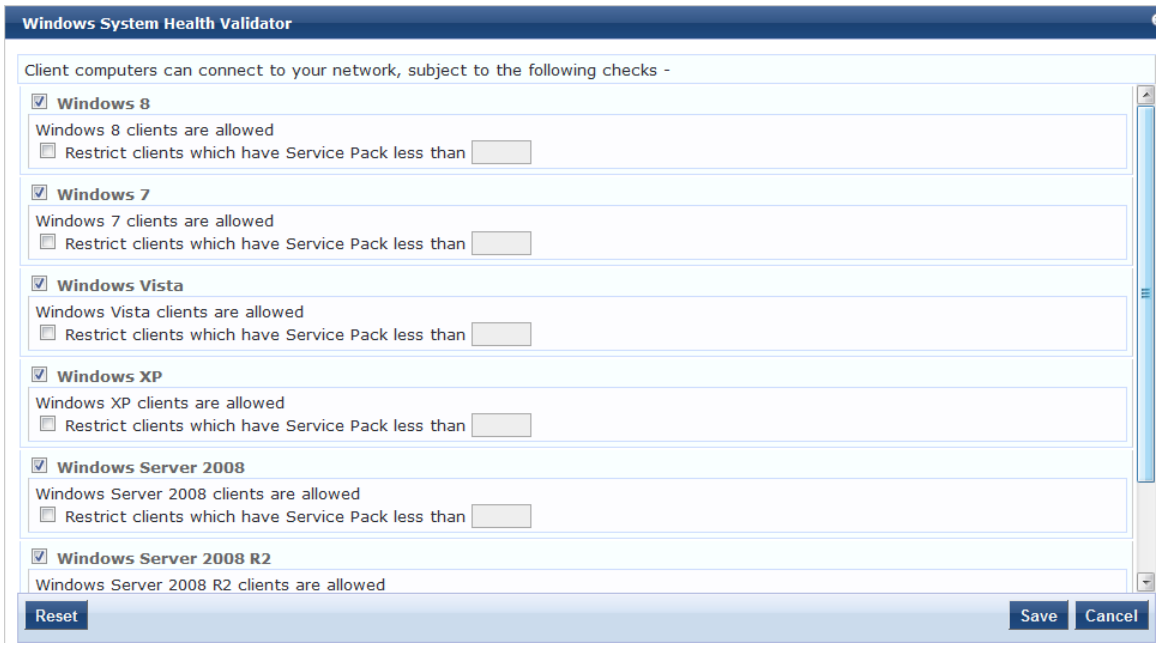
Windows System Health Validator - NAP Agent

The Windows System Health Validator - NAP Agent checks for the level of Windows Service Packs. To configure the minimum service pack level required, perform the following steps:

1. Click a check box to enable support of specific operating systems.
2. Enter the minimum Service Pack level required on the client computer to connect to your network.
3. Click **Save**.

The following figure displays the **Windows System Health Validator** page:

Figure 179: *Windows System Health Validator*

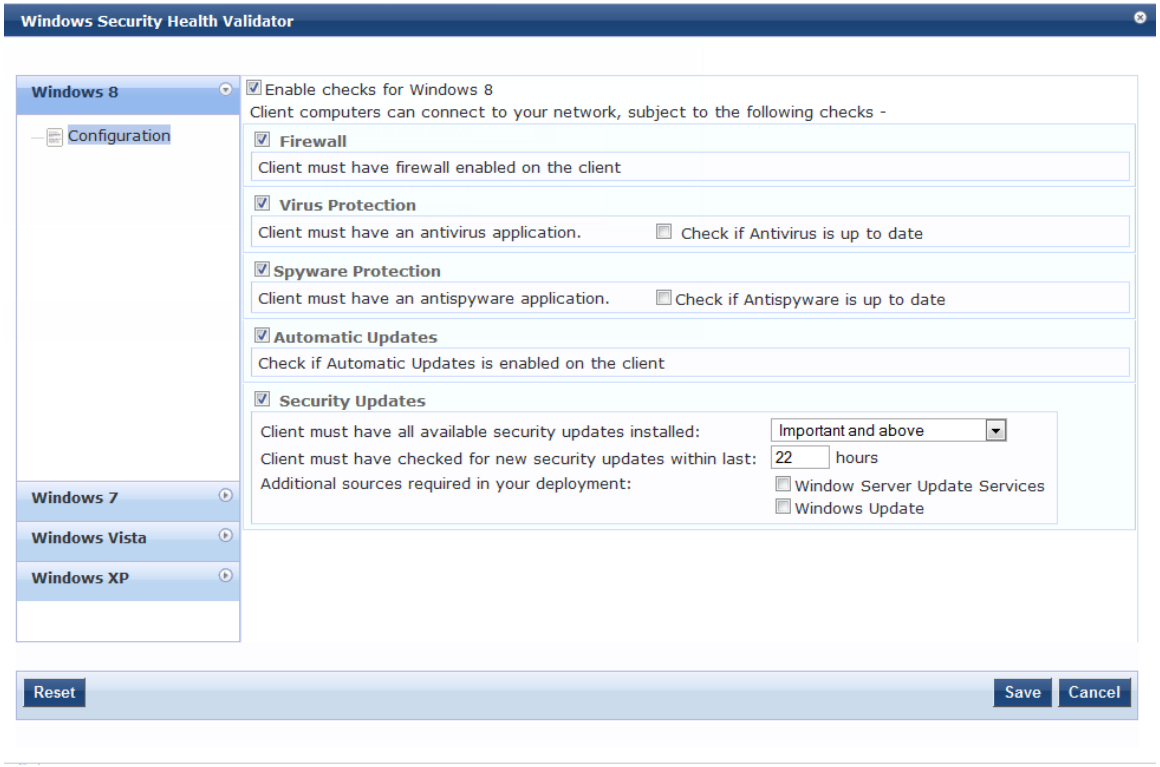


Windows Security Health Validator - NAP Agent

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.

The following figure displays the **Windows Security Health Validator** page:

Figure 180: *Windows Security Health Validator*



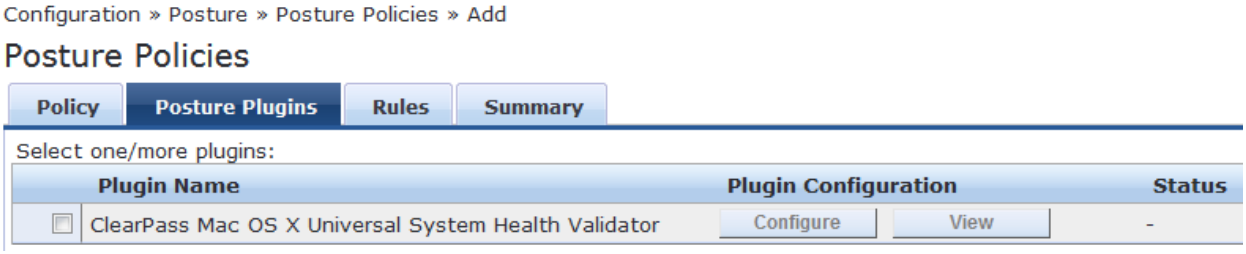
Configuring OnGuard Agent Plugins

If you select the **OnGuard Agent** option in the **Policy** tab of the **Posture Policies** page, the **Posture Plugins** tab allows you to configure different plugin types for hosts running Windows, Linux, and Mac OS X operating systems. Refer to the following topics for details on each plugin type:

- For Windows:
  - ClearPass Windows Universal System Health Validator - OnGuard Agent on page 238
  - Windows System Health Validator - OnGuard Agent on page 262
  - Windows Security Health Validator - OnGuard Agent on page 263
- For Linux: ClearPass Linux Universal System Health Validator Plugin on page 264
- For Mac OS X: ClearPass Mac OS X Universal System Health Validator - OnGuard Agent on page 266

The following figure displays the **Posture Policies - Posture Plugins** tab:

Figure 181: *OnGuard Agent Plugin Options for Mac OS X*

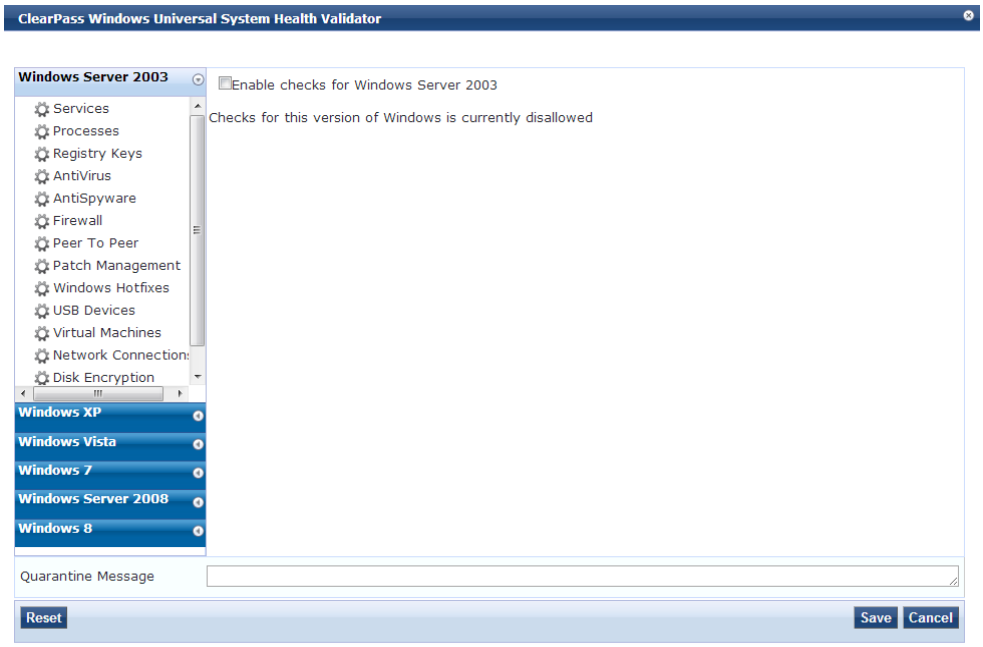


ClearPass Windows Universal System Health Validator - OnGuard Agent

Select **OnGuard Agent** and the **Windows** host operating system in the **Posture Plugins** tab (**Configuration** > **Posture** > **Posture Policies** > **Add**) to view the **ClearPass Windows Universal System Health Validator** page.

The following figure displays the **ClearPass Windows Universal System Health Validator** page:

Figure 182: *ClearPass Windows Universal System Health Validator*



Select a version of Windows and click the **Enable checks for Windows Server** check box to enable checks for the selected version. Enabling checks for a specific version displays the following set of configuration pages:

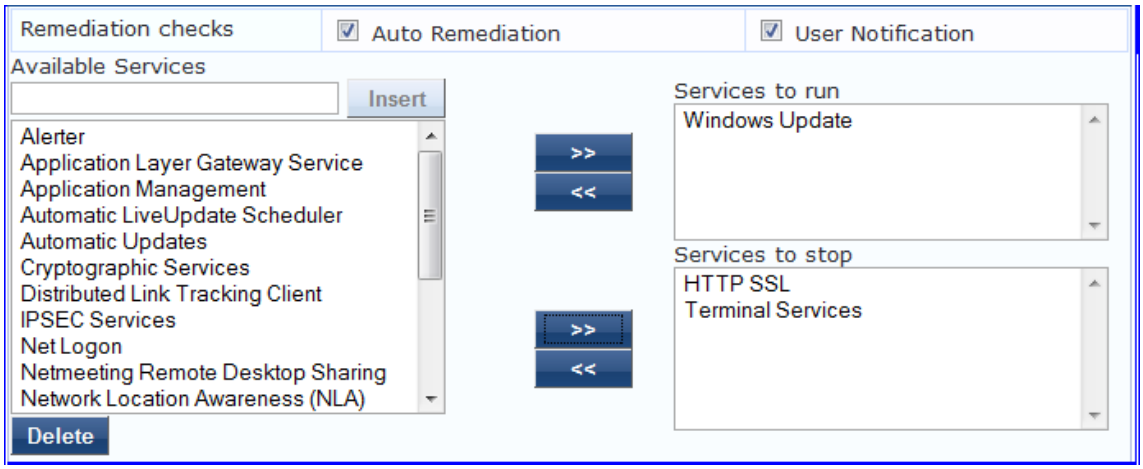
- Services on page 239
- Processes on page 240
- Registry Keys on page 242
- AntiVirus on page 245
- AntiSpyware on page 247
- Firewall on page 248
- Peer To Peer on page 249
- Patch Management on page 250
- Windows Hotfixes on page 254
- USB Devices on page 254

- Virtual Machines on page 255
- Network Connections on page 256
- Disk Encryption on page 258
- Installed Applications on page 258
- File Check on page 259

Services

The **Services** page provides a set of widgets for specifying services to run or stop.

Figure 183: *Services Page*



The following table describes the **Services** parameters:

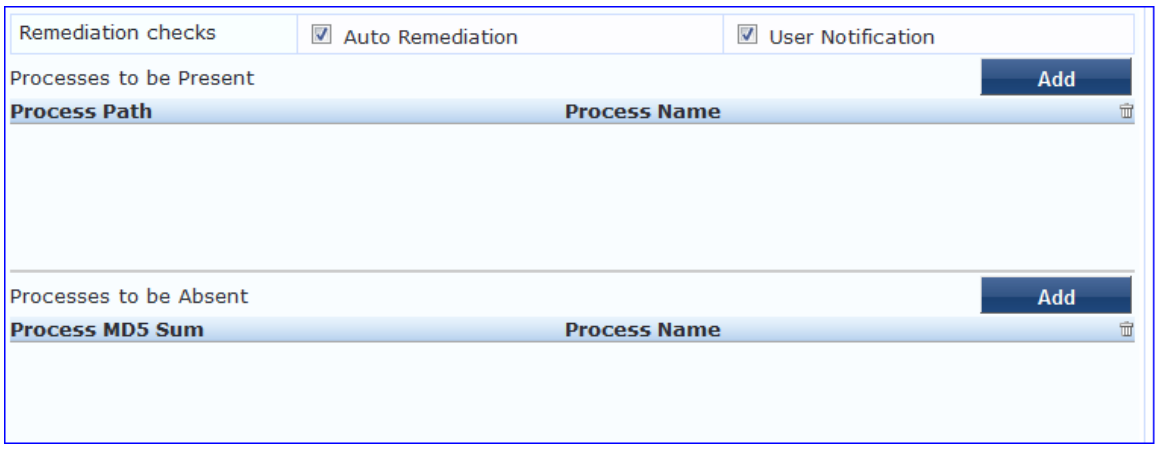
Table 122: *Services Page*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop or start services based on the entries in **Service to run** and **Services to stop** configuration).
User Notification	Enable to allow user notifications for service check policy violations.
Available Services	This scrolling list contains a list of services that you can select and move to the **Services to run** or **Services to stop** panels (using their associated widgets). This list varies depending on OS types. Click the **>>** or **<<** to add or remove, respectively, the services from the **Service to run** or **Services to stop** boxes.
Insert	To add a service to the list of available services, enter its name in the text box adjacent to this button, then click **Insert**.
Delete	To remove a service from the list of available services, select it and click **Delete**.

Processes

The **Processes** page provides a set of parameters to specify which processes to be explicitly present or absent on the system. The following figure displays the **Processes** page:

Figure 184: *Processes Page (Overview)*



The following table describes the **Process** parameters:

Table 123: *Process Page (Overview - Pre-Add)*

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

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

Processes to be Present

Figure 185: *Process to be Present Page (Detail)*

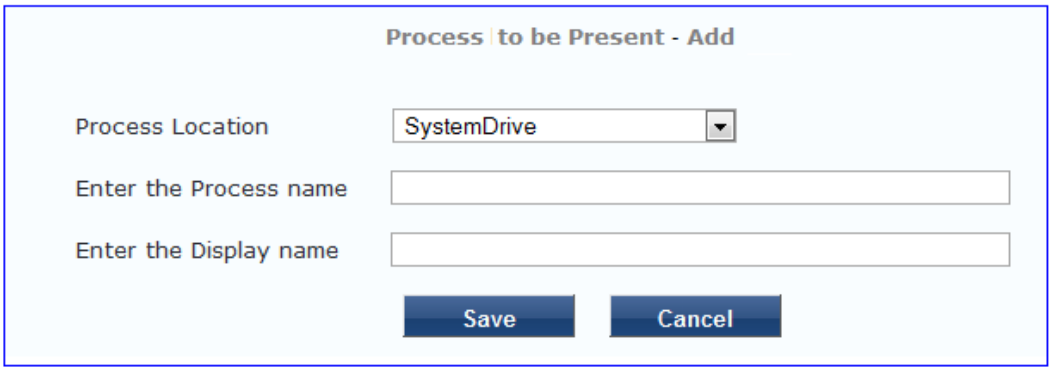


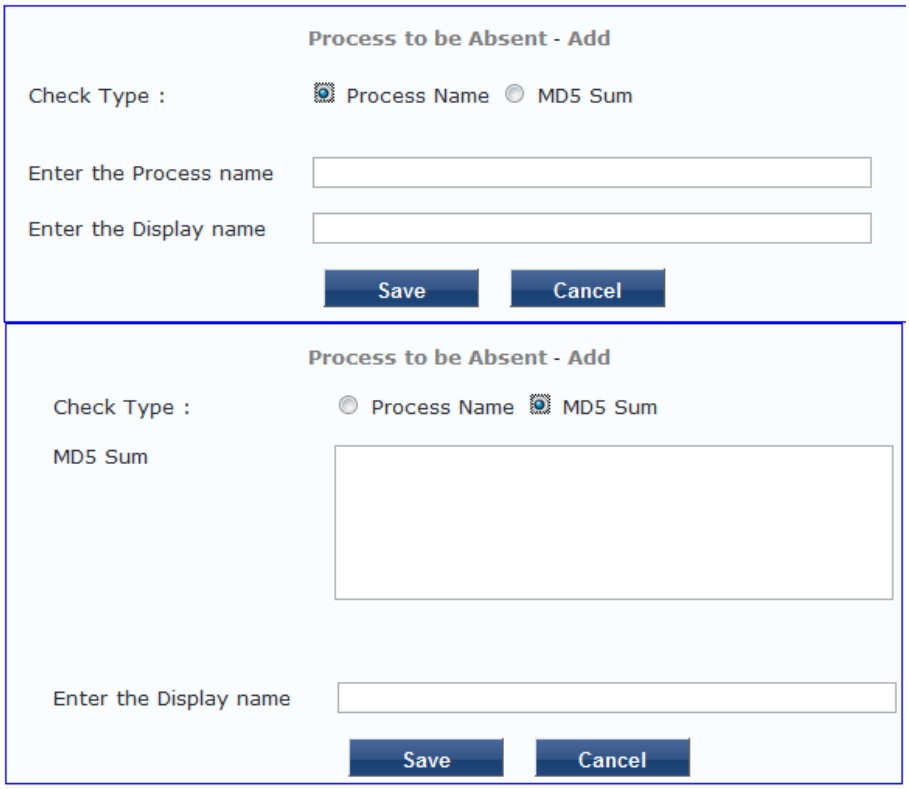
Table 124: *Process to be Present Page (Detail)*

Parameter	Description
Process Location	Choose from Applications: **UserBin**, **UserLocalBin**, **UserSBin**, or **None**.
Enter the Process name	Specifies the path name containing the process executable name.
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

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

Processes to be Absent

Figure 186: *Process to be Absent Page (Detail)*

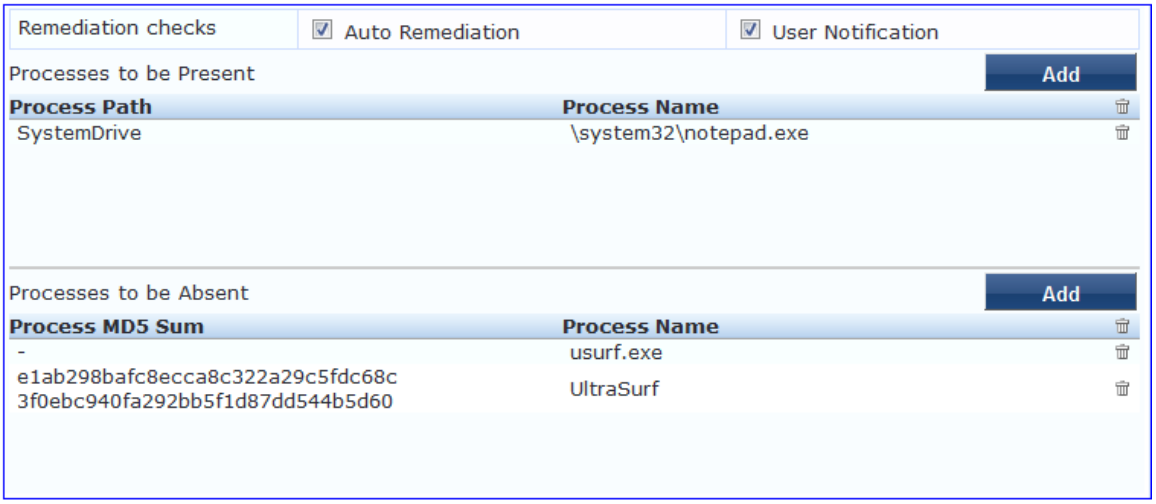


The following table describes the **Process to be Absent** parameters:

Table 125: *Process to be Absent Page (Detail)*

Parameter	Description
Check Type	Select the type of process check to perform. The agent can look for: • **Process Name** - The agent looks for all processes that matches with the given name. For example, if notepad.exe is specified, the agent kills all processes whose name matches, regardless of the location from which these processes were started. • **MD5 Sum** - This specifies one or more (comma separated) MD5 checksums of the process executable file. For example, if there are multiple versions of the process executable, you can specify the MD5 sums of all versions here. The agent enumerates all running processes on the system, computes the MD5 sum of the process executable file, and matches this with the specified list. One or more of the matching processes are then terminated.
Enter the Display name	Enter a user friendly name for the process. This is displayed in end-user facing messages.

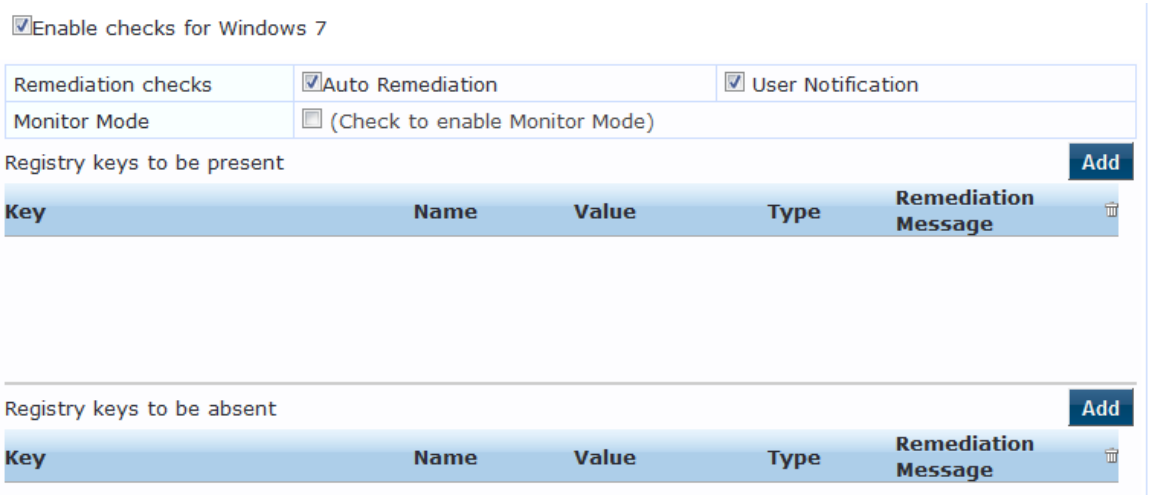
Figure 187: *Process Page (Overview - Post Add)*



Registry Keys

The **Registry Keys** page allows you to specify which registry keys are to be explicitly present or absent.

Figure 188: *Registry Keys Page (Overview)*



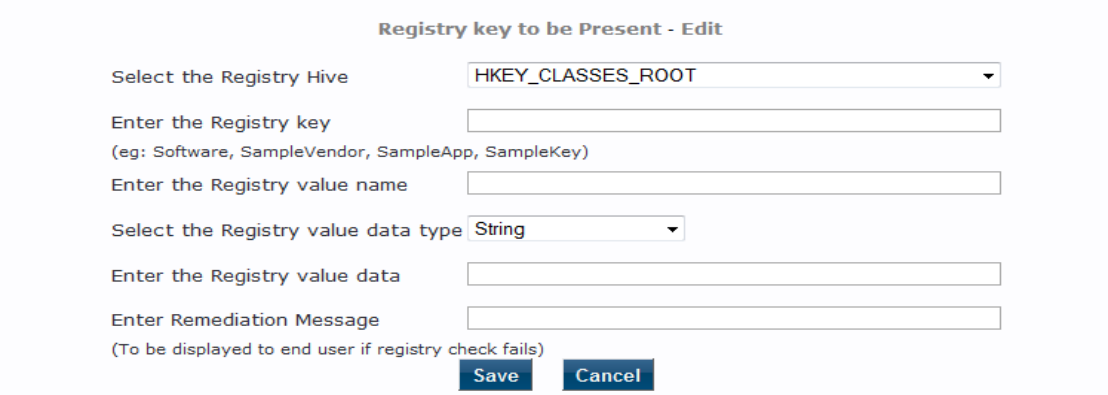
The following table describes the **Registry Keys** page parameters:

Table 126: *Registry Keys Page (Overview - Pre-Add)*

Parameter	Description
Auto Remediation	Enable auto remediation for registry checks. Use this page to automatically add or remove registry keys based on the entries in **Registry keys to be present** and **Registry keys to be absent** fields.
User Notification	Enable user notifications for registry check policy violations.
Monitor Mode	Enable this to set the health status of the **Registry Keys** health class healthy. This allows administrators to collect information related to missing registry keys without marking the clients as unhealthy even if some registry keys are missing.
Registry keys to be present	Click **Add** to specify a registry key to be added to the **Registry keys to be present** list. If the specified registry key is not present, the remediation message that is added in the **Registry Keys Page (Detail)** window is displayed on **OnGuard Agent**.
Registry keys to be absent	Click **Add** to add a registry key to the **Registry keys to be absent** list. If the specified registry key is not absent, the remediation message that is added in the **Registry Keys Page (Detail)** window is displayed on **OnGuard Agent**.

Click **Add** to display the **Registry** page detail.

Figure 189: *Registry Keys Page (Detail)*



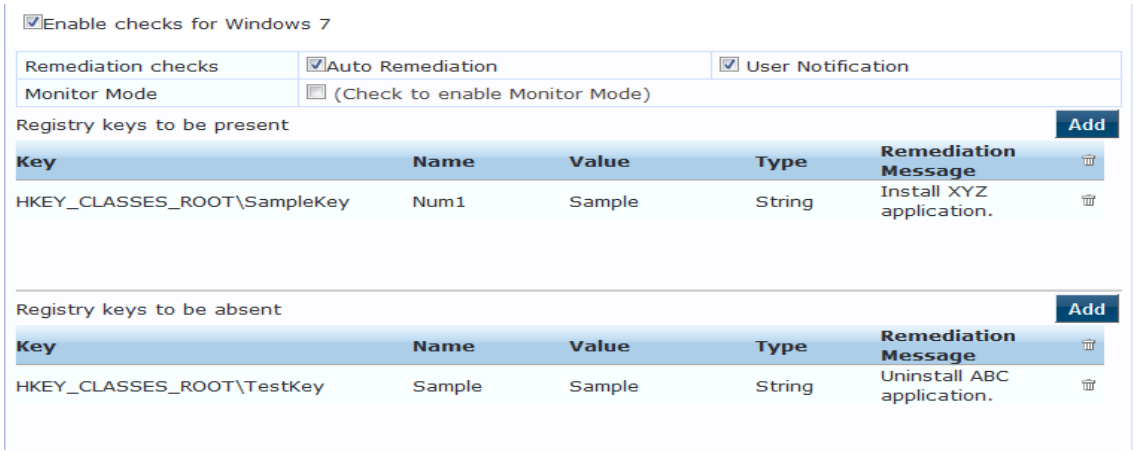
The following table describes the **Registry Keys - Detail** parameters:

Table 127: *Registry Keys Page (Detail)*

Parameter	Description
Select the Registry Hive	Specify the registry hive from the following options: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS • HKEY_CURRENT_CONFIG
Enter the Registry key	Specify the registry key using the examples given in the GUI.
Enter the Registry value name	Specify the name of the registry value.
Select the Registry value data type	Specify the registry value data types. The data type can be any of the following: • Multi String • String • DWORD • QWORD • Expandable String
Enter the Registry value data	Specify the registry value.
Enter Remediation Message	Specify the custom remediation message to be displayed to end users if registry check is failed.

After you save the registry details, the remediation message appears in the **Registry** page list.

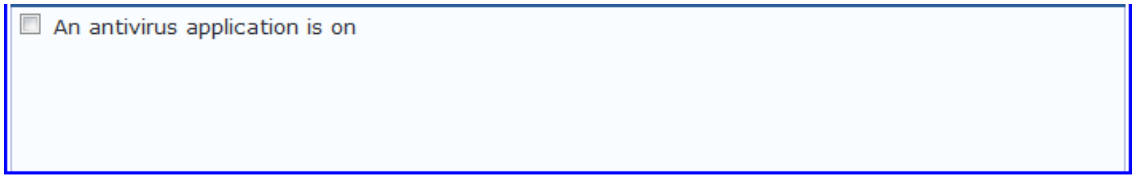
Figure 190: *Registry Keys Page (Overview - Post Add)*



AntiVirus

In the **Antivirus** page, you can turn on an Antivirus application. Click **An anti-virus application is on** to configure the Antivirus application information.

Figure 191: *Antivirus Page (Overview - Before)*

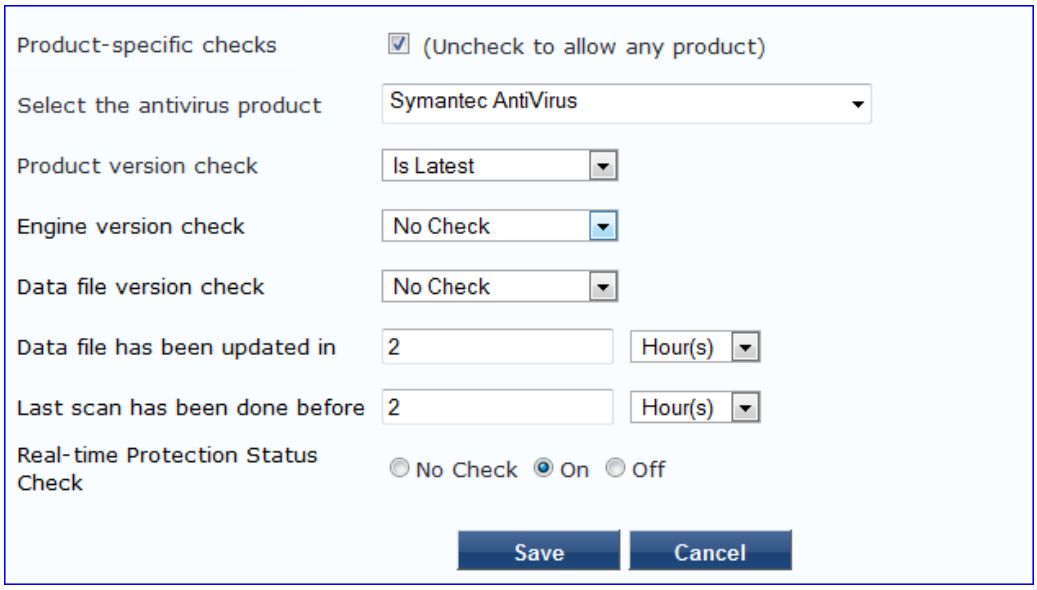


When enabled, the **Antivirus** detail page appears.

Figure 192: *Antivirus Page (Detail 1)*

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

Figure 193: *Antivirus Page (Detail 2)*



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

Figure 194: *Antivirus Page (Overview - After)*

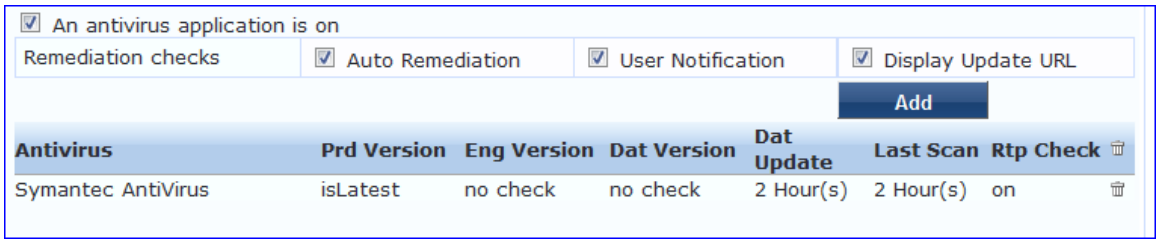


Table 128: *Antivirus Page*

Interface	Parameter	Description
Antivirus Page	• An Antivirus Application is On • Auto Remediation • User Notification • Display Update URL	• Click **Antivirus application is on** to enable testing of health data for configured Antivirus application(s). • Check the **Auto Remediation** check box to enable auto remediation of anti-virus status. • Check the **User Notification** check box to enable user notification of policy violation of anti-virus status. • Check the **Display Update URL** check box to show the origination URL of the update.
Antivirus Page (Detail 1)	• Add	• To configure Antivirus application attributes for testing against health data, click **Add**.
Antivirus Page (Detail 2)	• Product-specific checks • Select the antivirus product • Product version check • Engine version check	Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on

Table 128: *Antivirus Page (Continued)*

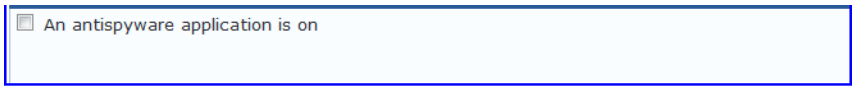
Interface	Parameter	Description

	• Engine version check
	• Datafile version check
	• Data file has been updated in
	• Last scan has been done before
	• Real-time Protection Status Check
		the UI.
		• Select the antivirus product - Select a vendor from the list.
		• Product version check - No Check, Is Latest (requires registration with ClearPass portal), At Least, In Last N Updates (requires registration with ClearPass Portal).
		• Engine version check - Same choices as product version check.
		• Data file version check - Same choices as product version check.
		• Data file has been updated in - Specify the interval in hours, days, weeks, or months.
		• Last scan has been done before - Specify the interval in hours, days, weeks, or months.
		• Real-time Protection Status Check
		  ▪ No Check - Dell Networking W-ClearPass Policy Manager does not use RTP Status value for health evaluation. This means that the client is treated as **healthy** irrespective of the value of RTP.
		  ▪ On - Client is marked as **healthy** only if the value of RTP status is On.
		  ▪ Off - Client is marked as **healthy** only if the value of RTP status is Off.

AntiSpyware

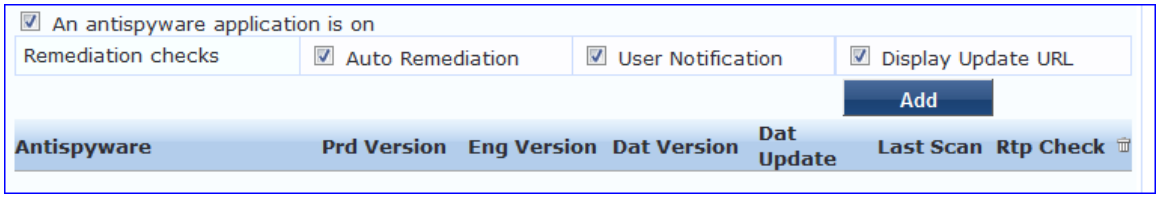
In the **AntiSpyware** page, an administrator can specify that an AntiSpyware application must be on and allows drill-down to specify information about the AntiSpyware application. Click **An Antipyware Application is On** to configure the AntiSpyware application information.

Figure 195: *AntiSpyware Page (Overview Before)*



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

Figure 196: *AntiSpyware Page (Detail 1)*



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

Figure 197: *AntiSpyware Page (Detail 2)*

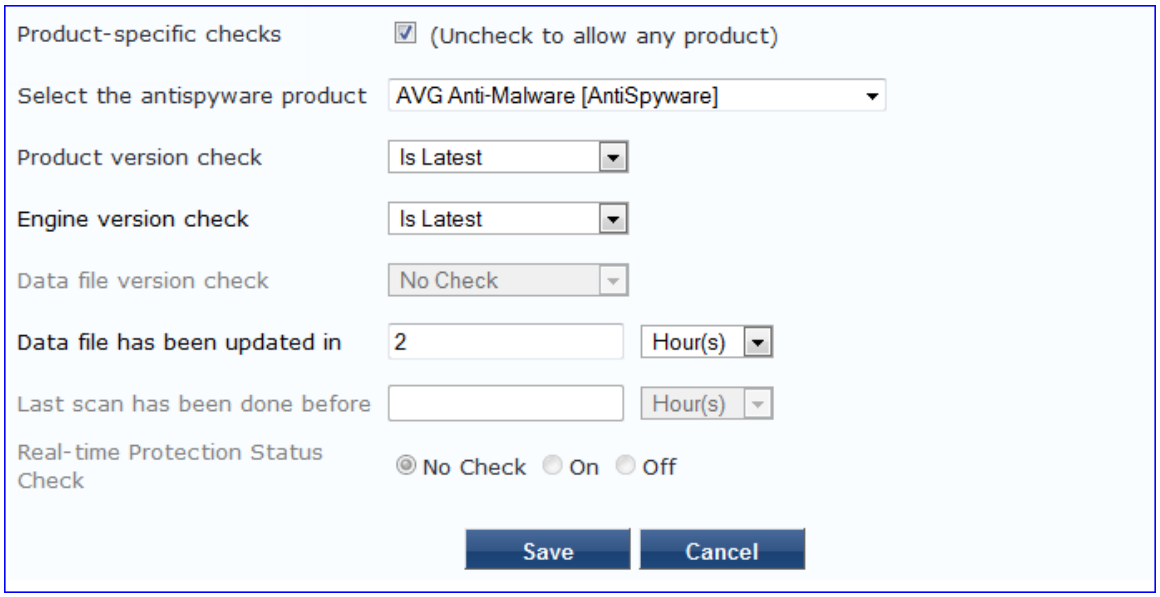


Figure 198: *AntiSpyware Page (Overview After)*

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

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

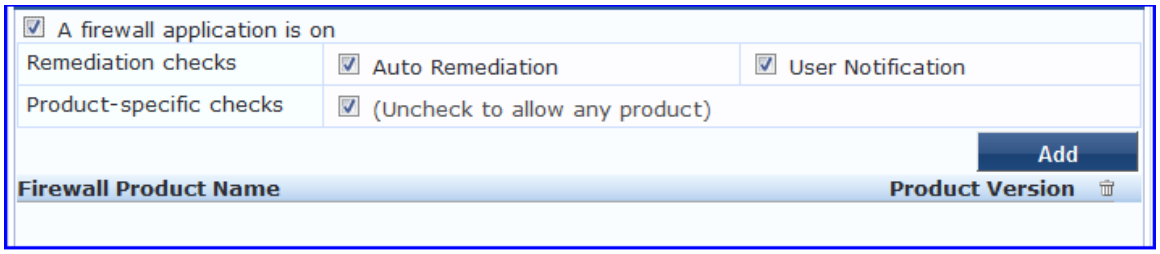
Firewall

In the **Firewall** page, you can specify that a Firewall application must be on and specify information about the Firewall application.

Figure 199: *Firewall Page (Overview Before)*

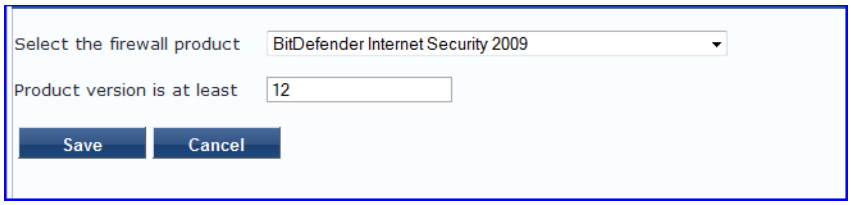
In the **Firewall** page, click **A Firewall Application is On** to configure the Firewall application information.

Figure 200: *Firewall Page (Detail 1)*



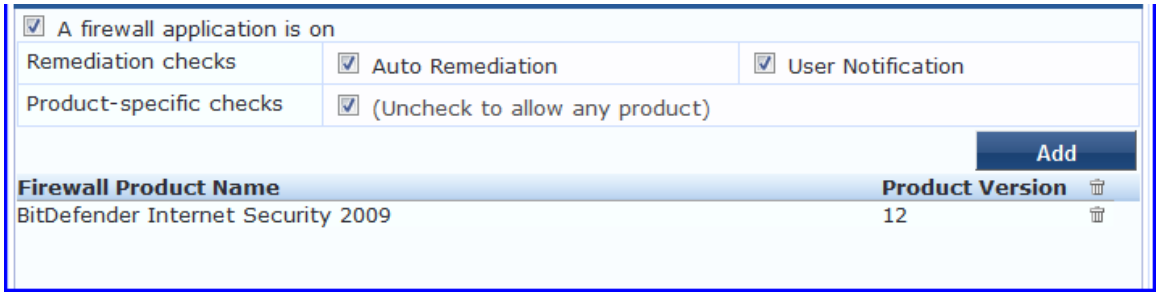
When enabled, the **Firewall** detail page appears.

Figure 201: *Firewall Page (Detail 2)*



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

Figure 202: *Firewall Page (Overview After)*



The following table describes the **Firewall** parameters:

Table 129: *Firewall Page Parameters*

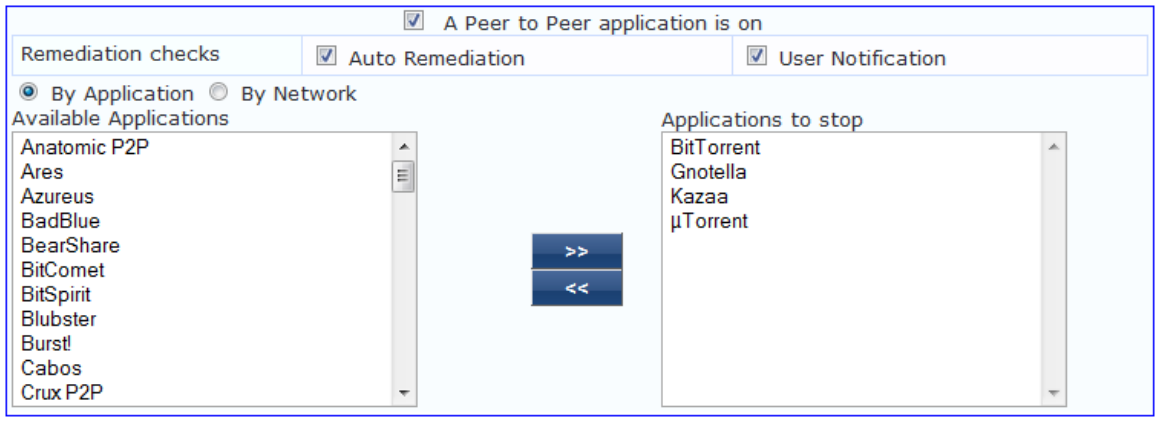
Interface	Parameter	Description
Firewall Page	• A Firewall Application is On • Auto Remediation • User Notification • Uncheck to allow any product	• Check the **Firewall Application is On** check box to enable testing of health data for configured firewall application(s). • Check the **Auto Remediation** check box to enable auto remediation of firewall status. • Check the **User Notification** check box to enable user notification of policy violation of firewall status. • Uncheck the **Uncheck to allow any product** check box to check whether any firewall application (any vendor) is running on the end host.
Firewall Page (Detail 1)	• Add • Trashcan icon	• To configure firewall application attributes for testing against health data, click **Add**. • To remove configured firewall application attributes from the list, click the **trashcan icon** in that row.
Firewall Page (Detail 2)	Product/Version	Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on the UI. • Select the firewall product - Select a vendor from the list • Product version is at least - Enter the version of the product.

Peer To Peer

The **Peer To Peer** page provides a set of widgets for specifying specific peer to peer applications or networks to be explicitly stopped. When you select a peer to peer network, all applications that make use of that network are stopped.

The following figure displays the **Peer To Peer** health class configuration page:

Figure 203: *Peer to Peer Page*



The following table describes the **Peer to Peer** parameters:

Table 130: *Peer to Peer Page*

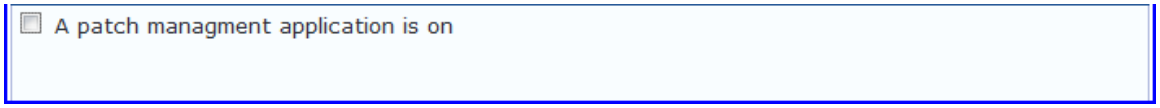
Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop peer to peer applications based on the entries in **Applications to stop** configuration).
User Notification	Enable to allow user notifications for peer to peer application/network check policy violations.
By Application / By Network	Select the appropriate radio button to select individual peer to peer applications or a group of applications that use specific p2p networks.
Available Applications	This scrolling list contains a list of applications or networks that you can select and move to the **Applications to stop** panel. Click the **>>** or **<<** to add or remove, respectively, the applications or networks from the **Applications to stop** box.

Patch Management

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

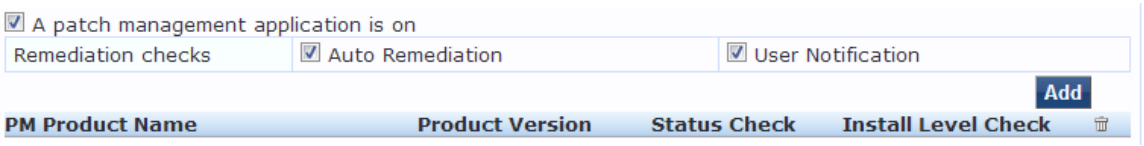
The following figure displays the **Patch Management** page:

Figure 204: *Patch Management Page (Overview - Before)*



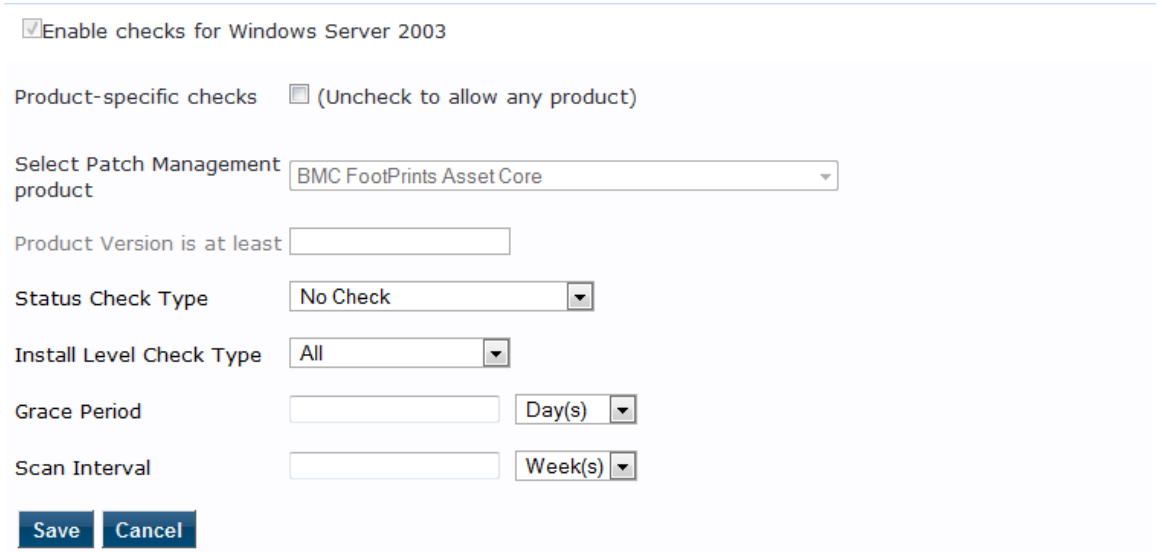
When enabled, the **Patch Management** detail pop-up appears.

Figure 205: *Patch Management Page (Detail 1)*



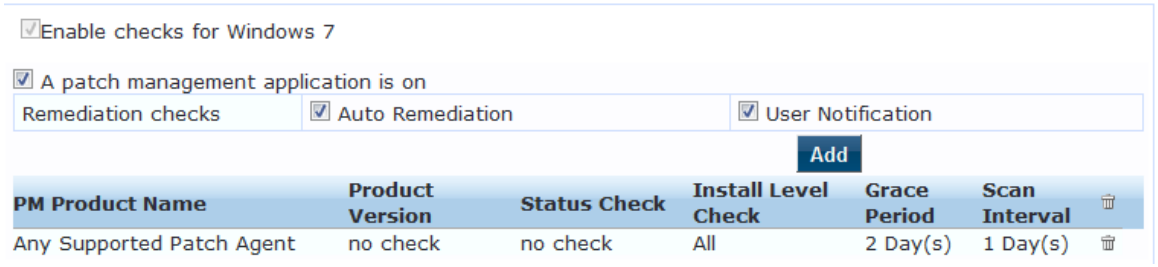
Click **Add** to specify PM Product Name, Product Version, Status Check, and Install Level Check information.

Figure 206: *Patch Management Page (Detail 2)*



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

Figure 207: *Patch Management Page (Overview - After)*



The following table describes the **Patch Management** parameters:

Table 131: *Patch Management Page Parameters*

Interface	Parameter	Description
Patch Management Page	• A patch management application is on • Auto Remediation • User Notification • Uncheck to allow any product	• Check the **A patch management application is on** to enable testing of health data for configured Antivirus application(s). • Check the **Auto Remediation** check box to enable auto remediation of patch management status. • Check the **User Notification** check box to enable user notification of policy violation of patch management status. • Clear **Uncheck to allow any product** check box to check whether any patch management application (any vendor) is running on the end host.
Patch Management Page (Detail 1)	• Add • Trashcan icon	• To configure patch management application attributes for testing against health data, click **Add**. • To remove configured patch management application attributes from the list, click the **trashcan icon** in that row.
Patch Management Page (Detail 2)	Product/Version	Configure settings for which to test against health data. All checks might not be available for some products. Where checks are not available, they are shown in disabled state on the UI. • **Select Patch Management product:** Select a vendor. This option is *only* enabled if the Product-specific checks check box is checked. • **Product version is at least:** Enter version number. This option is *only* enabled if the Product-specific checks check box is checked. • **Status Check Type:** Select this field to check whether Patch Agent is enabled or not. Dell Networking W-ClearPass Policy Manager server compares the Patch Agent Status sent by OnGuard Agent with the configured value. If the Patch Agent Status value is different from configured value, then client is treated as unhealthy. If Auto-remediation is enabled, then OnGuard Agent changes the Patch Agent Status on client to the configured value. Select any of the following options: ▪ **No Check** - Dell Networking W-ClearPass Policy Manager server ignores Patch Agent Status value. This means it will not check status of Patch Agent application on client. ▪ **Enabled** - Patch Agent is turned on and automatically update the client. ▪ **Disabled** - Patch Agent is disabled and it will not check for missing patches and update the client. ▪ **Notify Before Download** - Patch Agent is turned on and will notify user before downloading updates.

Table 131: *Patch Management Page Parameters (Continued)*

Interface	Parameter	Description
		▪ **Notify Before Install** - Patch Agent is turned on and will notify user before installing updates. **NOTE:** The values specific to the selected product are displayed in the **Status Check Type** field. For example, all the 5 values are displayed for **Microsoft Windows Automatic Update**. For **SCCM**, only **No Check**, **Disabled**, and **Notify Before Install** are displayed. • **Install Level Check Type:** Select No Check, All, Selected on Server, or Security. This option is only enabled if the **Product-specific checks** check box is checked. For Microsoft SCCM, selecting All, Selected on Server, or Security will return the full list of all missing patches. ▪ **All**: Check for all missing patches, and search for all available patches. ▪ **Selected on Server**: Check only for the patches pre-selected on the server. Some Patch Management products can push the patches to the endpoint device. This option provides the ability to check for only the pre-selected patches. ▪ **Security**: Check only for security updates. Some of the products can install only security-related patches. **NOTE:** If you select the **Microsoft Windows Update Agent** from the **Select Patch Management product** list and you select an option from the **Install Level Check Type** list, the results are listed below: ▪ **All**: Returns the full list of missing patches. ▪ **Selected on Server**: Returns a list of missing patches that are pre-selected on the server site. ▪ **Security**: Returns a list of missing patches that Microsoft classifies as Security Updates. ▪ **No Check** - Disables the **Grace Period** and **Scan Interval** fields. • **Grace Period**: Configure the time period for which OnGuard Agent should ignore missing patches. You can specify the grace period in hours, days, weeks, or months. For example, if the **Grace Period** is set to 3 days, then clients will be treated as 'healthy' for 3 days even if some patches are missing. After 3 days, OnGuard Agent will treat clients as 'unhealthy' if the patches are still missing. You can enable **Auto-remediation** to install the missing patches and to treat them as 'healthy'. This field is disabled if you selected **No Check** from the **Install Level Check Type** field.

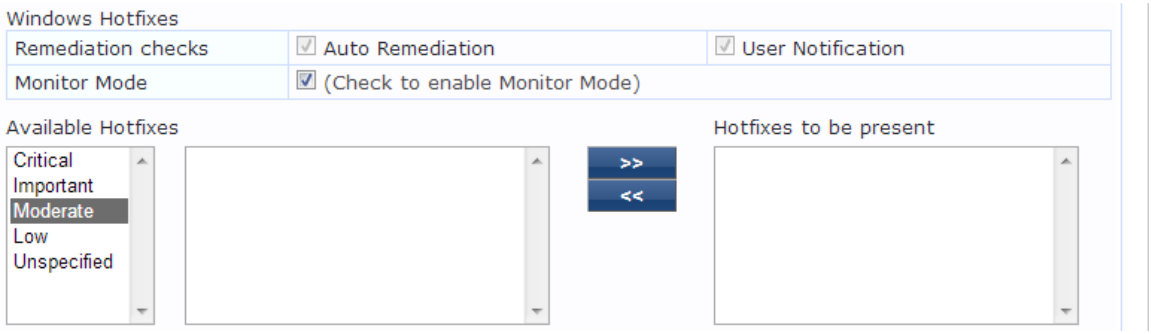
Table 131: *Patch Management Page Parameters (Continued)*

Interface	Parameter	Description
		• **Scan Interval**: Configure the time interval after which OnGuard Agent should check for missing patches. You can configure the time period in hours, days, weeks, or months. The default scan interval is 1 hour. This field is disabled if you selected **No Check** from the **Install Level Check Type** field.

Windows Hotfixes

The **Windows Hotfixes** page provides a set of widgets for checking if specific Windows hotfixes are installed on the endpoint. The following figure displays the **Windows Hotfixes** health class configuration page:

Figure 208: *Windows Hotfixes Page*



The following table describes the **Windows Hotfixes** parameters:

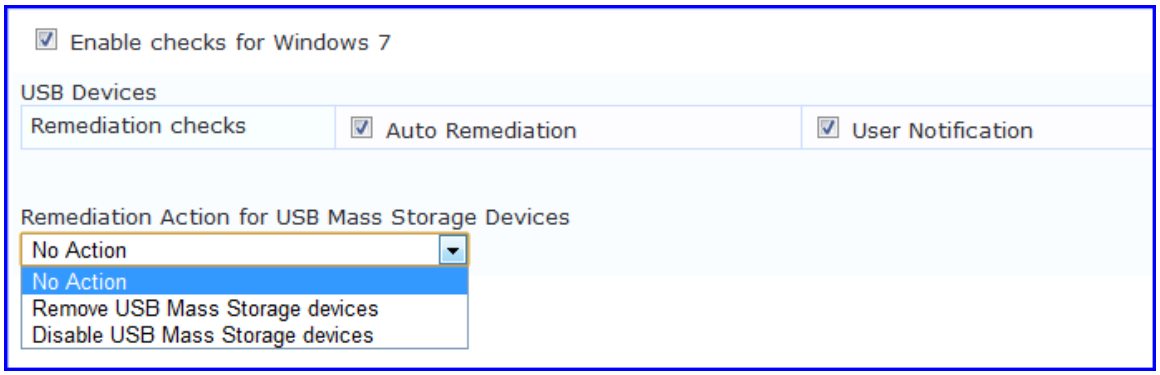
Table 132: *Windows Hotfixes Page Parameters*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for hotfixes checks (Automatically trigger updates of the specified hotfixes).
User Notification	Enable to allow user notifications for hotfixes check policy violations.
Monitor Mode	Click to enable **Monitor Mode**.
Available Hotfixes	The first scrolling list lets you select the criticality of the hotfixes. Based on this selection, the second scrolling list contains a list of hotfixes that you can select and move to the **Hotfixes to be present** panel (using their associated widgets). Click the **>>** or **<<** to add or remove, respectively, the hotfixes from the **Hotfixes to run** boxes.

USB Devices

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

Figure 209: *USB Devices*



The following table describes the **USB Devices** parameters:

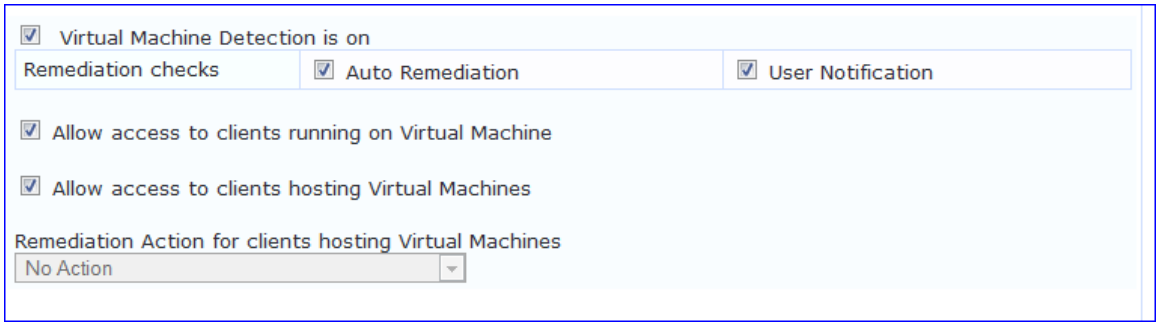
Table 133: *USB Devices*

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

Virtual Machines

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

Figure 210: *Virtual Machines*



The following table describes the **Virtual Machines** parameters:

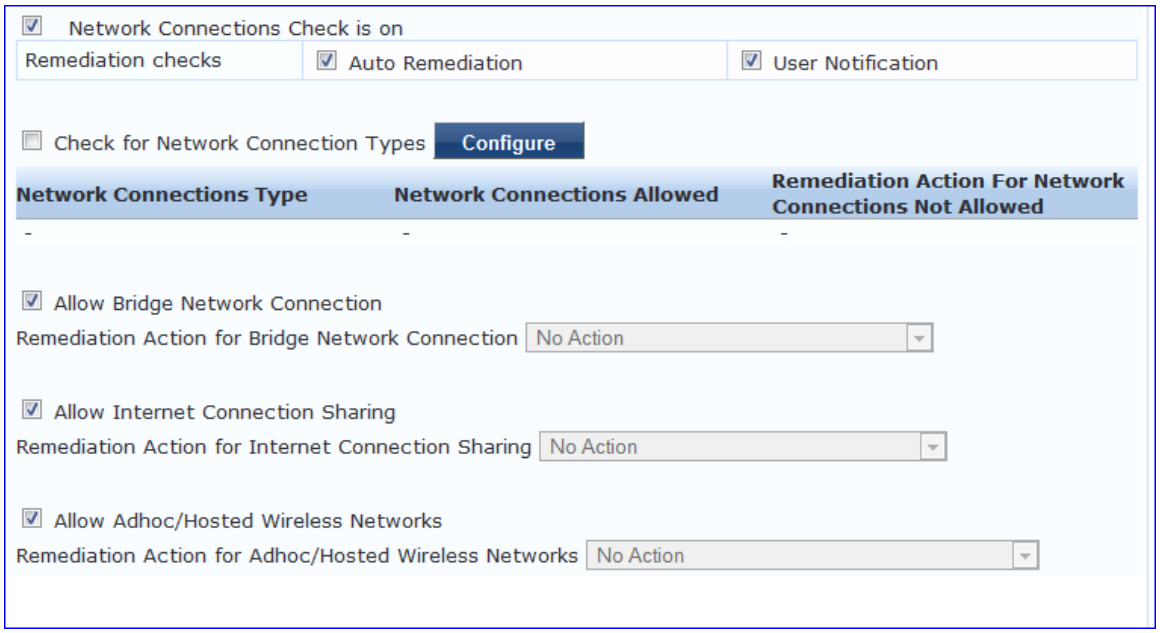
Table 134: *Virtual Machines*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for virtual machines connected to the endpoint.
User Notification	Enable to allow user notifications for virtual machine policy violations.
Allow access to clients running on Virtual Machine	Enable to allow clients that running a VM to be accessed and validated.
Allow access to clients hosting Virtual Machine	Enable to allow clients that hosting a VM to be accessed and validated.
Remediation Action for clients hosting Virtual Machines	• No Action - Take no action; do not stop or pause virtual machines. • Stop all Virtual Machines running on Host - Stop the VM clients that are running on Host. • Pause all Virtual Machines running on Host - Pause the VM clients that are running on Host.

Network Connections

The **Network Connections** page provides configuration to control network connections based on connection type. The following figure displays the **Network Connections** health class configuration page:

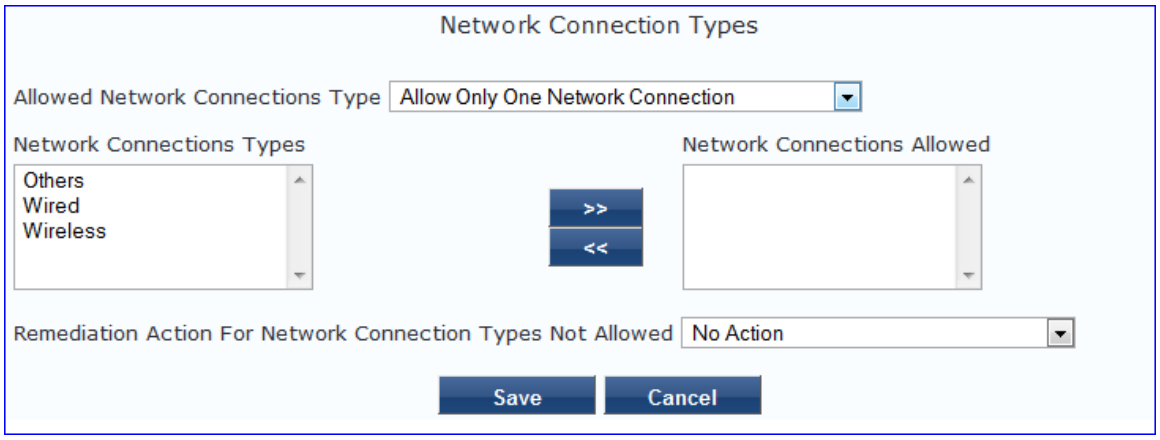
Figure 211: *Network Connections Page*



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

Configure Network Connection Type

Figure 212: *Network Connection Type Configuration*



The following table describes the **Network Connection Type Configuration** parameters:

Table 135: *Network Connection Type Configuration Page*

Parameter	Description
Allow Network Connections Type	• Allow Only One Network Connection • Allow One Network Connection with VPN • Allow Multiple Network Connections
Network Connection Types	Click the **>>** or **<<** to add or remove Others, Wired, and Wireless connection types.
Remediation Action for USB Mass Storage Devices	• No Action - Take no action; do not eject or disable the attached devices. • Disable Network Connections - Disable network connections for the configured network type.

Click **Save** after you finish. This returns you to the **Network Connections Configuration** page. The remaining fields on this page are described below:

Table 136: *Network Connections Configuration*

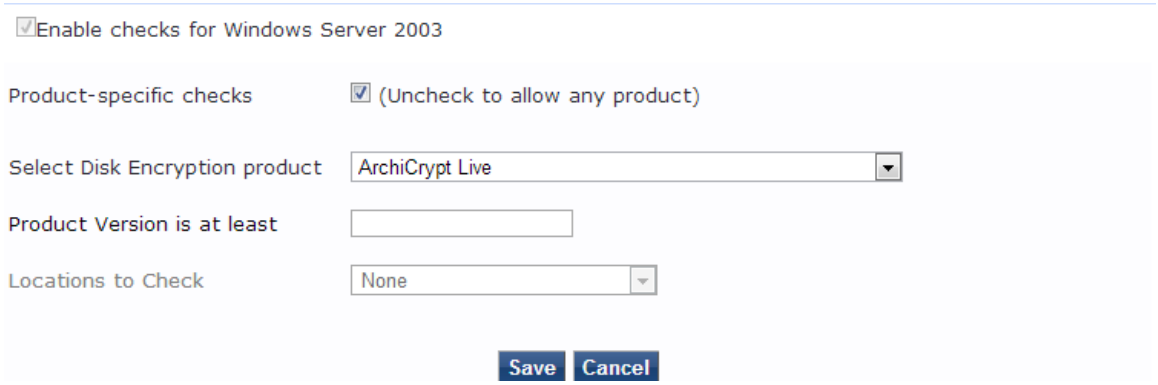
Parameter	Description
Auto Remediation	Enable to allow auto remediation for network connections.
User Notification	Enable to allow user notifications network connection policy violations.
Remediation Action for Bridge Network Connection	If **Allow Bridge Network Connection** is disabled, then specify whether to take no action when a bridge network connection exists or to disable all bridge network connections.
Remediation Action for Internet Connection Sharing	If **Allow Internet Connection Sharing** is disabled, then specify whether to take no action when Internet connection sharing exists or to disable Internet connection sharing.
Remediation Action for Adhoc/Hosted Wireless Networks	If **Allow Adhoc/Hosted Wireless Networks** is disabled, then specify whether to take no action when an adhoc wireless networks exists or to disable all adhoc/hosted wireless networks.

Disk Encryption

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

The following figure displays the **Disk Encryption** health class configuration page:

Figure 213: *Disk Encryption Configuration Page*



The following table describes the Disk Encryption parameters:

Table 137: *Disk Encryption Parameters*

Parameter	Description
User Notification	Enable to allow user notifications for virtual machine policy violations.
Product-specific checks	Clear to allow disk encryption on any product. The Select Disk Encryption product and Product Version is at least fields are disabled after you clear the check box.
Select Disk Encryption product	Select a specific disk encryption product.
Product Version is at least	Search for the production version of the selected product.
Locations to Check	Select location to check. The options are None, System Root Drive, All Drives, or Specific Locations.

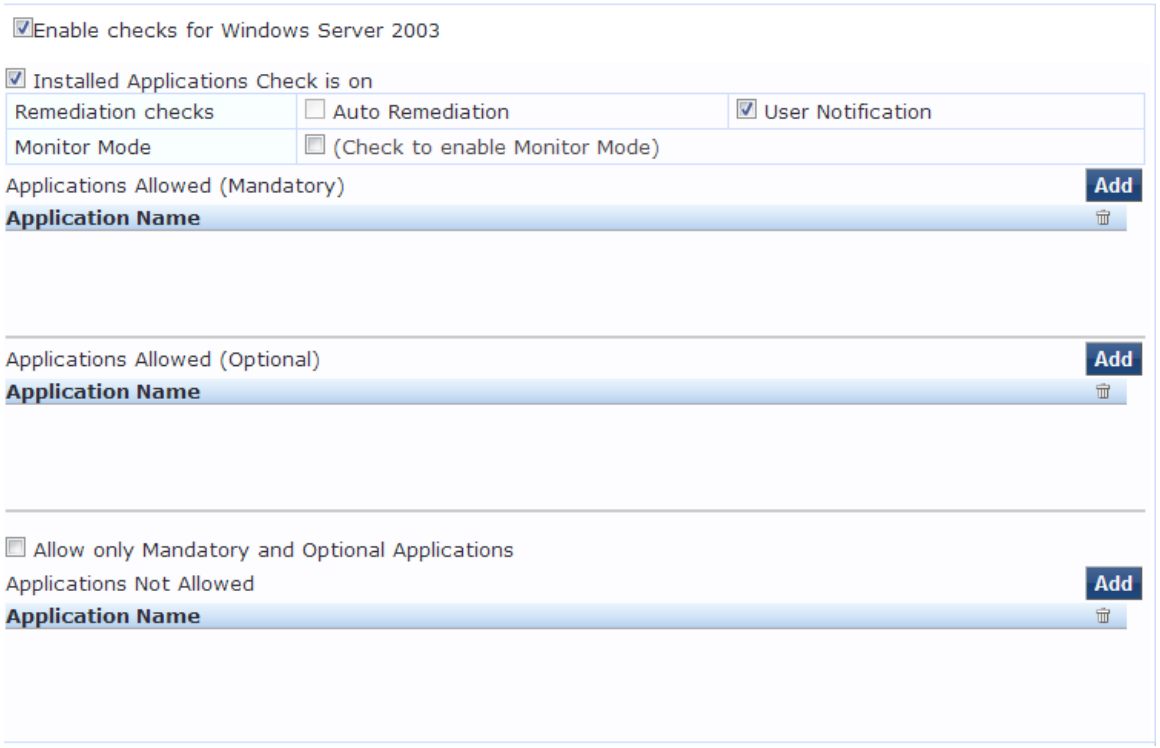
Installed Applications

The Installed applications category groups classes that represent software-related objects. Access to these objects is supported by Windows Installer. Examples of objects in this category are installed products, file specifications, and registration actions.

In the **Installed Applications** page, you can turn on the installed applications check and specify information about which installed applications you want to monitor. You can take the following actions:

- Specify installed applications to monitor on a mandatory basis.
- Specify installed applications to be monitored on an optional basis.

- Specify installed applications that are never monitored.
- Specify that only the mandatory and optional applications are monitored.



The following table describes the **Installed Applications Configuration** parameters:

Table 138: *Installed Applications Configuration Page Parameters*

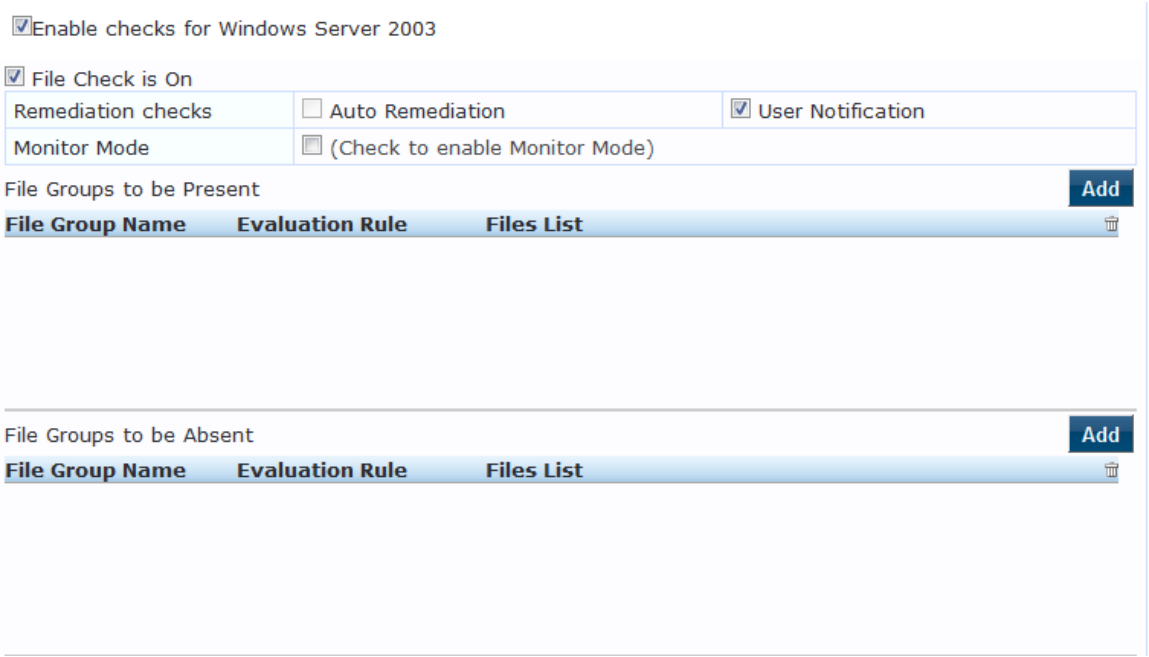
Parameter	Description
Remediation checks	Auto-remediation for Installed Applications health class is not supported.
User Notification	A Remediation message having a list of applications to install/uninstall will be displayed to end user.
Monitor Mode	Enable **Monitor Mode** to treat all the installed applications as always healthy.
Applications Allowed (Mandatory)	Enter the application name as it is shown in Add/Remove Programs.
Applications Allowed (Optional)	Enter the application name as it is shown in Add/Remove Programs.
Allow only Mandatory and Optional Applications	Check to allow only selected applications. All applications other than 'Allowed Applications, including both mandatory and optional' must be removed or uninstalled.

File Check

Use the **File Check** page to verify the group of files to present or absent. In the **File Check** page, you can turn on the file check and specify information about which the files you want to check.

The following figure displays the **File Check** health class configuration page:

Figure 214: *Windows File Check Health Class*

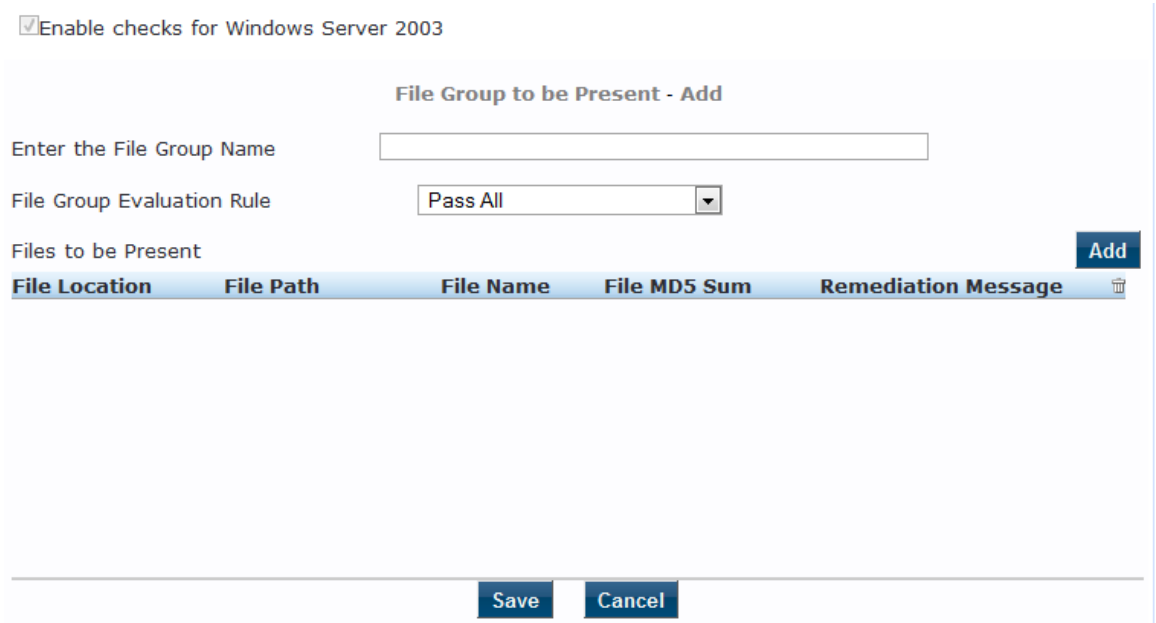


The following table describes the **File Check Configuration** parameters:

Table 139: *File Check Configuration Parameters*

Parameter	Description
Remediation checks	Auto-remediation for the **File Check** health class is not supported.
User Notification	A remediation message having a list of files to present/absent will be displayed to end user.
Monitor Mode	Enable **Monitor Mode** to treat all the file check health classes as always healthy.
File Groups to be Present	Click Add to add the files to be present in the **File Check** health class.
File Groups to be Absent	Click Add to add the files to be absent in the **File Check** health class.

Click **Add** to open the **File Group to be Present - Add** page in which you can configure the name of the file group and evaluation rule for the file group. The following figure displays the **File Group to be Present - Add** pop-up:



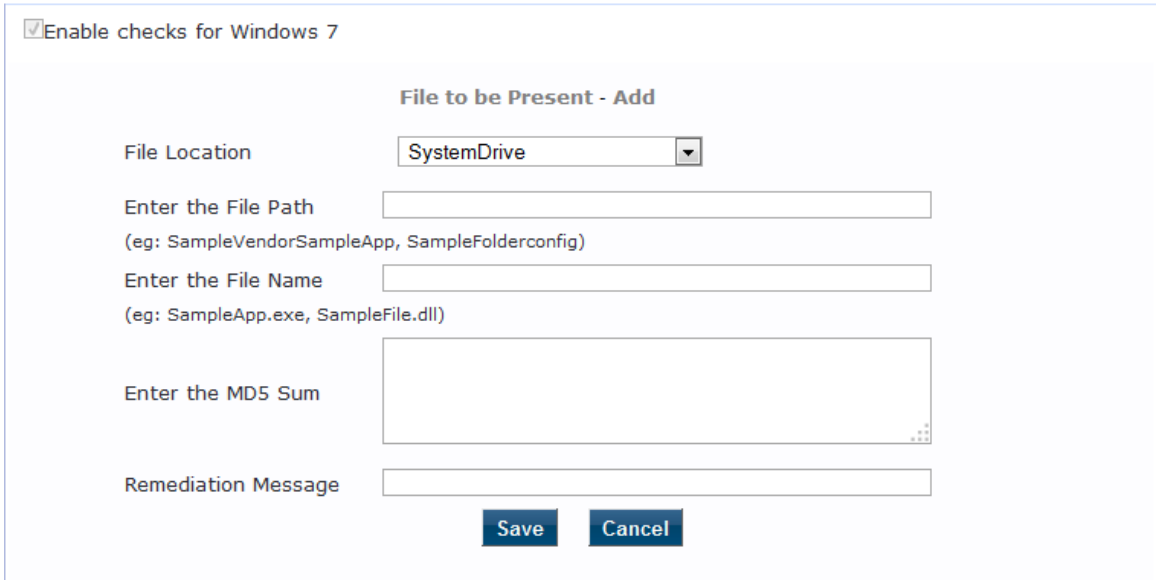
The following table describes the **File Group to be Present - Add** parameters:

Table 140: *File Group to be Present - Add Parameters*

Parameter	Description
Enter the File Group Name	Enter the name of the file group.
File Group Evaluation Rule	**Pass All** - Select this evaluation rule if you want the **File Check** health class to be deemed as 'healthy' only if all the configured file groups are present. **Pass Any One** - Select this evaluation rule if you want the **File Check** health class to be deemed as 'healthy' even any one of the configured file group is present.

Click **Add** from **File Groups to be Present** to configure the name of the file group and evaluation rule for the file group. The following figure displays the **File to be Present - Add** pop-up:

Figure 215: *File to be Present - Add Pop-up*



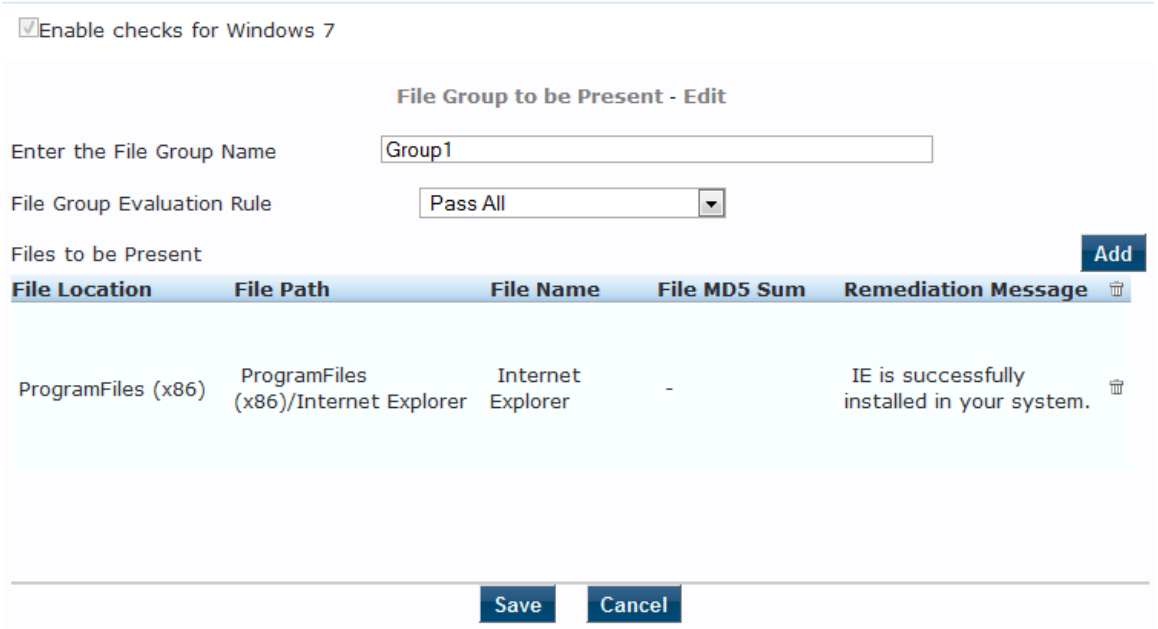
The following table describes the **File to be Present - Add** parameters:

Table 141: *File to be Present - Add Parameters*

Parameter	Description
File Location	Select any location of the file from the drop-down list: • SystemDrive • Systemroot • ProgramFiles • ProgramFiles (x86) • HOMEDRIVE • HOMEPATH • None
Enter the File Path	Enter the file path as described in the examples from the GUI.
Enter the File Name	Enter the name of the file.
Enter the MD5 Sum	Specifies one or more (comma separated) MD5 checksums of the process executable file. This field is optional.
Remediation Message	Specify the custom remediation message to be displayed to end users if **File check** is failed.

The parameters configured in the **File to be Present - Add** pop-up will reflect in the **File Groups to be Present** page as described in the following figure:

Figure 216: *File Group to be Present Pop-up*

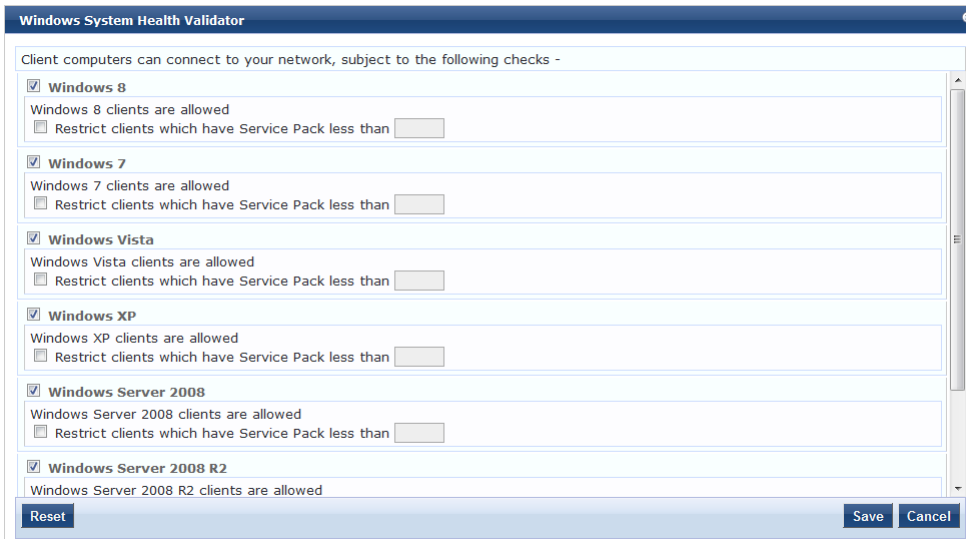


Windows System Health Validator - OnGuard Agent

This validator checks for current Windows Service Packs. The OnGuard Agent also supports legacy Windows operating systems such as and Windows Server 2003. An administrator can use the check boxes to enable

support of specific operating systems and to restrict access based on service pack level.

Figure 217: *Windows System Health Validator - OnGuard Agent (Overview)*

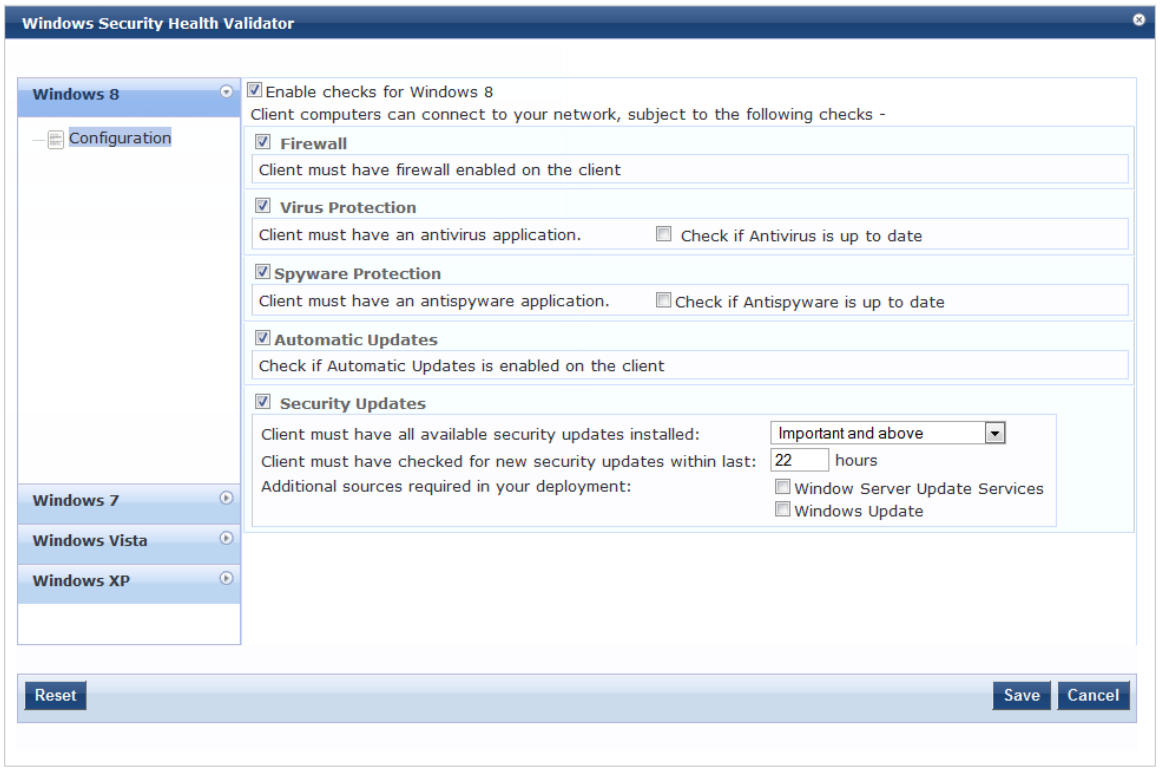


Windows Security Health Validator - OnGuard Agent

This validator checks for the presence of specific types of security applications. An administrator can use the options to restrict access based on the absence of the selected security application types.

The following figure displays the **Windows Security Health Validator** page:

Figure 218: *Windows Security Health Validator*



ClearPass Linux Universal System Health Validator Plugin

The **ClearPass Linux Universal System Health Validator** plugin appears on the **Posture Plugins** (**Configuration** > **Posture** > **Posture Policies** > **Add**) tab. Select the **Linux** host operating system and **OnGuard Agent** posture agent from the **Policy** tab in the **Posture Policy** page. Click **Configure** to configure antivirus settings and service types.

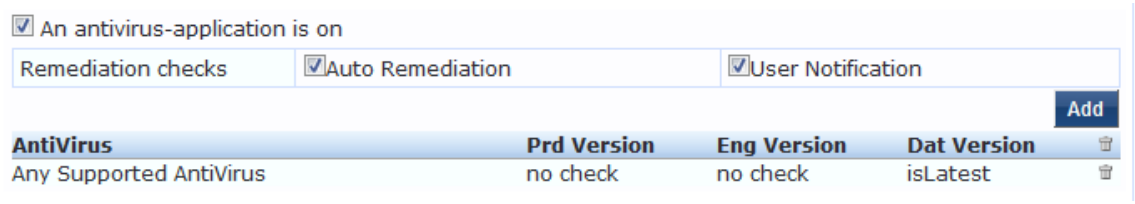
The OnGuard Dissolvable Agent version of the **ClearPass Linux Universal System Health Validator** plug-in supports the following health classes:

- Antivirus on page 264
- Services on page 266

Antivirus

Use the **Antivirus** page to turn on an Antivirus application. Click **An antivirus application is on** to configure the Antivirus application information. The following figure displays the **Antivirus** health class configuration page:

Figure 219: *Antivirus Page*



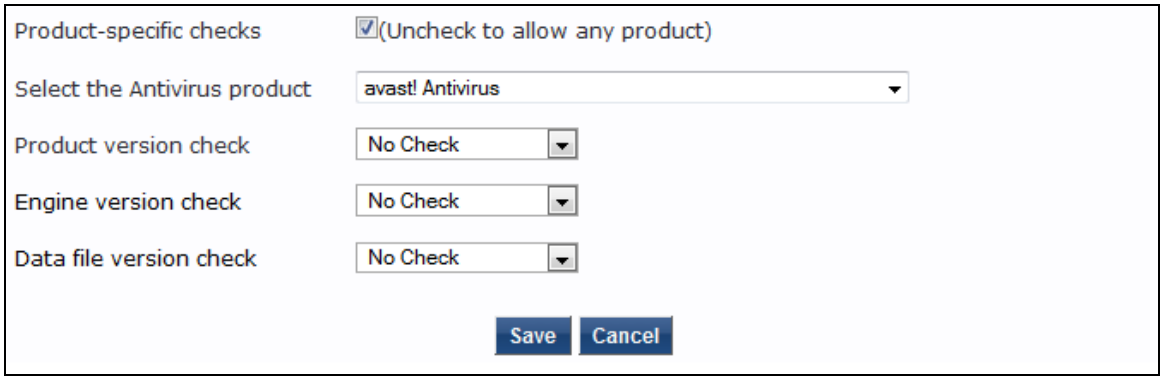
The following table describes the **Antivirus** parameters:

Table 142: *Antivirus Configuration Parameters*

Parameter	Description
Remediation checks	Auto-remediation for the **File Check** health class is not supported.
User Notification	A remediation message having a list of files to present/absent will be displayed to end user.
Antivirus	Shows the name of the Antivirus configured. Click **Add** to configure the name of the Antivirus.
Prd Version	Shows the version of the Antivirus.
Eng Version	Shows the version of the engine.
Dat Version	Shows the version of the data file.

Click **Add** to configure the Antivirus product specific checks. The values configured in the **Antivirus Product configuration** pop-up will be displayed in the **Antivirus** page. The following figure is an example of the **Antivirus Product configuration** pop-up:

Figure 220: *Antivirus Product configuration Pop-up*



The following table describes the **Antivirus Product configuration** parameters:

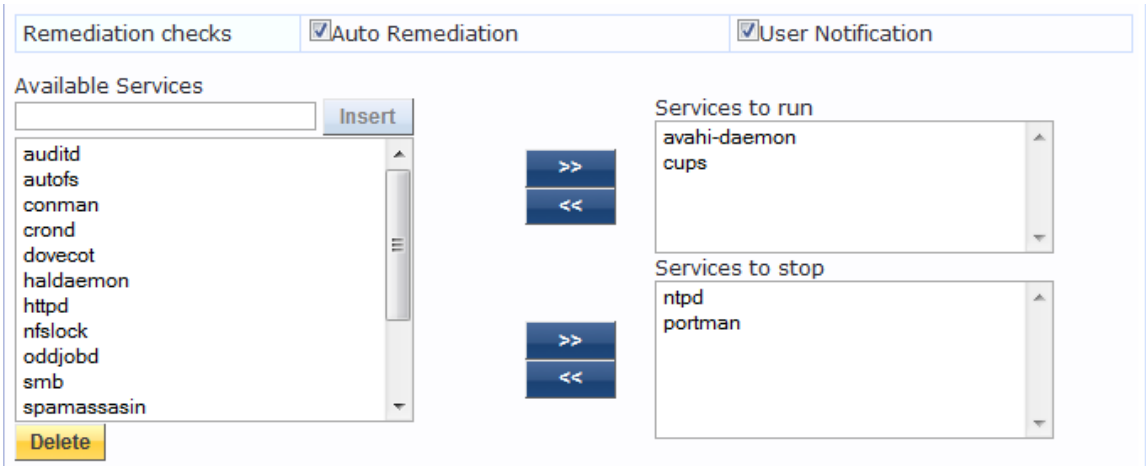
Table 143: *Antivirus Product configuration Parameters*

Parameter	Description
Product-specific checks	Select this check box if you want to configure a specific antivirus product. If you want to allow any antivirus product, do not select this field.
Select the Antivirus product	Select the Antivirus from the drop-down list.
Product version check	Select to check the product version from the options: No Check, Is Latest, or In Last N Updates.
Engine version check	Select to check the engine version from the options: No Check, Is Latest, or In Last N Updates.
Data file version check	Select to check the data file version from the options: No Check, Is Latest, or In Last N Updates.

Services

The **Services** page provides a set of widgets for specifying services to run or stop. The following figure displays the **Services** page:

Figure 221: *Services Page*



The following table describes the **Services** page parameters:

Table 144: *Services Page*

Parameter	Description
Auto Remediation	Enable to allow auto remediation for service checks (Automatically stop or start services based on the entries in **Service to run** and **Services to stop** configuration).
User Notification	Enable to allow user notifications for service check policy violations.
Available Services	This scrolling list contains a list of services that you can select and move to the **Services to run** or **Services to stop** panels (using their associated widgets). This list varies depending on OS types. Click the **>>** or **<<** to add or remove, respectively, the services from the **Service to run** or **Services to stop** boxes.
Insert	To add a service to the list of available services, enter its name in the text box adjacent to this button, then click **Insert**.
Delete	To remove a service from the list of available services, select it and click **Delete**.

ClearPass Mac OS X Universal System Health Validator - OnGuard Agent

Navigate to the **Configuration** > **Posture** > **Posture Policies** > **Add** page, and click **Configure** in the **Posture Plugins** tab of the **Posture** configuration page. Select **ClearPass Mac OS X Universal System Health Validator** and click **Configure**. The **ClearPass Mac OS X Universal System Health Validator** page opens. Select the **Enable checks for Mac OS X** check box to enable checks for Mac OS X.

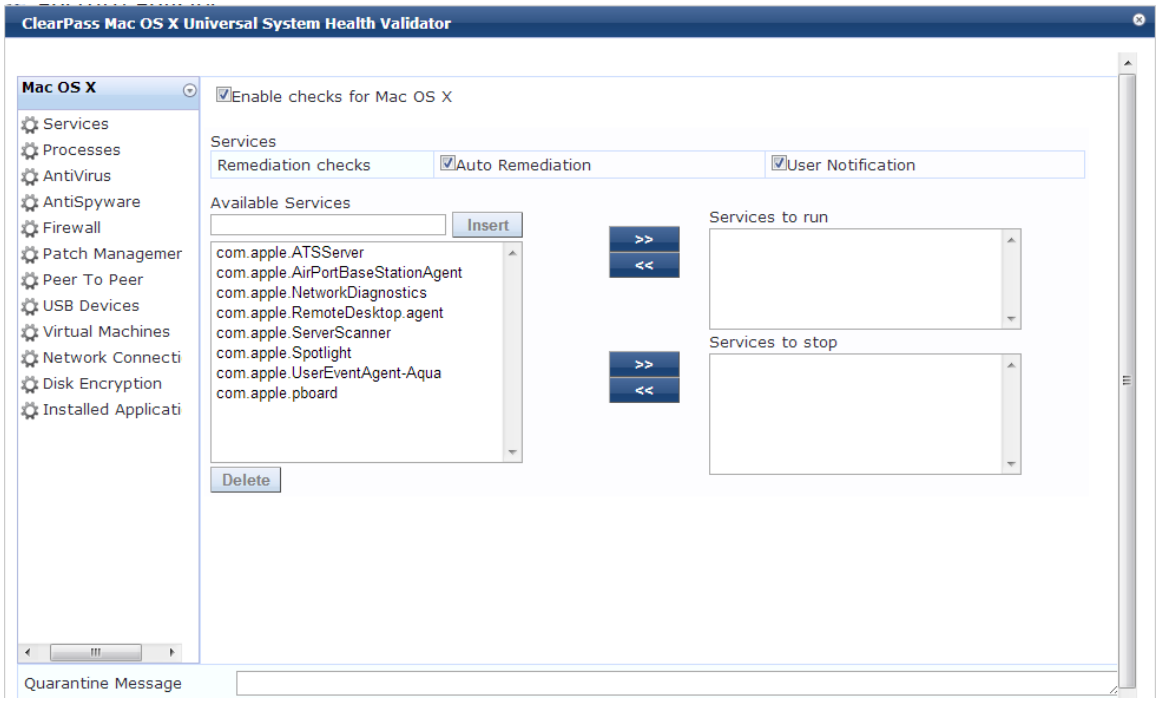
Enabling these check boxes display a corresponding set of configuration pages that are described in the following sections.

- Services on page 267
- Processes on page 268

- Antivirus on page 269
- AntiSpyware on page 269
- Firewall on page 270
- Patch Management on page 271
- USB Devices on page 272
- Virtual Machine on page 272
- Network Connections on page 273
- Disk Encryption on page 273
- Installed Applications on page 274

The following figure displays the **ClearPass Mac OS X Universal System Health Validator** page:

Figure 222: *ClearPass Mac OS X Universal System Health Validator - OnGuard Agent*

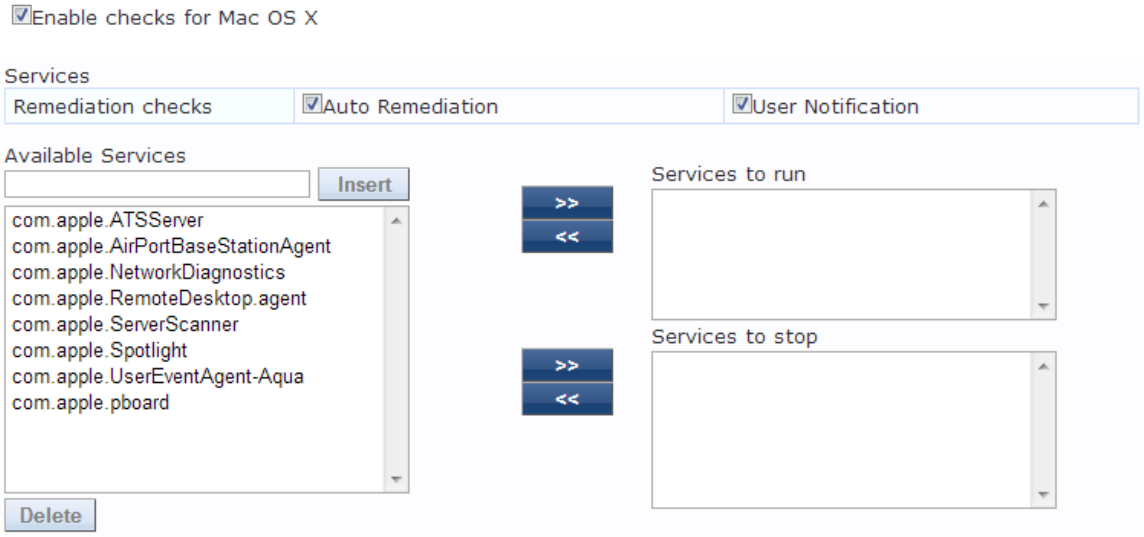


Services

From the **Services** page, you can configure which services to run and which services to stop. See ClearPass Windows Universal System Health Validator - OnGuard Agent on page 238 for description of the fields on this page.

The following figure displays the **Services** health class configuration page:

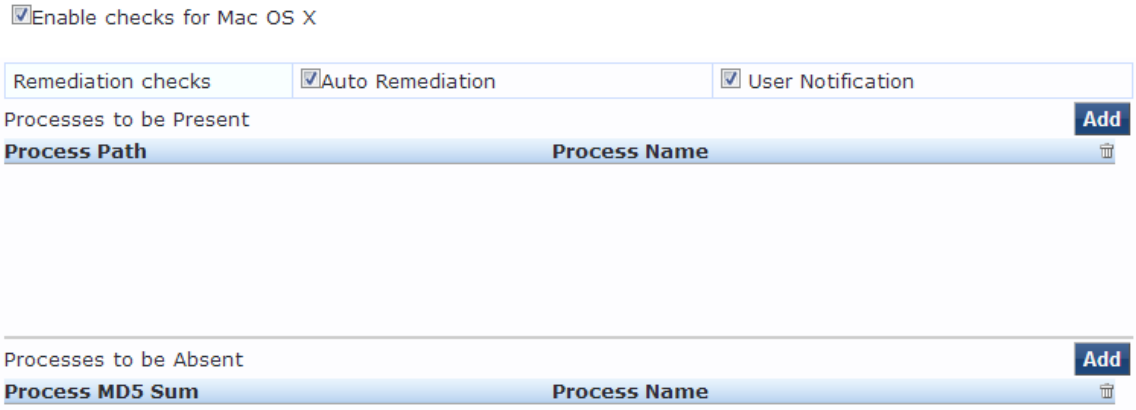
Figure 223: *Services Health Class Configuration Page*



Processes

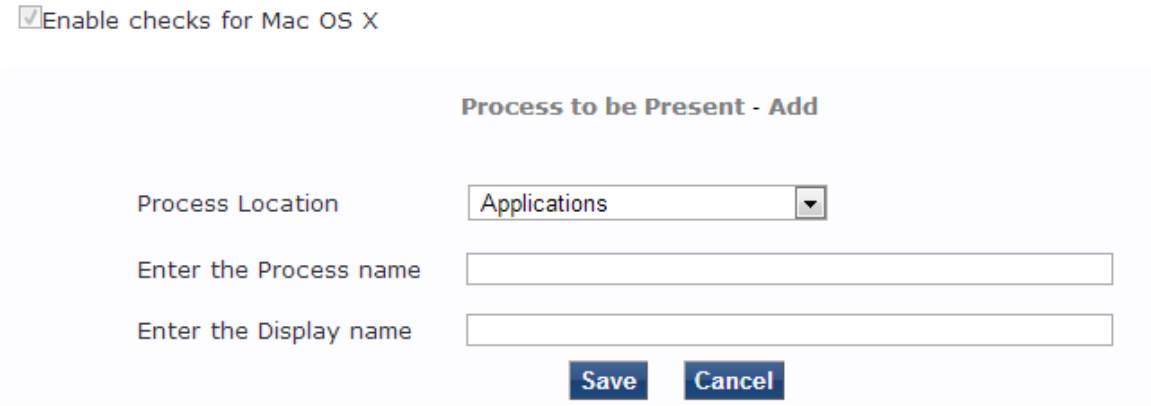
From the **Processes** page, you can view and add processes. Clicking **Enable checks for Mac OS X** provides a set of components to specify the processes that need to be explicitly present or absent on the system.

Figure 224: *Processes Page*



Click **Add** to open the page with options to configure the name, location, and display name of the processes. The following figure displays the **Process to be Present - Add** page:

Figure 225: *Processes to be Present - Add Page*

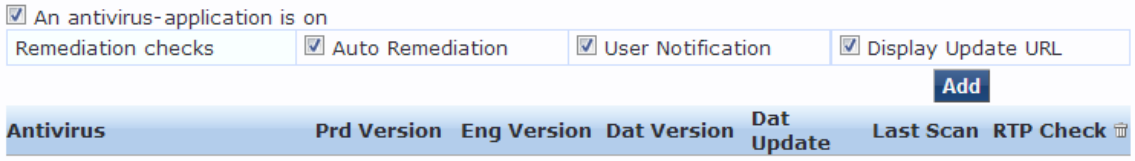


Antivirus

In the **Antivirus** page, you can specify information about the antivirus application. Click on **An antivirus-application is on** to configure the anti-virus application information.

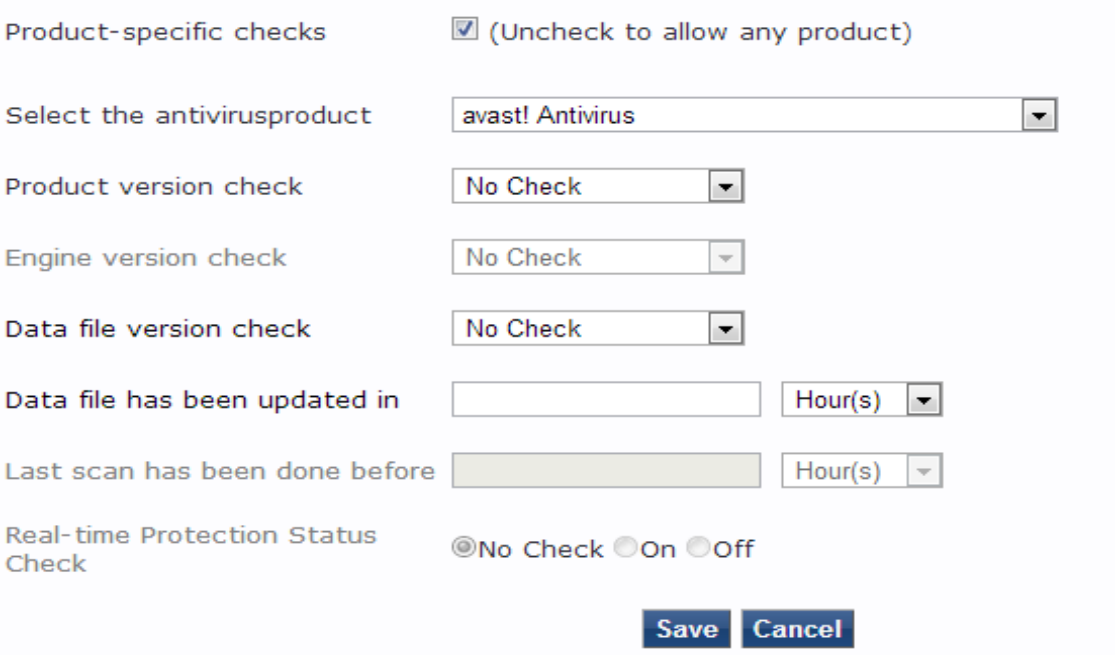
The following figure displays the **Antivirus** page:

Figure 226: *Antivirus Page (Detail 1)*



Click **Add** to specify product and version check information in the antivirus configuration page.

Figure 227: *Antivirus Configuration Page (Detail 2)*

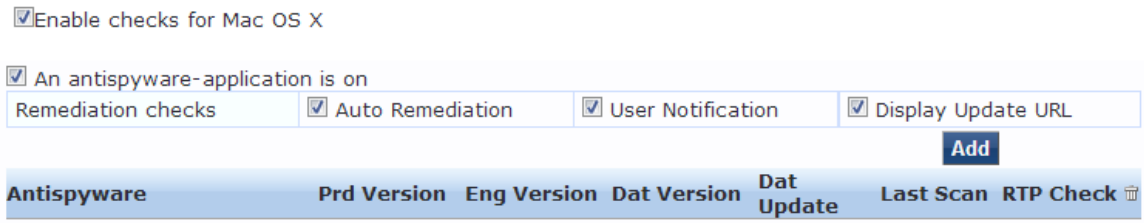


When you save your antivirus configuration, it appears in the **Antivirus** page list. See ClearPass Windows Universal System Health Validator - OnGuard Agent on page 238 for antivirus page and field descriptions.

AntiSpyware

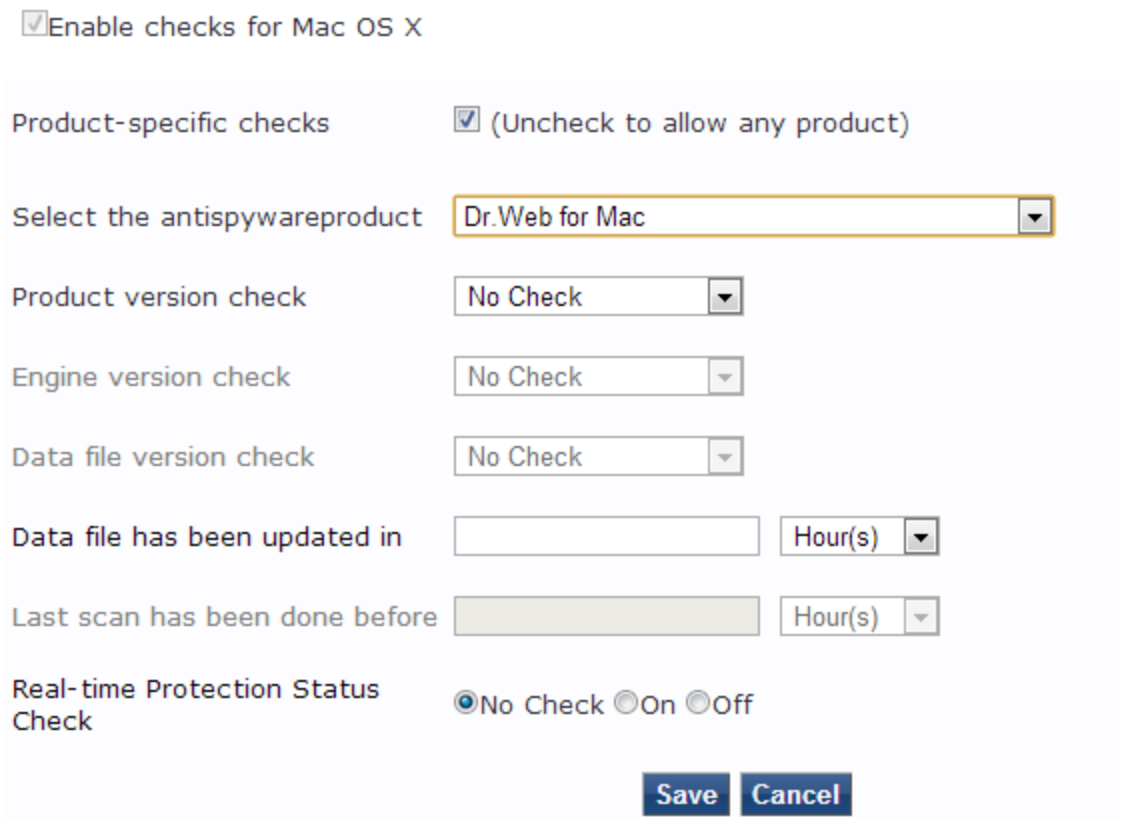
In the **AntiSpyware** page, an administrator can specify information about the antispyware application. The following figures describe the examples of the **AntiSpyware** page and the **AntiSpyware - Add** page:

Figure 228: *Anti-Spyware Page*



In the **Antispyware** page, click **An Antispyware Application is On** to configure different configuration elements specific to the antispyware product that you select. When you save the antispyware configuration, it appears in the **Antispyware** page list.

Figure 229: *Anti-Spyware Add Page*



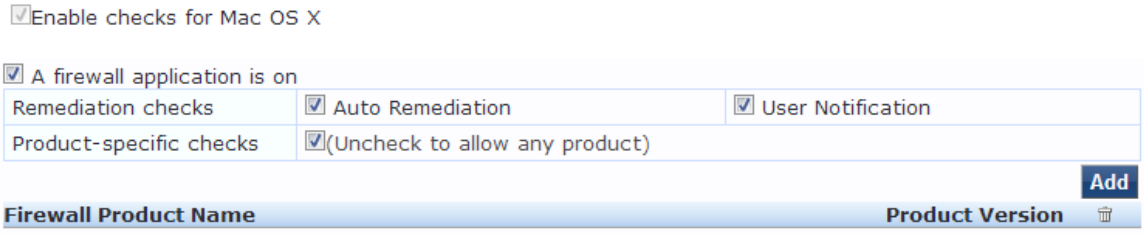
NOTE

The configuration elements are the same for antivirus and antispyware products.

Firewall

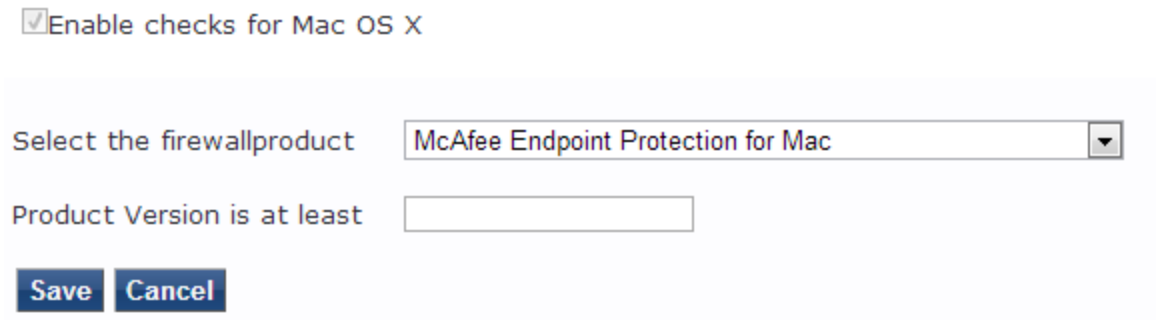
From the **Firewall** page, click **A Firewall Application is On** to configure the firewall application information. The following figure displays the **Firewall** page:

Figure 230: *Firewall Page*



Click **Add** from the **Firewall** page to configure different configuration elements specific to the firewall product that you select. When you save the firewall configuration, it appears in the **Firewall** page list.

Figure 231: *Firewall Add Page*



When enabled, the **Firewall** detail page appears. See ClearPass Windows Universal System Health Validator - OnGuard Agent on page 238 for firewall page and field descriptions.

Patch Management

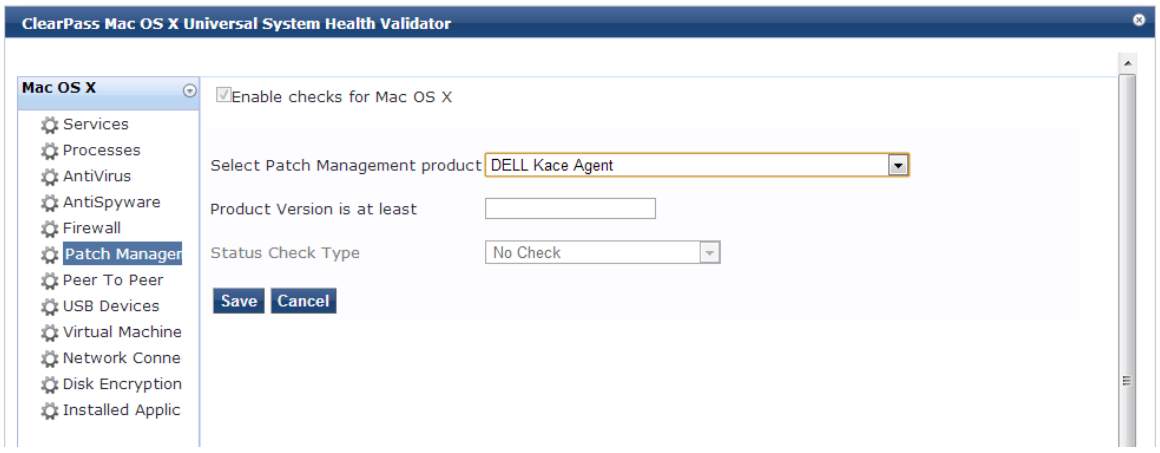
From the **Patch Management** page, you can view and add the patch management product. Select **A patch management application is on** to configure auto remediation and user notification features.

The following figure displays the **Patch Management** page:

Figure 232: *Patch Management Page*

Click **Add** in the **Patch Management** page to view the configuration options for the specific patch management product. The following figure displays the **Patch Management - Add** page:

Figure 233: *Patch Management - Add Page*

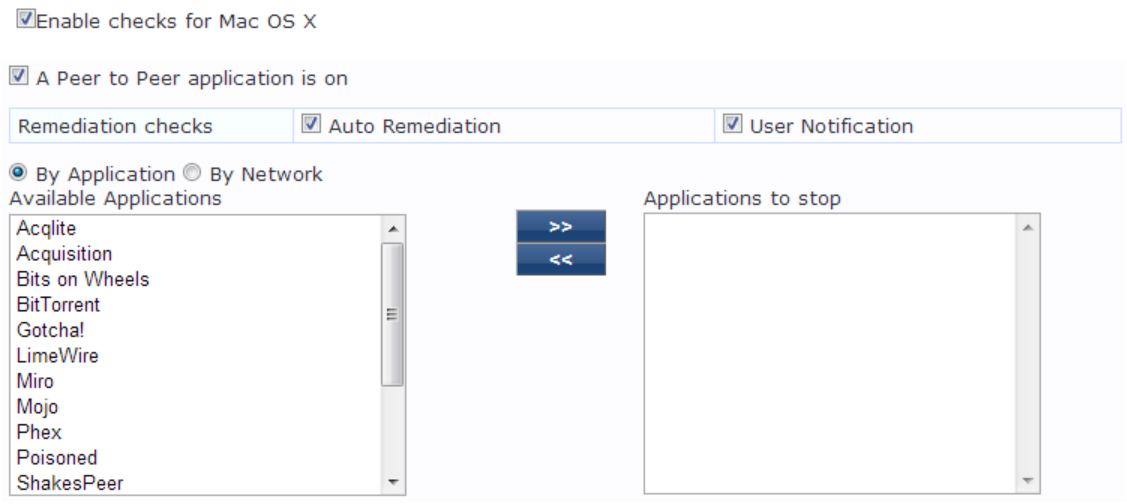


Peer To Peer

From the **Peer To Peer** page, you can view and add peer-to-peer applications. Clicking **A Peer to Peer application is on** provides configuration options to specify peer to peer applications or networks that need to be explicitly stopped. When you select a peer to peer network, all applications that make use of that network are stopped.

The following figure displays the **Peer To Peer** page:

Figure 234: *Peer To Peer Page*

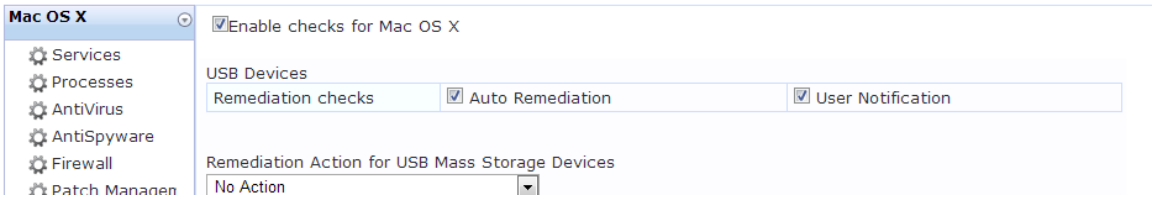


USB Devices

Use this page to configure the **Auto Remediation** and **User Notification** parameters. You can also configure the options to take remediation action for USB mass storage devices or to remove USB mass storage devices from the **Remediation Action for USB Mass Storage Devices** drop-down.

The following figure displays the **USB Devices** page:

Figure 235: *USB Devices Page*

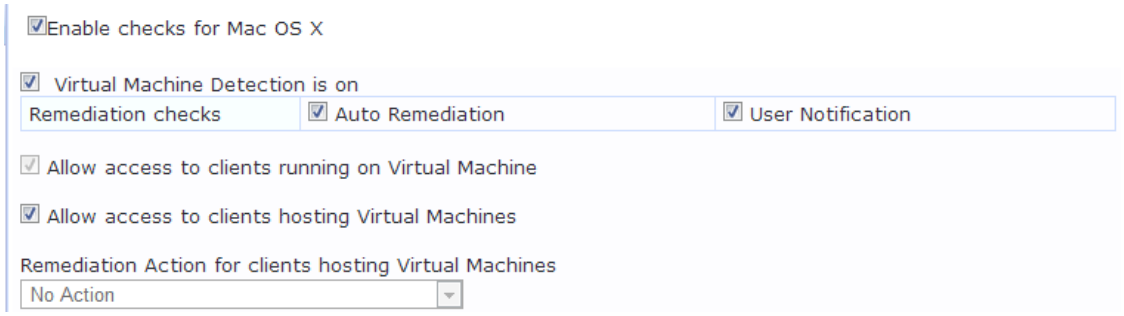


Virtual Machine

The **Virtual Machines** page provides configuration options to virtual machines utilized by the network. Select the **Virtual Machine Detection is on** option to enable the **Auto Remediation** and **User Notification** options.

The following figure displays the **Virtual Machine** page:

Figure 236: *Virtual Machine Page*

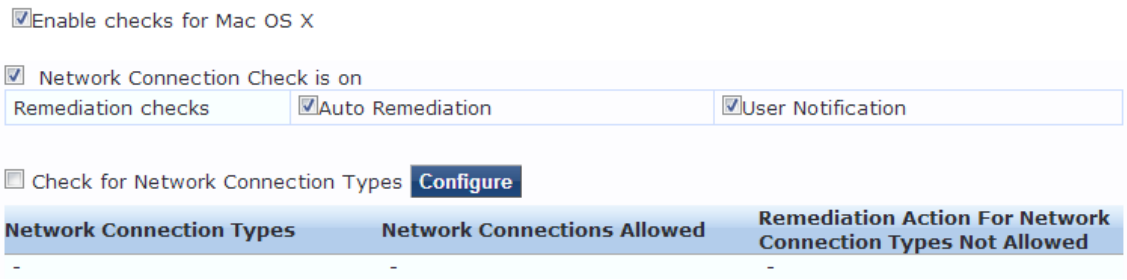


Network Connections

The **Network Connections** page provides configuration options to control network connections based on connection type. Enabling the **Network Connection Check is on** check box provides the options to specify the remediation checks or user notification.

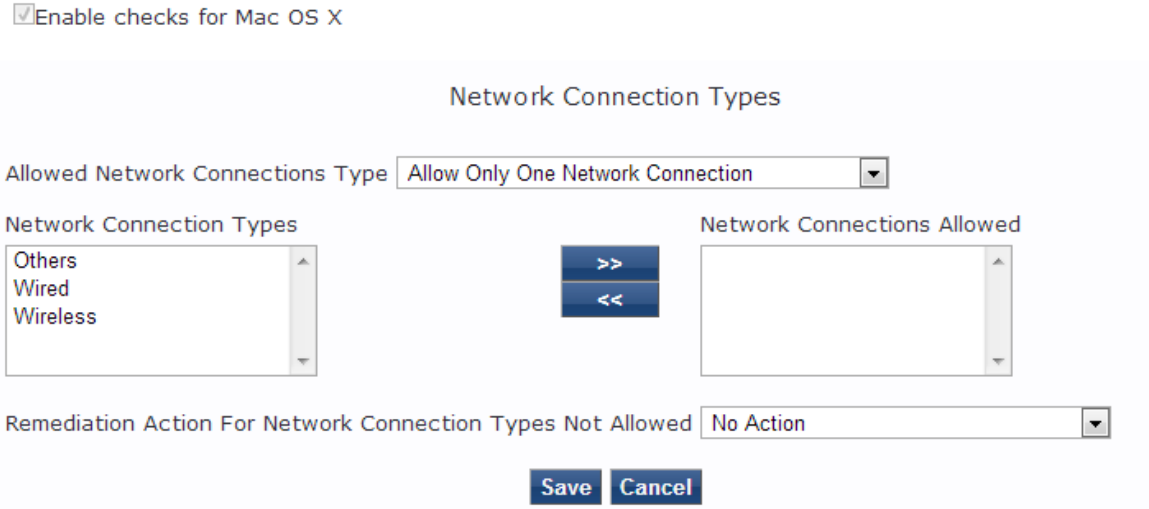
The following figure displays the **Network connections** page:

Figure 237: *Network Connections Page*



Select the **Check for Network Connection Types** check box from the **Network Connections** page, and then click **Configure** to specify type of network connection. You can select and allow the network connection types from the **Network Connections Configuration** page as described in the following figure:

Figure 238: *Network Connections Configuration Page*

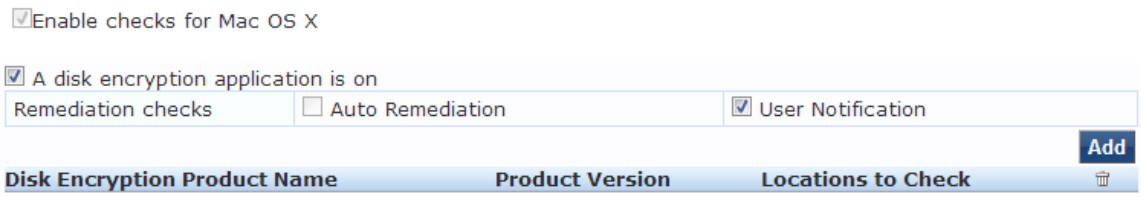


Disk Encryption

Disk encryption is a technology that protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

The following figure displays the **Disk Encryption** page:

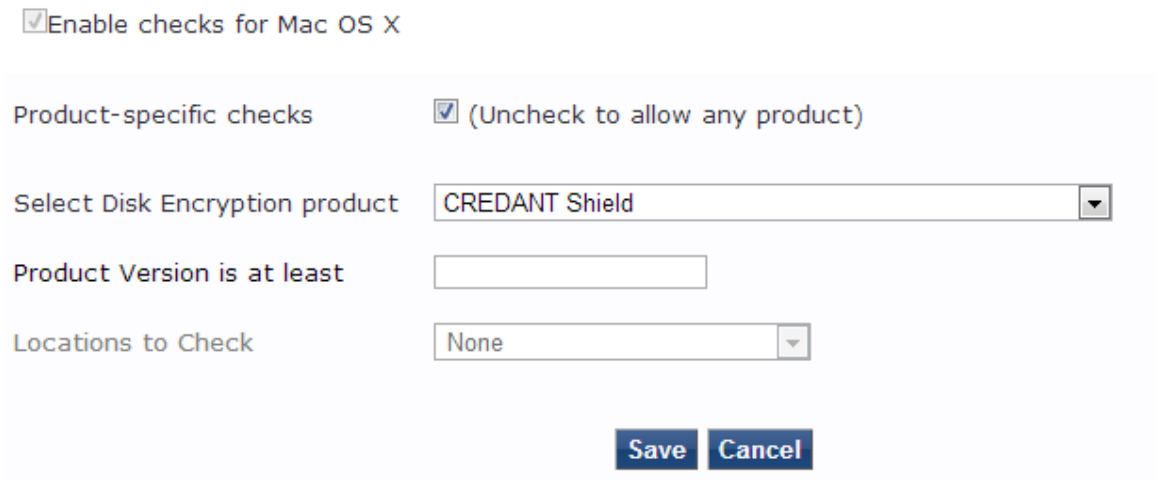
Figure 239: *Disk Encryption Page*



Click **A disk encryption application is on** from the **Disk Encryption** page to configure the remediation options. Click **Add** to configure the product specific encryption checks. You can select the **Uncheck to allow any product** check box from the **Product-specific checks** field to not to allow any encryption product to check disk encryption.

The following image is an example of the **Disk Encryption - Add** page:

Figure 240: *Disk Encryption Add Page*



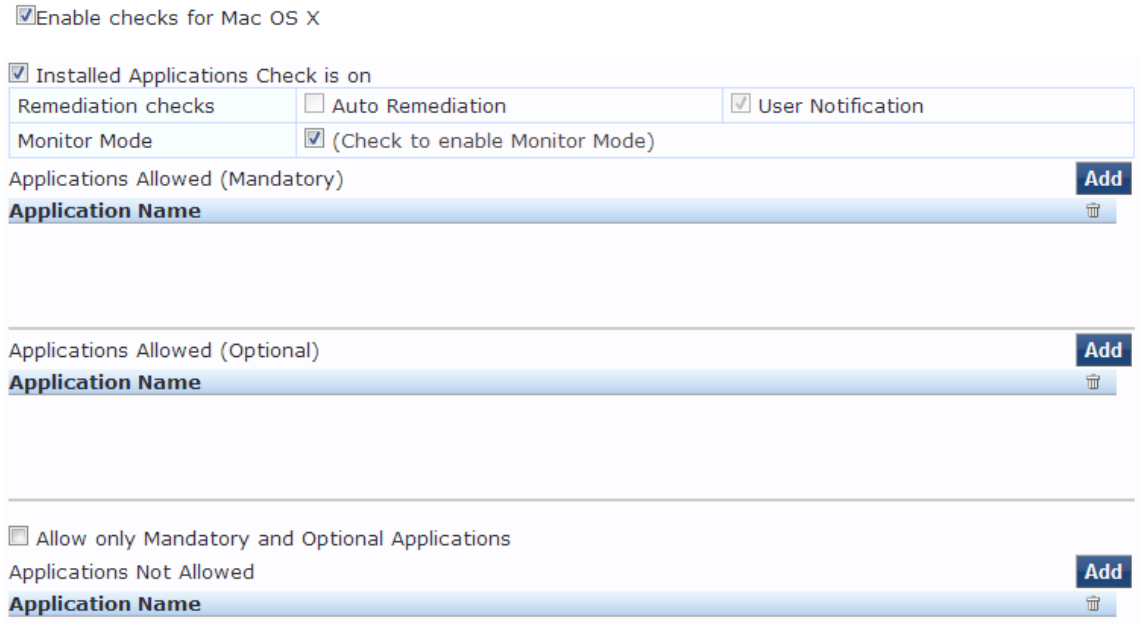
Installed Applications

The **Installed Applications** category groups classes that represent software-related objects. From the **Installed Applications** page, you can select the **Installed Applications Check is on** to specify information about which installed applications you want to monitor.

You can take the following actions:

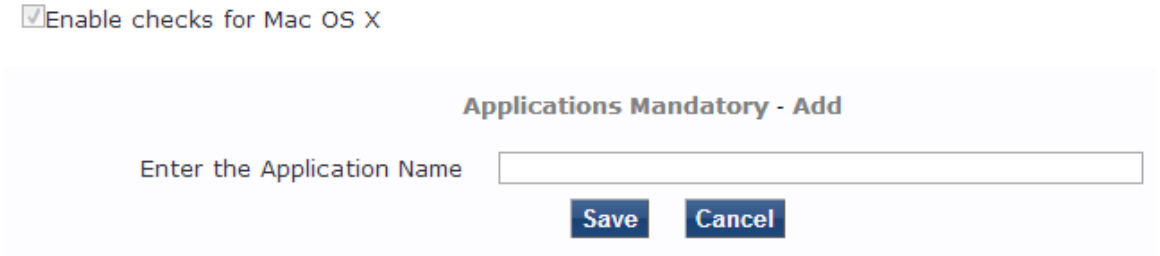
- Enable the auto remediation or user notification.
- Enable **Monitor Mode** to treat all the installed applications as always healthy.
- Specify installed applications to be monitored on a mandatory basis.
- Specify installed applications to be monitored on an optional basis.
- Specify installed applications that are never monitored.
- Specify that only the mandatory and optional applications to be monitored.

Figure 241: *Installed Applications Page*



Click **Add** in the **Installed Applications** page to configure the mandatory application that needs to be checked.

Figure 242: *Installed Applications Add Page*

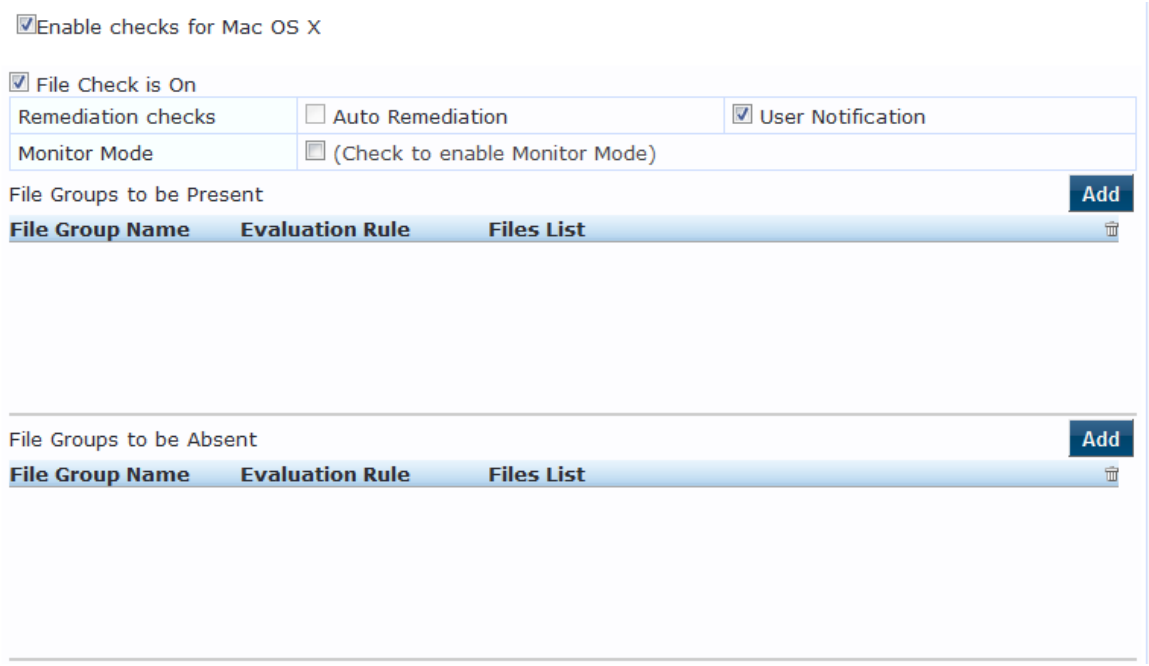


File Check

Use the **File Check** page to verify the group of files to present or absent. In the **File Check** page, you can turn on the file check and specify information about which the files you want to check.

The following figure is an example of the **File Check** health class configuration pop-up:

Figure 243: *Mac OS X File Check Health Class*



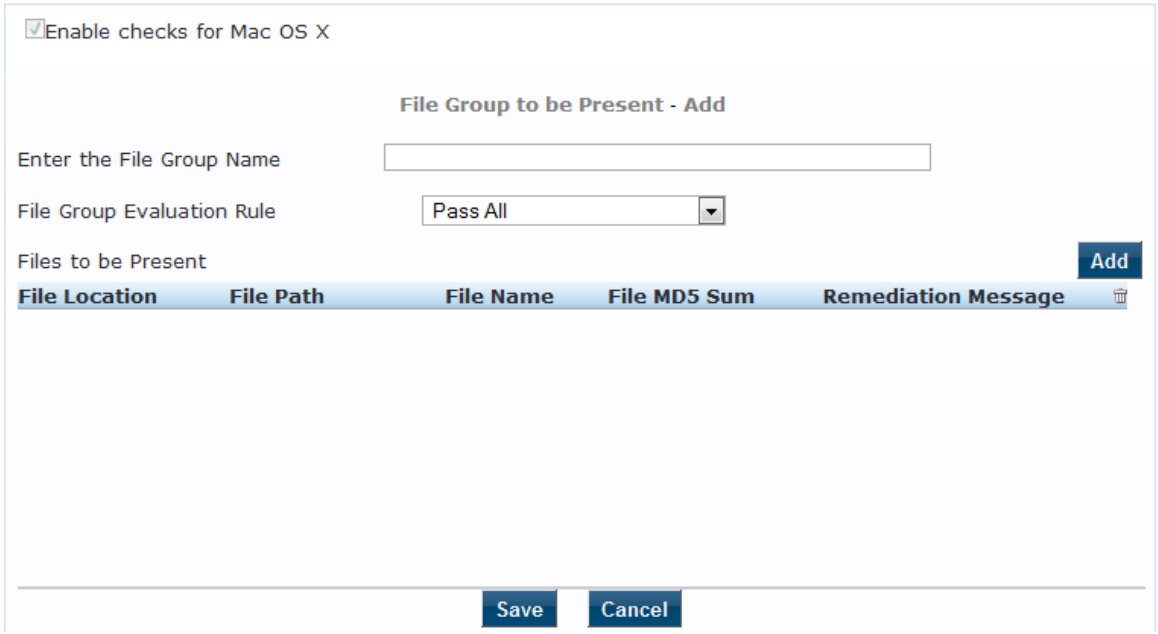
The following table describes the **File Check Configuration** parameters:

Table 145: *File Check Configuration Parameters*

Parameter	Description
Remediation checks	Auto-remediation for the **File Check** health class is not supported.
User Notification	A remediation message having a list of files to present/absent will be displayed to end user.
Monitor Mode	Enable **Monitor Mode** to treat all the file check health classes as always healthy.
File Groups to be Present	Click Add to add the files to be present in the **File Check** health class.
File Groups to be Absent	Click Add to add the files to be absent in the **File Check** health class.

Click **Add** to open the **File Group to be Present - Add** page in which you can configure the name of the file group and evaluation rule for the file group. The following figure displays the **File Group to be Present - Add** pop-up:

Figure 244: *MacOSX - File Group to be Present - Add Pop-up*



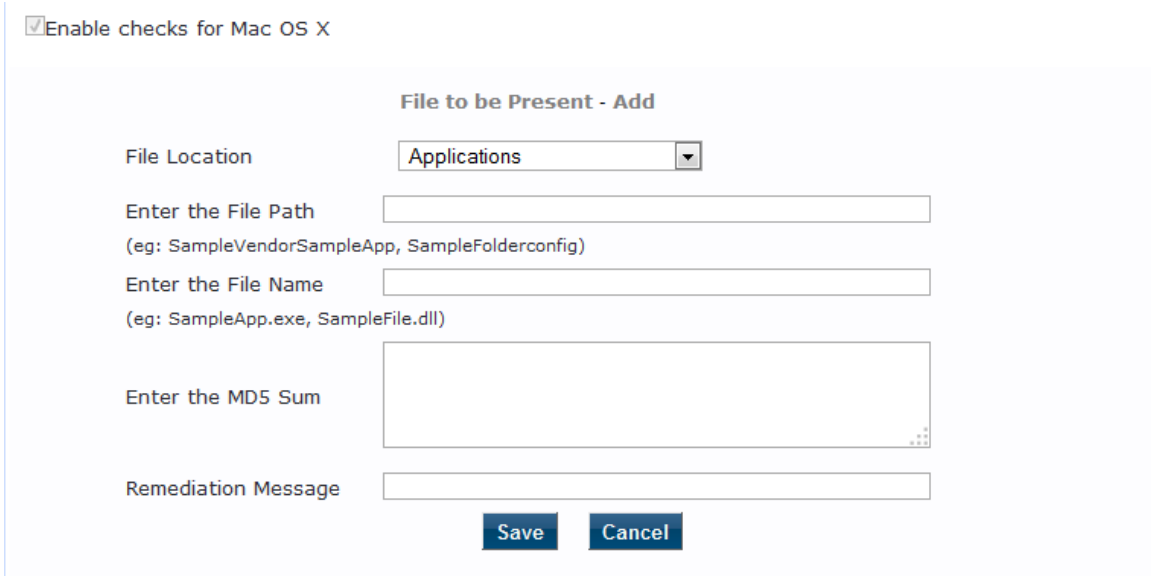
The following table describes the **File Group to be Present - Add** parameters:

Table 146: *File Group to be Present - Add Parameters*

Parameter	Description
Enter the File Group Name	Enter the name of the file group.
File Group Evaluation Rule	**Pass All** - Select this evaluation rule if you want the **File Check** health class to be deemed as 'healthy' only if all the configured file groups are present. **Pass Any One** - Select this evaluation rule if you want the **File Check** health class to be deemed as 'healthy' even any one of the configured file group is present.

Click **Add** from **File Groups to be Present** to configure the name of the file group and evaluation rule for the file group. The following figure displays the **File to be Present - Add** page:

Figure 245: *File to be Present - Add Pop-up*



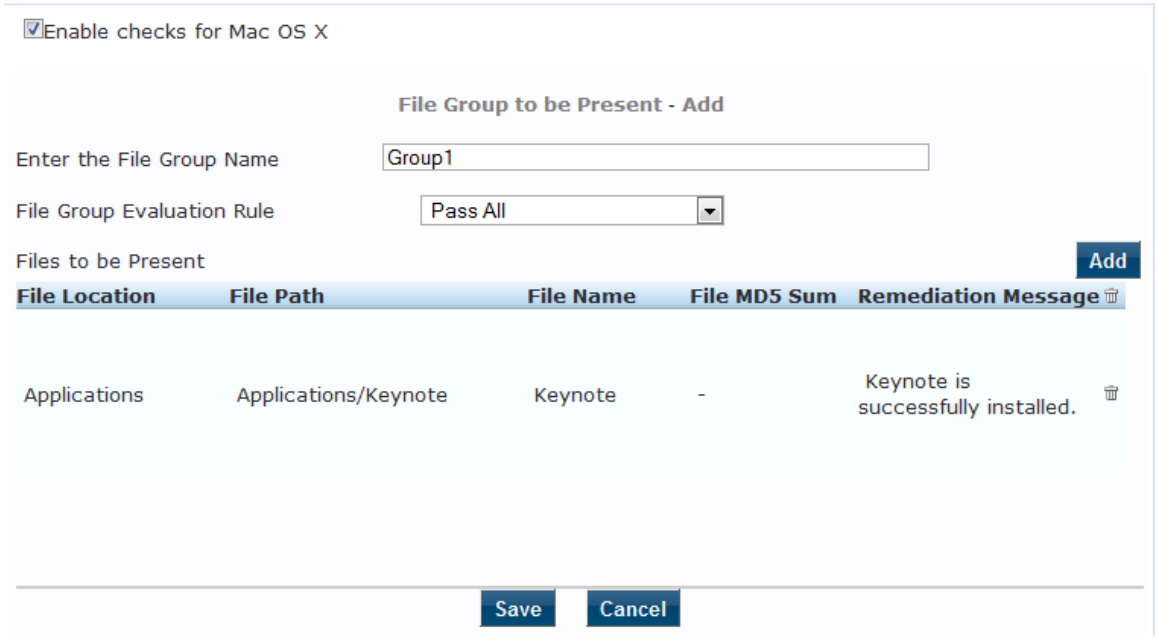
The following table describes the **File to be Present - Add** parameters:

Table 147: *File to be Present - Add Parameters*

Parameter	Description
File Location	Select any location of the file from the drop-down list: • Applications • UserBin • UserLocalBin • UserSBin • None
Enter the File Path	Enter the file path as described in the examples from the GUI.
Enter the File Name	Enter the name of the file.
Enter the MD5 Sum	Specifies one or more (comma separated) MD5 checksums of the process executable file. This field is optional.
Remediation Message	Specify the custom remediation message to be displayed to end users if **File check** is failed.

The parameters configured in the **File to be Present - Add** pop-up will reflect in the **File Groups to be Present** pop-up as described in the following figure:

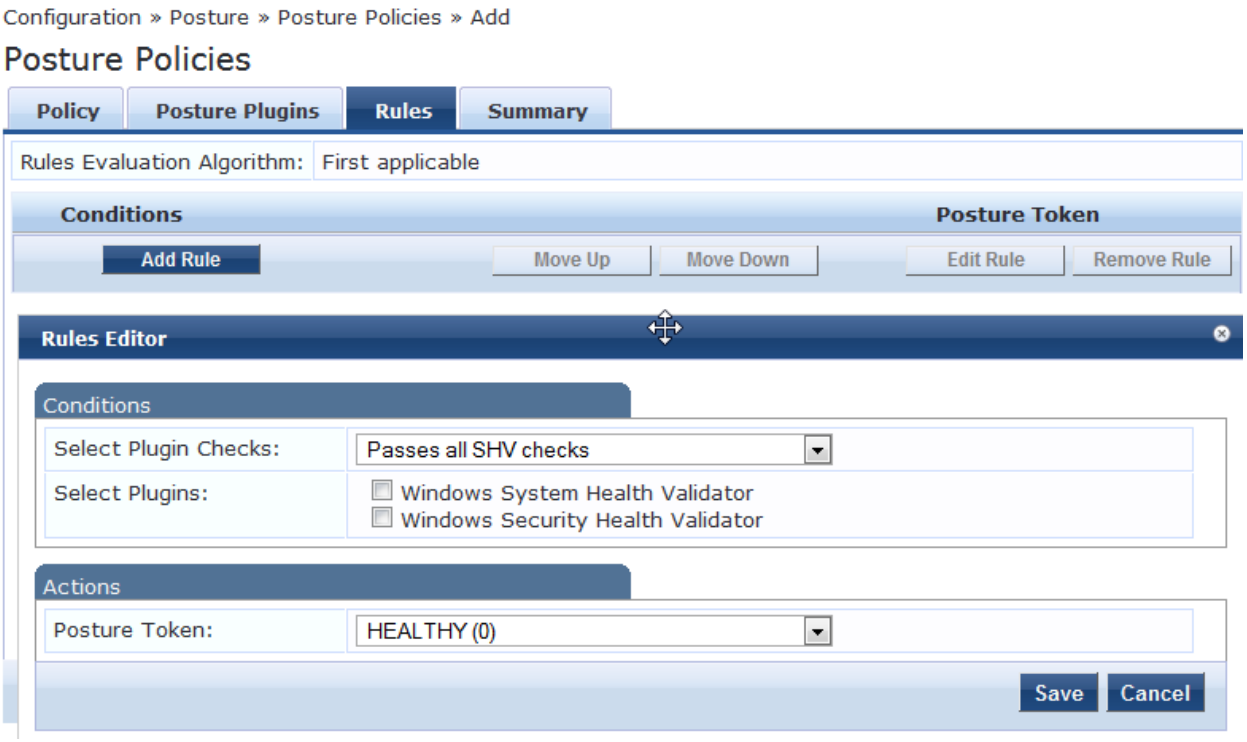
Figure 246: *File Group to be Present Pop-up*



Configuring Posture Policy Rules

Once you have defined the posture hosts, agents, and plugins, you must configure the rules for the posture policy. To configure posture policy rules, navigate to **Configuration > Posture > Posture Policies > Add**, and click the **Rules** tab on the **Posture Policies** window.

Figure 247: *Posture Policy Rules Tab and Rules Editor*



The following table describes the **Rules Editor** configuration parameters:

Table 148: *Posture Policy Rules Editor Parameters*

Parameter	Description
Select Plugin Checks	Click select one of the following plugin check types for System Health Validators (SHVs): • Passes all SHV checks • Passes one or more SHV checks • Fails all SHV checks • Fails one or more SHV checks
Select Plugins	Select the plug-in to which the plug-in checks should apply.
Posture Token	Select one of the following posture token types.

Configuring Posture for Services

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. To configure the posture for a service, navigate to the **Add Service** (**Configuration** > **Services** > **Add**) page. The **Posture** tab is not enabled by default. To enable posture checking for this service, select the **Posture Compliance** check box from the **More Options** field on the **Service** tab.

You can enable the posture checking for this kind of service, if you deploy any of the following:

- Policy Manager in a Microsoft Network Access Protection (NAP)
- Cisco Network Admission Control (NAC) Framework environment

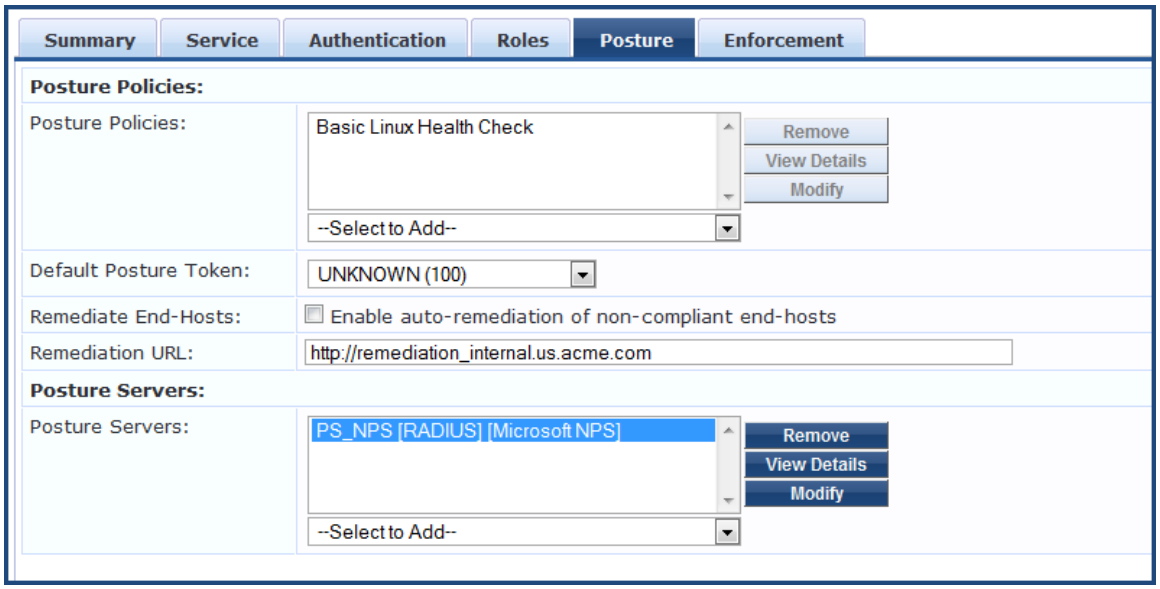
- Dell hosted captive portal that performs posture checks through a dissolvable agent

The following figure displays an example on how to configure a posture at the service level:

NOTE

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

Figure 248: *Posture Features at the Service Level*



You can configure the following components of a posture:

Table 149: *Posture Features at the Service Level*

Configurable Component	How to Configure
Sequence of Posture Policies	Select a policy, then select **Move Up**, **Move Down**, **Remove**, or **View Details**. • To add a previously configured policy, select from the **Select** drop-down list, then click **Add**. • To configure a new policy, click the **Add** link at the top-right corner of the **Configuration** > **Posture Policies** page. For more information, see Configuring Posture Policy Agents and Hosts on page 230. • To edit the selected posture policy, click **Modify**. For more information, see Configuring Posture Policy Agents and Hosts on page 230.
Default Posture Token	The default posture token is UNKNOWN (100). You can select the default posture token from the drop-down list.
Remediation End-Hosts	Select this check box to enable auto-remediation action on non-compliant endpoints.

Table 149: *Posture Features at the Service Level (Continued)*

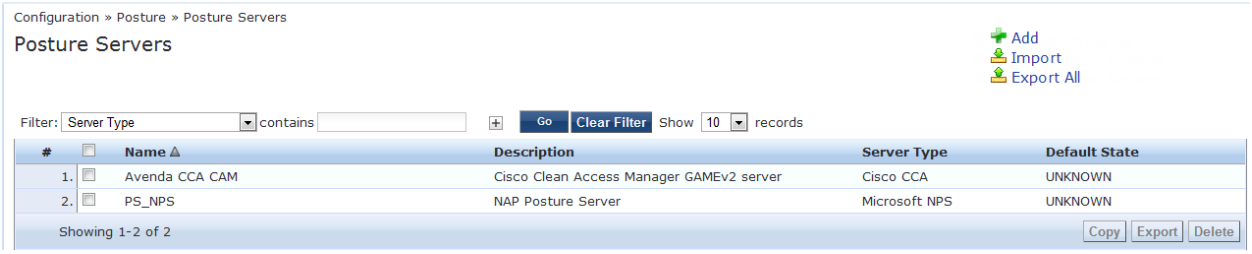
Configurable Component	How to Configure
Remediation URL	This URL defines where to send additional remediation information to endpoints.
Sequence of Posture Servers	Select a posture server, then select **Move Up**, **Move Down**, **Remove**, or **View Details**. • To add a previously configured posture server, select from the **Select** drop-down list, then click **Add.** • To configure a new posture server, click **Add** link at the top-right corner of the **Configuration** > **Posture Policies** page. For more information, see Configuring Posture Servers on page 282. • To edit the selected posture server, click **Modify**. For more information, see Configuring Posture Servers on page 282.
Enable auto-remediation of non-compliant end-hosts	Select the **Enable auto-remediation of non-compliant end-hosts** check box to enable the specified remediation server to enable auto-remediation. Remediation server is optional. A popup appears on the client box with the URL of the remediation server.

Configuring 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.

The following figure displays the **Posture Servers** page:

Figure 249: *Posture Servers Page*



You can configure a posture server in the following two different ways:

- Configure a posture server for new service using the **Add Service** wizard from the **Configuration > Services** page.
- Modify an existing posture server by selecting a server from the **Posture Servers** table on the **Configuration > Posture > Posture Servers** page.

The **Posture Servers** > **Add** page contains the following tabs:

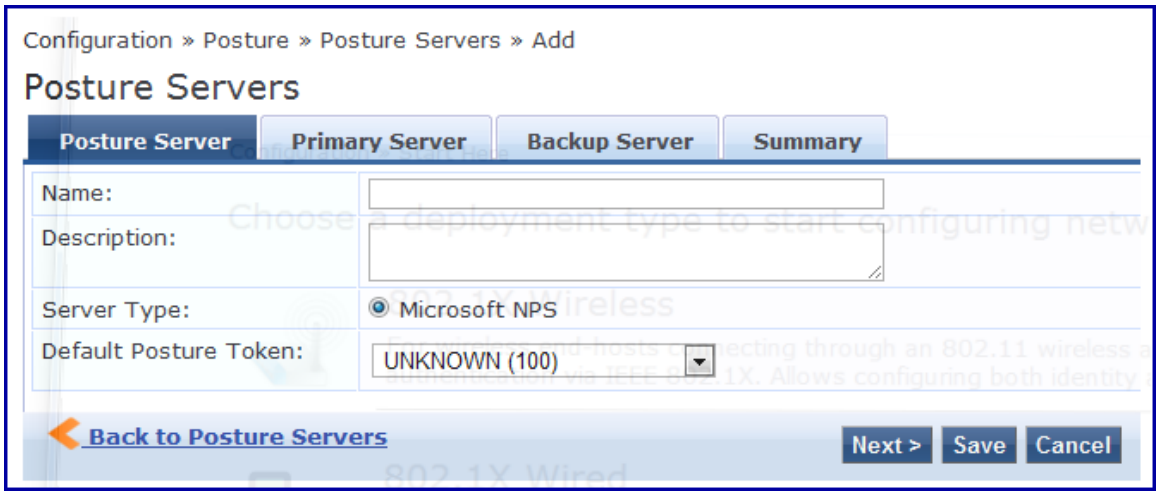
- Posture Server Tab on page 283
- Primary Server and Backup Server Tabs on page 284
- Primary Server and Backup Server Tabs on page 284
- Summary Tab

Posture Server Tab

When you click **Add Posture Server**, Policy Manager displays the **Posture Servers** configuration page. The tabs and fields that appear on the **Configuration** > **Posture** > **Posture Servers** > **Add** page may vary depending upon the protocol and credentials defined for that server.

The following figure displays the **Posture Server** tab:

Figure 250: *Posture Servers - Posture Server Tab*



The following table describes the **Posture Server** tab parameters:

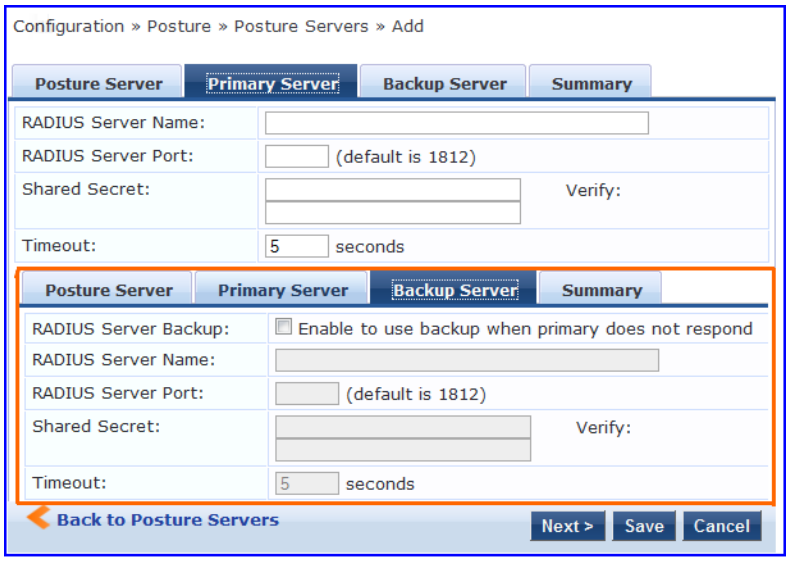
Table 150: *Posture Server Tab Parameters*

Parameter	Description
Name	Enter the name of the posture server.
Description	Enter the description that provides additional information about the posture server.
Server Type	Select the **Microsoft NPS** option when you want Policy Manager to have NAP Statement of Health (SoH) credentials evaluated by the Microsoft NPS server.
Default Posture Token	Click the **Default Posture Token** drop-down list and select the default status assigned to the server assigned if the server is unreachable or posture check is failed.

Primary Server and Backup Server Tabs

Use the **Primary Server** and **Backup Server** tabs to configure the RADIUS server name and port. The following figure displays the **Primary Server** and **Backup Server** tabs:

Figure 251: *Primary and Backup Server Tabs*



The following table describes the **Primary** and **Backup** server tabs parameters:

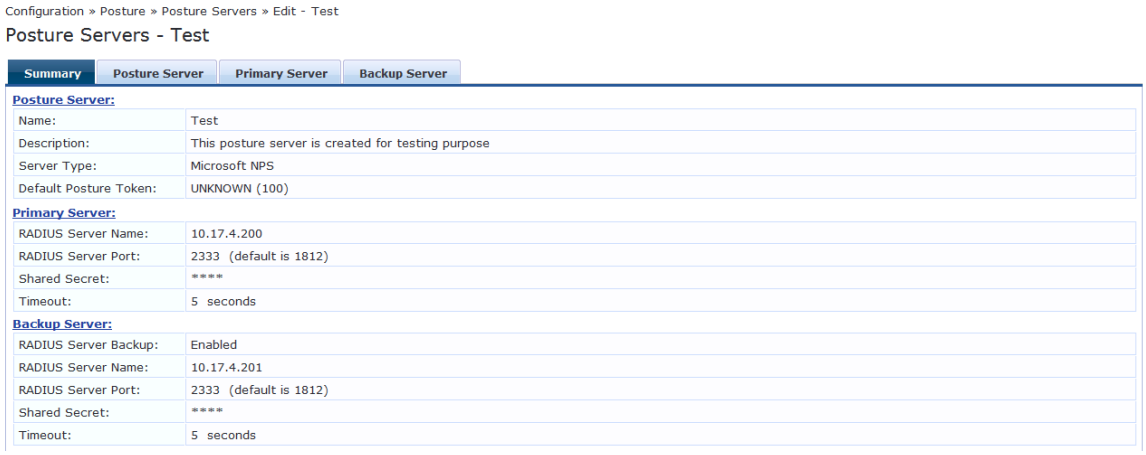
Table 151: *Primary and Backup Server Tabs Parameters*

Parameter	Description
RADIUS Server Backup	(Backup Server tab only) Select this option to enable failover to the backup server in the event that the primary server fails to respond.
RADIUS Server Name/Port	Specifiy the hostname or IP address of the server.
RADIUS ServerPort	Specify the RADIUS server UDP port. The default port is 1812.
Shared Secret	Enter the shared secret for RADIUS message exchange; the same secret has to be entered on the RADIUS server or Microsoft NPS server.
Timeout	Specify the number of seconds that must pass before Dell Networking W-ClearPass Policy Manager deems the connection dead. If a backup server is configured, Policy Manager will attempt to connect to the backup server after this timeout. For the backup server to be invoked on primary server failover, check the **Enable to use backup when primary does not respond** check box.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Posture Server**, **Primary Server**, and **Backup Server** tabs. The following figure displays the **Summary** tab:

Figure 252: *Posture Servers - Summary Tab*



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 with external audit servers, Policy Manager supports these servers externally.

For more information, see:

- Built-In Audit Servers on page 285
- Custom Audit Servers on page 288
- Post-Audit Rules on page 296

Built-In Audit Servers

When you configure an audit as part of a 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 from one of the following locations:
   - To configure an audit server for a new service (as part of the flow of the **Add Service** wizard), navigate to **Configuration > Services**. Select the **Add Services** link in the top-right corner. In the **Add Services** form, select the **Audit** tab.

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

   - To modify an existing audit server, navigate to **Configuration > Posture > Audit Servers**, then select an audit server from the list.
2. Configure auditing and complete the fields in the **Audit** tab as described in Figure 253:

Figure 253: *Audit Tab*

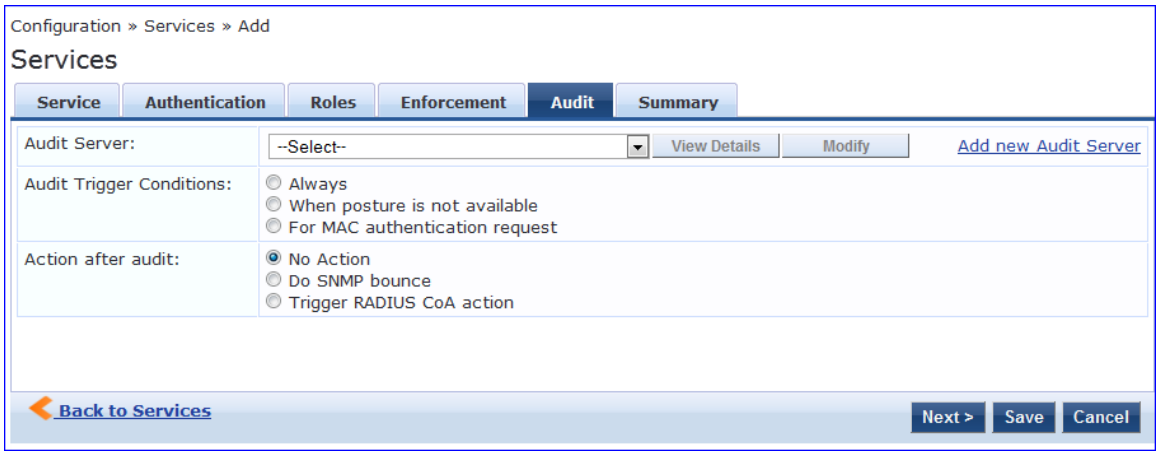


Table 152: *Audit tab*

Parameter	Description
Audit Server	Select a built-in server profile from the list: • The [Nessus Server] performs vulnerability scanning and returns a Healthy/Quarantine result. • The [Nmap Audit] performs network port scans. The health evaluation always returns a **Healthy** result. The port scan gathers attributes that allow determination of role(s) through post-audit rules. For Policy Manager to trigger an audit on an end-host, it needs to get the IP address of the end-host. The IP address of the end-host is not available at the time of initial authentication for 802.1X and MAC authentication requests. Policy Manager has a built-in DHCP snooping service that can examine DHCP request and response packets to derive the IP address of the end-host. For this to work, you need to use this service, Policy Manager must be configured as a DHCP "IP Helper" on your router/switch in addition to your main DHCP server. Refer to your switch documentation for "IP Helper" configuration. To audit devices that have a static IP address assigned, it is recommended to create a static binding between the MAC and IP address of the endpoint in your DHCP server. Refer to your DHCP server documentation for configuring such static bindings. **NOTE:** Policy Manager does not issue the IP address; it only examines the DHCP traffic to derive the IP address of the end-host.

Audit Trigger Conditions	Select from the following audit trigger conditions:
	• **Always**: Always perform an audit.
	• **When posture is not available**: Perform audit only when posture credentials are not available in the request.
	• **For MAC Authentication Request**: If you select this option, then Policy Manager presents the following three additional settings:
	  ▪ **For known end-hosts only:** For example, select this option when you want to reject unknown end-hosts and to audit known clients. Known end-hosts are defined as clients that are found in the authentication source(s) associated with this service.
	  ▪ **For unknown end-hosts only:** For example, select this option 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 end-hosts that are not found in any of the authentication sources associated with this service.
	  ▪ **For all end-hosts:** For both known and unknown end-hosts.

Action after audit	Select an **Action after audit**. Performing audit on a client is an asynchronous task, which means the audit can be performed only after the MAC authentication request is completed and the client has acquired an IP address through DHCP. Once the audit results are available, there should be a way for Policy Manager to re-apply policies on the network device. This can be accomplished in one of the following ways: • **No Action:** The audit will not apply policies on the network device after this audit. • **Do SNMP bounce:** This option will bounce the switch port or force an 802.1X reauthentication (both done using SNMP). Bouncing the port triggers a new 802.1X/MAC authentication request by the client. If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager. • **Trigger RADIUS CoA action:** This option sends a RADIUS CoA command to the network device.

Modifying Built-In Audit Servers

To reconfigure a default Policy Manager audit servers:

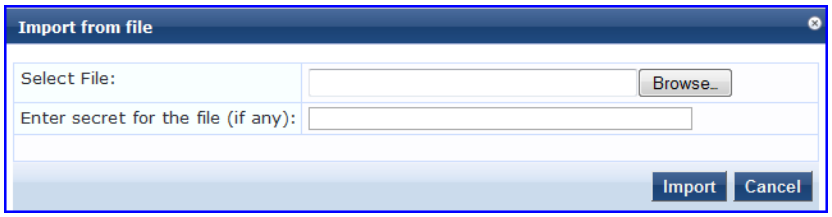
1. Open the audit server profile. Navigate to **Configuration > Posture > Audit Servers**, then select an audit server from the list of available servers.

Figure 254: *Audit Servers Listing*

2. Modify the profile, plugins, and/or preferences.
   - In the **Audit** tab, you can modify the **In Progress Posture Status** and **Default Posture Status**.
   - If you selected a NESSUS Server, then the **Primary/Backup Server** tabs allow you to specify a scan profile. In addition, when you add a new scan profile, you can select plugins and preferences for the profile. Refer to Nessus Scan Profiles on page 290 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 255: *Upload Nessus Plugins Popup*



   - In the **Rules** tab, you can create post-audit rules for determining role based on identity attributes discovered by the audit. Refer to Post-Audit Rules on page 296.

Custom Audit Servers

For enterprises with existing audit server infrastructure or preferring custom audit servers, Policy Manager supports NESSUS (2.x and 3.x) and NMAP scans using the NMAP plug-in on these external Nessus servers.

To configure a custom audit server:

1. Open the **Audit** page.
   - To configure an audit server for a new service (as part of the flow of the **Add Service** wizard), navigate to **Configuration > Posture > Audit Servers**, then click **Add Audit Server**.
   - To modify an existing audit server, navigate to **Configuration > Posture > Audit Server**, and select an audit server.
2. Add a custom audit server
   - When you click **Add Audit Server**, Policy Manager displays the **Add Audit Server** page. Configuration settings vary depending on audit server type:
     - Nessus Audit Server on page 289

- NMAP Audit Server on page 294

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 256: *Nessus Audit Server - Audit Tab*

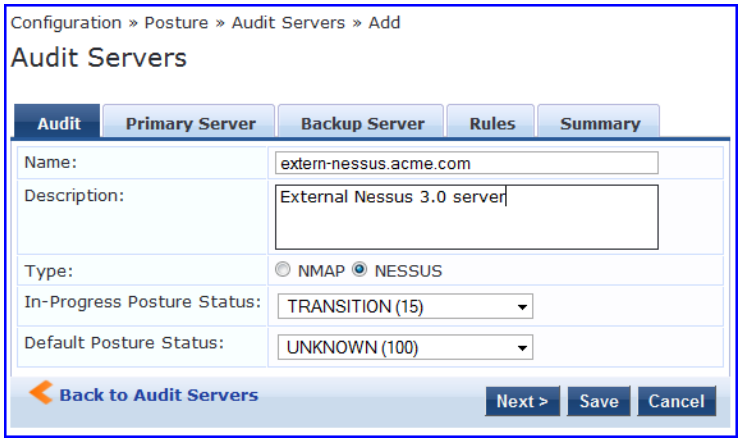


Table 153: *Nessus Audit Server - Audit Tab*

Parameter	Description
Name	Specify the name of the audit server.
Description	Enter the description that provides additional information about the audit server.
Type	Specify the type of audit server from NMAP or NESSUS.
In-Progress Posture Status	Specifies the posture status during audit. Select the status from the drop-down list.
Default Posture Status	Specifies the posture status if evaluation does not return a condition/action match. Select the status from the drop-down list.

The **Primary Server** and **Backup Server** tabs specify connection information for the NESSUS audit server.

Figure 257: *Nessus Audit Server - Primary and Backup Tabs*

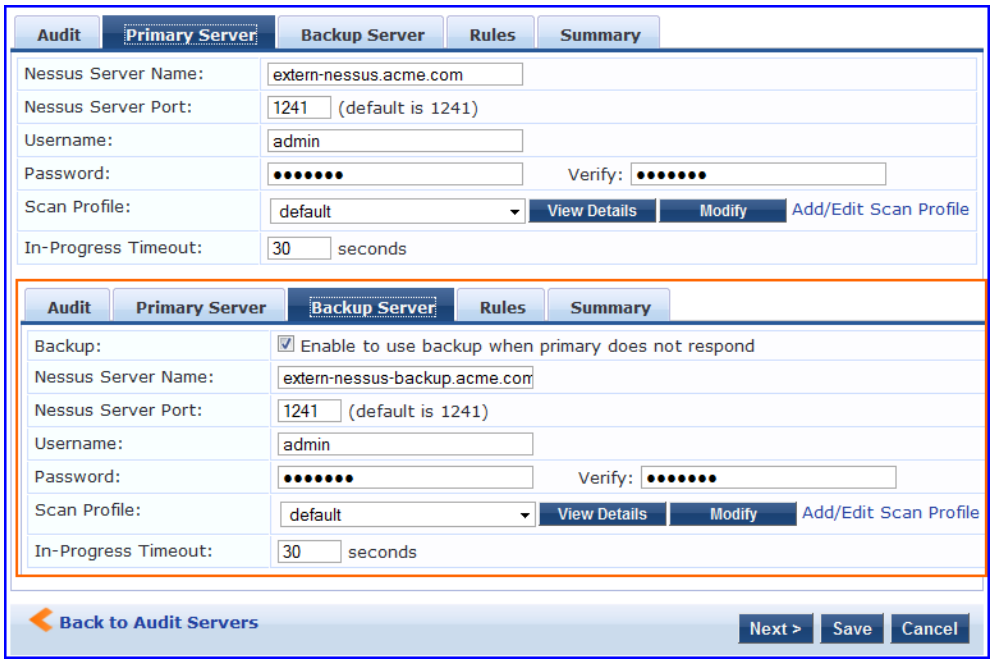


Table 154: *Nessus Audit Server - Primary and Backup Server Tabs*

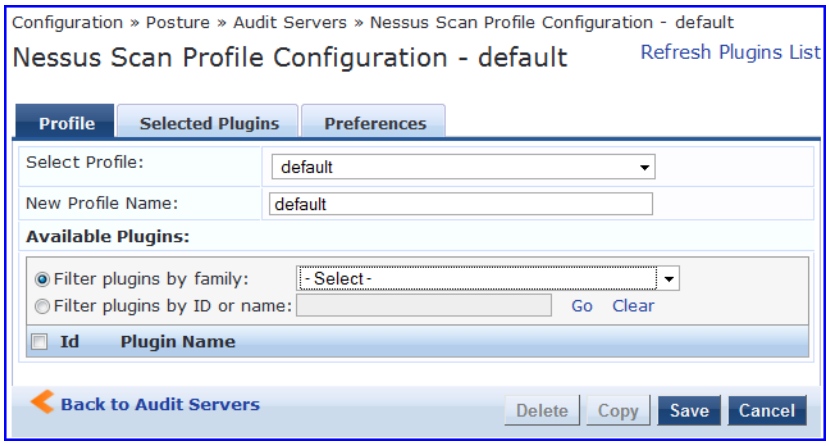
Parameter	Description
Server Name and Port/ Username/ Password	Specifies the standard NESSUS server configuration fields. **NOTE:** For the backup server to be invoked on primary server failover, check the **Enable to use backup when primary does not respond** check box.
Scan Profile	You can accept the default scan profile or select **Add/Edit Scan Profile** to create other profiles and add them to the scan profile list. Refer to Nessus Scan Profiles on page 290.

The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role. For more information, refer to Post-Audit Rules on page 296.

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.

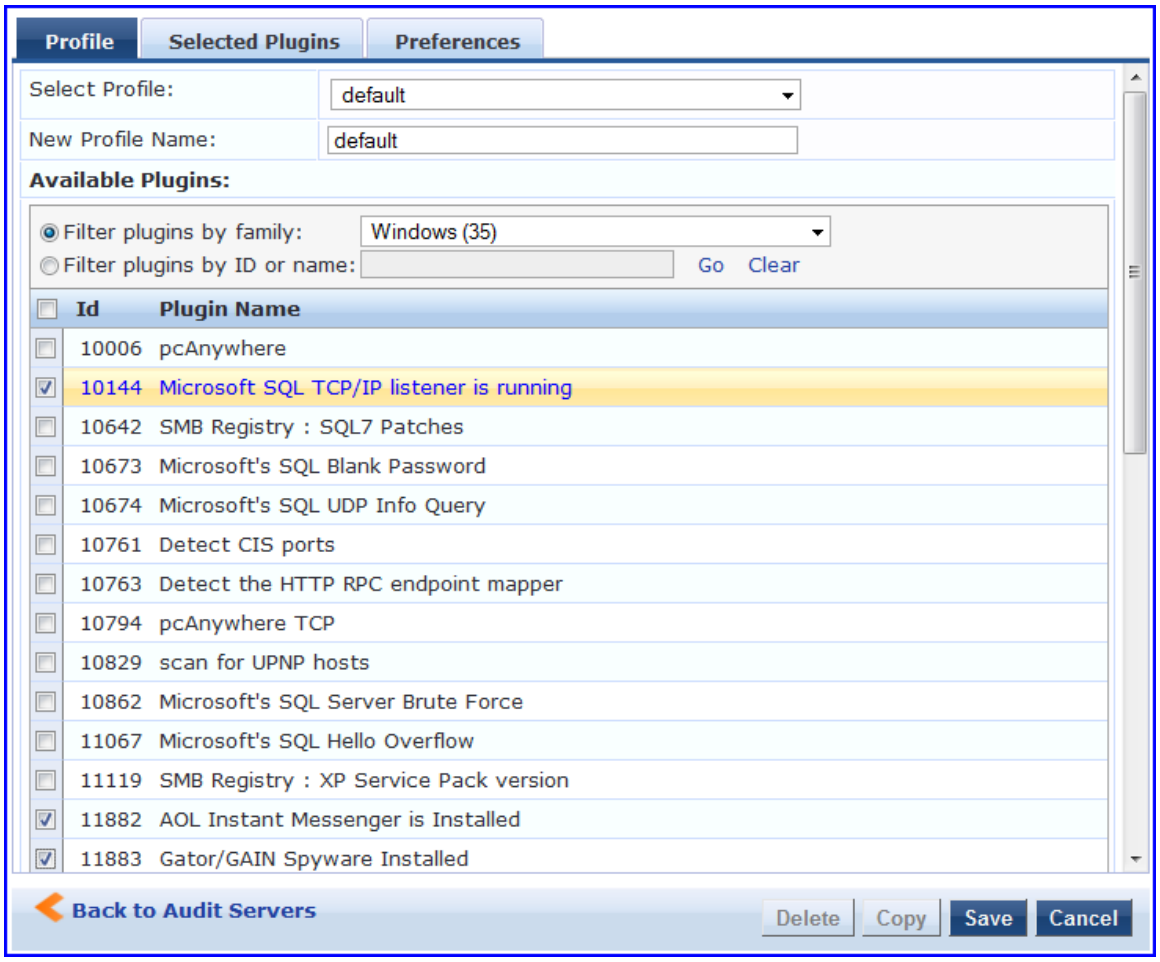
Figure 258: *Nessus Scan Profile Configuration Page*



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:

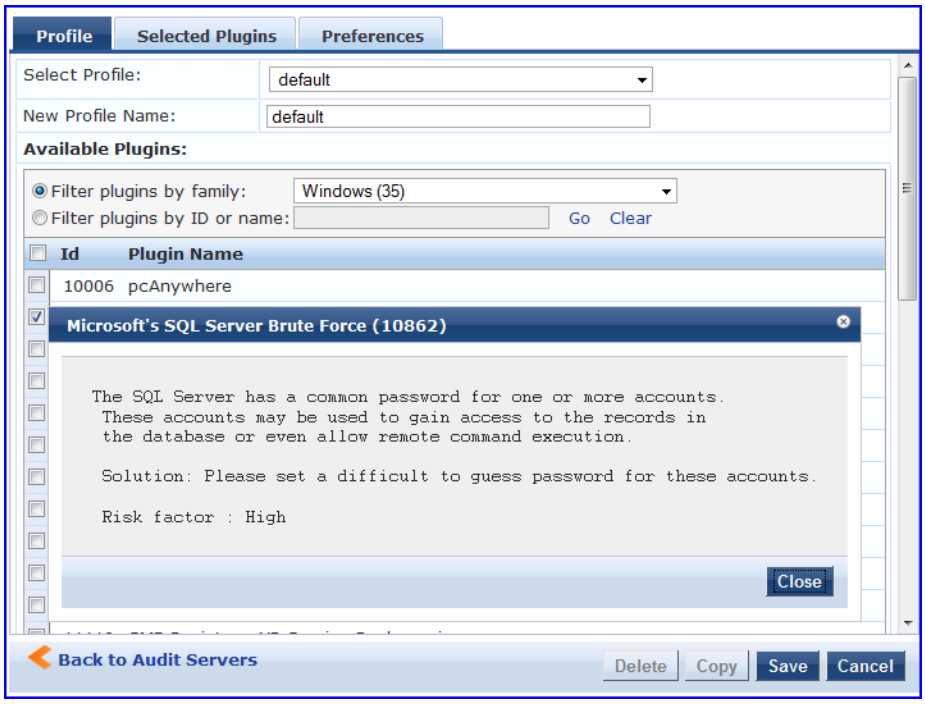
- The **Profile** tab identifies the profile and provides a mechanism for selection of plugins:
  - From the **Filter plugins by family** drop-down list, select a family to display all available member plugins in the list below. You may also enter the name of a plugin in **Filter plugins by ID** or name 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 259: *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 260: *Nessus Scan Profile Configuration Profile Tab - Plugin Synopsis*



NOTE

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

Figure 261: *Nessus Scan Profile Configuration - Selected Plugins Tab*

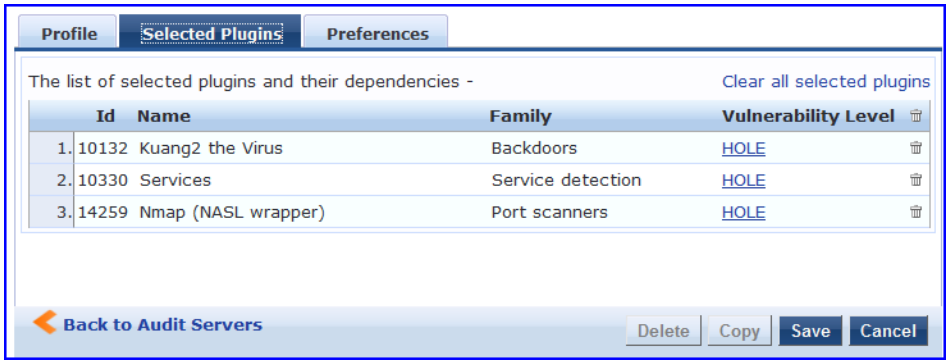


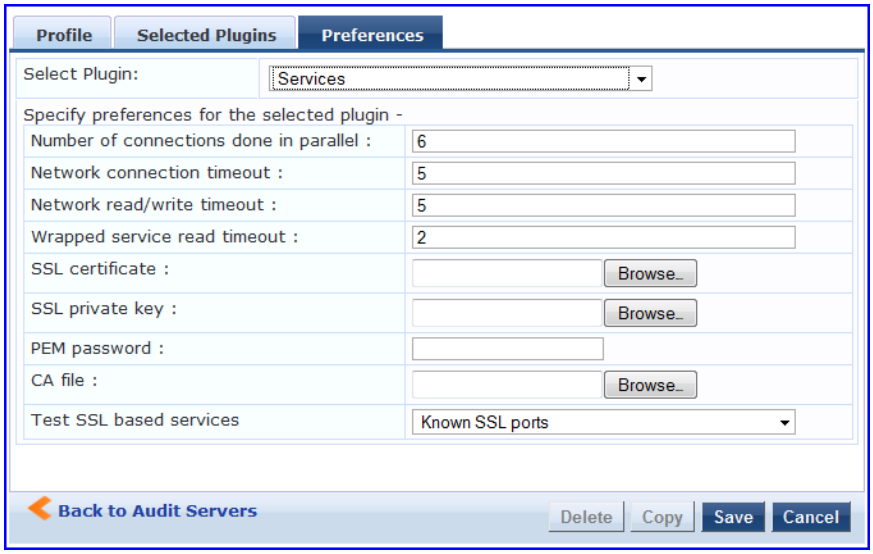
Figure 262: *Nessus Scan Profile Configuration Selected Plugins Tab - Vulnerability Level*

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 263: *Nessus Scan Profile Configuration - Preferences Tab*



After saving the profile, plugin, and preference information for your new (or modified) plugin, you can go to the **Primary/Backup Servers** tabs and select it from the **Scan Profile** drop-down list.

NMAP Audit Server

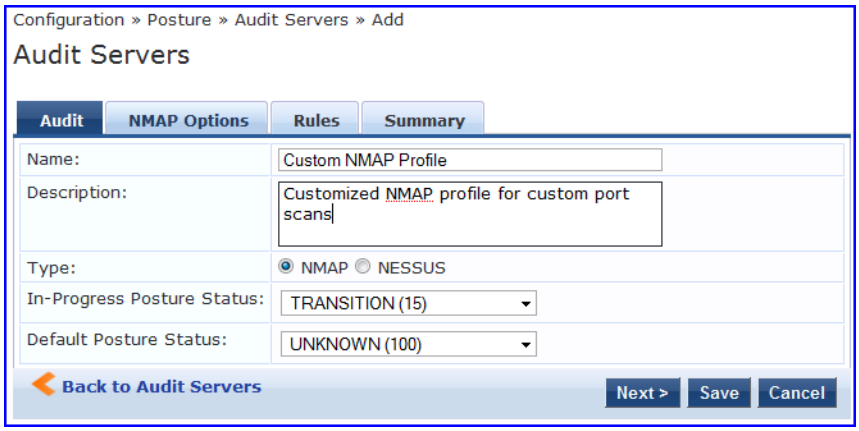
To create an NMAP audit server, Navigate to **Configuration** > **Posture** > **Audit Servers** page and click **Add**. From the **Audit** tab, select the **NMAP** radio button in the **Type** field. Policy Manager uses the NMAP audit server interface exclusively for network port scans. The health evaluation always returns the **Healthy** status. The port scan gathers attributes that allow determination of role(s) through post-audit rules. The **NMAP** audit server has the following tabs:

- Audit
- NMAP Options
- Rules
- Summary

Audit Tab

You can use the **Audit** tab to identify the server and define configuration details. Figure 264 shows an example of the **Audit** tab:

Figure 264: *Audit Tab - NMAP Audit Server*



The following table describes the parameters configured in the **Audit** tab:

Table 155: *Audit Tab Parameters*

Parameter	Description
Name	Enter the name of the NMAP audit server.
Description	Enter the description of the NMAP audit server that provides some additional information.
Type	Specify the type of an NMAP audit server. In this context, select **NMAP**.
In Progress Posture Status	Posture status during audit. Select a status from the drop-down list.
Default Posture Status	Select the posture status if evaluation does not return a condition/action match. Select a status from the drop-down list.

NMAP Options Tab

You can use the **NMAP Options** tab to specify scan configuration.

Figure 265: *NMAP Options Tab*

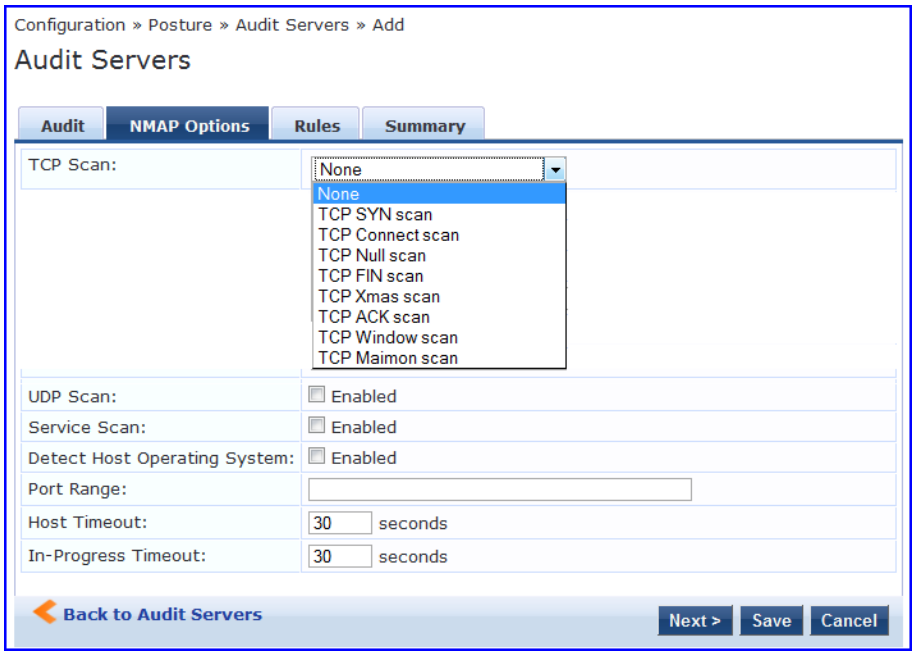


Table 156: *NMAP Options Tab*

Parameter	Description
TCP Scan	To specify a TCP scan, select from the **TCP Scan** drop-down list. Refer to NMAP documentation for more information on these options. NMAP option --scanflags.
UDP Scan	To enable, check the **UDP Scan** check box. NMAP option -sU.
Service Scan	To enable, check the **Service Scan** check box. NMAP option -sV.
Detect Host Operating System	To enable, check the **Detect Host Operating System** check box. NMAP option -A.
Port Range/ Host Timeout/ In Progress Timeout	• Port Range - Range of ports to scan. NMAP option -p. • Host Timeout - Give up on target host after this long. NMAP option --host-timeout • In Progress Timeout - How long to wait before polling for NMAP results.

The **Rules** tab provides specifies rules for post-audit evaluation of the request to assign a role. Refer to Post-Audit Rules on page 296.

Post-Audit Rules

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

Figure 266: *All Audit Server Configurations - Rules Tab*

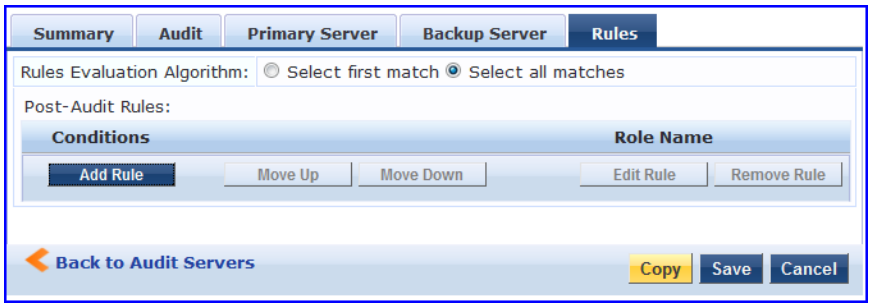


Table 157: *All Audit Server Configurations - Rules Tab*

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

Figure 267: *All Audit Server Configurations - Rules Editor*

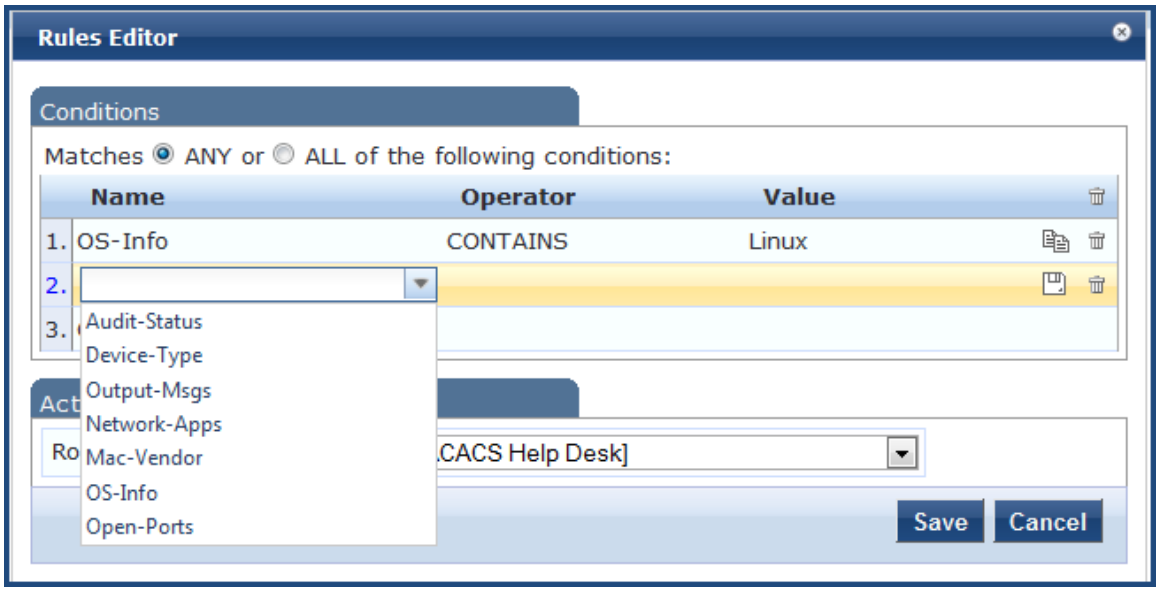


Table 158: *All Audit Server Configurations - Rules Editor*

Parameter	Description
Conditions	The **Conditions** list includes five dictionaries: Audit-Status, Device-Type, Output-Msgs, Mac-Vendor, Network-Apps, Open-Ports, and OS-Info. Refer to Namespaces on page 601.
Actions	The **Actions** list includes the names of the roles configured in Policy Manager.
Save	To commit a Condition/Action pairing, click **Save**.

Policy Manager controls network access by sending a set of access-control attributes to the request-originating Network Access Device (NAD). Policy Manager sends these attributes by evaluating an enforcement policy associated with the service. Each enforcement policy contains a rule or set of rules for matching conditions (role, posture, and time) to actions (enforcement profiles). Commonly used enforcement profiles include attributes for VLAN, Filter ID, Downloadable ACL, and Proxy ACL. For a general overview of network access enforcement policies, see Enforcement Architecture and Flow on page 31.

This chapter describes the following topics:

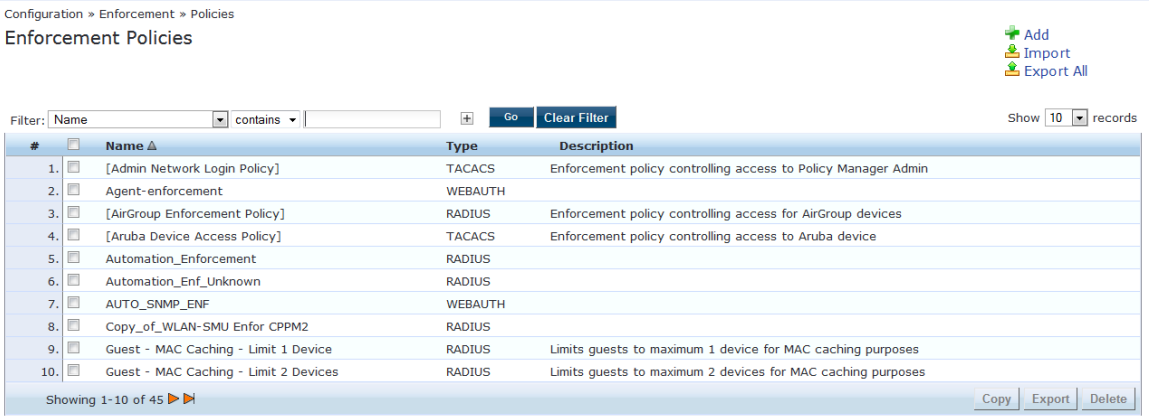
Configuring Enforcement Policies

One and only one enforcement policy can be associated with each service. Enforcement policies can be added in one of two ways:

- From the **Configuration > Enforcement > Enforcement Policies**.
- From the **Configuration > Services** page as part of the flow of the **Add Service** wizard.

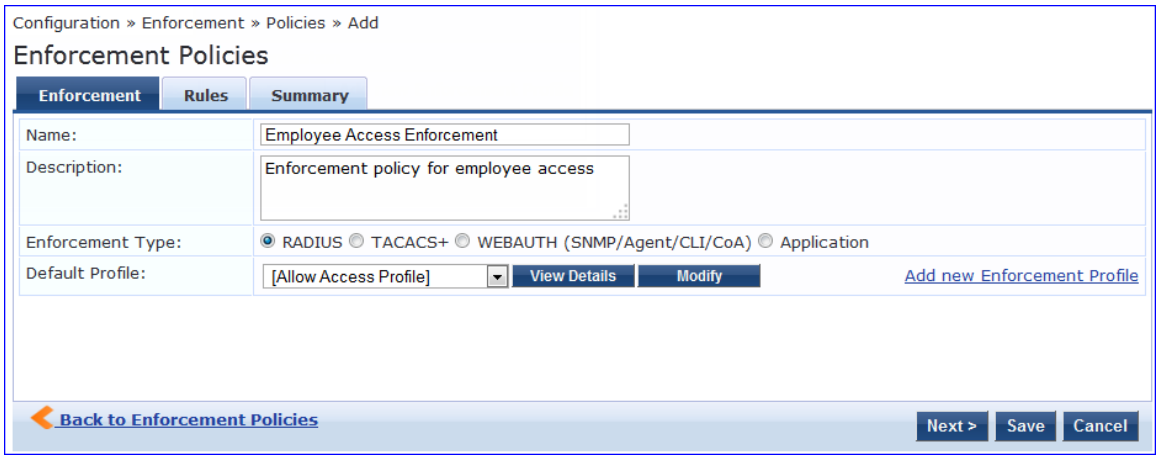
The following figure displays the **Enforcement Policies** page:

Figure 268: *Enforcement Policies Listing Page*



Click **Add Enforcement Policy** to open the **Add Enforcement Policy** wizard:

Figure 269: *Add Enforcement Policy - Enforcement tab*



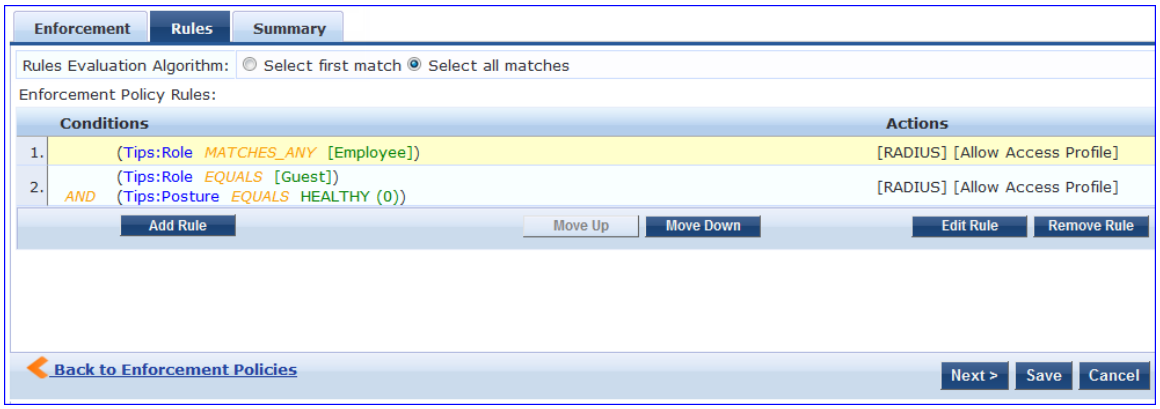
The following table describes the **Add Enforcement Policy - Enforcement** tab parameters:

Table 159: *Add Enforcement Policy - Enforcement Tab Parameters*

Parameter	Description
Name/Description	Freeform label and description.
Type	Select: **RADIUS, TACACS+, WebAuth (SNMP/CLI)/CoA** or **Application**. Based on this selection, the **Default Profile** list shows the right type of enforcement profiles in the drop-down list (See Below). **NOTE:** Web-based Authentication or WebAuth (HTTPS) is the mechanism used by authentications performed via a browser, and authentications performed via Dell W-OnGuard. Both SNMP and CLI (SSH/Telnet) based Enforcement Profiles can be sent to the network device based on the type of device and the use case.
Default Profile	An enforcement policy applies conditions (roles, health and time attributes) against specific values associated with those attributes to determine the enforcement profile. If none of the rules matches, Policy Manager applies the default profile. Click **Add new Enforcement Profile** to add a new profile (This is integrated into the flow. After you create a profile, Policy Manager brings you back to the current tab.)

In the **Rules** tab, click **New Rule** to display the **Rules Editor**:

Figure 270: *Add Enforcement Policy (Rules Tab)*



The following table describes the **Add Enforcement Policy - Rules** tab parameters:

Table 160: *Add Enforcement Policy (Rules tab)*

Field	Description
Add/Edit Rule	Bring up the rules editor to add/edit a rule.
Move Up/Down	Reorder the rules in the enforcement policy.
Remove Rule	Remove a rule.

Table 161: *Add Enforcement Policy (Rules Editor)*

Field	Description
Conditions/Enforcement Profiles	Select conditions for this rule. For each condition, select a matching action (enforcement profile). **NOTE:** A condition in an enforcement policy rule can contain attributes from the following namespaces: Tips:Role, Tips:Posture, and Date. **NOTE:** The value field for the Tips:Role attribute can be a role defined in Policy Manager, or a role fetched from the authorization source. (Refer to see how **Enable as Role** can be turned on for a fetched attribute). Role names fetched from the authorization source can be entered freeform in value field. To commit the rule, click **Save**.
Enforcement Profiles	If the rule conditions match, attributes from the selected enforcement profiles are sent to Network Access Device. If a rule matches and there are multiple enforcement profiles, the enforcement profile disambiguation rules apply. Refer to Configuring Enforcement Profiles on page 301 for a list of the default profiles.

Configuring Enforcement Profiles

You can configure Policy Manager enforcement profiles globally, but they must be referenced to an enforcement policy that is associated with a service.

For information about configuring individual enforcement profiles, see:

- Agent Enforcement on page 303
- Aruba Downloadable Role Enforcement on page 307
- Aruba RADIUS Enforcement on page 317
- Cisco Downloadable ACL Enforcement on page 319
- Cisco Web Authentication Enforcement on page 321
- ClearPass Entity Update Enforcement on page 323
- CLI Based Enforcement on page 325
- Filter ID Based Enforcement on page 327
- Generic Application Enforcement on page 329
- HTTP Based Enforcement on page 331
- RADIUS Based Enforcement on page 332
- RADIUS Change of Authorization (CoA) on page 334

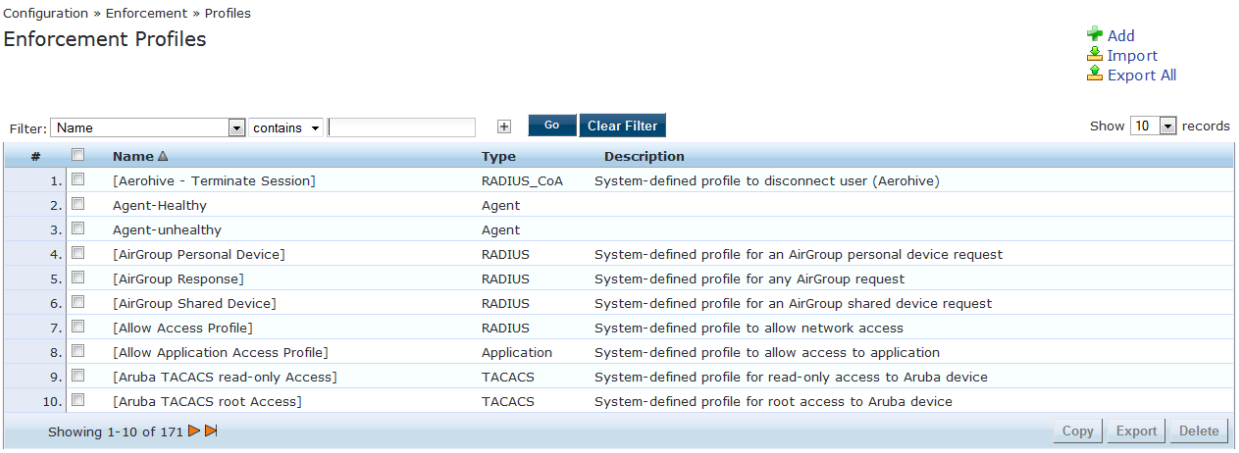
- Session Restrictions Enforcement on page 338
- SNMP Based Enforcement on page 340
- TACACS+ Based Enforcement on page 341
- VLAN Enforcement on page 343

To configure an enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.
2. Click **Add** at the top-right corner of the **Enforcement Policies** page and use the wizard. You can modify an existing enforcement profile directly from **Configuration > Enforcement > Profiles** page and then click a name in the **Enforcement Profile** listing.

The following figure displays the **Enforcement Profiles** page:

Figure 271: *Enforcement Profiles Page*



The following table describes the default profiles pre-packaged with Policy Manager:

Table 162: *Default Enforcement Profiles*

Profile	Available for the following Enforcement Types
[Aerohive - Terminate Session]	RADIUS_CoA
[AirGroup Personal Device]	RADIUS
[AirGroup Response]	RADIUS
[AirGroup Shared Device]	RADIUS
[Allow Access Profile]	RADIUS
[Allow Application Access Profile]	Application
[Aruba TACACS read-only Access]	TACACS
[Aruba TACACS root Access]	TACACS
[Aruba Terminate Session]	RADIUS_CoA

Table 162: *Default Enforcement Profiles (Continued)*

Profile	Available for the following Enforcement Types
[Cisco - Bounce-Host-Port]	RADIUS_CoA
[Cisco - Disable Host-Port]	RADIUS_CoA
[Cisco - Reauthenticate-Session]	RADIUS_CoA
[Cisco - Terminate-Session]	RADIUS_CoA
[Deny Access Profile]	RADIUS
[Deny Application Access Profile]	Application
[Drop Access Profile]	RADIUS
[Handle AirGroup Time Sharing]	HTTP
[HP - Terminate Session]	RADIUS_CoA
[Juniper Terminate Session]	RADIUS_CoA
[Motorola - Terminate Session]	RADIUS_CoA
[Operator Login - Admin Users]	Application
[Operator Login - Local Users]	Application
[TACACS API Admin]	TACACS
[TACACS Deny Profile]	TACACS
[TACACS Help Desk]	TACACS
[TACACS Network Admin]	TACACS
[TACACS Read-only Admin]	TACACS
[TACACS Receptionist]	TACACS
[TACACS Super Admin]	TACACS
[Trapeze - Terminate Session]	RADIUS_CoA
[Update Endpoint Known]	Post-Authentication

Agent Enforcement

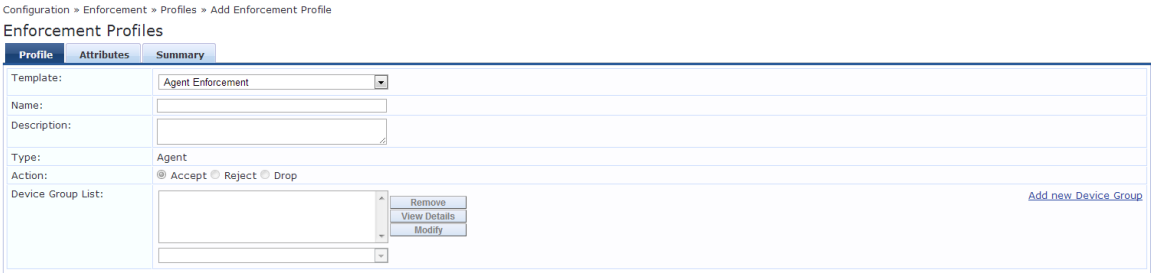
Use this page to configure profile and attribute parameters for the **Agent Enforcement** profile. The **Agent Enforcement** profile contains the following configuration tabs:

- Profile Tab on page 304
- Attributes Tab on page 305
- Summary Tab on page 307

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Agent Enforcement - Profile** tab:

Figure 272: *Agent Enforcement - Profile Tab*



The following table describes the **Agent Enforcement - Profile** tab parameters:

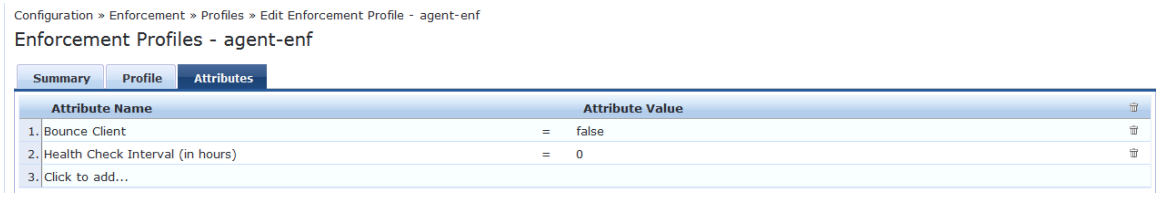
Table 163: *Add Agent Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select **Agent Enforcement**.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration** > **Enforcement** > **Profiles** page.
Description	Enter a description of the profile. This description is displayed in the **Description** column on the **Configuration** > **Enforcement** > **Profiles** page.
Type	This field is populated automatically.
Action	By default, this field is disabled. Enabled only when RADIUS type is selected. Click to Accept, Deny, or Drop to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new device group, click the **Add new Device Group** link. For more information, see Adding and Modifying Device Groups on page 353.

Attributes Tab

Use the **Attributes** tab to configure the attribute name and attribute value. The following figure displays the **Agent Enforcement- Attributes** tab:

Figure 273: *Agent Enforcement - Attributes Tab*



The following table describes the **Agent Enforcement - Attributes** tab parameters:

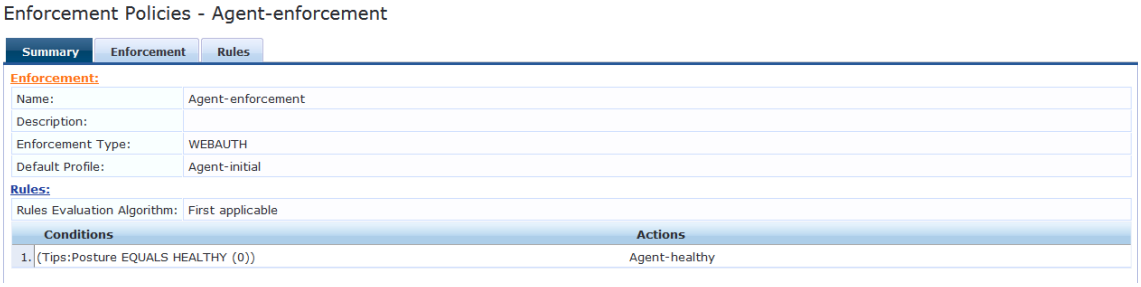
Table 164: *Agent Enforcement - Attributes Tab Parameters*

Attribute	Parameter
Attribute Name	Select one of the following attribute names: • **Bounce Client -** Set the value to **true** by checking the box to terminate the network connection. • **Message -** Enter the message that needs to be notified on the endpoint. • **Enable to hide Retry button** - Set the value to **true** to hide the **Retry** button in the OnGuard Agent. • **Enable to hide Logout button** - Set the value to **true** to hide the **Logout** button in the OnGuard Agent. • **Health Check Interval (in hours)** - Specify the health check interval value in hours for different Agent Enforcement Profiles for different users. The allowed range is of 0 – 1000 hours. For example, you can create Student-Enforcement-Profile with a value of 8 hours and Staff-Enforcement-Profile with a value of 48 hours. The value configured in the **Health Check Quiet Period (in hours)** field in the **Agent Enforcement Attribute** tab takes precedence over the value configured in the **Global Agent Settings** field. If both the values are configured, then the **Agent Enforcement Attribute** value is used by OnGuard Agent. The value of the **Policy result cache timeout** (path: Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > General tab) field must be greater than the highest value of all the **Health Check Interval (in hours)** field values. For example, if you have created the profiles Student-Enforcement-Profile and Staff-Enforcement-Profile with health check interval configured, then the value of the **Policy result cache timeout** field must be greater than the highest value of **Health Check Quiet Period (in hours)** configured in the following fields: ▪ Global Agent Settings ▪ Student-Enforcement-Profile ▪ Staff-Enforcement-Profile Note the following information when you set the **OnGuard Health Check Interval** parameter: ▪ You can set this parameter if OnGuard mode is set to health only. ▪ This parameter is valid only for wired and wireless interface types. ▪ This parameter is not applicable for the OnGuard Dissolvable Agent, VPN, and other interface types. • **Session Timeout (in seconds) -** Configure the agent session timeout interval to re-evaluate the system health again. OnGuard triggers auto-remediation using this value to enable or disable AV-RTP status check on endpoint. Agent re-authentication is determined based on session-time out value. You can specify the session timeout interval from 60 – 600 seconds. Setting the lower value for session timeout interval results numerous authentication requests in **Access Tracker** page. The default value is 0.
Attribute Value	Set the value depends on the selected **Attribute Name**.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs. The following figure displays the **Agent Enforcement - Summary** tab:

Figure 274: *Agent Enforcement - Summary Tab*



Aruba Downloadable Role Enforcement

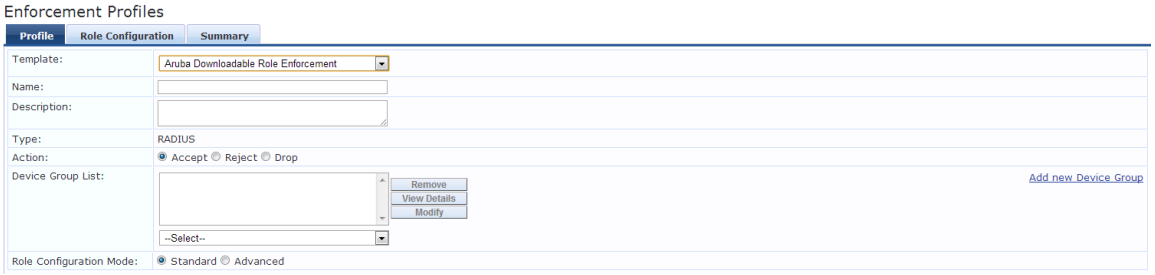
Use this page to configure profile and role configuration attributes for the **Aruba Downloadable Role Enforcement** profile. The **Aruba Downloadable Role Enforcement** profile contains the following tabs:

- Profile Tab on page 307
- Role Configuration Tab on page 308
- Summary Tab on page 317

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Aruba Downloadable Role Enforcement - Profile** tab:

Figure 275: *Aruba Downloadable Role Enforcement - Profile Tab*



The following table describes the **Aruba Downloadable Role Enforcement - Profile** parameters:

Table 165: *Aruba Downloadable Role Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Aruba Downloadable Role Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. This description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.

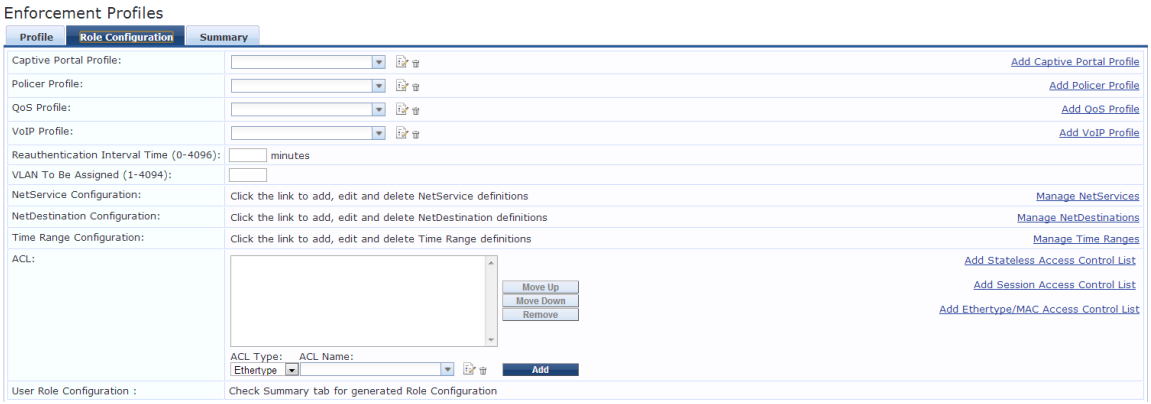
Table 165: *Aruba Downloadable Role Enforcement - Profile Tab Parameters (Continued)*

Parameter	Description
Type	Specifies the type of authentication. In this context, RADIUS. This field is automatically populated.
Action	Click **Accept**, **Reject**, or **Drop** to define the action taken on the request. The default action is **Accept**.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups)** page. After adding one or more device group(s), you can select a group and perform one of the following actions: • Click **Remove** to delete the selected device group list entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new device group, click the **Add new Device Group** link. For more information, see Adding and Modifying Device Groups on page 353.

Role Configuration Tab

The fields on the **Role Configuration** tab require you to select a link to launch a new page where you set role configuration attributes. For example, adding a **Captive Portal** profile. The following figure displays the **Aruba Downloadable Role Enforcement Role Configuration** tab:

Figure 276: *Aruba Downloadable Role Enforcement Role - Configuration Tab*



The following table describes the **Role Configuration - Attributes** parameters:

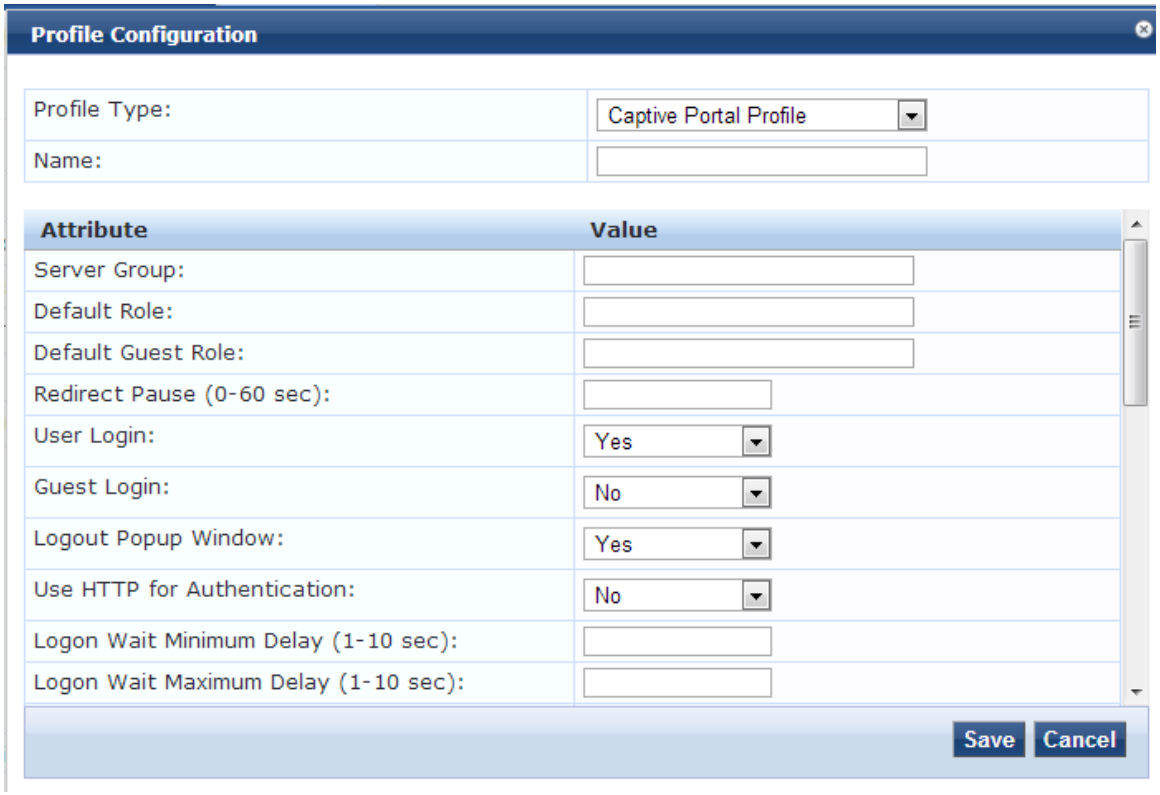
Table 166: *Role Configuration - Attributes Page Parameters*

Parameters	Configuration
Captive Portal Profile	Select the captive portal profile from the drop-down list if already configured. Click **Add Captive Portal Profile** link to add a new captive portal profile. For more information, seeCaptive Portal Profile on page 310.
Policer Profile	Select the policer profile from the drop-down list if already configured. Click **Add Policer Profile** link to add a new policer profile. For more information, see Policer Profile on page 311.
QoS Profile	Select the QoS profile from the drop-down list if already configured. Click **Add QoS Profile** link to add a new QoS profile. For more information, see QOs Profile on page 312.
VoIP Profile	Select the VoIP profile from the drop-down list if already configured. Click **Add VoIP Profile** link to add a new VoIP profile. For more information, see VoIP Profile on page 313.
Reauthentication Interval Time (0-4096)	Enter the number of minutes between reauthentication intervals. You can select the range between 0 to 4096 minutes.
VLAN To Be Assigned (1-4904)	Enter a number between 1 and 4094 that defines when the VLAN is to be assigned.
NetService Configuration	Select the **Manage NetServices** link to add, edit, and delete the NetService definitions.
NetDestination Configuration	Select the **Manage NetDestinations** link to add, edit, and delete the NetDestinations definitions.
Time Range Configuration	Select the **Manage Time Ranges** link to add, edit, and delete time range definitions.
NAT Pool Configuration	Select the **Manage NAT Pool** link to add, edit and delete NAT Pool definitions.
ACL Type	Select from the following ACL types: • Ethertype • MAC • Session • Stateless
ACL Name	Click the name of the ACL type. Click **Add** to move the **ACL Name** to the **ACL** field. Click **Move Up**, **Move Down**, or **Remove** to modify the names in the ACL list.
User Role Configuration	Check the **Summary** tab for generated role configuration.

Captive Portal Profile

Click the **Add Captive Portal Profile** link. Enter a name of the profile and configure the required attributes. The following figure displays the **Add Captive Portal Profile** pop-up:

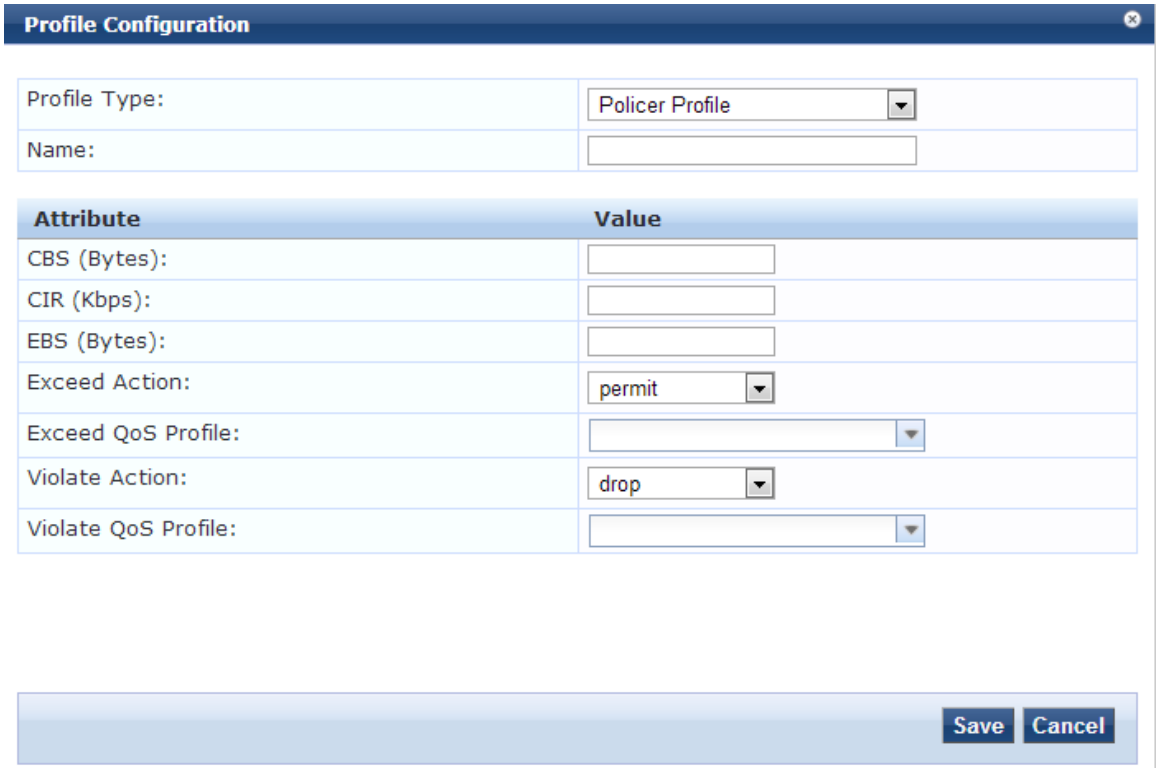
Figure 277: *Add Captive Portal Profile Pop-up*



Policer Profile

Click the **Add Policer Profile** link. Enter a name of the profile and configure the required attributes. The following figure displays the **Add Policer Profile** pop-up:

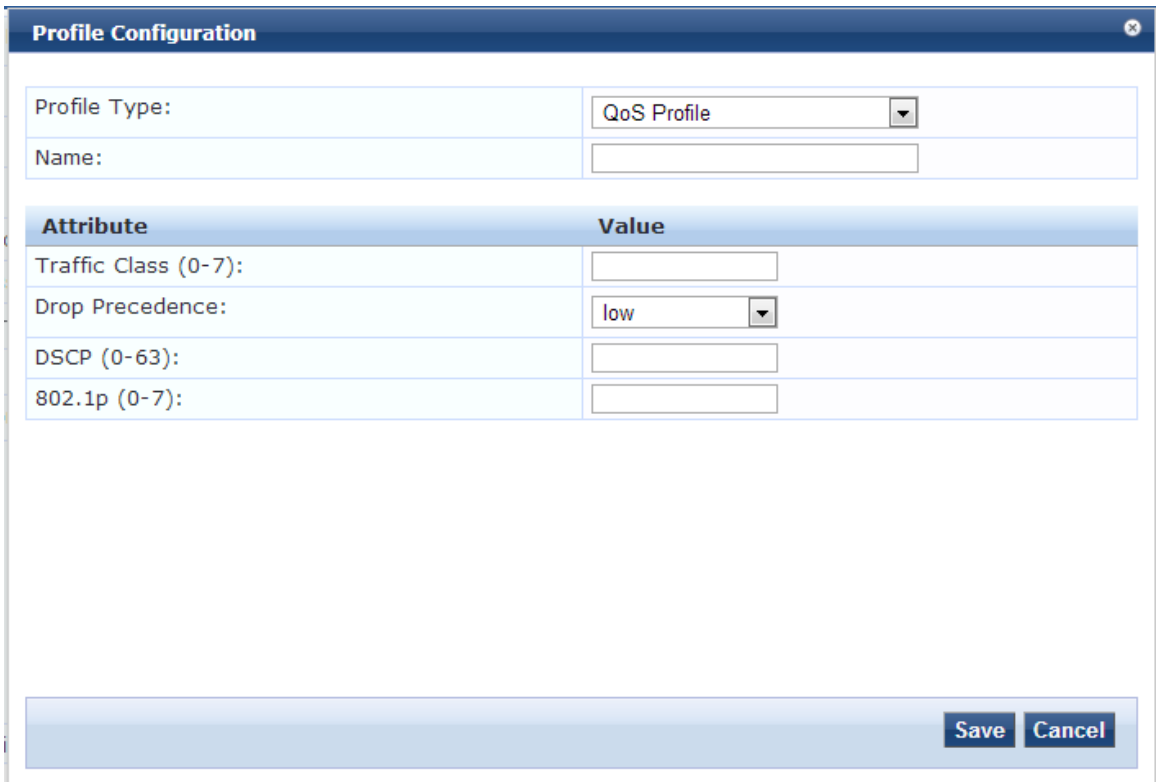
Figure 278: *Add Policer Profile Pop-up*



QOs Profile

Click the **Add QoS Profile** link. Enter a name of the profile and configure the required attributes. The following figure displays the **Add QoS Profile** pop-up:

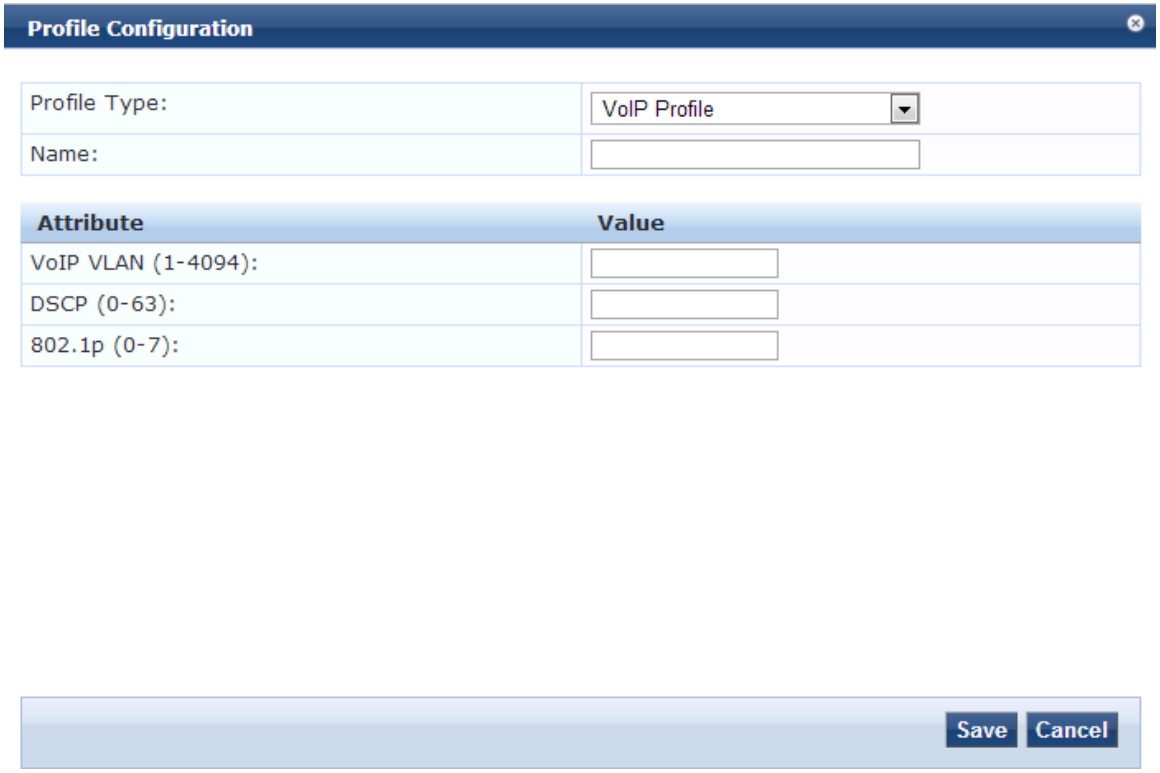
Figure 279: *Add QosProfle Pop-up*



VoIP Profile

Click the **Add VoIP Profile** link. Enter a name for the profile and configure the required attributes. The following figure displays the **Add VoIP Profile** pop-up:

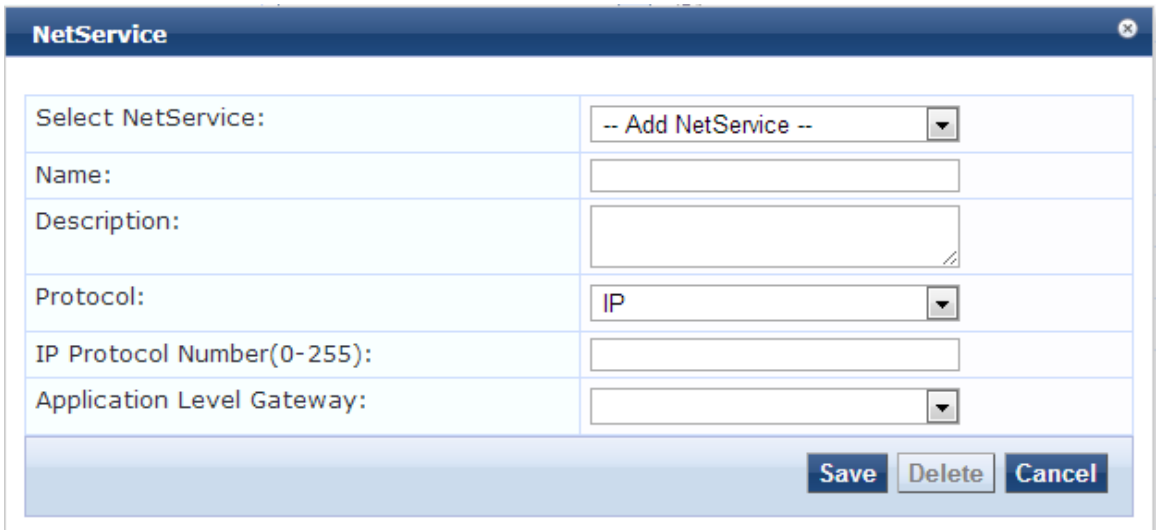
Figure 280: *Add VoIP Profile Pop-up*



NetService Configuration

Click the **Manage NetServices** link and configure the required attributes. The following figure displays the **Manage NetServices** pop-up:

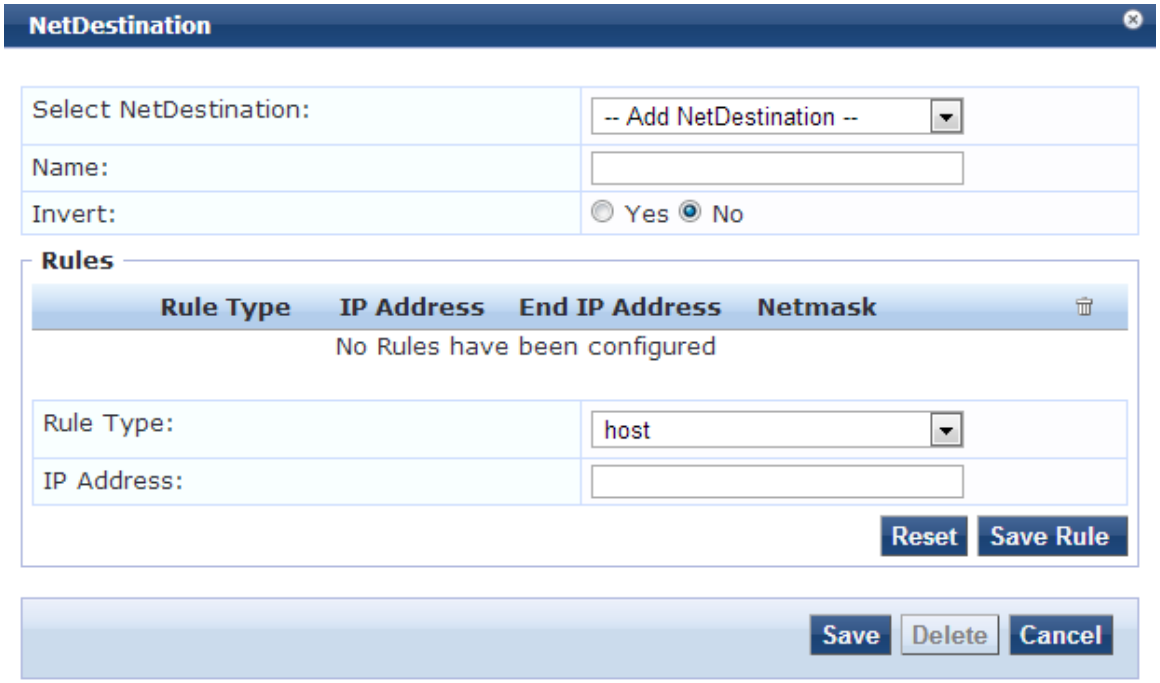
Figure 281: *Manage NetServices Pop-up*



NetDestination Configuration

Click the **Manage NetDestinations** link and configure the required attributes. The following figure displays the **Manage NetDestinations** pop-up:

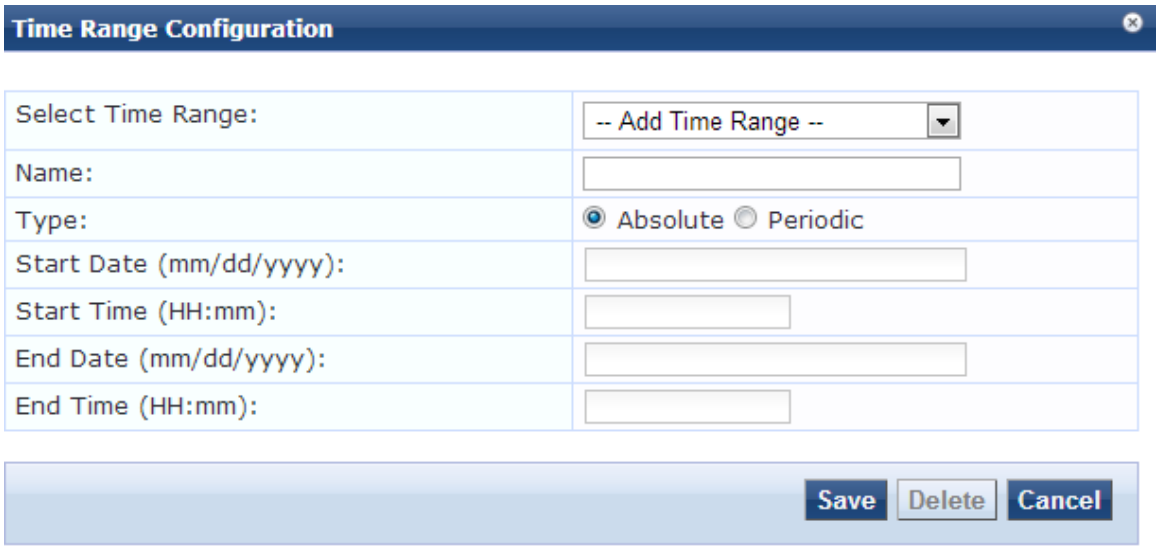
Figure 282: *Manage NetDestinations Pop-up*



Time Range Configuration

Click the **Manage Time Ranges** link and configure the required attributes. The following figure displays the **Manage Time Ranges** pop-up:

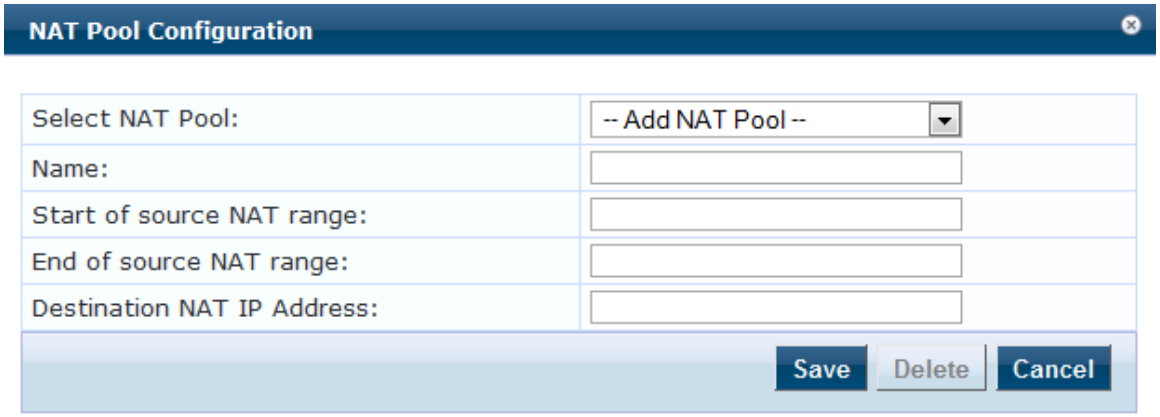
Figure 283: *Time Range Configuration Pop-up*



NAT Pool Configuration

Use the **NAT Pool Configuration** page to configure the start and end of the source NAT range and associate them with session ACLs. The following figure displays the **NAT Pool Configuration** pop-up:

Figure 284: *NAT Pool Configuration Pop-up*

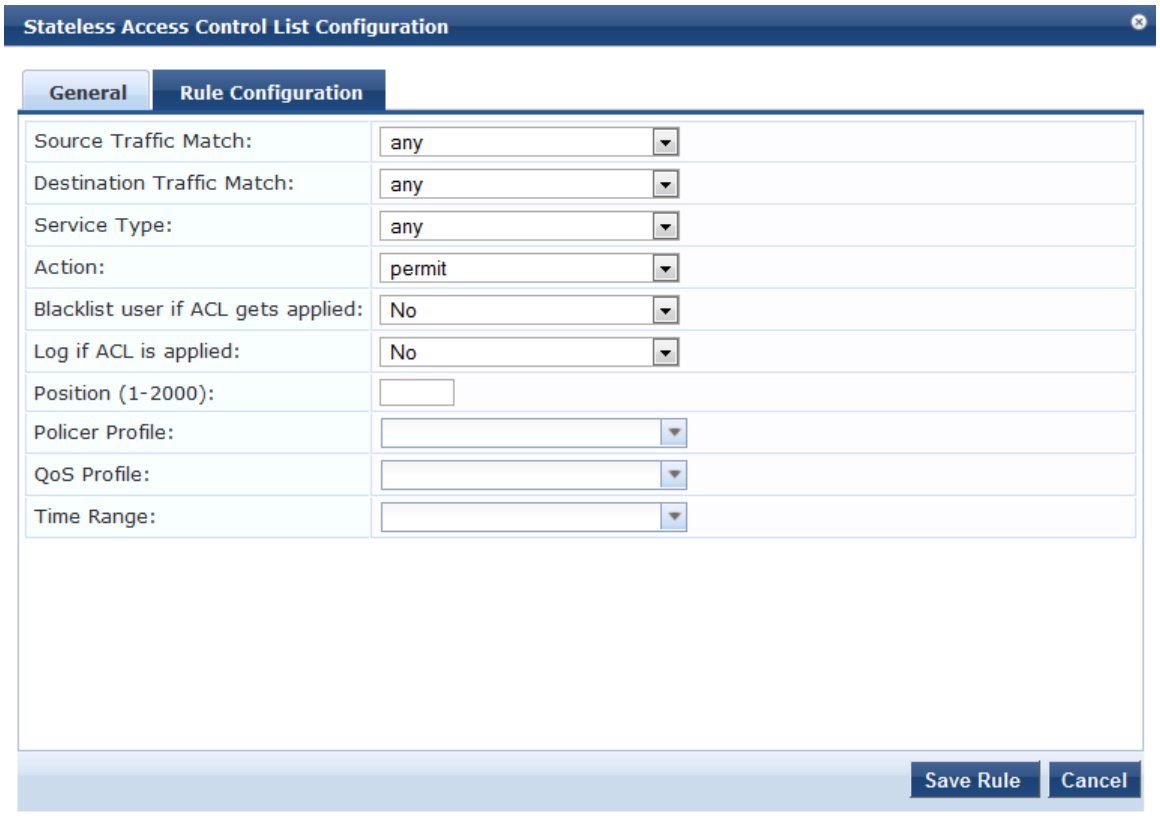


ACL

Click the **Add Stateless Access Control List** link. Enter a name for the Stateless ACL. Click the **Add Rule** link on the **General** tab. Enter the required attributes in the **Rule Configuration** tab and click **Save Rule** or **Cancel**.

The following figure displays the **Add Stateless Access Control List** pop-up:

Figure 285: *Stateless Access Control List Configuration Pop-up*

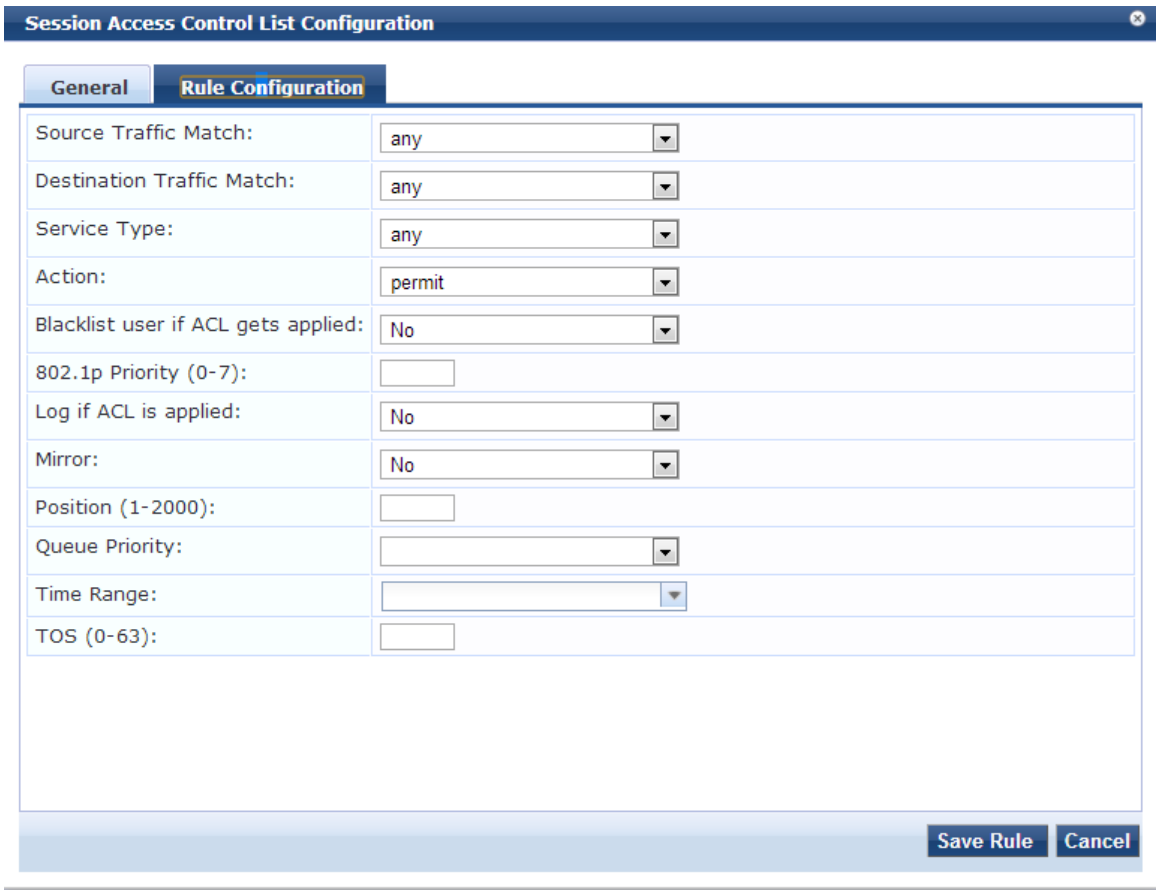


Click the **Add Session Access Control List** link and enter the name for the Session ACL. Click the **Add Rule** link on the **General** tab. You can view different fields depends on the **Action** type you choose from the drop-

down list. For example, if you select the dual-nat action type, you can view the **Dual NAT Pool** field additionally to specify the action. Enter the required attributes in the **Rule Configuration** tab and click **Save Rule** or **Cancel**.

The following figure displays the **Session Access Control List Attributes** pop-up:

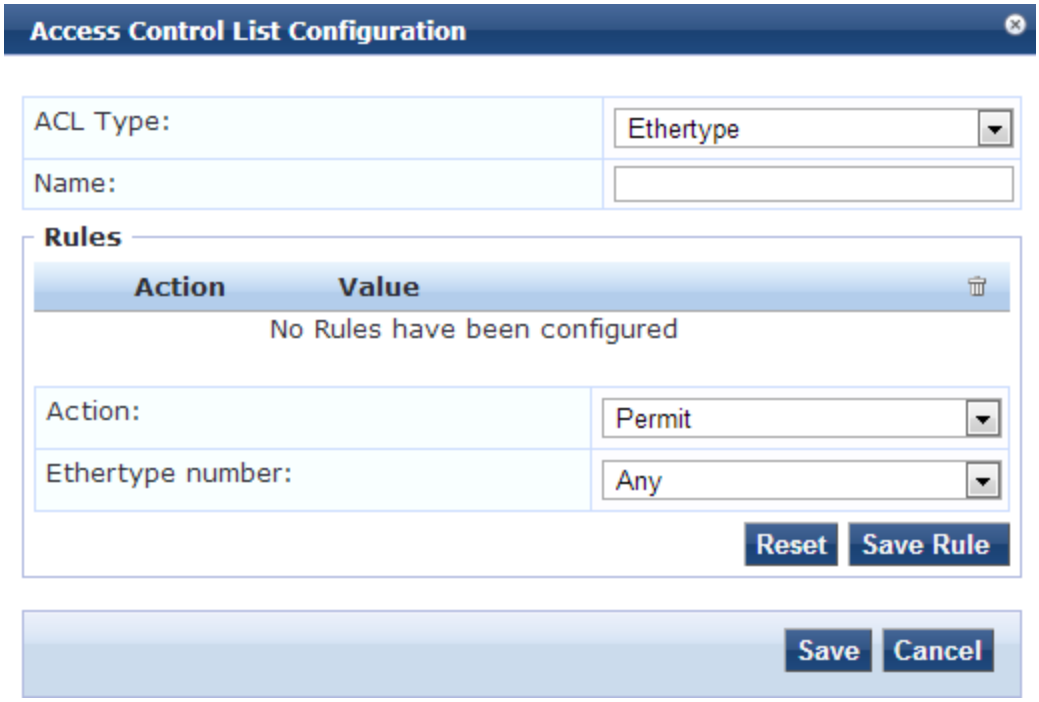
Figure 286: *Session Access Control List Attributes Pop-up*



Click the **Add Ethernet/MAC Access Control List** link. Enter a name for the Ethernet/MAC ACL. Enter the required attributes in the **Rules** section of the page and click **Reset**, **Save Rule**. Then click **Save** or **Cancel**.

The following figure displays the **Ethernet/MAC Access Control List Attributes** pop-up:

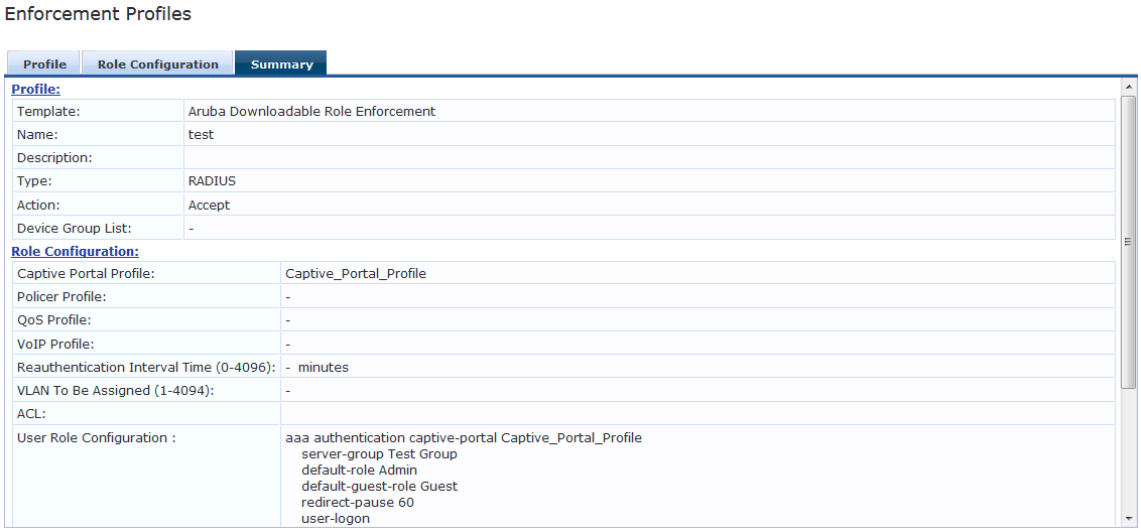
Figure 287: *Ethernet/MAC Access Control List Attributes Pop-up*



Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Role Configuration** tabs. The following figure displays the **Aruba Downloadable Role Enforcement - Summary** tab:

Figure 288: *Aruba Downloadable Role Enforcement - Summary Tab*



Aruba RADIUS Enforcement

Use this page to configure profile and attribute parameters for the **Aruba RADIUS Enforcement** profile. The the **Aruba RADIUS Enforcement** profile contains the following configuration tabs:

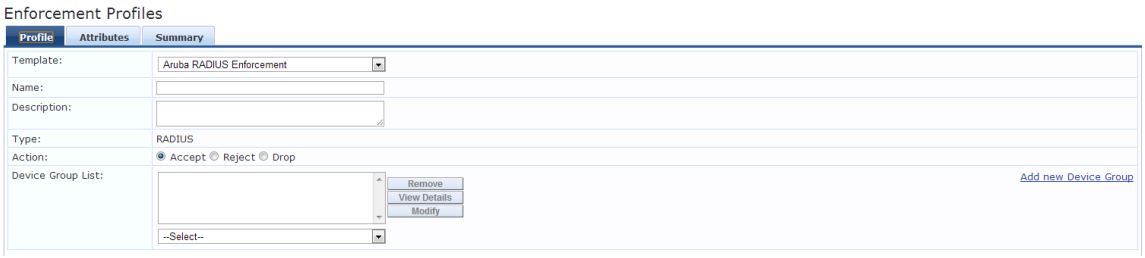
- Profile Tab on page 318
- Attributes Tab on page 319

- Summary Tab on page 319

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Aruba RADIUS Enforcement - Profile** tab:

Figure 289: *Aruba RADIUS Enforcement - Profile Tab*



The following table describes the **Aruba RADIUS Enforcement - Profile** tab parameters:

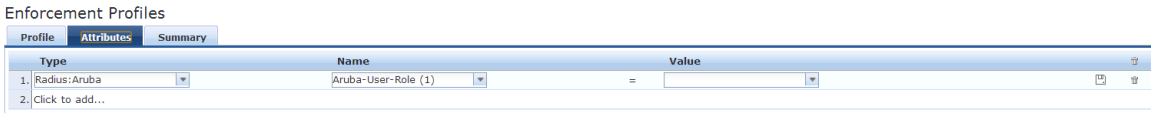
Table 167: *Aruba RADIUS Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Aruba RADIUS Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration** > **Enforcement** > **Profiles** page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the **Description** column on the **Configuration** > **Enforcement** > **Profiles** page.
Type	This field is populated automatically.
Action	Click **Accept**, **Reject**, or **Drop** to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After adding one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 353.

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **Aruba RADIUS Enforcement - Attributes** tab:

Figure 290: *Aruba RADIUS Enforcement - Attributes Tab*



The following table describes the **Aruba RADIUS Enforcement - Attributes** tab parameters:

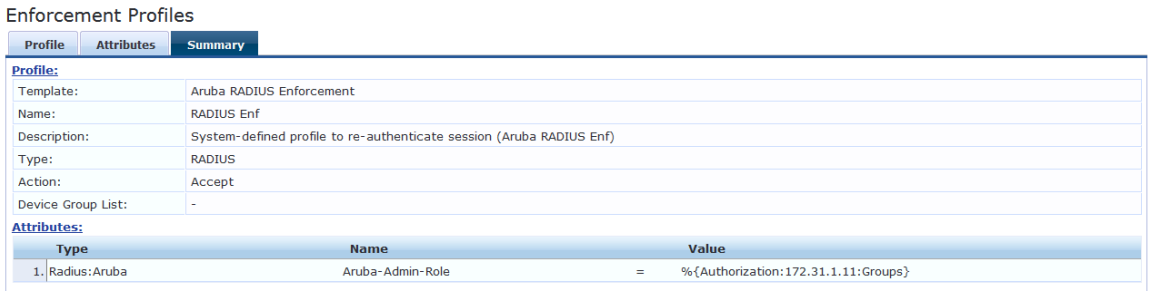
Table 168: *Aruba RADIUS Enforcement - Attributes Tab Parameters*

Attribute	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610.
Name	Specifies the options displayed for the **Name** attribute depend on the **Type** attribute selected.
Value	Specifies the options displayed for the **Value** attribute depend on the **Type** and **Name** attributes selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **Aruba RADIUS Enforcement - Summary** tab:

Figure 291: *Aruba RADIUS Enforcement - Summary Tab*



Cisco Downloadable ACL Enforcement

Use this page to configure profile and attribute parameters for the Cisco Downloadable ACL Enforcement profile. The **Cisco Downloadable ACL Enforcement** profile contains the following configuration tabs:

- Profile Tab on page 320
- Attributes Tab on page 320
- Summary Tab on page 321

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Cisco Downloadable ACL Enforcement - Profile** tab:

Figure 292: *Cisco Downloadable ACL Enforcement - Profile Tab*

The following table describes the **Cisco Downloadable ACL Enforcement - Profile** parameters:

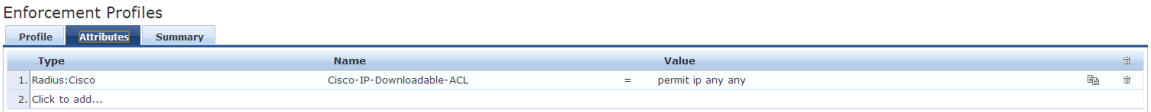
Table 169: *Cisco Downloadable ACL Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select **Cisco Downloadable ACL Enforcement**.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	The field is populated automatically.
Action	Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After adding one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected device group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the **Add new Device Group** link. For more information, see Adding and Modifying Device Groups on page 353.

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **Cisco Downloadable ACL Enforcement - Attributes** tab:

Figure 293: *Cisco Downloadable ACL Enforcement - Attributes Tab*



The following table describes the **Cisco Downloadable ACL Enforcement - Attributes** parameters:

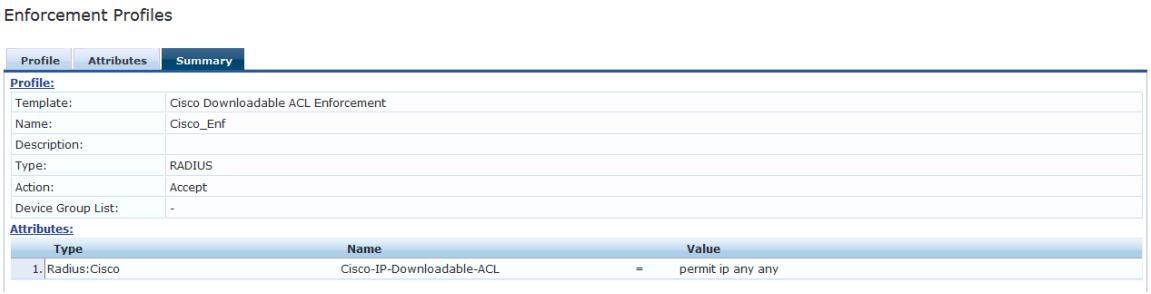
Table 170: *Cisco Downloadable ACL Enforcement - Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs. The following figure displays the **Cisco Downloadable ACL Enforcement - Summary** tab:

Figure 294: *Cisco Downloadable ACL Enforcement - Summary Tab*



Cisco Web Authentication Enforcement

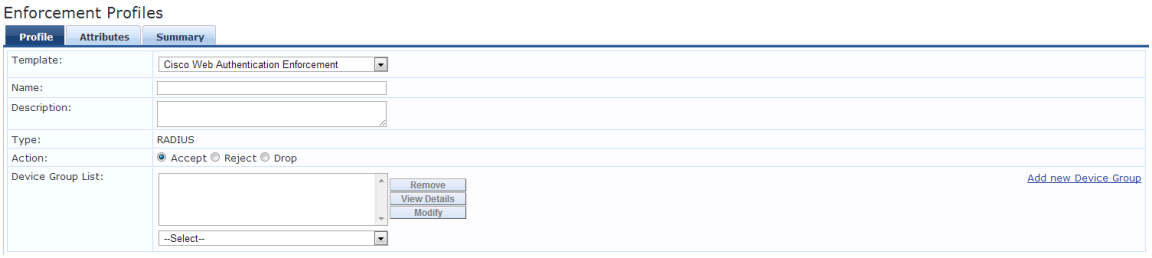
Use this page to configure profile and attribute parameters for the **Cisco Web Authentication Enforcement** profile. The **Cisco Web Authentication Enforcement** profile contains the following tabs:

- Profile Tab on page 322
- Attributes Tab on page 322
- Summary Tab on page 323

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Cisco Web Authentication Enforcement - Profile** tab:

Figure 295: *Cisco Web Authentication Enforcement - Profile Tab*



The following table describes the **Cisco Web Authentication Enforcement - Profile** tab parameters:

Table 171: *Cisco Web Authentication Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Cisco Web Authentication Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	This field is populated automatically.
Action	Click **Accept**, **Reject**, or **Drop** to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After adding one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 353.

Attributes Tab

Use the **Attributes** tab to configure the attribute name and attribute value. The following figure displays the **Cisco Web Authentication Enforcement - Profile** tab:

Figure 296: *Cisco Web Authentication Enforcement - Attributes Tab*

The following table describes the **Cisco Web Authentication Enforcement - Attribute** parameters:

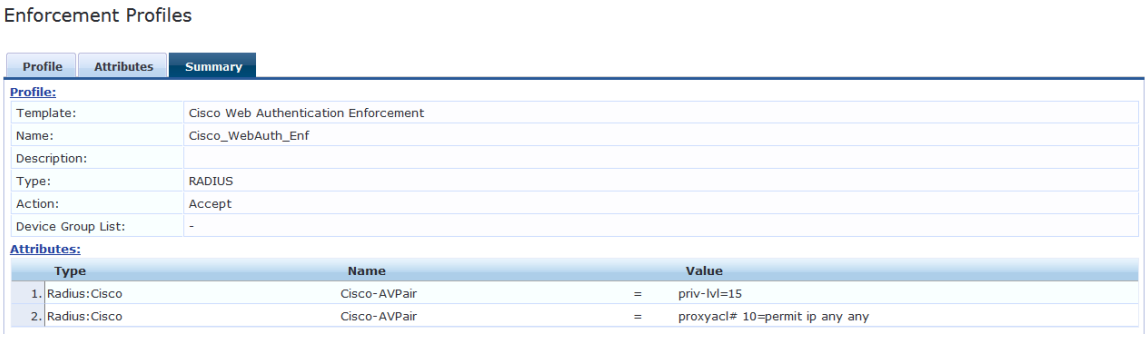
Table 172: *Cisco Web Authentication Enforcement - Attribute Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs. The following figure displays the **Cisco Web Authentication Enforcement - Summary** tab:

Figure 297: *Cisco Web Authentication Enforcement - Summary Tab*



ClearPass Entity Update Enforcement

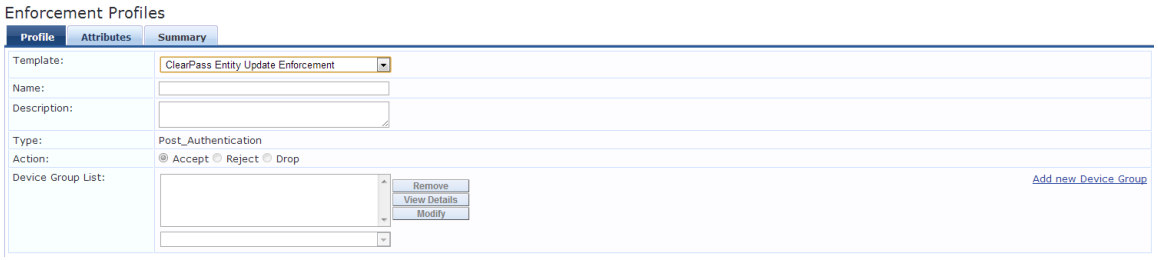
Use this page to configure profile and attribute parameters for the **ClearPass Entity Update Enforcement** profile. The **ClearPass Entity Update Enforcement** profile contains the following tabs:

- Profile Tab on page 324
- Attributes Tab on page 324
- Summary Tab on page 325

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **ClearPass Entity Update Enforcement - Profile** tab:

Figure 298: *ClearPass Entity Update Enforcement - Profile Tab*



The following table describes the **ClearPass Entity Update Enforcement - Profile** tab parameters:

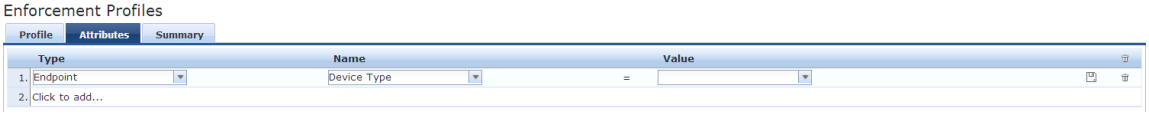
Table 173: *ClearPass Entity Update Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select ClearPass Entity Update Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the **Description** column on the **Configuration** > **Enforcement** > **Profiles** page.
Type	This field is populated automatically.
Action	Click **Accept**, **Reject**, or **Drop** to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After adding one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 353.

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **ClearPass Entity Update Enforcement - Attributes** tab:

Figure 299: *ClearPass Entity Update Enforcement Attributes tab*



The following table describes the **ClearPass Entity Update Enforcement - Attributes** tab parameters:

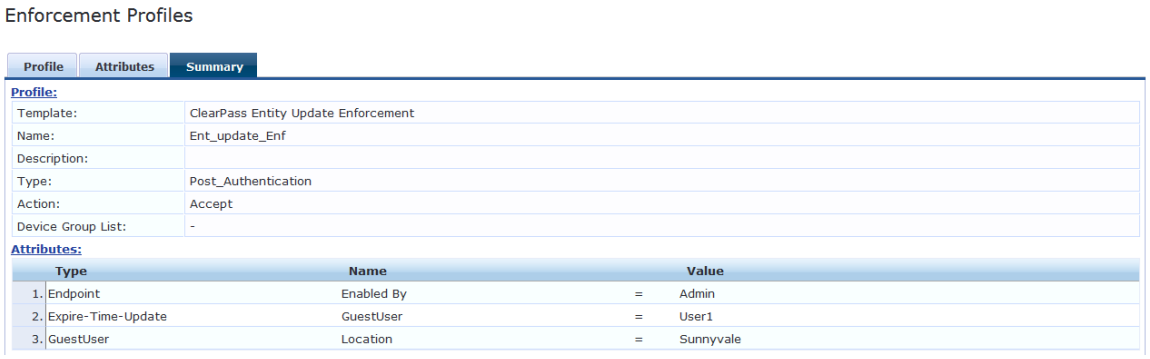
Table 174: *ClearPass Entity Update Enforcement - Attributes Tab Parameters*

Attribute	Description
Type	Select one of the following attribute types: • Endpoint • Expire-Time-Update • GuestUser • Status-Update
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **ClearPass Entity Update Enforcement - Summary** tab:

Figure 300: *ClearPass Entity Update Enforcement - Summary Tab*



CLI Based Enforcement

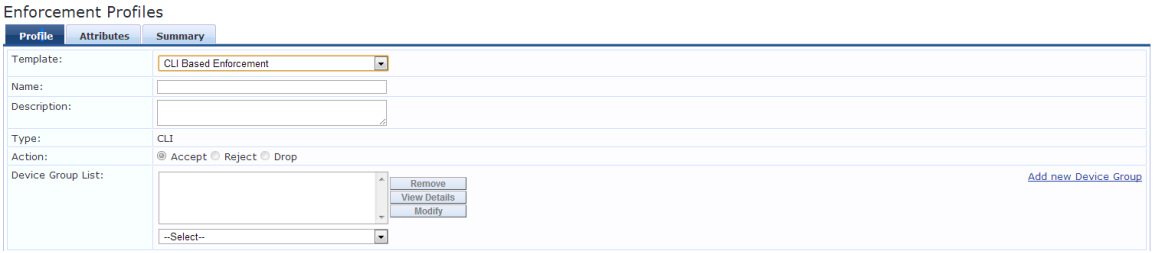
Use this page to configure profile and attribute parameters for the **CLI Based Enforcement** profile. The **CLI Based Enforcement** profile contains the following tabs:

- Profile Tab on page 326
- Attributes Tab on page 326
- Summary Tab on page 327

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **CLI Based Enforcement - Profile** tab:

Figure 301: *CLI Based Enforcement - Profile Tab*



The following table describes the **CLI Based Enforcement - Profile** tab parameters:

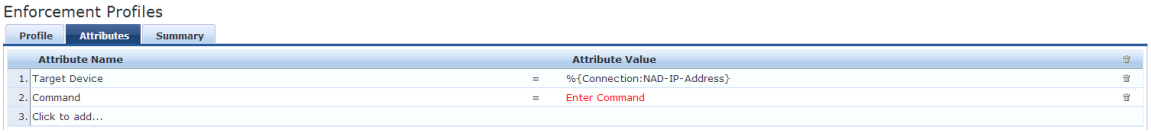
Table 175: *CLI Based Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select CLI Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the **Description** column on the **Configuration** > **Enforcement** > **Profiles** page.
Type	This field is populated automatically.
Action	Click **Accept**, **Reject**, or **Drop** to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After adding one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 353.

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **CLI Based Enforcement - Attributes** tab:

Figure 302: *CLI Based Enforcement - Attributes Tab*



The following table describes the **CLI Based Enforcement - Attributes** tab parameters:

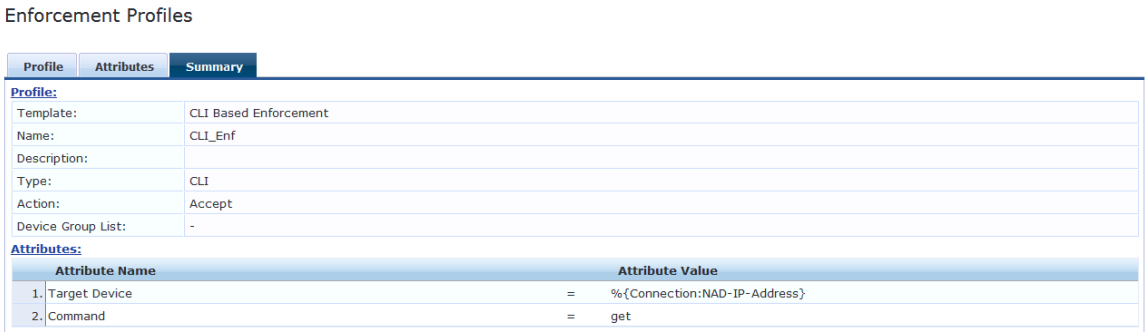
Table 176: *CLI Based Enforcement - Attributes Tab Parameters*

Attribute	Parameter
Attribute Name	Select Command or Target Device.
Attribute Value	Displays the options for the **Attribute Value** depend on the selected **Attribute Name**.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **CLI Based Enforcement - Summary** tab:

Figure 303: *CLI Based Enforcement - Summary Tab*



Filter ID Based Enforcement

Use this page to configure profile and attribute parameters for the Filter ID based enforcement profile. The **Filter ID Based Enforcement** profile contains the following tabs:

- Profile Tab on page 327
- Attributes Tab on page 328

Profile Tab

The following figure displays the **Filter ID Based Enforcement - Profile** tab:

Figure 304: *Filter ID Based Enforcement Profile tab*

The following table describes the **Filter ID Based Enforcement Profile** tab parameters:

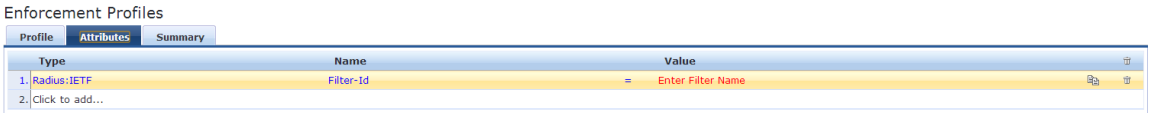
Table 177: *Filter ID Based Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Filter ID Based Enforcement
Name	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 353.

Attributes Tab

The following figure displays the **Filter ID Based Enforcement Profile - Attributes** tab:

Figure 305: *Filter ID Based Enforcement Profile - Attributes Tab*



The following table describes the **Filter ID Based Enforcement - Attributes** tab parameters:

Table 178: *Filter ID Based Enforcement Profile - Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** attribute and **Name** attribute that were selected.

Generic Application Enforcement

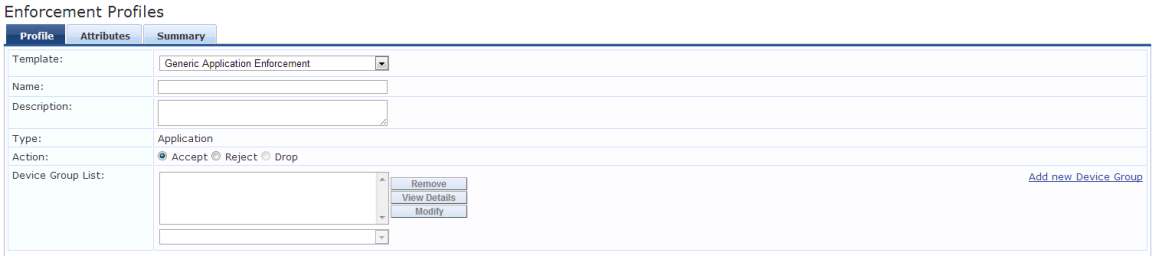
Use this page to configure profile and attribute parameters for the **Generic Application Enforcement** profile. The **Generic Application Enforcement** profile contains the following tabs:

- Profile Tab on page 329
- Attributes Tab on page 330
- Summary Tab on page 331

Profile Tab

Use the **Profile** tab to configure the template, type of the profile, and device group list. The following figure displays the **Generic Application Enforcement - Profile** tab:

Figure 306: *Generic Application Enforcement - Profile Tab*



The following table describes the **Generic Application Enforcement - Profile** tab parameters:

Table 179: *Generic Application Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Generic Application Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description that provides additional information about the profile. This description is displayed in the **Description** column on the **Configuration** > **Enforcement** > **Profiles** page.
Type	This field is populated automatically.
Action	Click **Accept**, **Reject**, or **Drop** to define the action taken on the request.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After adding one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 353.

Attributes Tab

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile. The following figure displays the **Generic Application Enforcement - Attributes** tab:

Figure 307: *Generic Application Enforcement - Attributes Tab*

The following table describes the **Generic Application Enforcement - Attributes** tab parameters:

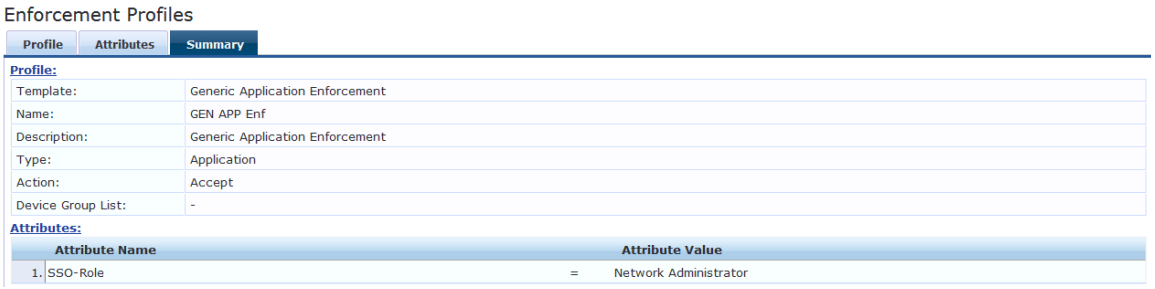
Table 180: *Generic Application Enforcement - Attributes Tab Parameters*

Parameter	Description
Attribute Name	Select an attribute name from the drop-down list. The list has multiple names.
Attribute Value	Displays the options for the **Attribute Value** depend on the selected **Attribute Name**.

Summary Tab

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **Generic Application Enforcement - Summary** tab:

Figure 308: *Generic Application Enforcement - Summary Tab*



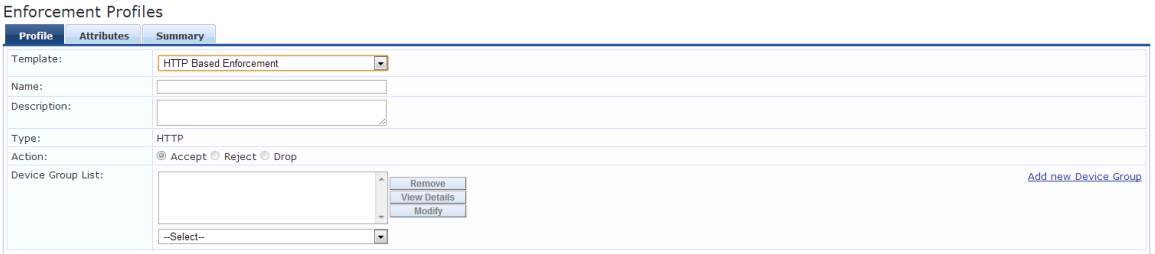
HTTP Based Enforcement

Use this page to configure profile and attribute parameters for the HTTP based enforcement profile.

Profile Tab

The following figure displays the **HTTP Based Enforcement - Profile** tab:

Figure 309: *HTTP Based Enforcement Profile tab*



The following table describes the **HTTP Based Enforcement - Profile** tab parameters:

Table 181: *HTTP Based Enforcement Profile tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select HTTP Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	Specifies the type of authentication. In this context, HTTP. This field is populated automatically.

Table 181: *HTTP Based Enforcement Profile tab Parameters (Continued)*

Parameter	Description
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 353.

Attributes Tab

Figure 310: *HTTP Based Enforcement Attributes tab*

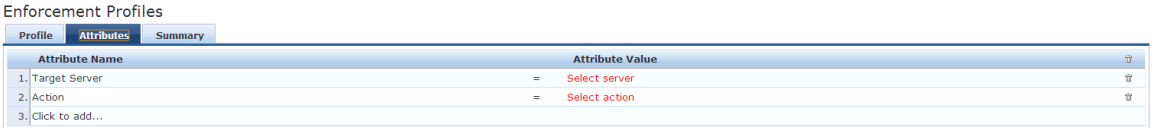


Table 182: *HTTP Based Enforcement Attributes tab Parameters*

Parameter	Description
Attribute Name	Select Target Server or Action.
Attribute Value	The options displayed for the Attribute Value depend on the Attribute Name that was selected.

RADIUS Based Enforcement

Use this page to configure profile and attribute parameters for the RADIUS based enforcement profiles.

Profile Tab

The following figure displays the **RADIUS Based Enforcement Profile** tab:

Figure 311: *RADIUS Based Enforcement - Profile Tab*

The following table describes the **RADIUS Based Enforcement Profile** tab parameters:

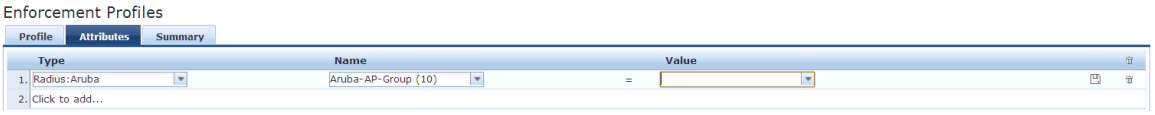
Table 183: *RADIUS Based Enforcement Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select RADIUS Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the Configuration > Enforcement > Profiles page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the Configuration > Enforcement > Profiles page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device GroupsConfiguration > Network > Device Groups** page. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry • Click **View Details** to see the device group parameters • Click **Modify** to change the parameters of the selected device group
Add new Device Group	To add a new a device group, click the Add new **Device Group** link and see Adding and Modifying Device Groups on page 353.

Attributes Tab

The following figure displays the **RADIUS Based Enforcement - Attributes** tab:

Figure 312: *RADIUS Based Enforcement Attributes Tab*



The following table describes the **RADIUS Based Enforcement - Attributes** tab parameters:

Table 184: *RADIUS Based Enforcement - Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

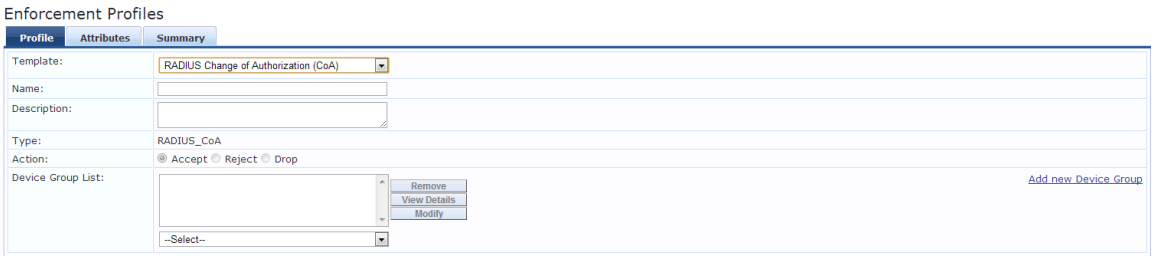
RADIUS Change of Authorization (CoA)

Use this page to configure profile and attribute parameters for the RADIUS Change of Authorization (CoA) enforcement profile.

Profile Tab

The following figure displays the **Radius Change of Authorization (CoA) - Profile** tab:

Figure 313: *Radius Change of Authorization (CoA) Profile Tab*



The following table describes the **Radius Change of Authorization (CoA) - Profile** tab parameters:

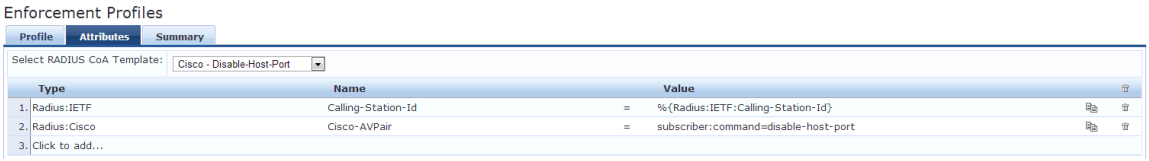
Table 185: *Radius Change of Authorization (CoA) Profile Tab Parameters*

Parameter	Description
Template	Select from: • Cisco-Disable-Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate-Session • HP - Change-VLAN • HP - Generic-CoA • Aruba - Change-User-Role • IETF - Terminate-Session-IETF • Aruba - Change-VPN-User-Role • IETF- Generic-CoA-IETF
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610
Name	The options displayed for the Name Attribute depend on the RADIUS CoA Template selected and the Type Attribute that were selected.
Value	The options displayed for the Value Attribute depend on the RADIUS CoA Template selected and the Type Attribute that were selected.
Type	RADIUS_CoA. The field is populated automatically.
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed on the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 353.

Attributes Tab

The following figure displays the **Radius Change of Authorization (CoA) - Attributes** tab:

Figure 314: *Radius Change of Authorization (CoA) - Attributes Tab*



The following table describes the **Radius Change of Authorization (CoA) - Attributes** tab parameters:

Table 186: *Radius Change of Authorization (CoA) Attributes Tab Parameters*

Parameter	Description
RADIUS CoA Template	Select from: • Cisco-Disable-Host-Port • Cisco - Bounce-Host-Port • Cisco - Reauthenticate-Session • HP - Change-VLAN • HP - Generic-CoA • Aruba - Change-User-Role • IETF - Terminate-Session-IETF • Aruba - Change-VPN-User-Role • IETF- Generic-CoA-IETF
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610
Name	The options displayed for the Name Attribute depend on the Template and Type Attribute that were selected.
Value	The options displayed for the Value Attribute depend on the Template, Type Attribute and Name Attribute that were selected.

Session Notification Enforcement

Use this page to configure profile and attribute parameters for **Session Notification Enforcement** profile. Notification of a change in IP address can now be sent to any external context server (such as a firewall) by configuring that server as a generic HTTP server and adding the appropriate generic HTTP context server actions. The content of the payload to be posted by Policy Manager to the external server is based on the REST API defined by the external server for communication.

The **Session Notification Enforcement** page contains the following tabs:

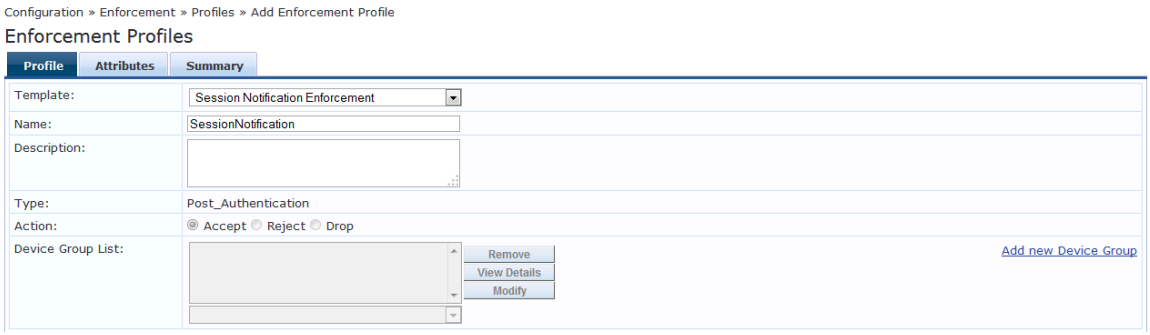
- Profile Tab on page 337
- Attributes Tab on page 337

- Summary Tab on page 338

Profile Tab

The following figure displays the **Session Notification Enforcement - Profile** tab:

Figure 315: *Session Notification Enforcement - Profile Tab*



The following table describes the **Session Notification Enforcement - Profile** tab parameters:

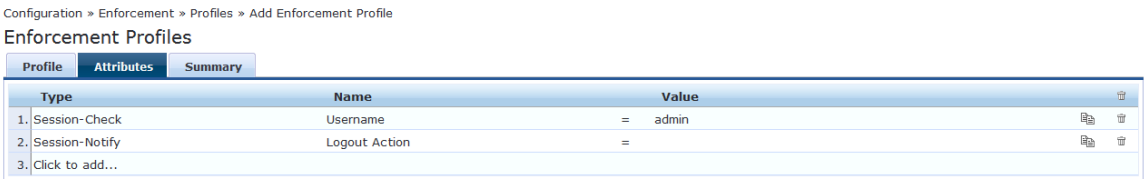
Table 187: *Session Notification Enforcement Profile Tab Parameters*

Parameter	Description
Template	Select **Session Notification Enforcement**.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The Description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	Post_Authentication. The field is populated automatically.
Action	Disabled.
Device Group List	Select a device group from the drop-down list. The list displays all configured device groups. All configured device groups are listed in the **Device Groups Configuration > Network > Device Groups** page.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 353.

Attributes Tab

The following figure displays the **Session Notification Enforcement - Attributes** tab:

Figure 316: *Session Notification Enforcement - Attributes Tab*



The following table describes the **Session Notification Enforcement - Attributes** tab:

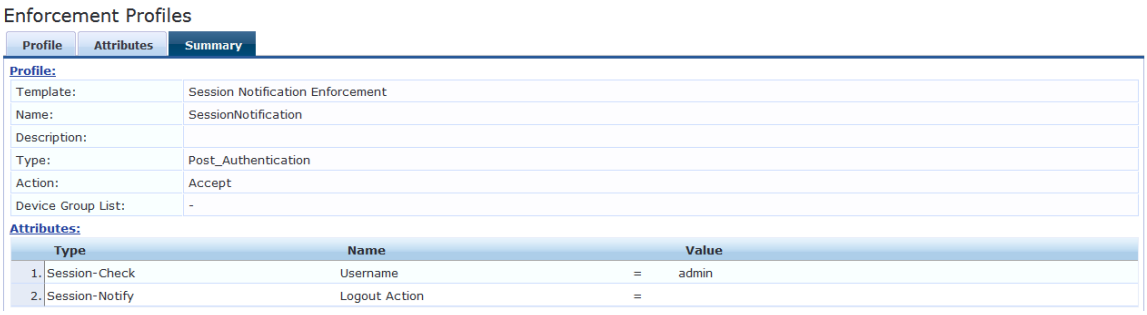
Table 188: *Session Notification Enforcement - Attributes Tab*

Parameter	Description
Type	Select from: • Session-Check • Session-Notify Palo Alto integration is extended to Guest MAC Caching use cases. Configure the following: **Session-Check::Username = %{Endpoint:Username}** **NOTE:** Post Auth sends the Guest username instead of the MAC Address in the user id updates. For **Session-Notify Type** attribute, the **Name** can be Server Type, Server IP, Login Action, or Logout Action. The values for **Server Type** can be Generic HTTP, Palo Alto Networks Panorama, or Palo Alto Networks Firewall. Selecting Server IP for **Name** provides a choice of ipaddress/hostnames for corresponding type of server as **Value**. Once the server IP is selected, **Login Action** and **Logout Action** can be selected (the list of actions defined for the selected server will be shown as available choices for value). This enforcement type should be used both for Palo Alto Devices and any Generic HTTP servers. Pre-6.5 configurations containing **Session Restrictions Enforcement** profile for Palo Alto devices (with attribute Session-Check::IP-Address-Change-Notify) will be migrated to this new enforcement profile during an upgrade (any profiles defined with more than one Palo Alto device or combined with any other Session Restrictions attributes will not be migrated and need to re-configured).
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** attribute and **Name** attribute that were selected.

Summary Tab

This tab summarizes the parameters configured in the **Summary** tab. The following figure displays the **Session Notification Enforcement - Summary** tab:

Figure 317: *Session Notification Enforcement - Summary Tab*



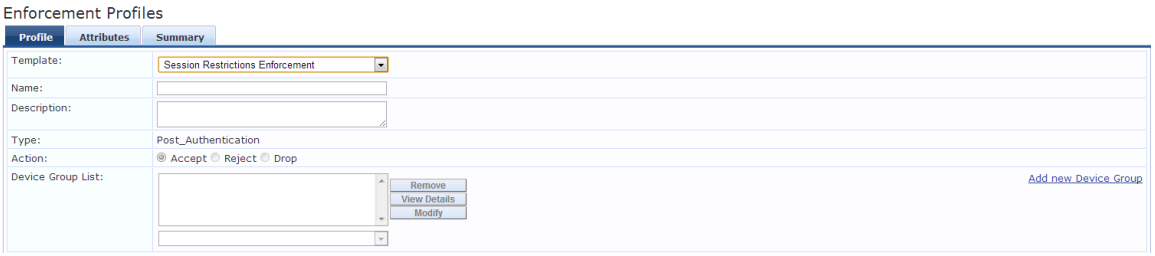
Session Restrictions Enforcement

Use this page to configure profile and attribute parameters for Session Restrictions enforcement profile.

Profile Tab

The following figure displays the **Session Restrictions Enforcement - Profile** tab:

Figure 318: *Session Restrictions Enforcement Profile Tab*



The following table describes the **Session Restrictions Enforcement - Profile** tab parameters:

Table 189: *Session Restrictions Enforcement Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select Session Restrictions enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The Description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	Post_Authentication. The field is populated automatically.
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the Add new Device Group link and see Adding and Modifying Device Groups on page 353.

Attributes Tab

The following figure displays the **Session Restrictions Enforcement - Attributes** tab:

Figure 319: *Session Restrictions Enforcement Attributes Tab*

The following table describes the **Session Restrictions Enforcement - Attributes** parameters:

Table 190: *Session Restrictions Enforcement Attributes Tab*

Parameter	Description
Type	Select from: • Bandwidth-Check • Expire-Check • Post-Auth-Check • Session-Check
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

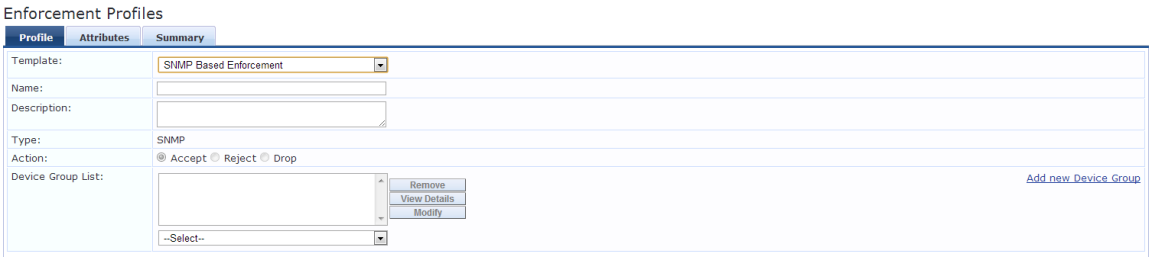
SNMP Based Enforcement

Use this page to configure profile and attribute parameters for the SNMP based enforcement profile.

Profile Tab

The following figure displays the **SNMP Based Enforcement - Profile** tab:

Figure 320: *SNMP Based Enforcement - Profile Tab*



The following table describes the **SNMP Based Enforcement - Profile** parameters:

Table 191: *SNMP Based Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select SNMP Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The Description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	SNMP. The field is populated automatically.

Table 191: *SNMP Based Enforcement - Profile Tab Parameters (Continued)*

Parameter	Description
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected **Device Group List** entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the **Add new Device Group** link and see Adding and Modifying Device Groups on page 353.

Attributes tab

The following figure displays the **SNMP Based Enforcement - Attributes** tab:

Figure 321: *SNMP Based Enforcement - Attributes Tab*

The following table describes the **SNMP Based Enforcement - Attributes** tab parameters:

Table 192: *SNMP Based Enforcement Attributes Tab Parameters*

Parameter	Description
Attribute Name	Select from: • VLAN ID • Session Timeout (in seconds) • Reset Connection (after the settings are applied)
Attribute Value	The options displayed for the **Attribute** value is depend on the **Attribute** name that was selected.

TACACS+ Based Enforcement

Use this page to configure profile, service, and attribute parameters for the TACACS+ based enforcement profile.

Profile Tab

The following figure displays the **TACACS+ Based Enforcement - Profile** tab:

Figure 322: *TACACS+ Based Enforcement Profile Tab*

The following table describes the **TACACS+ Based Enforcement Profile - Profile** tab parameters:

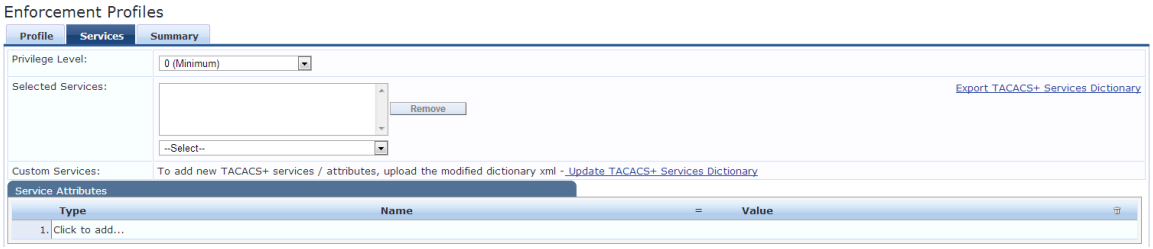
Table 193: *TACACS+ Based Enforcement Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select TACACS+ Based Enforcement.
Name	Enter the name of the profile. The name is displayed in the Name column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The Description is displayed in the Description column on the **Configuration > Enforcement > Profiles** page.
Type	TACACS. The field is populated automatically.
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** (**Configuration > Network > Device Groups**) page. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the **Add new Device Group** link and see Adding and Modifying Device Groups on page 353.

Services Tab

The following figure displays the **TACACS+ Based Enforcement - Services** tab:

Figure 323: *TACACS+ Based Enforcement Services Tab*



The following table describes the **TACACS+ Based Enforcement Profile - Service** tab parameters:

Table 194: *TACACS+ Based Enforcement Services Tab Parameters*

Parameter	Description
Privilege Level	Select a level between 0 and 15.
Selected Services	Select a service from the list and add it to the Selected Services: field. Click **Remove** to remove a service from the field.
Export All	Click this link to download the TACACS+ Services dictionary is downloaded to the local computer.
Custom Services	To add new TACACS+ services / attributes, upload the modified dictionary xml click Update TACACS+ Services Dictionary.
Type	Select a service attribute parameter from the list.
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

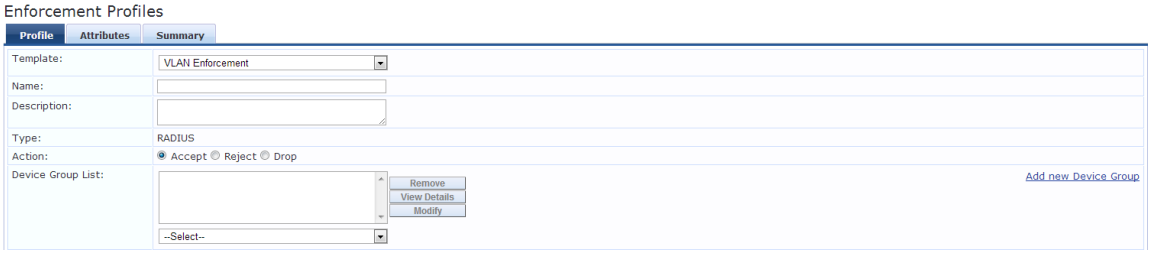
VLAN Enforcement

Use this page to configure profile and attribute parameters for the VLAN enforcement profile.

Profile Tab

The following figure displays the **VLAN Enforcement - Profile** tab:

Figure 324: *VLAN Enforcement - Profile Tab*



The following table describes the **VLAN Enforcement - Profile** tab parameters:

Table 195: *VLAN Enforcement - Profile Tab Parameters*

Parameter	Description
Template	Select the template from the drop-down list. In this context, select VLAN Enforcement.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The Description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	RADIUS. The field is populated automatically.
Action	Enabled. Click Accept, Reject, or Drop to define the action taken on the request.
Device Group List	Select a Device Group from the drop-down list. The list displays all configured Device Groups. All configured device groups are listed in the **Device Groups** page: **Configuration > Network > Device Groups**. After you add one or more device group(s), you can select a group and take one of the following actions: • Click **Remove** to delete the selected Device Group List entry. • Click **View Details** to see the device group parameters. • Click **Modify** to change the parameters of the selected device group.
Add new Device Group	To add a new a device group, click the **Add new Device Group** link and see Adding and Modifying Device Groups on page 353.

Attributes Tab

The following figure displays the **VLAN Enforcement - Attributes** tab:

Figure 325: *VLAN Enforcement Attributes Tab*

The following table describes the **RADIUS Based Enforcement - Attributes** tab parameters:

Table 196: *VLAN Enforcement Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: • Radius:Aruba • Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda For more information, see RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

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. You can add or modify a device or a device group from the Policy Manager server.

For Policy Manager server to discover and access the network devices, you must perform the following tasks:

- Configure SNMP read credentials on the network device to enable Policy Manager server to query against network devices or perform SNMP write operations.
- Configure SNMP trap configurations on the network device to send SNMP traps to the Policy Manager server. Ensure that the same SNMP Trap credentials are configured in the **SnmpService** section under the **Administration > Server Configuration > Service Parameters** tab of the Policy Manager UI.
- Configure SNMPTRAPD on the Policy Manager server to receive SNMP traps. For SNMP enforcement on the network device, one or more of the following traps must be configured on the device:
  - Link Up trap
  - Link Down trap
  - MAC Notification trap

  In addition, the device must also support one or more of the following SNMP MIBs:
  - RFC-1213 MIB
  - IF-MIB, BRIDGE-MIB
  - ENTITY-MIB
  - Q-BRIDGE-MIB
  - CISCO-VLANMEMBERSHIP-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.
- Configure SSH CLI data on the Policy Manager server to allow phantom login to network devices.
- Configure DHCP Relay configuration on the network device to ensure that DHCP requests are forwarded from the clients.

This chapter describes the following tasks that you can perform by using the Policy Manager UI:

- Adding and Modifying Devices on page 347
- Adding and Modifying Device Groups on page 353
- Adding and Modifying Proxy Targets on page 356

Adding and Modifying Devices

Network Access Device (NAD) must belong to the global list of devices in the Policy Manager database to connect with Policy Manager using any of the supported protocols. The Policy Manager **Devices** page displays the device name, IP address or subnet, and a brief description of each configured device. To view this page, navigate to **Configuration > Network > Devices**.

The following figure displays the **Network Devices** page:

Figure 326: *Network Devices page*

This page includes the following additional tasks:

- Adding a Device on page 348
- Additional Tasks on page 353

Adding a Device

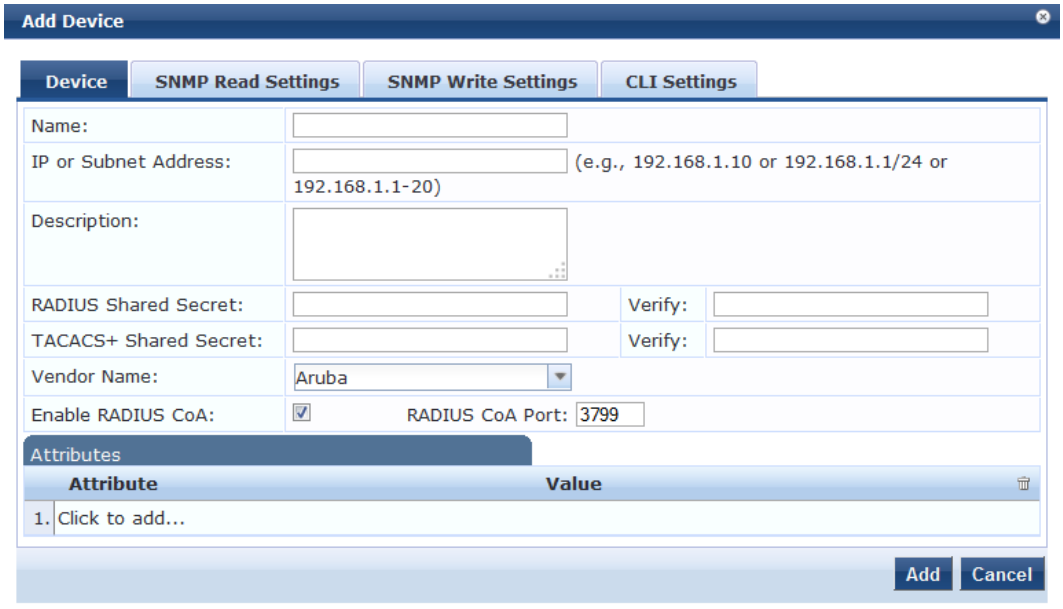
To add a device, navigate to the **Configuration** > **Network** > **Devices** page and click **Add** link at the top-right corner. The **Add Device** page appears. This page contains the following tabs used to configure device settings:

- Device on page 348
- SNMP Read Settings on page 349
- SNMP Write Settings on page 351
- Adding a Device on page 348

Device

Use the **Device** tab to define the device name, IP address, shared secret, and device attributes. The following displays the **Add Device** tab:

Figure 327: *Device Tab*



The following table describes the **Device** tab parameters:

Table 197: *Device Tab Parameters*

Parameter	Description
Name	Enter the name of the device.
Description	Enter the description that provides additional information to identify the device.
IP Address or Subnet	Specify the IP address or the subnet of the device. You can use a hyphen to indicate the range of device IP addresses following the format a.b.c.d-e. For example, 192.168.1.1-20.
RADIUS/TACACS+ Shared Secret	Enter a shared secret for each of the two supported request protocols.
Vendor	Specify the dictionary to be loaded for this device. This field is optional. **NOTE:** RADIUS:IETF, the dictionary containing the standard set of RADIUS attributes, is always loaded. When you specify a vendor here, the RADIUS dictionary associated with this vendor is automatically enabled.
Enable RADIUS CoA RADIUS CoA Port	Enable RADIUS CoA (RFC 3576/5176) for this device. Set the UDP port on the device to send CoA actions. The default value is 3799.
Attributes	Add custom attributes for this device. Click on the "Click to add..." row to add custom attributes. By default, four custom attributes appear in the **Attribute** drop down: Location, OS-Version, Device-Type, and Device-Vendor. You can enter any name in the **Attribute** field. All attributes are of string datatype. The **Value** field can also be populated with any string. Each time you enter a new custom attribute, it is available for selection in the **Attribute** drop down for all devices. **NOTE:** All attributes entered for a device are available in the role mapping rules editor under the Device namespace.

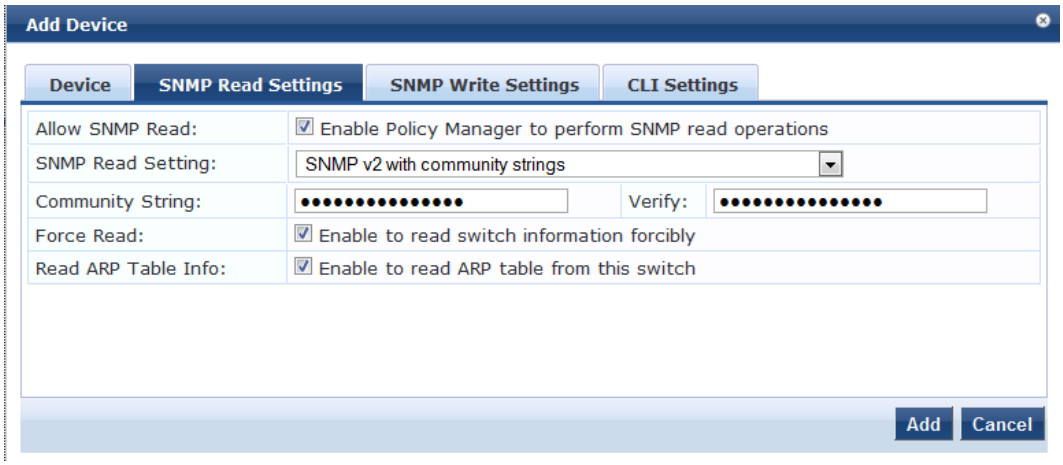
SNMP Read Settings

Use the **SNMP Read Settings** tab to define values that allow Dell Networking W-ClearPass Policy Manager to read information from the device using SNMPv1, SNMPv2, or SNMPv3.

The following figure displays the **SNMP Read Settings** tab:

Large or geographically spread cluster deployments, typically do not want each CPPM node to probe all SNMP configured devices. By default, a CPPM node in a cluster only reads network device information for devices configured to send traps to that CPPM node.

Figure 328: *SNMP Read Settings Tab*



The following table describes the **SNMP Read Settings** tab parameters:

Table 198: *SNMP Read Settings Parameters*

Parameter	Description
Allow SNMP Read	Toggle to enable or disable SNMP read.
SNMP Read Setting	Specify the SNMPrRead settings for the device. You can set any of the following options: • SNMP v1 with community strings • SNMP v2 with community strings • SNMP v3 with no Authentication • SNMP v3 with Authentication using MD5 and no Privacy • SNMP v3 with Authentication using MD5 and with Privacy • SNMP v3 with Authentication using SHA and no Privacy • SNMP v3 with Authentication using SHA and with Privacy **NOTE:** The MD5 authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** (**Administration** > **Server Manager** > **Server Configuration** > **FIPS**) mode.
Community String (SNMP v2 only)	Enter the community string for sending the traps.
Verify	Re-enter the community string for sending the traps.
Force Read (SNMP v1 and v2 only)	Enable this setting to ensure that all Dell Networking W-ClearPass Policy Manager nodes in the cluster read SNMP information from this device regardless of the trap configuration on the device. This option is useful when demonstrating a static IP-based device profiling because this does not require any trap configuration on the network device.
Read ARP Table Info	Enable this setting on a Layer 3 device if you intend to use the ARP table on this device to discover endpoints in the network. Static IP endpoints are discovered this way are further probed using SNMP to profile the device.

Table 198: *SNMP Read Settings Parameters (Continued)*

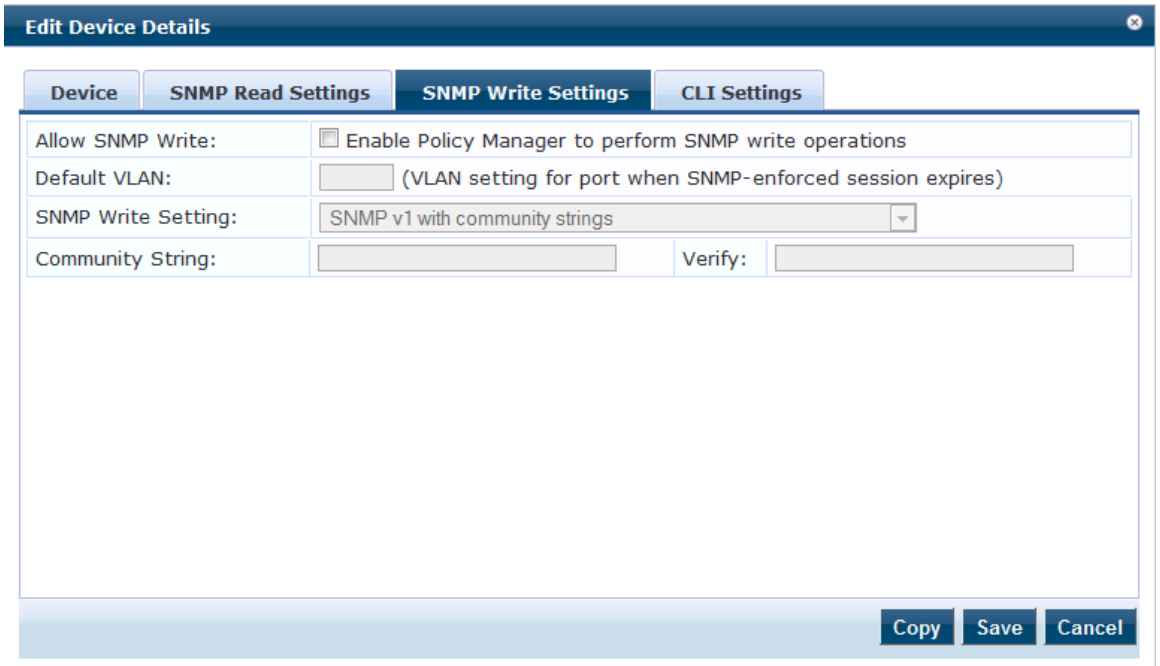
Parameter	Description
Username (SNMP v3 only)	Specify the Admin user name to use for SNMP read operations.
Authentication Key (SNMP v3 only)	Specify the SNMP v3 with authentication option (SHA or MD5). **NOTE:** The **EAP-MD5** authentication type is not supported if you run Dell Networking W-ClearPass Policy Manager in the FIPS (**Administration** > **Server Manager** > **Server Configuration** > **FIPS**) mode.
Privacy Key (SNMP v3 only)	Specify the SNMP v3 with privacy option.
Privacy Protocol (SNMP v3 with privacy only)	Choose one of the available privacy protocols: • DES-CBC • AES-128

SNMP Write Settings

Use the **SNMP Write Settings** tab to define values that allow Dell Networking W-ClearPass Policy Manager to write to (manage) the device using SNMPv1, SNMPv2, or SNMPv3.

The following figure displays the **SNMP Write Settings** tab:

Figure 329: *SNMP Write Settings Tab*



The following table describes the **SNMP Write Settings** parameters:

Table 199: *SNMP Write Settings Tab Parameters*

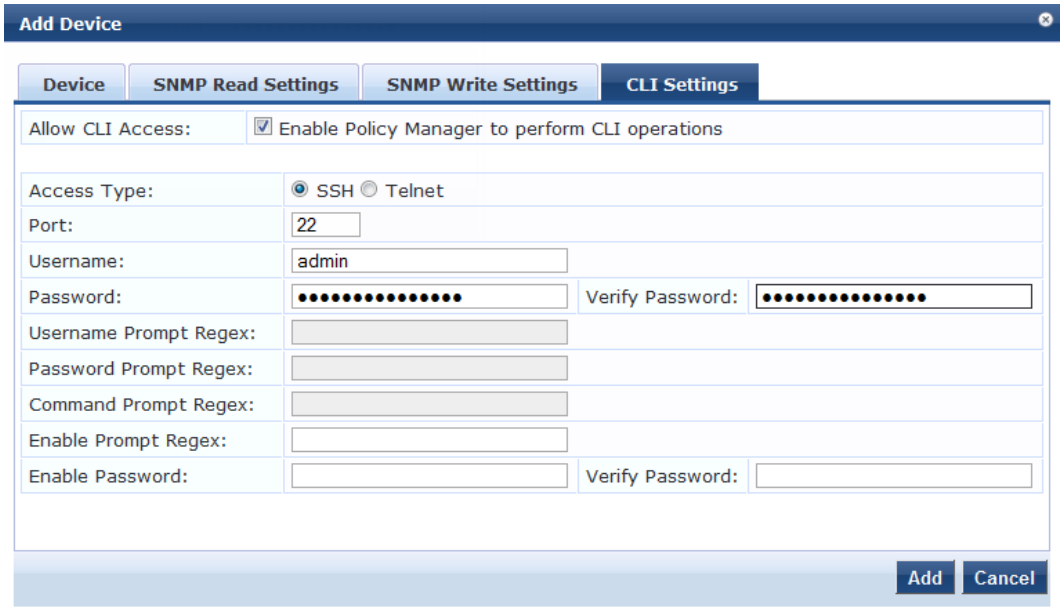
Parameter	Description
Allow SNMP Write	Toggle to enable or disable SNMP write.
Default VLAN	Specify the VLAN port setting after SNMP-enforced session expires.
SNMP Write Settings	Specify the SNMP Write settings for the device. You can set any of the following options: • SNMP v1 with community strings • SNMP v2 with community strings • SNMP v3 with no Authentication • SNMP v3 with Authentication using MD5 and no Privacy • SNMP v3 with Authentication using MD5 and with Privacy • SNMP v3 with Authentication using SHA and no Privacy • SNMP v3 with Authentication using SHA and with Privacy **NOTE:** The MD5 authentication type is not supported if you use Dell Networking W-ClearPass Policy Manager in the **FIPS** (**Administration** > **Server Manager** > **Server Configuration** > **FIPS**) mode.
Community String	Enter the community string for sending the traps.
Verify	Re-enter the community string for sending the traps.

CLI Settings

Use the **CLI Settings** tab to enable or disable the CLI, and define user names, passwords, and port settings for accessing the CLI.

The following figure displays the **CLI Settings** tab:

Figure 330: *CLI Settings Tab*



The following table describes the **CLI Settings** tab parameters:

Table 200: *CLI Settings Tab Parameters*

Parameter	Description
Allow CLI Access	Toggle to enable or disable CLI access.
Access Type	Select SSH or Telnet. Policy Manager uses the selected access method to log into the device CLI.
Port	Specify the SSH or Telnet TCP port number.
Username	Enter the username to log into the CLI.
Password	Enter the password to log into the CLI.
Username Prompt Regex	Specify the regular expression for the username prompt. Policy Manager looks for this pattern to recognize the telnet username prompt.
Password Prompt Regex	Specify the regular expression for the password prompt. Policy Manager looks for this pattern to recognize the telnet password prompt.
Command Prompt Regex	Specify the regular expression for the command line prompt. Policy Manager looks for this pattern to recognize the telnet command line prompt.
Enable Prompt Regex	Specify the regular expression for the command line in the **enable** prompt. Policy Manager looks for this pattern to recognize the telnet command line prompt.
Enable Password	Enter and re-enter the credentials for **Enable** the password in the CLI.

Additional Tasks

- To import a device, click **Import**. In the **Import from File** page, 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**. In the **Export to File** page, specify a file path, and then click **Export**. In the **Export to File** page, you can choose to encrypt the exported data with a key. This protects data such as shared secret from being visible in the exported file. To import it back, you specify the same key with which you exported.
- To export a single device from the configuration, select it (using the check box on the left), and then click **Export**. In the **Save As** popup, specify a file path, and then click **Export**.

For more information, see Importing on page 35 and Exporting on page 36.

Adding and Modifying Device Groups

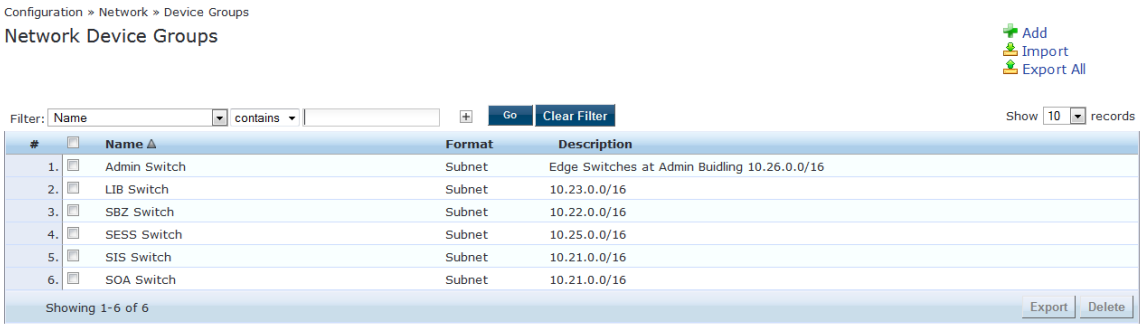
Policy Manager groups devices into **Device Groups**, which function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles; Policy Manager sends the

attributes associated with these profiles only if the request originated from a device belong to the device groups.

Administrators configure device groups at the global level. Device groups can contain the members of the IP address of a specified subnet, regular expression-based variation, or devices that are previously configured in the Policy Manager database.

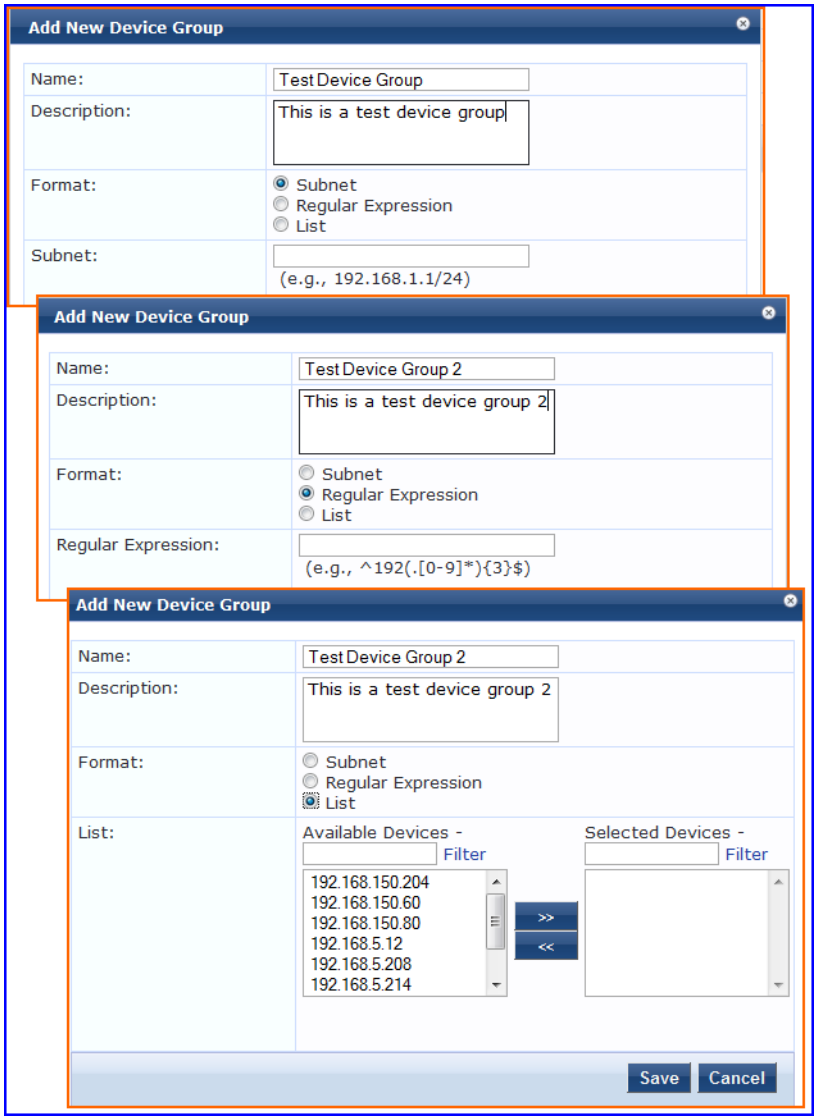
Policy Manager lists all configured device groups in the **Device Groups** (**Configuration > Network > Device Groups**) page. The following figure displays the **Network Device Groups** page:

Figure 331: *Device Groups Page*



To add a device group, click **Add** at the top-right corner of the **Network Device Groups** page. Complete the fields in the **Add New Device Group** page as described in the following figure:

Figure 332: *Add New Device Group Page*



The following table describes the **Add New Device Group** page parameters:

Table 201: *Add New Device Group Page*

Parameter	Description
Name	Enter the name of the device group.
Description	Enter the description that provides additional information about the device group.
Format	Select the format: Subnet, Regular Expression, or List.

Table 201: *Add New Device Group Page (Continued)*

Parameter	Description
Subnet	Enter a subnet consisting of network address and the network suffix (CIDR notation). For example, 192.168.5.0/24.
Regular Expression	Specify a regular expression that represents all IPv4 addresses matching that expression. For example, ^192(.[0-9]*){3}$.
List: Available/Selected Devices	Use the widgets to move device identifiers between **Available** and **Selected**. Click **Filter** to filter the list based on the text in the associated text box.

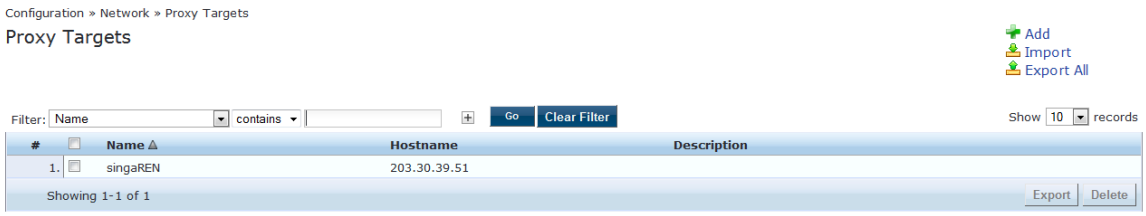
Adding and Modifying Proxy Targets

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 be used in configuring RADIUS proxy services. Refer to Policy Manager Service Types on page 122 for more information. Policy Manager lists all configured proxy servers in the **Proxy Targets** page. To view the **Proxy Targets** page, navigate to **Configuration > Network > Proxy Targets**.

The following figure displays the **Proxy Targets** page:

Figure 333: *Proxy Targets Page*

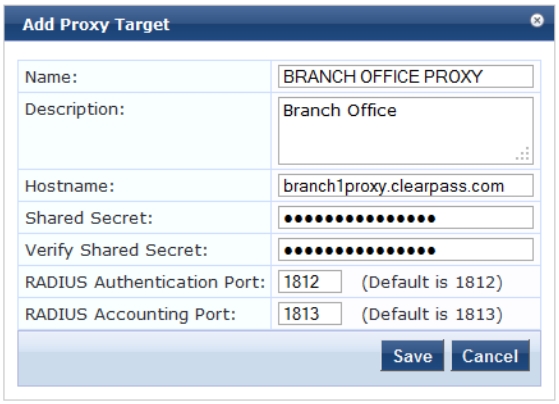


Adding a Proxy Target

To add a proxy target, click **Add** and complete the fields in the **Add Proxy Target** popup. You can also add a new proxy target from the **Services** page (**Configuration > Services**) as part of the flow of the **Add Service** wizard for a RADIUS proxy service type.

The following figure displays the **Add Proxy Target** pop-up:

Figure 334: *Add Proxy Target Pop-up*



The following table describes the **Add Proxy Target** pop-up parameters:

Table 202: *Add Proxy Target pop-up*

Parameter	Description
Name	Enter the name of the proxy target.
Description	Enter the description that provides additional information about the proxy target.
Hostname/Shared Secret	Specify the 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.

Profile is a Dell Networking W-ClearPass Policy Manager module that automatically classifies endpoints using attributes obtained from software components called Collectors. You can use Profile to implement "Bring Your Own Device" (BYOD) flows, where access must be controlled, based on the type of the device and the identity of the user. While offering a more efficient and accurate way to differentiate access by endpoint type (laptop or tablet), ClearPass Profile associates an endpoint with a specific user or location and secures access for devices like printers and IP cameras. Profile can be set up in a network with a minimal amount of configuration.

For more information, see:

- Device Profile on page 359
- Collectors on page 359
- Fingerprint Dictionaries on page 364
- Profiling on page 365

Device Profile

A device profile is a hierarchical model consisting of 3 elements – DeviceCategory, DeviceFamily, and DeviceName that are derived by a profile from endpoint attributes.

- **DeviceCategory** - This is the broadest classification of a device. It denotes the type of the device. For example, Computer, Smartdevice, Printer, or Access Point.
- **DeviceFamily** - This element classifies devices into a category and is organized based on the type of operating system or vendor. For example, when the category is Computer, Dell Networking W-ClearPass Policy Manager shows a DeviceFamily of Windows, Linux, or Mac OS X.
- **DeviceName** - Devices in a family are further organized based on more granular details such as operating system version. For example, in a DeviceFamily of Windows, Dell Networking W-ClearPass Policy Manager shows a DeviceName of Windows 7 or Windows 2008 Server.

This hierarchical model provides a structured view of all endpoints accessing the network. In addition to these, profile also collects and stores the following:

- IP Address
- Hostname
- MAC Vendor
- Timestamp when the device was first discovered
- Timestamp when the device was last seen

Collectors

Collectors are the network elements that provide data to profile endpoints. For more information, see:

- DHCP on page 360
- ClearPass Onboard on page 360
- HTTP User-Agent on page 360
- MAC OUI on page 360*
- ActiveSync Plugin on page 361

- CPPM OnGuard on page 361
- SNMP on page 361
- Subnet Scan on page 362

* Acquired through various authentication mechanisms such as 802.1X, and MAC authentication.

DHCP

DHCP attributes such as option55 (parameter request list), option60 (vendor class), and options list from the DISCOVER and REQUEST packets can uniquely fingerprint most devices that use the DHCP mechanism to acquire an IP address on the network. Switches and controllers can be configured to forward DHCP packets such as DISCOVER, REQUEST, and INFORM to CPPM. These DHCP packets are decoded by CPPM to arrive at the device category, family, and name. Apart from fingerprints, DHCP also provides hostname and IP address.

Sending DHCP Traffic to CPPM

Perform the following steps to configure your Dell W-Series controller and Cisco switch to send DHCP Traffic to CPPM:

```
interface <vlan_name>
ip address <ip_addr> <netmask>
ip helper-address <dhcp_server_ip>
ip helper-address <cppm_ip>end
end
```

Notice that multiple **ip helper-address** statements can be configured to send DHCP packets to servers other than the DHCP server.

ClearPass Onboard

ClearPass Onboard collects rich and authentic device information from all devices during the onboarding process. Onboard then posts this information to Profile via the Profile API. Because the information collected is definitive, Profile can directly classify these devices into their Category, Family, and Name without having to rely on any other fingerprinting information.

HTTP User-Agent

In some cases, DHCP fingerprint alone cannot fully classify a device. A common example is the Apple® family of smart devices; DHCP fingerprints cannot distinguish between an iPad® or 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
- ClearPass Onboard
- Dell W-Series controller through IF-MAP interface

MAC OUI

MAC OUI can be useful in some cases to classify endpoints better. 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, or Motorola® Android. MAC OUI is also useful to profile devices like printers that may be configured with static IP addresses.

ActiveSync Plugin

You can install the ActiveSync plugin on Microsoft Exchange servers. When a device communicates with exchange server using active sync protocol, it provides attributes such as device-type and user-agent. These attributes are collected by the plug-in software and are sent to the CPPM profiler. Profiler uses dictionaries to derive profiles from these attributes.

CPPM OnGuard

The ClearPass OnGuard agent performs advanced endpoint posture assessment. It can collect and send OS details from endpoints during authentication. The Policy Manager Profiler uses the os_type attribute from OnGuard to derive a profile.

SNMP

Endpoint information obtained by reading SNMP MIBs of network devices is used to discover and profile static IP devices in the network. The following information read via SNMP is used:

- sysDescr information from RFC1213 MIB is used to profile the device. This is used both for profiling switches/controllers/routers configured in CPPM, and for profiling printers and other static IP devices discovered through SNMP or subnet scans.
- cdpCacheTable information read from CDP (Cisco Discovery Protocol) capable devices is used to discover neighbor devices connected to switch/controller configured in CPPM
- lldpRemTable information read from LLDP (Link Layer Discovery Protocol) capable devices is used to discover and profile neighbor devices connected to switch/controller configured in CPPM
- ARPtable read from network devices is used as a means to discover endpoints in the network.

The SNMP based mechanism is only capable of profiling devices if they respond to SNMP, or if the device advertises its capability via LLDP. When performing SNMP reads for a device, CPPM uses SNMP Read credentials configured in Network Devices, or defaults to using SNMP v2c with "public" community string.

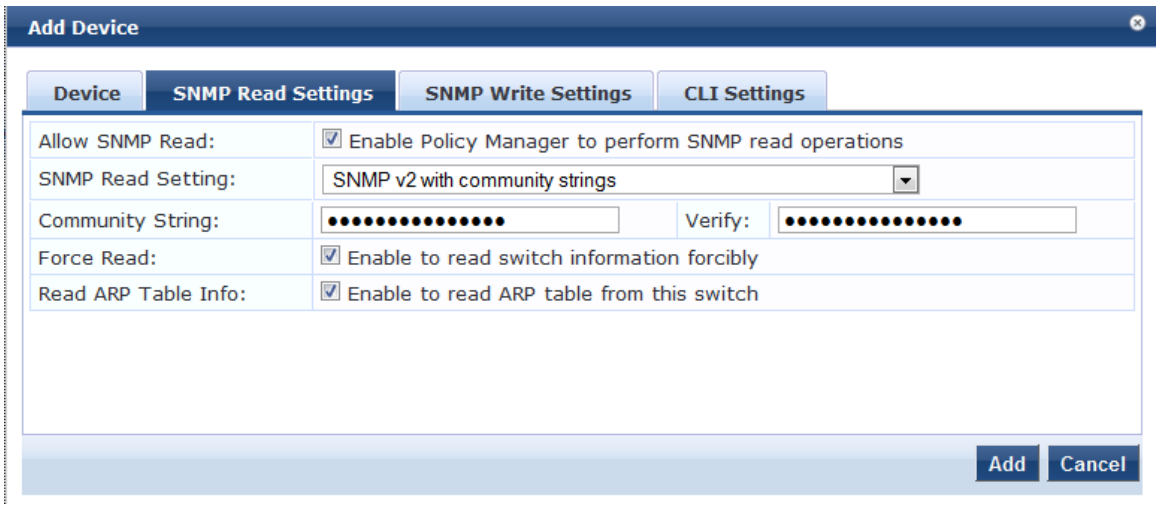
Note that the SNMP based mechanism is only capable of profiling devices if they respond to SNMP, or if the device advertises its capability via LLDP. When performing SNMP reads for a device, CPPM uses SNMP Read credentials configured in Network Devices, or defaults to using SNMP v2c with "public" community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

Network Devices configured with SNMP Read enabled are polled periodically for updates based on the time interval configured in **Administration > Server Configuration > Service Parameters tab > ClearPass network services option > Device Info Poll Interval**.

The following additional settings are included with profile support:

- Read ARP Table Info - Enable this setting if this is a Layer 3 device, and you want to use ARP table on this device as a way to discover endpoints in the network. Static IP endpoints discovered this way are further probed via SNMP to profile the device.
- Force Read - Enable this setting to ensure that all CPPM nodes in the cluster read SNMP information from this device regardless of trap configuration on the device. This option is especially useful when demonstrating static IP-based device profiling because this does not require any trap configuration on the network device.

Figure 335: *SNMP Read/Write Settings Tabs*



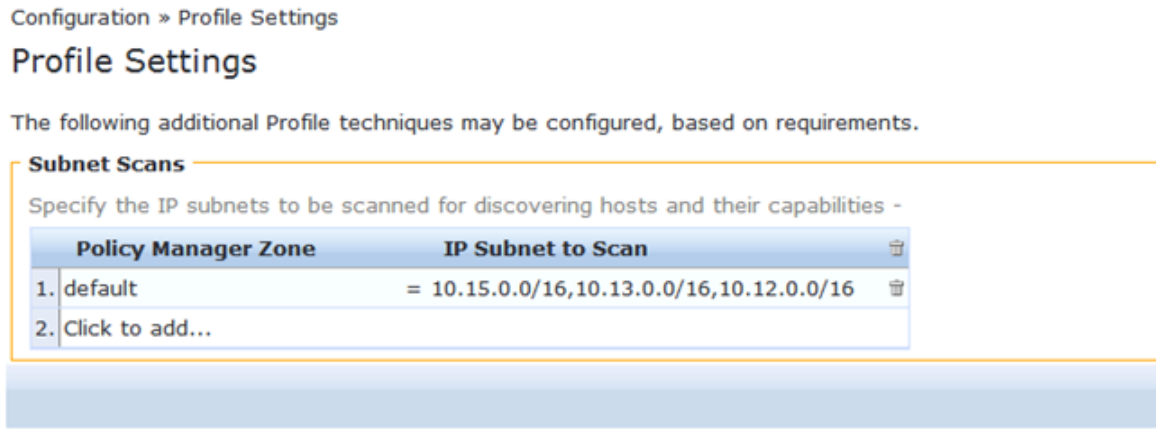
In large or geographically spread cluster deployments, you do not want all CPPM nodes to probe all SNMP configured devices. The default behavior is for a CPPM node in the cluster to read network device information only for devices configured to send traps to that CPPM node.

Subnet Scan

A network subnet scan is used to discover IP addresses of devices in the network. The devices discovered this way are further probed using SNMP to fingerprint and assign a profile to the device. Network subnets to scan 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 for a minimum of one node per zone. For more information, see Policy Manager Zones on page 435.

The following figure displays the **Subnet Scans** page:

Figure 336: *Subnet Scans Page*



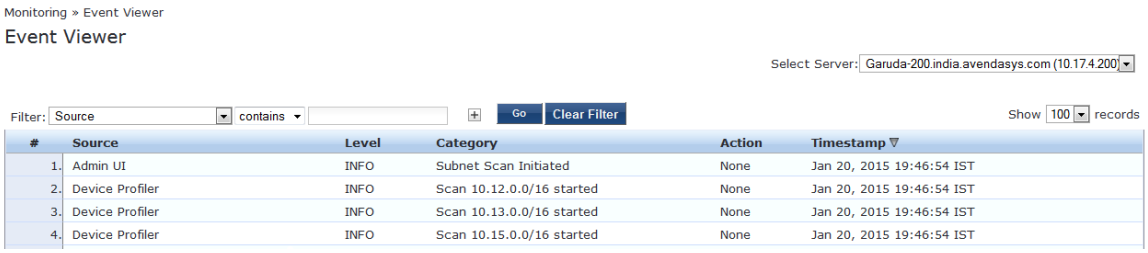
To configure the subnet scans:

1. Navigate to the **Configuration** > **Profile Settings** page.
2. Select a **Policy Manager Zone** by clicking **Click to add** drop-down.
3. Click **IP Subnet to Scan** to enter the IP subnets and click the **Save** icon.

4. Click the **On-demand Subnet Scan** link. The **Initiate On-Demand Subnet Scan** pop-up opens. Specify the IP subnets to be scanned in the **Subnets to scan** field for discovering hosts.
5. Click **Submit**. The subnet scan progress is shown on the **Profile Settings** page. You can view the subnet scan events in the **Event Viewer** (**Monitoring** > **Event Viewer**) page.

The following figure displays the subnet scan logs in the **Event Viewer** page:

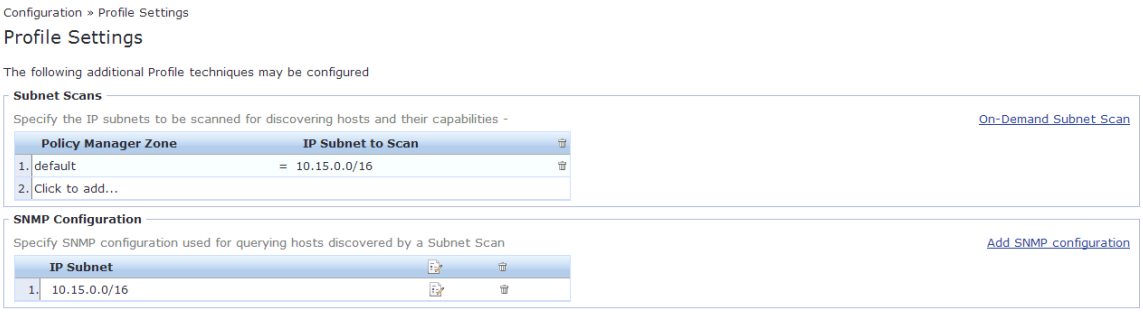
Figure 337: *Event Viewer - Subnet Scan*



SNMP Configuration

For wired network profiling, a list of multiple SNMP community strings can now be configured and used to query static IP devices discovered by the Profiler. If a static IP device does not respond to queries from the default public community string, the SNMP service can use the credentials from this custom list to query the device.

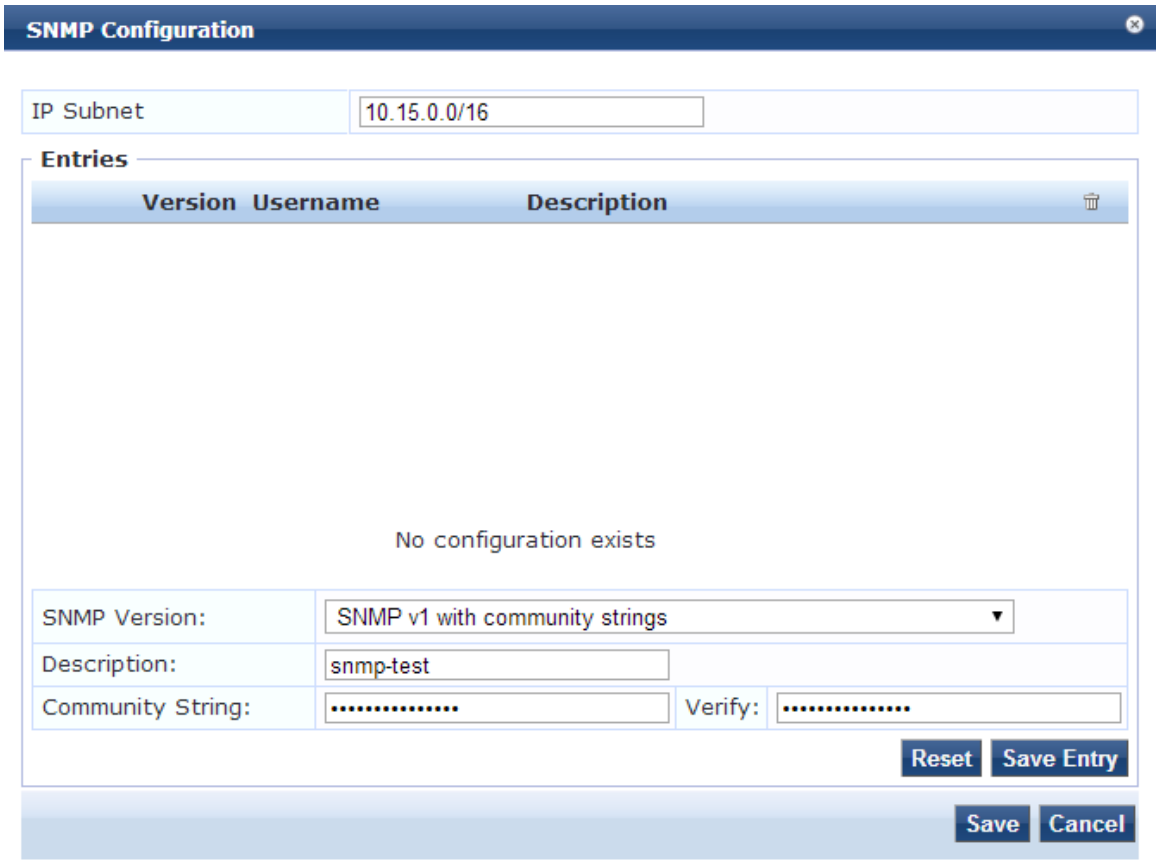
The following figure displays the **SNMP Configuration** page:



To configure SNMP community strings:

1. Click **Add SNMP configuration**. The **SNMP Configuration** pop-up opens.

Figure 338: *Profile Settings - SNMP Configuration*



2. Enter the IP subnet in the **IP Subnet** field.
3. You can set any of the following SNMP versions from the **SNMP Version** field:
   - SNMP v1 with community strings
   - SNMP v2 with community strings
   - SNMP v3 with no Authentication
   - SNMP v3 with Authentication using MD5 and no Privacy
   - SNMP v3 with Authentication using MD5 and with Privacy
   - SNMP v3 with Authentication using SHA and no Privacy
   - SNMP v3 with Authentication using SHA and with Privacy
4. Enter the description that provides additional information in the **Description** field.
5. Enter the community strings to verify.
6. Click **Save Entry** and click **Save**.

Fingerprint Dictionaries

CPPM uses a set of dictionaries and built-in rules to perform device fingerprinting. For more information, see Fingerprints Dictionary on page 543. Because these dictionaries can change frequently and CPPM provides a way to automatically update fingerprints from a hosted portal. If external access is provided to CPPM, the fingerprints file can be downloaded and imported through CPPM admin. For more information, see Software Updates on page 556.

Profiling

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

Stage 1

Stage 1 tries to derive device profiles using static dictionary lookups. Based on the available attributes available, Stage 1 looks up DHCP, HTTP, ActiveSync, MAC OUI, and SNMP dictionaries and derives multiple matching profiles. After multiple matches are returned, the priority of the source that provided the attribute is used to select the appropriate profile.

The following list shows the decreasing order of priority:

- OnGuard/ActiveSync plugin
- HTTP User-Agent
- SNMP
- DHCP
- MAC OUI

Stage 2

CPPM comes with a built-in set of rules that evaluates to a device-profile. Rules engine uses all input attributes and device profiles from Stage 1. The resulting rule evaluation may or may not result in a profile. Stage 2 is intended to refine the results of profiling.

Example

With DHCP options, Stage 1 can identify an Android device. Stage 2 uses rules to combine this with MAC OUI to further classify an Android device as Samsung Android and HTC Android.

For more information, see:

- Post Profile Actions on page 365

The Profiler User Interface

CPPM provides interfaces pages that administrators can use to search and view profiled endpoints and also provides basic statistics about the profiled endpoints. The Cluster Status Dashboard widget shows basic distribution of device types.

The **Monitoring > Live Monitoring > Endpoint Profiler** page provides detailed device distribution information and a list of endpoints. From this page, you can search for endpoint profiles based on category, family, and name.

For more information, see:

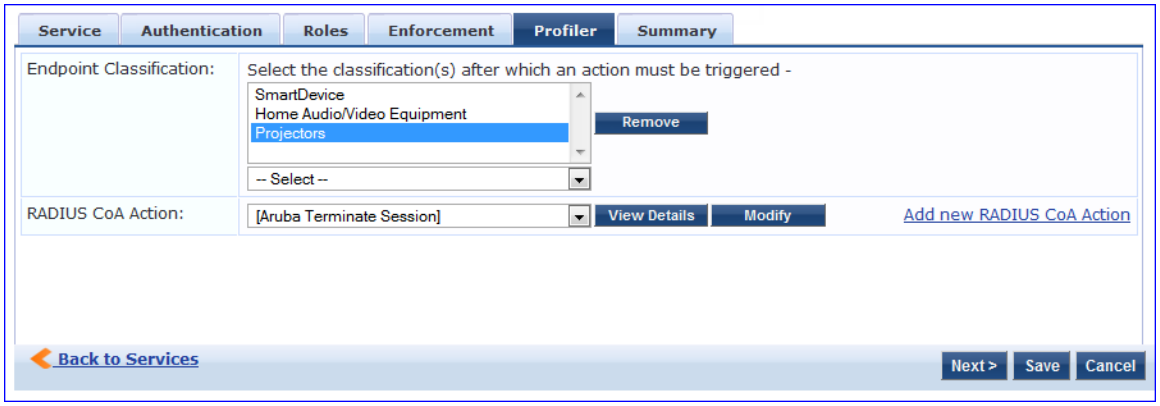
- Live Monitoring: Endpoint Profiler on page 69
- Policy Manager Dashboard on page 39

Post Profile Actions

After profiling an endpoint, use the **Profiler** tab to configure parameters to perform CoA on the network device to which an endpoint is connected. Post profile configurations are configured under service. The administrator can select a set of categories and a CoA profile to be applied when the profile matches one of the selected categories. CoA is triggered using the selected CoA profile. Any option from Endpoint Classification can be used to invoke CoA on a change of any one of the fields (category, family, and name).

The following figure displays the **Profiler** tab:

Figure 339: *Profiler tab*



The following table describes the **Profiler** tab parameters:

Table 203: *Profiler tab Parameters*

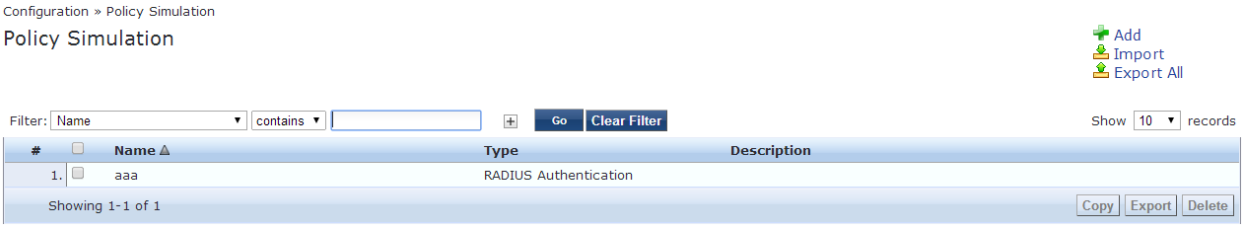
Parameter	Description
Endpoint Classification	Select the classification after which an action must be triggered. You can select a new action, or remove a current action.
RADIUS CoA Action	Select an action. Click **View Details** to view details about the selected action. Click **Modify**to change the values of the selected action.
Add new RADIUS CoA Action	Click to add a RADIUS CoA action to the list.

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

This chapter describes the following types of simulations:

The following figure displays the **Policy Simulation** page:

Figure 340: *Policy Simulation page*



The following table describes the **Policy Simulation** page parameters:

Table 204: *Policy Simulation Configuration Parameters*

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

Active Directory Authentication

This simulation tests authentication against an Active Directory domain or trusted domain to verify that the CPPM domain membership is valid.

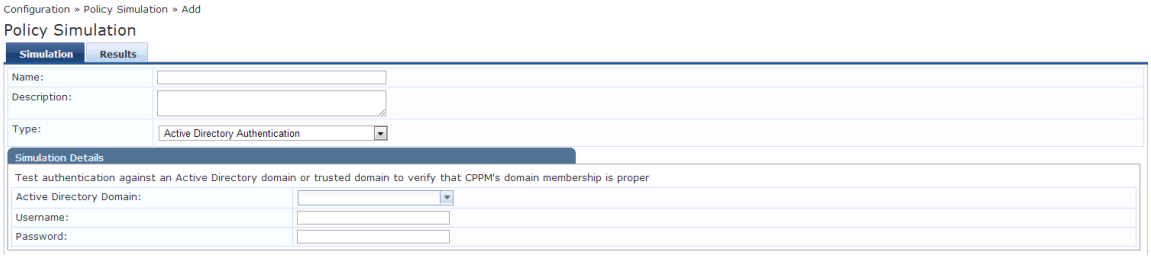
NOTE

The **Attributes** tab is not available for this simulation type.

Simulation Tab

The figure below displays the **Active Direction Authentication** policy simulation settings available on the **Configuration > Policy Simulation > Add** page. The following figure displays the **Active Directory Authentication - Simulation** tab:

Figure 341: *Active Directory Authentication - Simulation Tab*



The following table describes the **Active Directory Authentication - Simulation** tab parameters:

Table 205: *Active Directory Authentication Simulation Tab Parameters*

Parameter	Description
Active Directory Domain	Select the domain(s) to which the node is joined.
Username	Enter the username to login to the domain.
Password	Enter the password to login to the domain.

Results Tab

The **Results** tab for the **Active Directory Authentication** simulation displays a summary of the Authentication test and provides a status message. The following figure displays the **Active Directory Authentication - Results** tab:

Figure 342: *Active Directory Authentication Results Tab*

Table 206: *Active Directory Authentication Results Tab Parameters*

Parameter	Description
Summary	Displays the results of the Active Directory Authentication simulation.
Status	Displays the status message.

Application Authentication

This simulation tests authentication requests generated from ClearPass Guest. The following figure displays the **Application Authentication** policy simulation settings available on the **Configuration > Policy Simulation > Add** page:

Simulation Tab

Figure 343: *Application Authentication - Simulation Tab*

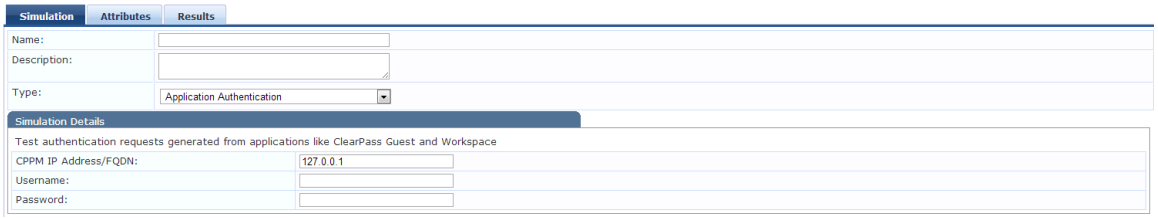


Table 207: *Application Authentication Simulation Tab Parameters*

Parameter	Description
CPPM IP Address/FQDN	Enter the IP Address or FQDN of the domain(s) to which the node is joined.
Username	Enter the username.
Password	Enter the password.

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the **Application Authentication - Attributes** tab:

Figure 344: *Application Authentication - Attributes Tab*

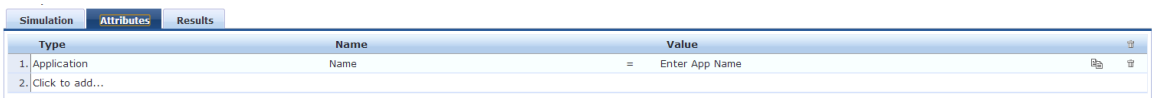


Table 208: *Application Authentication - Attributes Tab Parameters*

Attribute	Parameter
Type	Select Application or select Application:ClearPass. See Application Namespace on page 602
Name	The options displayed for the Name Attribute depend on the Type Attribute that was selected.
Value	The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.

Results tab

The Results tab of the Application Authentication simulation displays the outcome of the **Authentication Result** and the **Application Authentication Output Attributes**. The following figure displays the

Application Authentication Results tab:

Figure 345: *Application Authentication Results Tab*

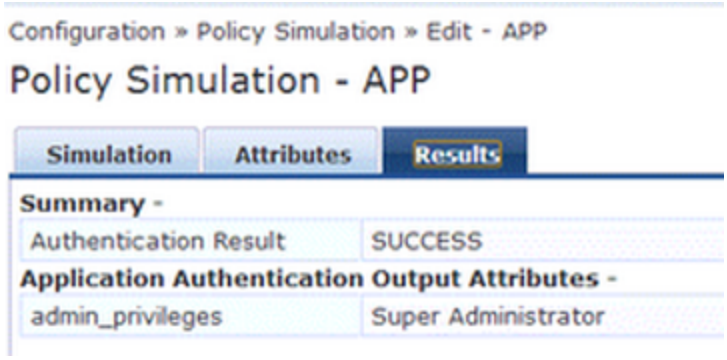


Table 209: *Application Authentication Results Tab Parameters*

Parameter	Description
Summary	Displays the results of the Active Directory Authentication simulation.
Application Authentication Output Attributes	Displays the output attributes, such as Super Administrator.

Audit

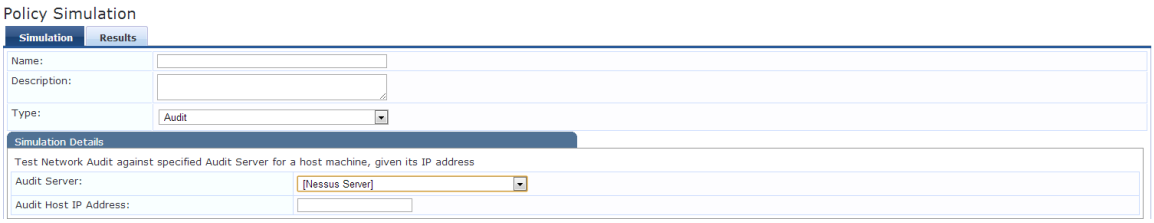
This simulation allows you to specify an audit against a Nessus Server or Nmap Server with its IP address.

The **Attributes** tab is not available for this simulation type.

Audit simulations can take more than 30 minutes. An **AuditinProgress** status message is displayed until the audit is completed.

The following figure displays the **Audit Simulation** tab:

Figure 346: *Audit Simulation - Simulation Tab*



The following table describes the **Audit Simulation - Simulation** tab parameters:

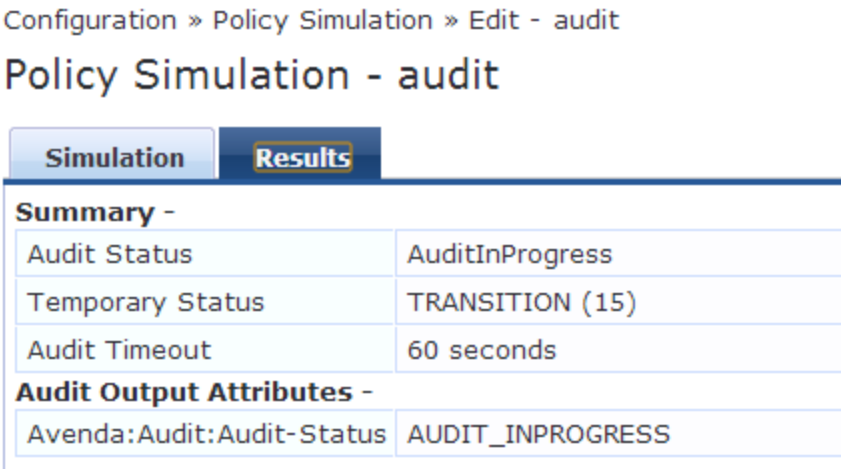
Table 210: *Audit Simulation Tab Parameters*

Parameter	Description
Audit Server	Select [Nessus Server] or [Nmap Audit].
Audit Host IP Address	Enter the host IP address of the audit host.

Results Tab

The following figure displays the **Audit Simulation - Results** tab:

Figure 347: *Audit Simulation Results Tab*



The following table describes the **Audit Simulation - Results** tab parameters:

Table 211: *Audit Results Tab Parameters*

Parameter	Description
Summary	Displays information about the Audit Status, Temporary Status, and Audit Timeout.
Audit Output Attributes	Displays the Audit-Status such as AUDIT_INPROGRESS.

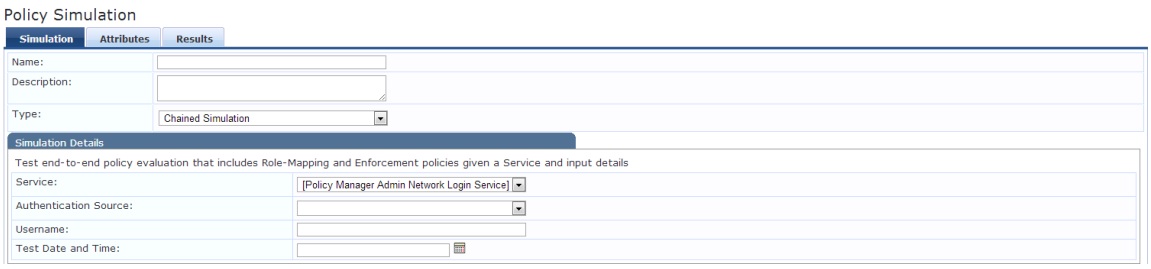
Chained Simulation

Given the service name, authentication source, user name, and an optional date and time, the chained simulation combines the results of role mapping, posture validation and enforcement policy simulations and displays the corresponding results.

Simulation Tab

The following figure displays the **Chained Simulation Simulation** tab:

Figure 348: *Chained Simulation Tab*



The following table describes the **Chained Simulation - Results** tab parameters:

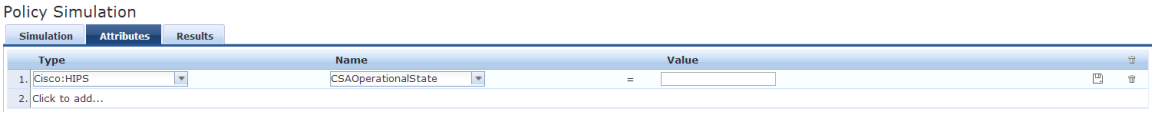
Table 212: *Chained Simulation Tab Parameters*

Parameters	Description
Service	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Authentication Source	Default Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Default Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching Values = [Guest Device Repository] *or* [Local User Repository] if you select [Guest Operator Logins]
Username	Enter the username.
Test Date and Time	Click the calendar icon to select a start date and time for simulation test. For more information, see Date Namespaces on page 608

Attributes Tab

Enter the attributes of the policy component to be tested.

Figure 349: *Chained Simulation Attributes Tab*



The following table describes the **Chained Simulation Attributes - Results** tab parameters:

Table 213: *Chained Simulation Attributes tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 609
Authentication	See Authentication Namespaces on page 603
Connection	See Connection Namespaces on page 607

Attribute	Parameter
Application	See Application Namespace on page 602
Certificate	See Certificate Namespaces on page 606
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba • Trend:AV • Cisco: HIPS • Cisco:HOST • Cisco:PA • NAI:AV • Symantec:AV	See RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Results Tab

The following figure displays the **Chained Simulation - Results** tab:

Figure 350: *Chained Simulation Results Tab*

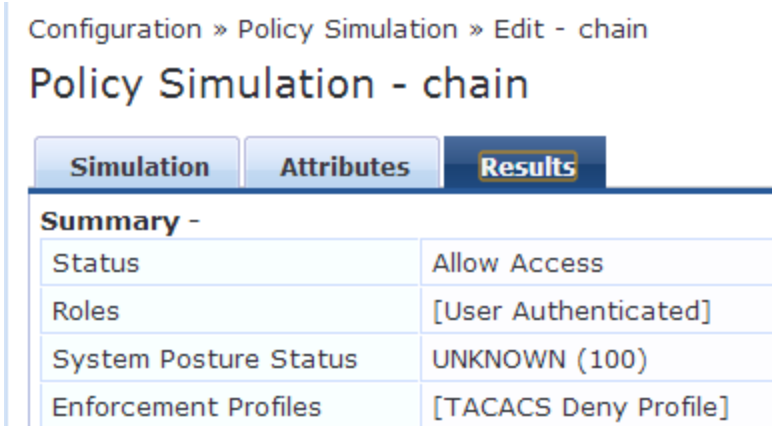


Table 214: *Chained Simulation Results Tab Parameters*

Parameter	Description
Summary	Provides the following information about the chained simulation: • Status • Roles • System Posture Status • Enforcement Profiles

Enforcement Policy

Given the service name (and the associated enforcement policy), a role or a set of roles, the system posture status, and an optional date and time, the enforcement policy simulation evaluates the rules in the enforcement policy and displays the resulting enforcement profiles and their contents.

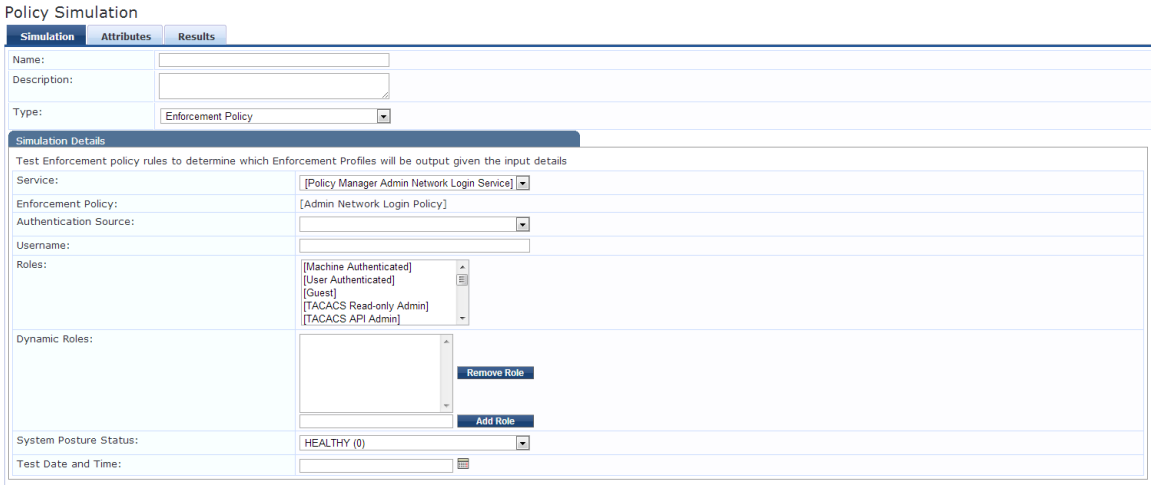
Authentication Source and User Name inputs are used to derive dynamic values in the enforcement profile that are retrieved from the authorization source. These inputs are optional.

Dynamic roles are attributes that are enabled as a role retrieved from the authorization source. For an example of enabling attributes as a role, see Generic LDAP and Active Directory on page 170.

Simulation Tab

The following figure displays the **Enforcement Policy Simulation** tab:

Figure 351: *Enforcement Policy Simulation Tab*



The following table describes the **Enforcement Policy Simulation** tab parameters:

Table 215: *Enforcement Policy Simulation tab Parameters*

Parameter	Description
Service	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Enforcement Policy	• Autofilled with **[Admin Network Login Policy]** if you select [Policy Manager Admin Network Login Service] • Autofilled with **[AirGroup Enforcement Policy]** if you select [AirGroup Authorization Service] • Autofilled with **[Aruba Device Access Policy]** if you select [Aruba Device Access Service] • Autofilled with **[Guest Operator Logins]** if you select [Guest Operator Logins] service • Autofilled with **Copy_of_Guest Access Policy** if you select Guest Access service • Autofilled with **Guest Access With MAC Caching Policy** if you select Guest Access With MAC Caching
Authentication Source	Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching Values = [Local User Repository] *or* [Guest Device Repository] if you select Guest Operator Logins
Username	Enter username.
Roles	Select from: • [Machine Authenticated] • [User Authenticated] • [Guest] • [TACACS Read-only Admin] • [TACACS API Admin] • [TACACS Help Desk] • [TACACS Receptionist] • [TACACS Network Admin] • [TACACS Super Admin] • [Contractor] • [Other] • [Employee] • [MAC Caching • [Onboard Android]

Table 215: *Enforcement Policy Simulation tab Parameters (Continued)*

Parameter	Description
	• [Onboard Windows] • [Onboard Mac OS X] • Onboard iOS] • [Aruba TACACS root Admin] • [Aruba TACACS read-only Admin] • [Device Registration] • [BYOD Operator] • [AirGroup V1] • [AirGroup v2]
Dynamic Roles	Add Role: Enter the name of a dynamic role in the Add Role field and click the Add Role button to populate the Dynamic Roles list. Remove role: Highlight a dynamic role and click Remove Role button.
System Posture Status	Select from: • HEALTHY (0) • CHECKUP (10) • TRANSITION (15) • QUARANTINE (20) • INFECTED (30) • UNKNOWN (100) See Posture Namespaces on page 610
Test Date and Time	Click calendar icon to select start date and time for simulation test. See Date Namespaces on page 608

Attributes tab

Enter the attributes of the policy component to be tested. The following figure displays the **Enforcement Policy - Attributes** tab:

Figure 352: *Enforcement Policy Attributes Tab*

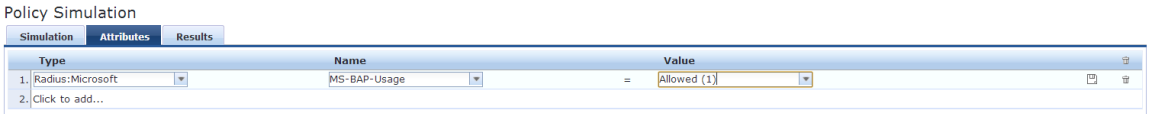


Table 216: *Enforcement Policy Attributes tab Parameters*

Attribute	Description
Type:	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 609
Authentication	See Authentication Namespaces on page 603
Connection	See Connection Namespaces on page 607

Table 216: *Enforcement Policy Attributes tab Parameters (Continued)*

Attribute	Description
Application	See Application Namespace on page 602
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba	See RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Results Tab

The following figure displays the **Enforcement Policy - Results** tab:

Figure 353: *Policy Simulation Results Tab*

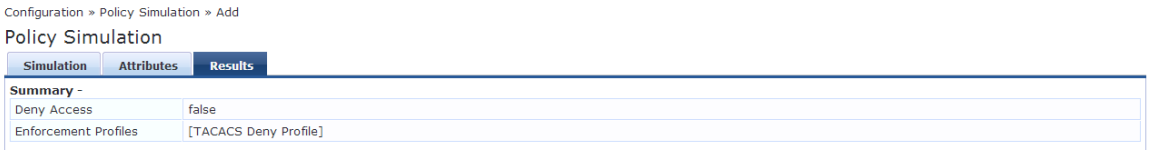


Table 217: *Enforcement Policy Results Tab Parameters*

Parameter	Description
Deny Access	Displays the output of the Deny Access test.
Enforcement Profile	Displays the name of the Enforcement Profile.

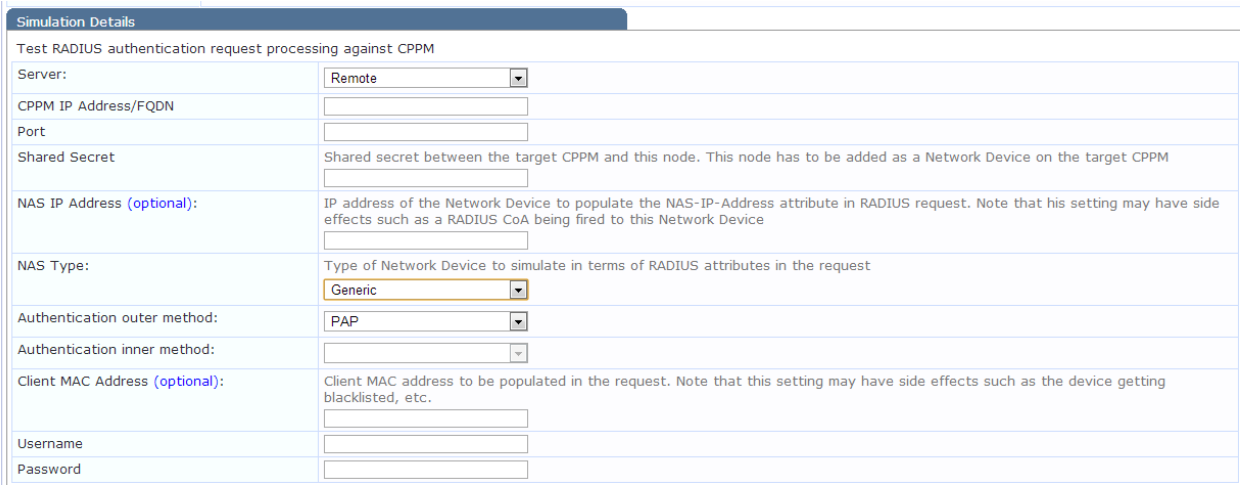
RADIUS Authentication

Dictionaries in the RADIUS namespace come pre-packaged with the product. The administration interface does provide a way to add dictionaries into the system (see RADIUS Dictionary on page 538 for more information). The RADIUS namespace uses the notation RADIUS:*Vendor*, where *Vendor* is the name of the Company that has defined attributes in the dictionary. Sometimes, the same vendor has multiple dictionaries, in which case the "Vendor" portion has the name suffixed by the name of the device or some other unique string.

Simulation tab

Use this tab to define the RADIUS authentication server for the authentication test. The following figure displays the **RADIUS Authentication Simulation** settings available on the **Configuration > Policy Simulation > Add** page:

Figure 354: *RADIUS Authentication Simulation Tab (Remote Server selected)*



The following table describes the **RADIUS Simulation** tab parameters:

Table 218: *RADIUS Simulation Tab Parameters*

Parameter	Description
Server	Select Local or Remote.
CPPM IP Address or FQDN	**NOTE:** This field is only displayed if Remote Server is selected. Enter the IP Address or FQDN of the remote CPPM server.
Port	**NOTE:** This field is only displayed if Remote Server is selected. Enter the port number of the remote CPPM server. The default port number is 1812.
Shared Secret	**NOTE:** Only displayed if Remote Server is selected. Enter the shared secret between the target CPPM and this node. You must add the node as a Network Device on the target CPPM server.
Shared Secret	This field is only displayed if Remote Server is selected.
NAS IP Address (optional)	Enter the IP address of the network device to populate the NAS-IP-Address attribute in a RADIUS request.
NAS Type	Select the type of network device to simulate in terms of RADIUS attributes in the request. The NAS types are: • Aruba Wireless Controller • Aruba Wired Switch • Cisco Wireless Controller • Generic
Authentication outer method	• PAP - Authentication inner method: field is disabled. • CHAP - Authentication inner method field: is disabled. • MSCHAPv2 - Authentication inner method field: is disabled. • PEAP - Authentication inner method field: is enabled. The selections are: ▪ EAP-MSCHAPv2

Table 218: *RADIUS Simulation Tab Parameters (Continued)*

Parameter	Description
	▪ EAP-GTC ▪ EAP-TLS • TTLS -Authentication inner method field: is enabled. The selections are: ▪ PAP ▪ CHAP ▪ MSCHAPv2 ▪ EAP-MSCHAPv2 ▪ EAP-GTC ▪ EAP-TLS • TLS - Authentication inner method: field is disabled. For more information, see Authentication Namespaces on page 603
Client MAC Address (optional)	Enter the client MAC address to be populated in the request.
Username	Enter the username.
Password	Enter the password.
CA Certificate (optional)	1. Click **Choose File**. 2. Navigate to the optional Root CA certificate that is required to verify the RADIUS server's certificate. 3. Click **Open**. 4. Click **Upload**.
Client Certificate PKCS12 (PFX)*	1. Click **Choose File**. 2. Navigate to the client certificate that is used for TLS in PKCS12 - .pfx format, or .pfx or .p12 format. 3. Click **Open**. 4. Click **Upload**.
Passphrase for PFX file*	Enter the Passphrase for the selected PFX file.
* These fields are only displayed if you select TTLS *or* PEAP as the Authentication outer method: *and* you select EAP-TLS as the Authentication inner method.	

Attributes tab

Enter the attributes of the policy component to be tested.

The attributes that you set depend on the NAS Type selected on the **Simulation** page.

NAS Type: Aruba Wireless Controller

Figure 355: *Aruba Wireless Controller Type - Attributes Tab*

Table 219: *Aruba Wireless Controller Required - Attribute Settings*

Attribute	Parameter
Line 1: • Type = Radius:IETF • Name = NAS-Port-Type • Value = Wireless-802.11 (19)	
Line 2: • Type = Radius:IETF • Name = Service-Type • Value = Login-User (1)	
Line 3: • Type = Radius:Aruba • Name = Aruba-Essid-Name • Value = SSID	

NAS Type: Aruba Wired Switch Controller

Figure 356: *NAS Type: Aruba Wired Switch Controller Attributes Tab*

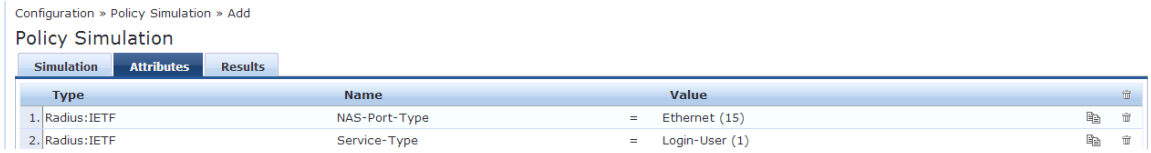


Table 220: *NAS Type: Aruba Wired Switch Controller Required Attribute Settings*

Attribute	
Line 1: • Type = Radius:IETF • Name = NAS-Port-Type • Value = Ethernet (15)	
Line 2: • Type = Radius:IETF • Name = Service-Type • Value = Login-User (1)	

NAS Type: Cisco Wireless Switch

Figure 357: *NAS Type: Cisco Wireless Switch Attributes Tab*

Table 221: *[NAS Type: Cisco Wireless Switch Required Attribute Settings*

Attribute	
Line 1: • Type = Radius:IETF • Name = NAS-Port-Type • Value = 802.11(19)	
Line 2: • Type = Radius:IETF • Name = Service-Type • Value = Framed-User(2)	

Results Tab

The followin figure displays the **Policy Simulation RADIUS - Results** tab:

Figure 358: *Results Tab*

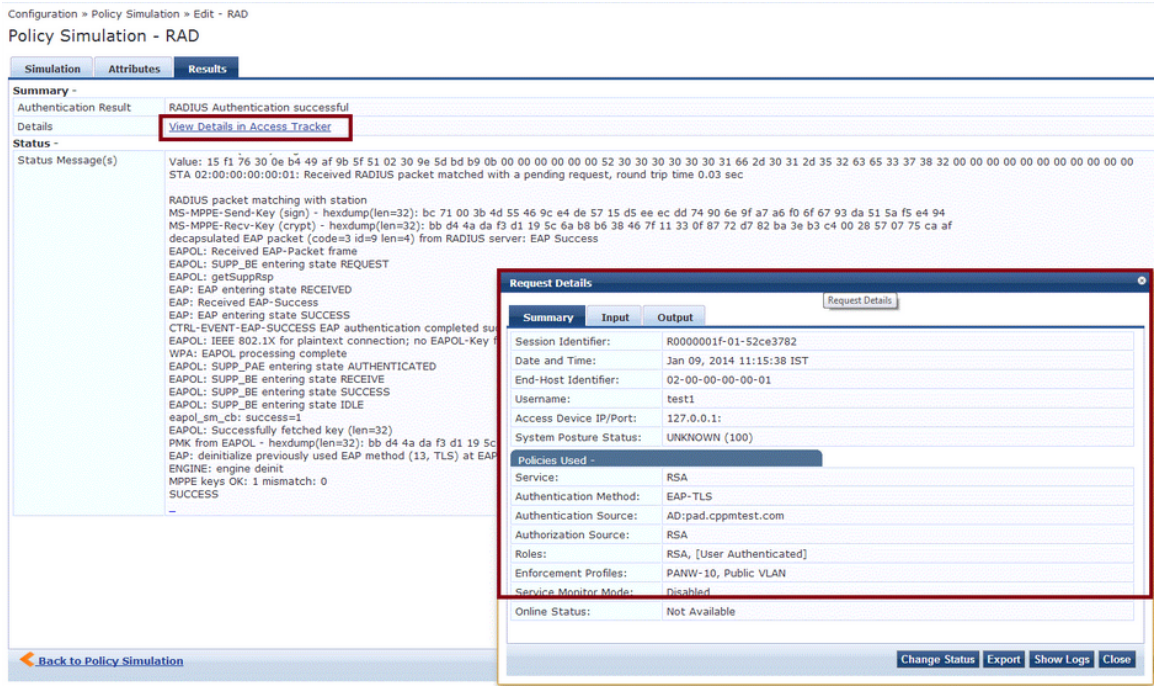


Table 222: *RADIUS Authentication Results Tab Parameters*

Parameter	Description
Summary	Displays a summary of the simulation.
Authentication Result	Displays the outcome of the Authentication test.
Details	Click this link to open a popup that provides details about the Authentication test. You can take the following actions: • Click the Summary, Input, and Output tabs • Click the Change Status, Show Logs, Export, or Close buttons.
Status Message(s)	Displays the status messages resulting from the test.

Role Mapping

The role mapping simulation tests Role-Mapping policy rules to determine which roles will be output, given the service name (and associated role mapping policy), the authentication source and the user name.

You can also use role mapping simulation to test whether the specified authentication source is reachable.

Simulation Tab

The following figure displays the **Role Mapping Simulation** tab:

Figure 359: *Role Mapping Simulation Tab*

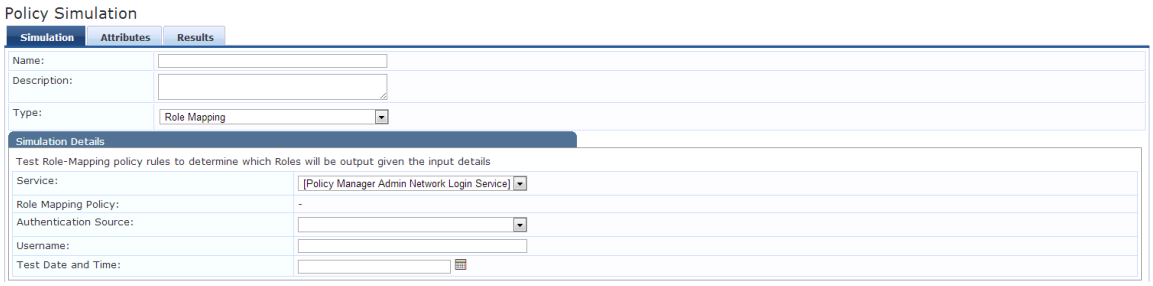


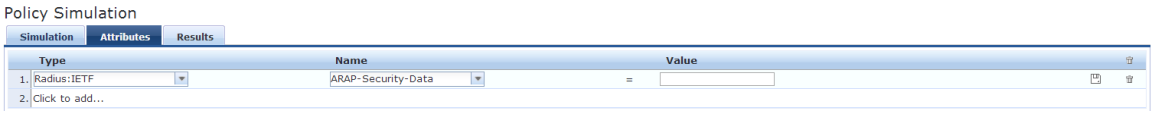
Table 223: *Role Mapping Simulation Tab Parameters*

Parameter	Description
Service	Select from: • [Policy Manager Admin Network Login Service] • [AirGroup Authorization Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Guest Access • Guest Access With MAC Caching
Role Mapping Policy	Field is disabled if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] • [Guest Operator Logins] • Field is auto-filled with **[AirGroup Version Match]** if you select [AirGroup Authorization Service] • Field is autofilled with **[Guest Roles]** if you select Guest Access • Field is autofilled with **Guest MAC Authentication Role Mapping** if you select Guest Access With MAC Caching
Authentication Source	Value = [Local User Repository] if you select: • [Policy Manager Admin Network Login Service] • [Aruba Device Access Service] Value = [Guest Device Repository] if you select: • [AirGroup Authorization Service] • Guest Access • Guest Access With MAC Caching Values = [Guest Device Repository] *or* [Local User Repository] if you select [Guest Operator Logins]
Username	Enter the user name.
Test Date and Time	Click calendar icon to select start date and time for simulation test. For more information, see Date Namespaces on page 608

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the **Role Mapping Simulation Attributes** tab:

Figure 360: *Role Mapping Simulation Attributes Tab*



The following table describes the **Role Mapping Simulation Attributes** tab parameters:

Table 224: *Role Mapping Simulation Attributes Tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 609
Authentication	See Authentication Namespaces on page 603
Connection	See Connection Namespaces on page 607
Application	See Application Namespace on page 602
Certificate	See Certificate Namespaces on page 606
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba	See RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Results Tab

The following figure displays the **Role Mapping Simulation - Results** tab:

Figure 361: *Results Tab*

The following table describes the **Role Mapping Simulation - Results** tab parameters:

Table 225: *Role Mapping Results Tab Parameters*

Parameter	Description
Summary	Displays the results of the simulation.

Service Categorization

A service categorization simulation allows you to specify a set of attributes in the RADIUS or Connection namespace and test which configured service the request will be categorized into. The request attributes that you specify represent the attributes sent in the simulated request.

Simulation Tab

The following figure displays the **Service Categorization Simulation - Simulation** tab:

Figure 362: *Service Categorization Simulation Tab*

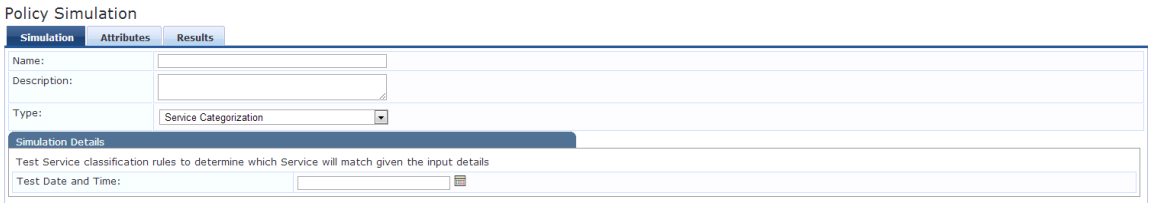


Table 226: *Service Categorization Simulation Tab Parameter s*

Parameter Type	Namespace Details
Test Date and Time	Click calendar widget and select: • Test start date • Test start time

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the **Service Categorization Simulation - Attributes** tab:

Figure 363: *Service Categorization Attributes Tab*

Table 227: *Service Categorization Simulation Attributes Tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 609
Authentication	See Authentication Namespaces on page 603
Connection	See Connection Namespaces on page 607
Application	See Application Namespace on page 602

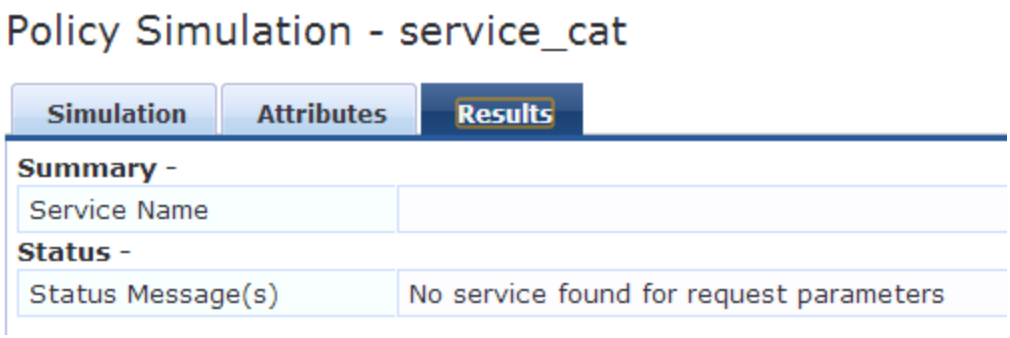
Table 227: *Service Categorization Simulation Attributes Tab Parameters (Continued)*

Attribute	Parameter
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Aruba	See RADIUS Namespaces on page 610
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Results Tab

The following figure displays the **Service Categorization - Results** tab:

Figure 364: *Results Tab*



The following table describes the **Service Categorization Simulation Results** tab parameters:

Table 228: *Service Configuration Results Tab Parameters*

Parameter	Description
Summary	Gives the name of the service.

Import and Export Simulations

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

Figure 365: *Import Simulations*

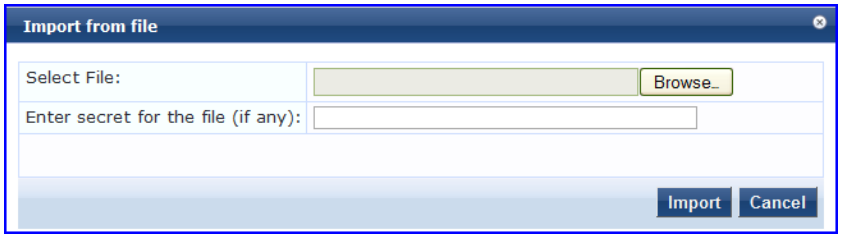


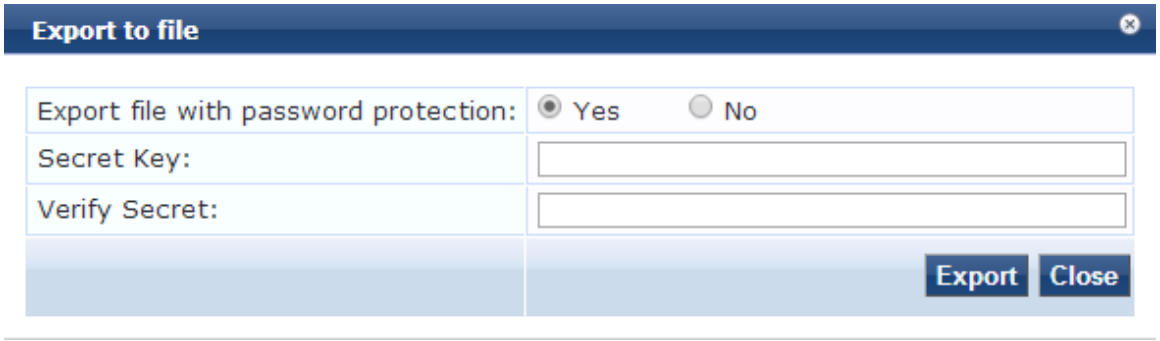
Table 229: *Import from file page Parameters*

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

Export Simulations

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

Figure 366: *Export Simulations*



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

Table 230: *Export Simulations*

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

Chapter 13
Administration

All administrative activities including server configuration, log management, certificate and dictionary maintenance, portal definitions, and administrator user account maintenance are done from the following Administration menus:

- ClearPass Portal
  - ClearPass Portal on page 390
- Users and privileges
  - Admin Users on page 391
  - Admin Privileges on page 393
- Server Manager
  - Server Configuration on page 399
  - Log Configuration on page 457
  - Local Shared Folders on page 460
  - License Management on page 461
- External Servers
  - SNMP Trap Receivers on page 466
  - Syslog Targets on page 470
  - Syslog Export Filters on page 475
  - Messaging Setup on page 487
  - Endpoint Context Servers on page 489
  - File Backup Servers on page 522
- Certificates
  - Server Certificate on page 523
  - Certificate Trust List on page 535
  - Certificate Revocation Lists on page 537
- Dictionaries
  - RADIUS Dictionary on page 538
  - Posture Dictionary on page 540
  - TACACS+ Services Dictionary on page 542
  - Fingerprints Dictionary on page 543
  - Attributes on page 544
  - Applications Dictionaries on page 547
  - Endpoint Context Server Actions on page 548
- Agents and Software Updates
  - OnGuard Settings on page 553
  - Software Updates on page 556
- Support
  - Contact Support on page 561
  - Remote Assistance on page 561

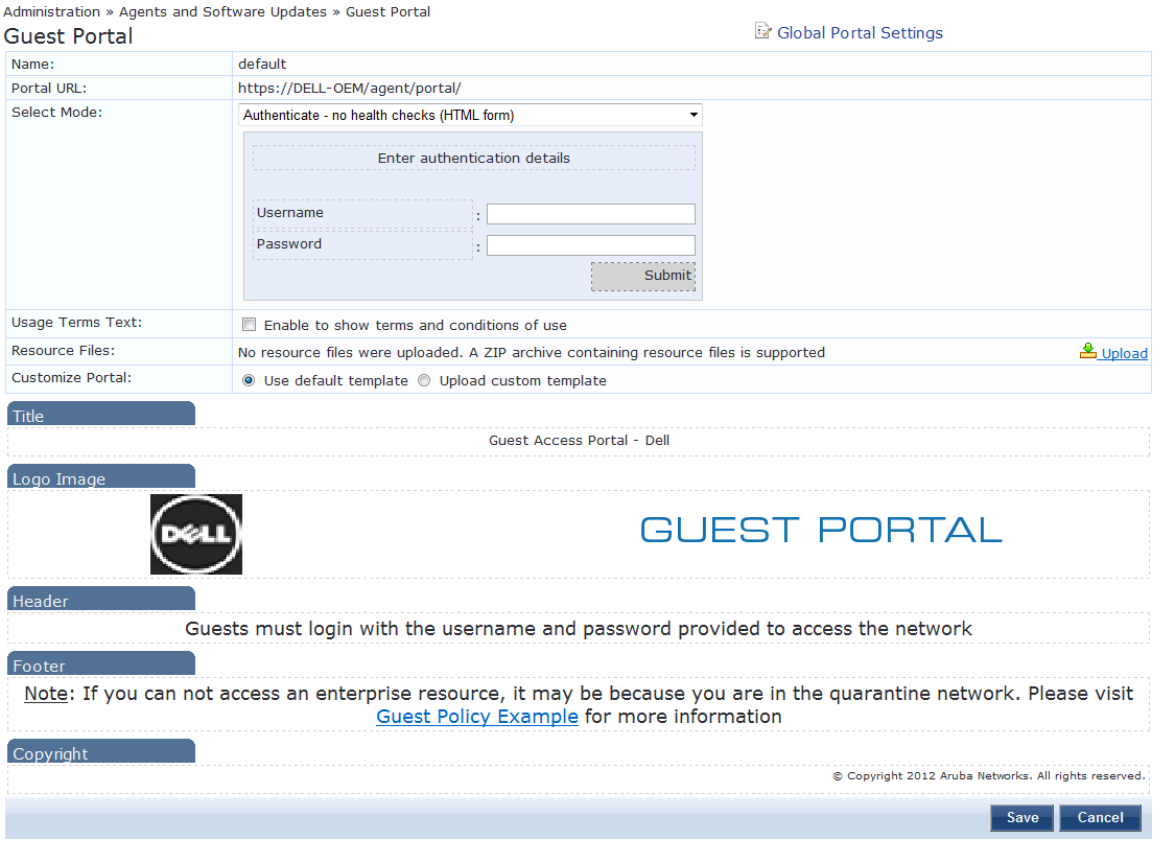
■ Documentation on page 564

ClearPass Portal

Navigate to the **Administration > Agents and Software Updates > ClearPass Portal** page. Using this page you can customize the content for your enterprise.

The following figure displays the ClearPass Portal page:

Figure 367: *ClearPass Portal*



The following table describes the ClearPass Portal parameters:

Table 231: *ClearPass Portal Parameters*

Parameter	Description

Select Option	Select the page that the user first sees after logging in to ClearPass:
	• Default Landing Page
	• Application Login Page:
	  ▪ ClearPass Policy Manager
	  ▪ ClearPass Guest
	  ▪ ClearPass Insight
	  ▪ ClearPass Onboard
	• Guest Portal

Page Title	Click and type the text to appear as the page title in the default landing page.
Logo Image	Click and browse to select an image for the banner in the default landing page.
Top section	Click and type the text to appear as the header in the default landing page.
Bottom section	Click and type the text to appear as the footer in the default landing page.
Copyright	Click and type the copyright text to appear in the default landing page.

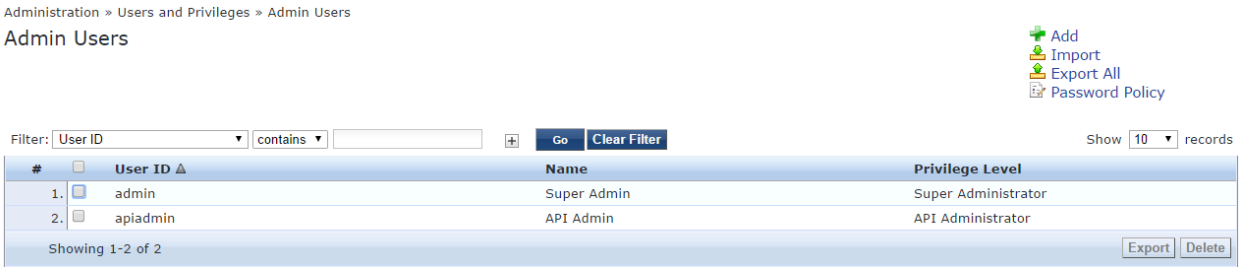
Both HTTP and HTTPS protocols are supported for Guest Portal re-direction.

Admin Users

You can navigate to **Administration > Users and Privileges > Admin Users** to view a list of all the Dell Networking W-ClearPass Policy Manager administrators. In this page, you can view the administrator details such as user ID, user name, and privilege level. You can also add, import, export, and set password policies for the admin users by using the links provided at the top right corner of this page.

The following figure displays the **Admin Users** page:

Figure 368: *Admin Users*



This section describes the following topics:

- Adding an Admin User on page 392
- Importing and Exporting Admin Users on page 392

- Setting Password Policy for Admin Users

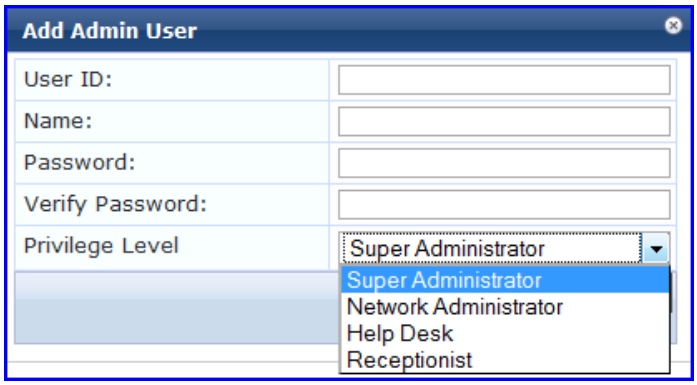
Adding an Admin User

To add a new admin user to the **Admin Users** table:

1. Click the **Add** link at the top right corner the page. The **Add Admin User** pop-up is displayed.
2. In the **User ID** and **Name** fields, specify a user ID and name for the admin user.
3. In the **Password** and **Verify Password** fields, specify a password for the admin user.
4. Select a privilege level from the **Privilege Level** drop down list.
5. Click **Add**.

The following figure displays the **Add Admin User** pop-up:

Figure 369: *Add Admin User*



Importing and Exporting Admin Users

You can import or export the admin user accounts by using the **Import** and **Export All** links at the top-right corner of the **Admin Users** page. You can also export specific admin user accounts by using the **Export** button that appears after selecting one or more admin user accounts from the list. For more information on importing and exporting admin users, see Importing on page 35 and Exporting on page 36.

NOTE

The passwords of the admin user accounts are not stored in cleartext when exported to an XML file.

Setting Password Policy for Admin Users

To set password policies for the administrators:

1. Click the **Password Policy** link at the top right corner of the page. The **Password Policy** pop-up is displayed.
2. Specify the minimum length required for the password in the **Minimum Length** field.
3. Select the complexity setting from the **Complexity** drop-down list. The complexity settings can be one of the following:
   - No password complexity requirement
   - At least one uppercase and one lowercase letter
   - At least one digit
   - At lease one letter and one digit
   - At least one of each: uppercase letter, lowercase letter, digit
   - At least one symbol

- At least one of each: uppercase letter, lowercase letter, digit, and symbol

4. Specify the characters not to be allowed in the password in the **Disallowed Characters** field.
5. Specify the words not to be allowed in the password in the **Disallowed Words (CSV)** field.
6. Select any additional checks, if required. The options are:
   - May not contain User ID or its characters in reversed order
   - May not contain repeated character four or more times consecutively
7. Set the password expiry time for the admin users. The allowed range is 0–500 days. The default value is 0.

NOTE

If the value is set to 0, the password never expires. For any other value, the admin users are forced to reset the expired password when they log in to the UI. The Policy Manager UI alerts the users five days before the password expires.

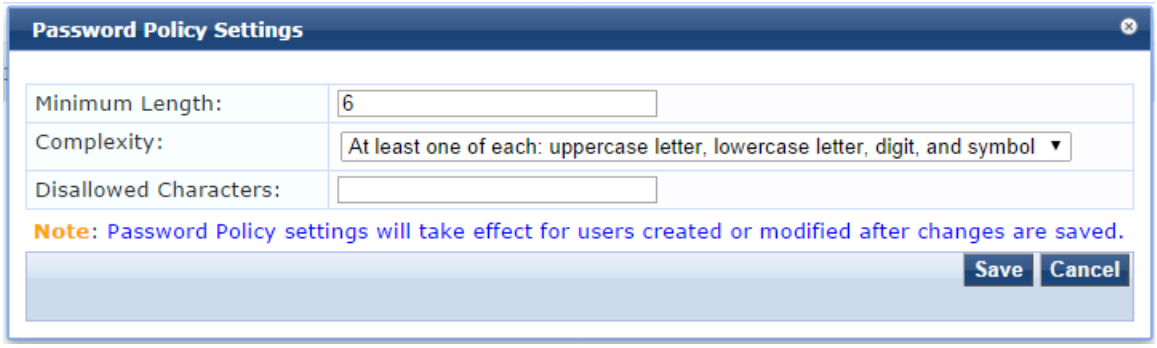
8. Click **Save**.

NOTE

Password Policy settings are effective only for the users created or modified after the changes are saved.

The following figure displays the **Password Policy Settings** pop-up:

Figure 370: *Set (Admin) Password Policy*



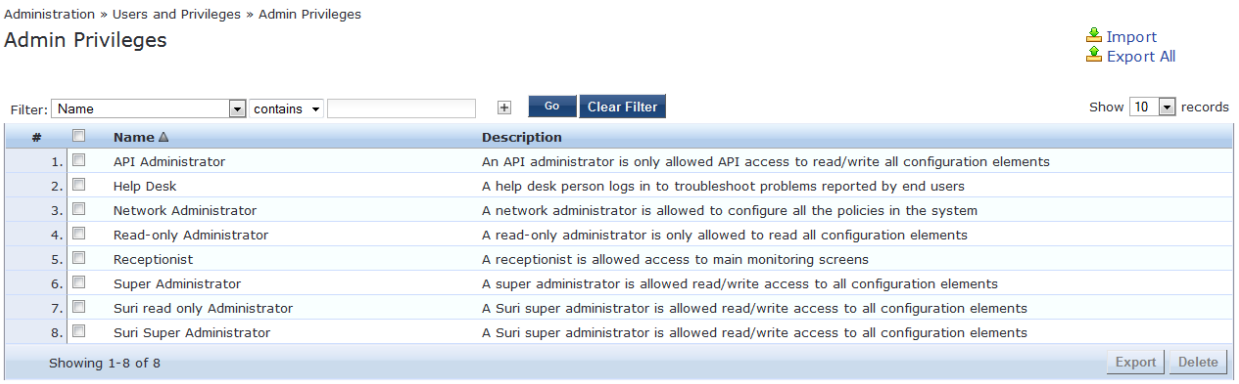
Admin Privileges

Dell Networking W-ClearPass Policy Manager ships with six read-only default administrator privilege XML files. You can export one or more default files and modify the file to create a customized administrator privileges file. Customized administrator privileges are defined in an XML file with a specific format and then imported into Dell Networking W-ClearPass Policy Manager on the **Admin Privileges** page.

To view the available admin Privileges, navigate to **Administration > Users and Privileges > Admin Privileges** page.

The following figure displays the **Admin Privileges** page:

Figure 371: *Admin Privileges Page*



For more information about the admin privileges file structure, refer to the following topics:

- Creating Custom Administrator Privileges on page 394
- Administrator Privilege XML File Structure on page 394
- Administrator Privileges and IDs on page 395
- Sample Administrator Privilege XML File on page 398

Creating Custom Administrator Privileges

To create a custom admin privilege XML file, you must use a plain text or XML editor.

Do not use word processing applications such as Microsoft Word which introduce tags and corrupt the XML file.

To create a custom administrator privilege:

1. Create an XML file that defines a privilege.
2. Store the new file.
3. Navigate to **Administration > Users and Privileges > Admin Privileges**.
4. Click **Import Admin Privileges**.
5. Import the administrator privilege file you created in step 1. For more information on importing a file, see Importing on page 35.

After you complete steps 1-5, the new administrator privileges document is displayed on the **Admin Privileges** page.

Administrator Privilege XML File Structure

Admin privilege files are XML files with a specific structure. It must have a header at the beginning of the file in the following format:

```
<?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 which must be in the following format:

```
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
⋮
</TipsContents>
```

An optional `TipsHeader` tag can follow the `TipsContents` tag. The actual admin privileges information is defined with the `AdminPrivilege` and `AdminTask` tags. You can use one `AdminPrivilege` tag for each admin privilege you want to define. The `AdminPrivilege` tag contains the following two attributes:

- `name`
- `description`

You can have one or more `AdminTask` tags inside the `AdminPrivilege` tag. Each `AdminTask` tag defines a lace within the Dell Networking W-ClearPass 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 contains an attribute, `type` which can take a value, `RO` (read only) or `RW` (read/write).

The following sample gives the basic structure of an admin privilege file:

```
<AdminPrivileges>
  <AdminPrivilege name="" description="">
    <AdminTask taskid="">
      <AdminTaskAction type=""/>
    </AdminTask>
    <AdminTask taskid="">
      <AdminTaskAction type=""/>
    </AdminTask>
  </AdminPrivilege>
</AdminPrivileges>
```

Administrator Privileges and IDs

Every UI element in the Dell Networking W-ClearPass Policy Manager application has a task ID associated with it. The users have access to the elements based on the permissions set for each task or element. By default, any permission provided for a task is applicable for all its sub-tasks. For example, if you give RW permissions for the task, **Enforcements** (con.en), it is automatically applied to its sub-tasks, **Policies** (con.en.epo) and **Profiles** (con.en.epr). Hence, you need not explicitly define the same permission for those sub-tasks.

The following list provides the tasks and sub-tasks of the Dell Networking W-ClearPass Policy Manager application and their associated task IDs:

Table 232: *Administrator Privileges and IDs*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
Dashboard	dnd
Monitoring	mon
• Live Monitoring	mon.li
▪ Access Tracker	mon.li.ad
▪ Accounting	mon.li.ac
▪ Onguard Activity	mon.li.ag
▪ Analysis and Trending	mon.li.sp
▪ Endpoint Profiles	mon.li.ep

Table 232: *Administrator Privileges and IDs (Continued)*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
▪ System Monitor	mon.li.sy
• Audit Viewer	mon.av
• Blacklisted Users	mon.bl
• Event Viewer	mon.ev
• Data Filters	mon.df
Configuration	con
• Start Here (Services Wizard)	con.sh
• Services	con.se
• Service Templates	con.st
• Authentication	con.au
▪ Methods	con.au.am
▪ Sources	con.au.as
• Identity	con.id
▪ Single Sign-On	con.id.sso
▪ Local Users	con.id.lu
▪ Endpoints	con.id.ep
▪ Static Host Lists	con.id.sh
▪ Roles	con.id.rs
▪ Role Mappings	con.id.rm
• Posture	con.pv
▪ Posture Policies	con.pv.in
▪ Posture Servers	con.pv.ex
▪ Audit Servers	con.pv.au
• Enforcements	con.en
▪ Policies	con.en.epo

Table 232: *Administrator Privileges and IDs (Continued)*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
▪ Profiles	con.en.epr
• Network	con.nw
▪ Devices	con.nw.nd
▪ Device Groups	con.nw.ng
▪ Proxy Targets	con.nw.pr
Policy Simulation	con.ps
Profile Settings	con.prs
Administration	adm
• User and Privileges	adm.us
▪ ClearPass Portal	adm.po.cp
▪ Admin Users	adm.us.au
▪ Admin Privileges	adm.us.ap
• Server Manager	adm.mg
▪ Server Configuration	adm.mg.sc
▪ Log Configuration	adm.mg.ls
▪ Local Shared Folders	adm.mg.sf
▪ Licensing	adm.mg.li
• External Servers	adm.xs
▪ SNMP Trap Receivers	adm.xs.st
▪ Syslog Targets	adm.xs.es
▪ Syslog Export Filters	adm.xs.sx
▪ Messaging Setup	adm.xs.me
▪ Endpoint Context Servers	adm.xs.cs
▪ Context Server Actions	adm.di.csa
• Certificates	adm.cm

Table 232: *Administrator Privileges and IDs (Continued)*

Area (Dell Networking W-ClearPass Policy Manager Menu)	Task ID
▪ Server Certificate	adm.cm.mc
▪ Trust List	adm.cm.ctl
▪ Revocation List	adm.cm.crl
• Dictionaries	adm.di
▪ RADIUS	adm.di.rd
▪ Posture	adm.di.pd
▪ TACACS+ Services	adm.di.td
▪ Fingerprints	adm.di.df
▪ Attributes	adm.di.at
▪ Applications	adm.di.ad
• Agents and Software Updates	adm.po
▪ Onguard Settings	adm.po.aas
▪ Software Updates	adm.po.es
• Support	adm.su
▪ Contact Support	adm.su.cs
▪ Remote Assistance	adm.su.ra
▪ Documentation	adm.su.doc

If you provide permission for an area, the same permission for all sub-areas is included by default. For example, if you give RW permissions for Enforcements (con.en), you grant permissions for its sub-areas, in this case, Policies (con.en.epo) and Profiles (con.en.epr), and you do not have to explicitly define the same permission for those sub-areas.

Sample Administrator Privilege XML File

This section provides sample XML files with different admin privileges for various UI elements.

The following sample provides Read Only (RO) Privilege to all the sections (dnd, con, mon, adm):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Read-only Administrator" description="A read-only administrator is
only allowed to read all configuration elements">
      <AdminTask taskid="con"> //Refers to Configuration
        <AdminTaskAction type="RO"/>
```

```
      </AdminTask>
      <AdminTask taskid="dnd"> //Refers to DashBoard
        <AdminTaskAction type="RO"/>
      </AdminTask>
      <AdminTask taskid="mon"> //Refers to Monitoring
        <AdminTaskAction type="RO"/>
      </AdminTask>
      <AdminTask taskid="adm"> //Refers to Administration
        <AdminTaskAction type="RO"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

The following sample provides Read/Write access only to Guest, Local and Endpoint Repository:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Read/Write Access to Guest, Local and Endpoint Repository"
description="A read-only administrator is only allowed to read all configuration elements">
      <AdminTask taskid="con.id.lu"> //Refers to Local Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.gu"> //Refers to Guest Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.ep"> //Refers to Endpoints Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

The following sample provides Read/Write permissions to DashBoard/ Monitoring and ReadOnly permissions to Server Configuration:

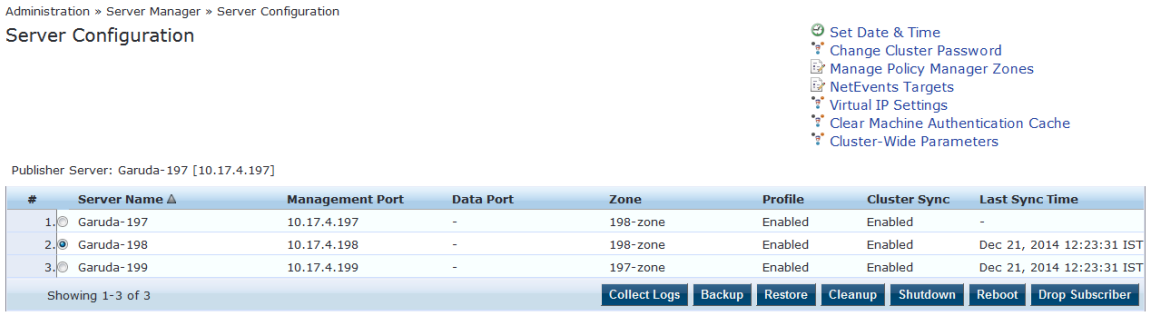
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Thu Jul 26 17:57:50 IST 2012" version="6.0"/>
  <AdminPrivileges>
    <AdminPrivilege name="Limited access permission" description="A read-only administrator 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

You can perform various server configuration tasks by navigating to **Administration > Server Manager > Server Configuration** page in the Dell Networking W-ClearPass Policy Manager UI.

The following figure displays the Server Configuration page:

Figure 372: *Server Configuration Page*



This section describes the following server configuration tasks:

- Edit Server Configuration Settings on page 400
- Set Date & Time on page 432
- Change Cluster Password on page 434
- Policy Manager Zones on page 435
- NetEvents Targets on page 436
- Virtual IP Settings on page 437
- Clear Machine Authentication Cache on page 438
- Make Subscriber on page 439
- Upload Nessus Plugins on page 440
- Cluster-Wide Parameters on page 440
- Collect Logs on page 452
- Backup on page 453
- Restore on page 454
- Shutdown/Reboot on page 457
- Drop Subscriber on page 457

Edit Server Configuration Settings

You can edit the configuration settings of a server by clicking the server name listed in the **Administration > Server Manager > Server Configuration** page.

You can perform the following additional tasks only for a disabled node:

- Setting Time Zone
- Synchronizing Cluster Password
- Promoting to Publisher
- Joining a Server Back to Cluster

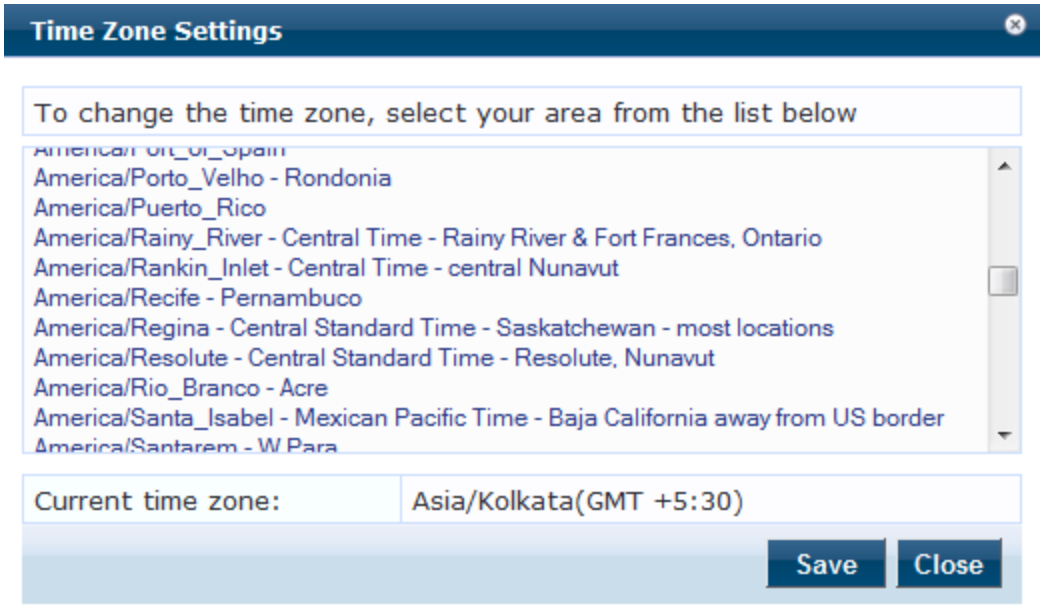
The **Server Configuration** pop-up contains the following tabs:

- System Tab on page 404
- Services Control Tab on page 409
- Service Parameters Tab on page 410
- System Monitoring Tab on page 423
- Network Tab on page 425
- FIPS Tab on page 430

Setting Date and Time

Use the **Set Time Zone** link at the top-right corner of the **Server Configuration** (**Administration** > **Server Manager** > **Server Configuration**) page to set the date and time specific to the selected node in a cluster. To set the date and time, select a time zone from the areas listed. The selected time zone is displayed in the **Current time zone** field. The following figure displays the **Time Zone Settings** pop-up:

Figure 373: *Time Zone Settings*

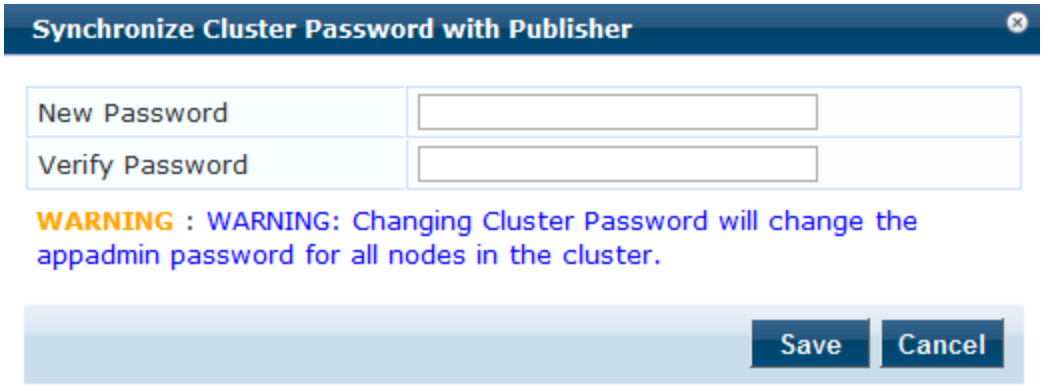


Synchronizing Cluster Password

Use the **Synchronize Cluster Password** link to synchronize the password of the selected node with cluster. Synchronizing the cluster password will change the appadmin password for all the nodes in the cluster.

The following figure displays the **Synchronize Cluster Password with Publisher** pop-up:

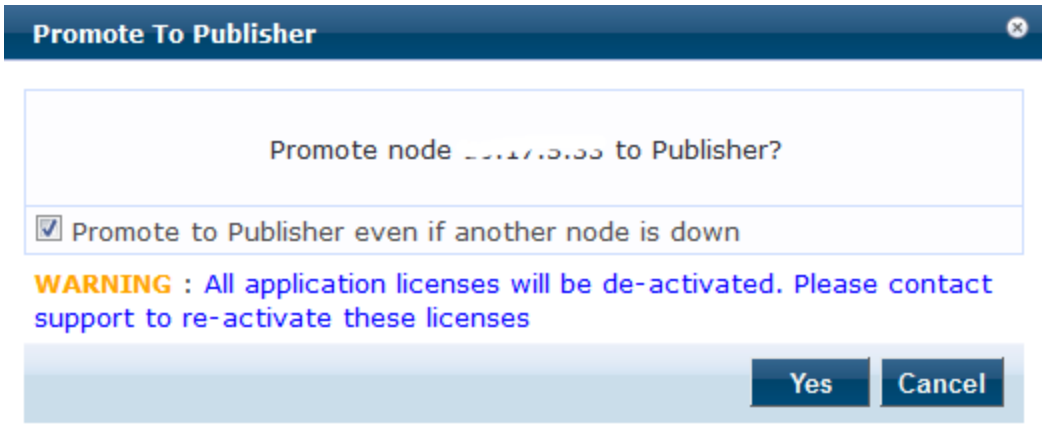
Figure 374: *Synchronize Cluster Password with Publisher*



Promoting to Publisher

Use the **Promote To Publisher** link to promote the selected node as a publisher node. You can enable this node as a publisher node using any other active node which is part of the same cluster. All application licenses will be de-activated and you need to contact support to re-activate these licenses. The following figure displays the **Promote To Publisher** pop-up:

Figure 375: *Promote to publisher*

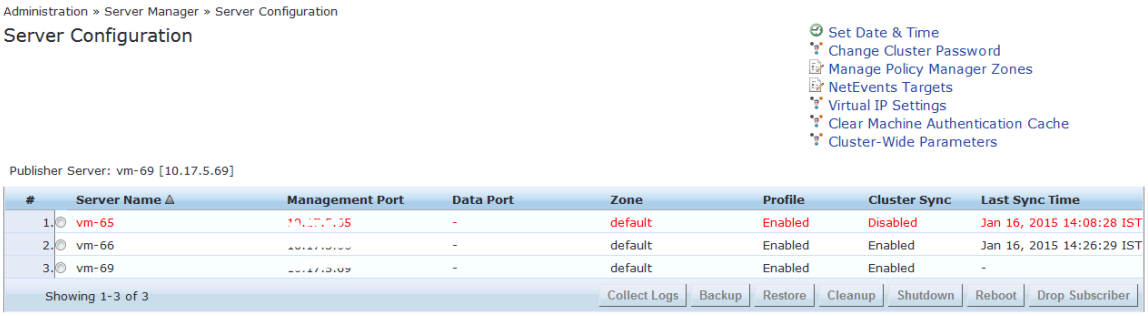


Joining a Server Back to Cluster

Use the **Join server back to cluster** link to join server back to cluster. You can use this option only to a server that is in the **Disabled** state in the **Server Configuration** (**Administration** > **Server Manager** > **Server Configuration**) page.

The following figure displays the **Server Configuration** page:

Figure 376: *Server Configuration Page with Disabled Node*



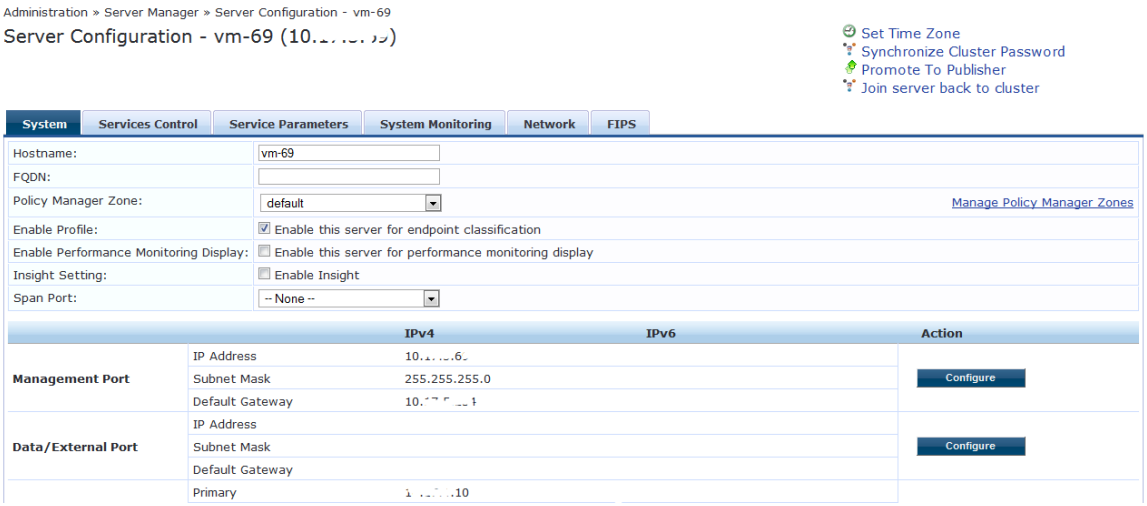
For more information on the **Service Configuration**, see Server Configuration on page 399.

The users with Admin access only can join a server back to cluster.

To join a server back to the cluster, use the following steps:

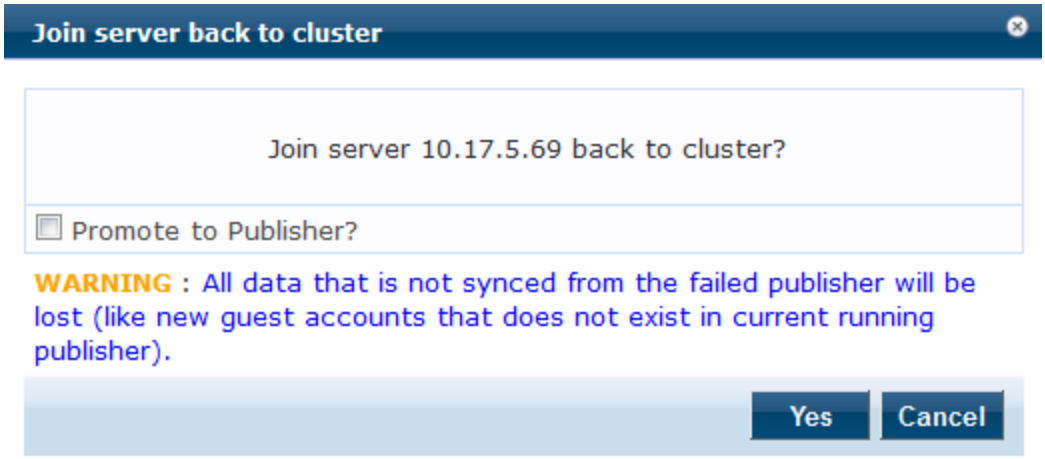
1. Select a subscriber node which is in **Disabled** state. The **Server Configuration – System** tab opens.

Figure 377: *Server configuration - Join server back to cluster*



2. Click the **Join server back to cluster** link at the top-right corner. A warning message appears with a prompt to promote the node to 'Publisher'. This option can only be triggered from a node that is currently active in the cluster. The following message displays the warning message:

Figure 378: *Join server back to cluster*



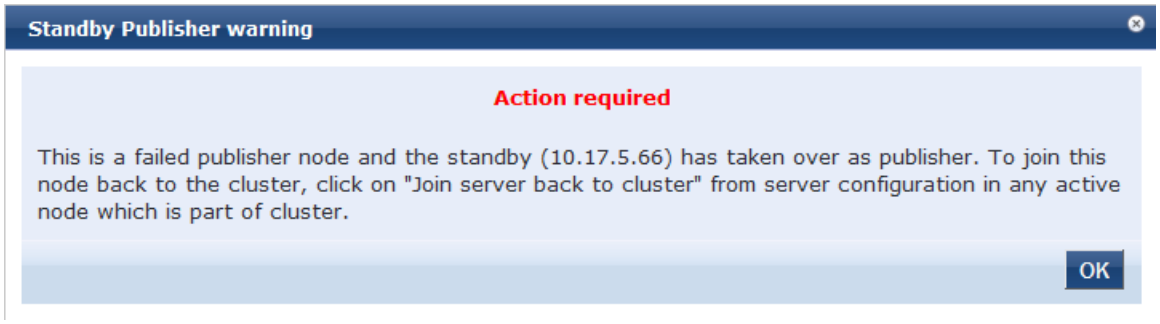
3. Click **Yes** from the warning message pop-up. A progress indicator shows the progress with log entries.

The following figure displays the Join server back to cluster progress indicator:

Figure 379: *Join server back to cluster - Progress*

4. For a failed publisher node, the following message will be displayed in the **Dashboard** page:

Figure 380: *Publisher Warning Message*

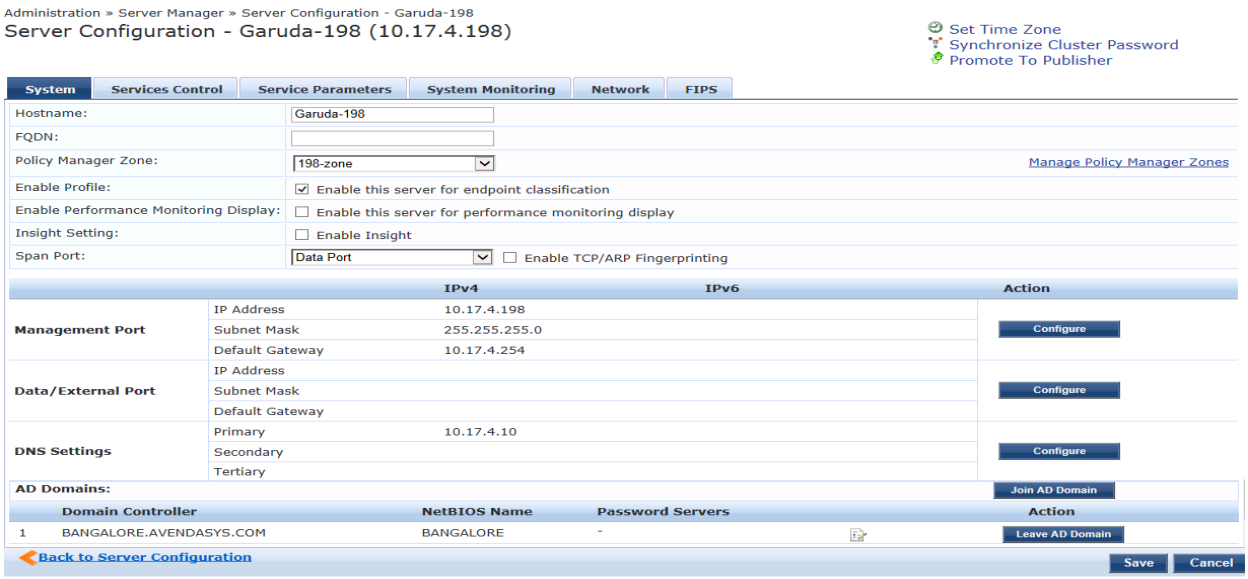


System Tab

By default, the **Server Configuration** page opens on the **System** tab.

The following figure displays the **System** tab:

Figure 381: *System Tab*



The following table describes the **System** tab parameters:

Table 233: *Server Configuration System Tab Parameters*

Parameter	Description
Hostname	Specify the hostname of Policy Manager appliance. You need not enter the fully qualified domain name in this field.
Policy Manager Zone	Select a previously configured timezone from the drop-down list. Click on the **Policy Manager Timezone** link to add and edit timezones. For more information on adding or editing timezones, see Policy Manager Zones on page 435
Enable Profile	Select the check box to enable the server to perform endpoint classifications.
Enable Performance Monitoring	Select the check box to enable the server to perform performance monitoring.
Insight Setting	Select the **Enable Insight** check box to enable the Insight reporting tool on this node. **NOTE:** • When the administrator enables this check box for Insight on a node in a cluster, the [Insight Repository] configuration is updated automatically to point to the management IP of that server. • When this check box is enabled for other servers in the cluster, they are added as backups for the same authentication source. • The order of the primary and backup servers in the [Insight Repository] is same in which the user enables Insight on the server.
Enable as Insight Master	In a cluster environment, you can specify the current server as an Insight Master. **NOTE:** This option is available only if **Enable Insight** is selected.

Table 233: *Server Configuration System Tab Parameters (Continued)*

Parameter	Description
Span Port	Select a port for DHCP spanning. This field is optional. On selecting a port, the **Enable TCP/ARP Fingerprinting** checkbox appears.
Enable TCP/ARP Fingerprinting	Select the check-box to enable TCP/ARP fingerprinting. This feature allows the Netbridge service to capture TCP and ARP packets and post the derived inputs to the device profiler. **NOTE:** This option appears only when you select a **Span Port** .
Management Port	Click the **Configure** button to open the **Configure Management Port** window and configure the following management interface parameters: • **Select IP Version**—Select the IP version as IPv4 or IPv6. • **IP Address**—IP address to access the Dell Networking W-ClearPass Policy Manager UI. Specify an IPv4 or IPv6 address. • **Subnet Mask**—Specify the management interface subnet mask for IPv4 address. • **Default Gateway**—Specify the default gateway for the management interface. **NOTE:** IPv6 addresses do not require a netmask as they use Classless Inter-Domain Routing (CIDR).
Data/External Port	Click the **Configure** button to open the **Configure Data/External Port** window and configure the following data or external port parameters: • **Select IP Version**—Select the IP version as IPv4 or IPv6. • **IP Address**—Specify the IP address of the data interface. All authentication and authorization requests appear on the data interface. • **Subnet Mask**—Specify the data interface subnet mask for IPv4 address. • **Default Gateway**—Specify the default gateway for the data interface. **NOTE:** IPv6 addresses use Classless Inter-Domain Routing (CIDR) so you do not need to specify a netmask for IPv6 addresses.
DNS Settings	Click the **Configure** button to open the **Configure DNS Settings** window and configure the following DNS settings: • **Primary DNS**—Specify the primary DNS for name lookup. • **Secondary DNS**—Specify the secondary DNS for name lookup. • **Tertiary DNS**—Specify the tertiary DNS for name lookup.
AD Domains	Displays a list of joined active directory domains. You can access the **Join AD Domain** window to join an active directory domain by clicking **Join Domain**. For more information on joining AD domains, see Join AD Domain on page 406 . After an AD Domain is added, the domain controller can be setup as a password server. For more information on adding a password server, see Add Password Server on page 408.

Join AD Domain

You can join CPPM to an Active Directory (AD) domain to authenticate users and computers that are members of an Active Directory domain. If you join CPPM to an Active Directory domain, it creates a computer account for the CPPM node in the AD database. Users can then authenticate into the network using 802.1X and EAP methods, such as PEAP-MSCHAPv2, with their own their own AD credentials.

If you need to authenticate users belonging to multiple AD forests or domains in your network, and there is no trust relationship between these entities, then you must join CPPM to each of these untrusted forests or domains.

NOTE

CPPM does not require to join multiple domains belonging to the same AD forest because a one-way trust relationship exists between those domains. In this case, CPPM can join the root domain.

CPPM can join or leave an AD domain by using the following two buttons in the **System** tab of the **Server Configuration** page:

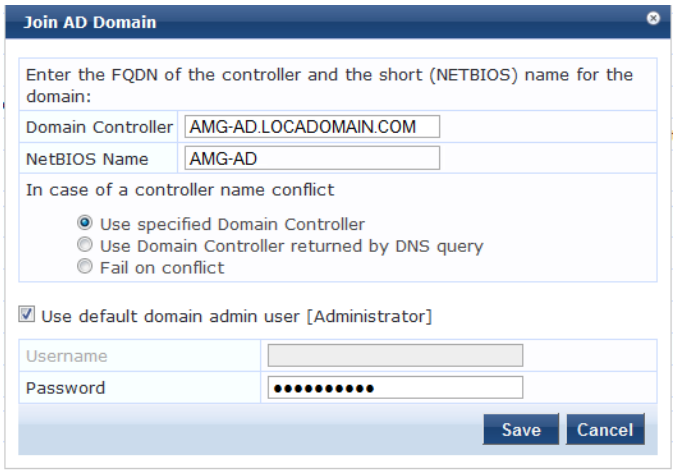
- **Join Domain**—Click this button to join this CPPM appliance to an Active Directory domain. Password servers can be configured after Policy Manager is successfully joined. For more information on adding a password server, see Add Password Server on page 408.
- **Leave Domain—** If the server is already part of multiple AD domains, click this button to disassociate this Policy Manager appliance from an Active Directory domain.

NOTE

For most use cases, if you have multiple nodes in the cluster, you must join each node to the same Active Directory domain.

The following figure displays the **Join AD Domain** window:

Figure 382: *Join AD Domain*



The following table describes the **Join AD Domain** parameters:

Table 234: *Join AD Domain Parameters*

Parameter	Description
Domain Controller	Fully qualified name of the Active Directory domain controller.
NETBIOS name (optional)	The NETBIOS name of the domain. Enter this value only if this is different from your regular Active Directory domain name. If this is different from your domain name (usually a shorter name), enter that name here. Contact your AD administrator about the NETBIOS name. **NOTE:** If you enter an incorrect value for the NETBIOS name, you see a warning message in the UI. If you see this warning message, leave the domain by clicking on the **Leave Domain** button, which replaces the **Join Domain** button once you join the domain. After leaving the domain, join again with the right NETBIOS name.
Domain Controller name conflict	In some deployments (especially if there are multiple domain controllers, or if the domain name has been wrongly entered in the last step), the domain controller FQDN returned by the DNS query can be different from what was entered. In this case, you may: • **Use specified Domain Controller** - Continue to use the domain controller name that you entered. • **Use Domain Controller returned by DNS query** - Use the domain controller name returned by the DNS query. • **Fail on conflict** - Abort the Join Domain operation.
Use default domain admin user	Check this box to use the Administrator user name to join the domain
Username	User ID of the domain administrator account. This field is disabled if the **Use default domain admin user** checkbox is selected.
Password	Password of the domain administrator account.

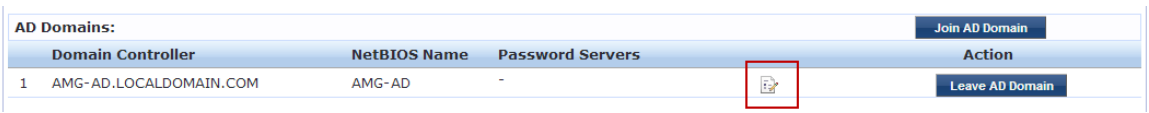
Add Password Server

After CPPM successfully joins an AD domain, you can configure a restricted list of domain controllers to be used for MSCHAP authentication. If not configured, then all available domain controllers obtained from DNS will be included.

To add a password server:

1. In the **AD Domains** section of the **System** tab, click the Add Password Server icon . This icon appears only after CPPM joins at least one AD domain (See Figure 383).

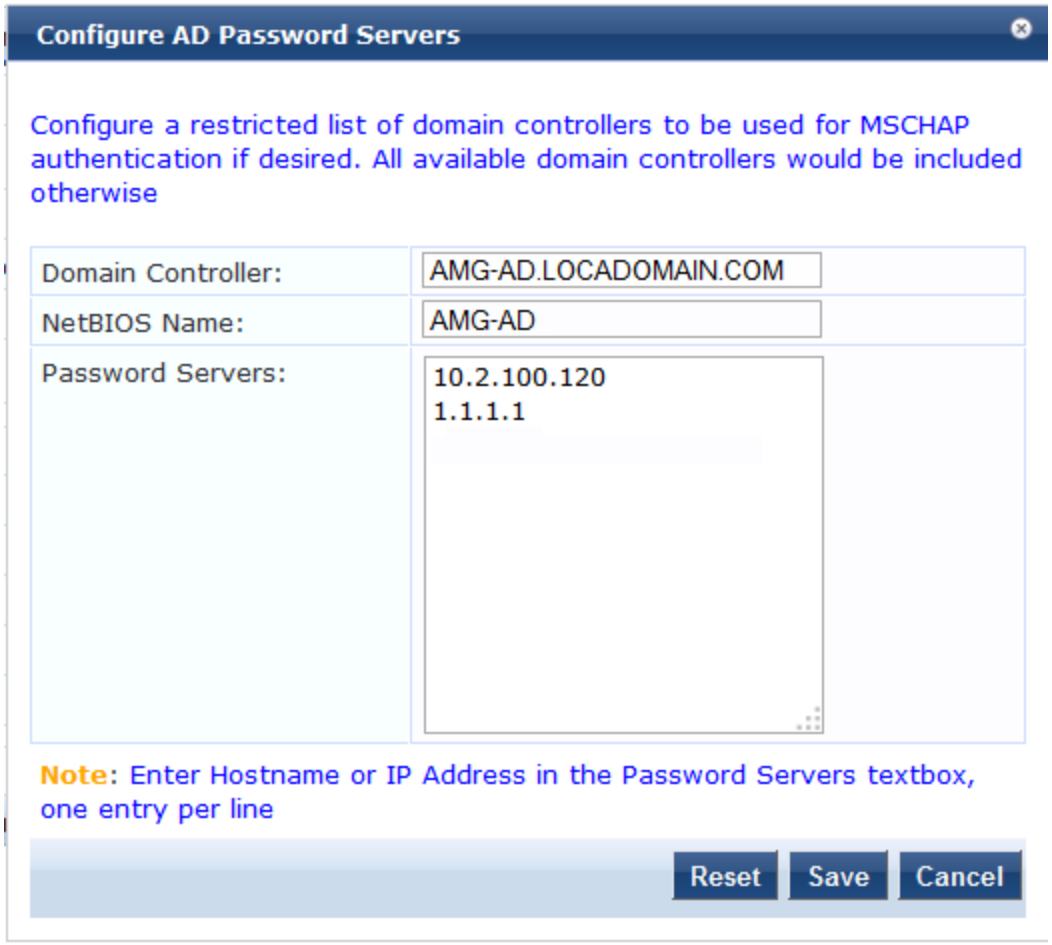
Figure 383: *Add Password Server icon*



2. The **Configure AD Password Servers** page appears. Specify the domain name, NetBIOS Name, and the password servers. The password servers can be hostname or IP address. Use a new line for each entry.
3. Click **Save** to complete adding the password servers.

The Following figure displays the Configure AD Password Servers window:

Figure 384: *Configure AD Password Servers*

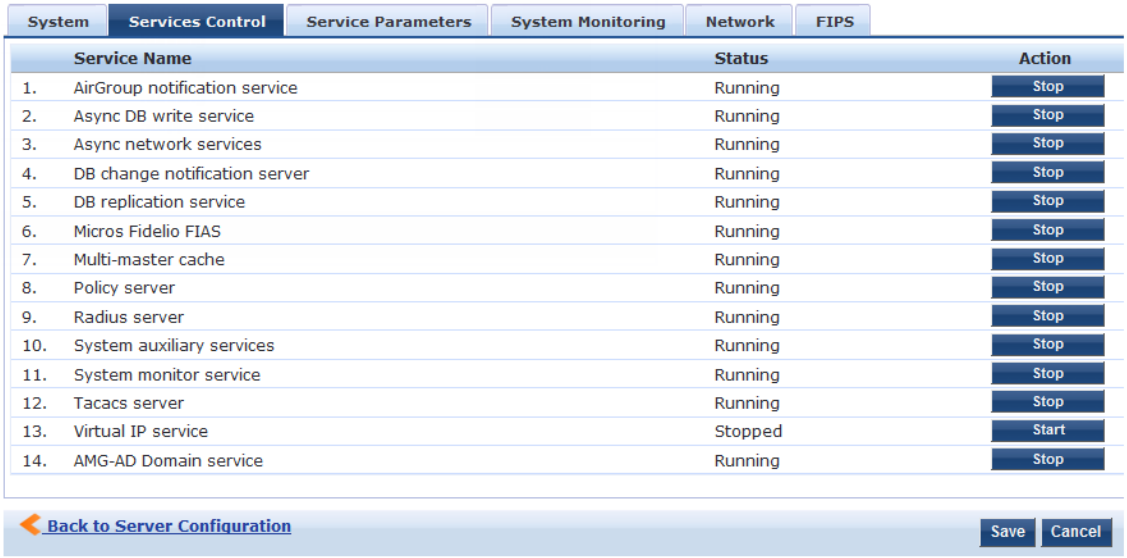


Services Control Tab

From the **Services Control** tab, you can view a service status and control (stop or start) various Policy Manager services, including any AD Domains that the server joins.

The following figure displays the Services Control tab:

Figure 385: *Services Control Tab*



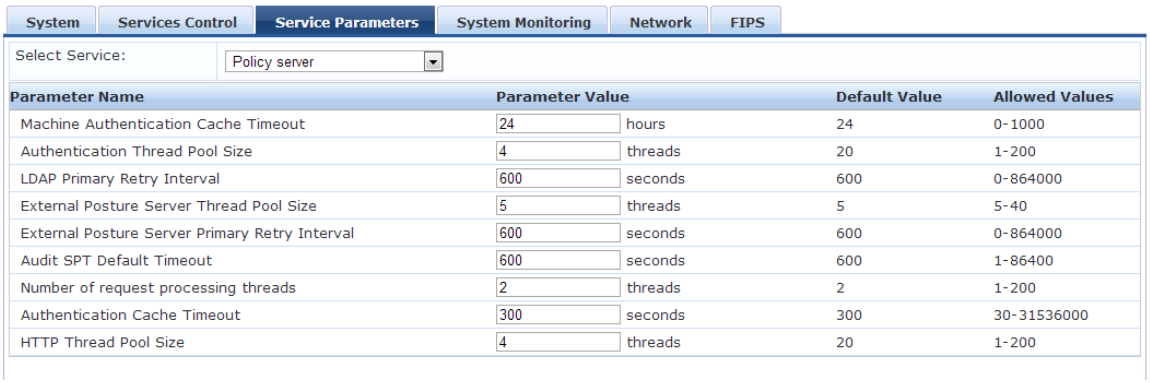
Service Parameters Tab

Navigate to the **Service Parameters** tab to change system parameters of a variety of services. The options on this page vary based on the selected service. Determine the service that you want to edit.

This section describes the following topics:

The following figure displays the Service Parameters tab:

Figure 386: *Service Parameters tab - Policy server example*

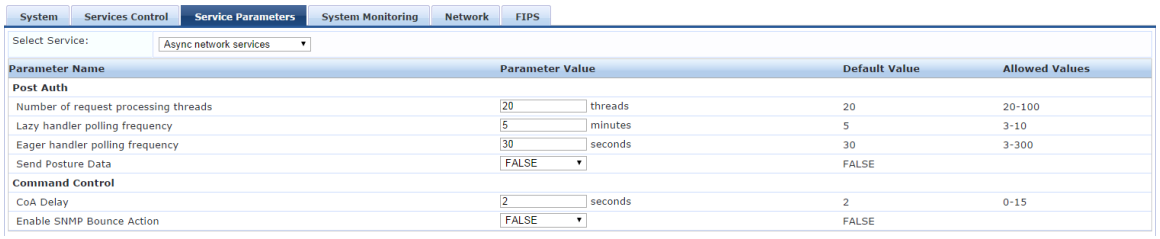


Async Network Services Options

Configure the Post-Auth and Command Control parameters for the Async network service in this tab.

The following figure displays the **Async network services** parameters in the **Service Parameters** tab:

Figure 387: *Async Network Services*



The following table describes the **Async network services** parameters in the **Service Parameters** tab:

Table 235: *Service Parameters - Async Network Services*

Parameter	Description
Post Auth	
Number of request processing threads	Set the number of request processing threads. The default value is 20 threads, and the allowed values are between 20 and 100.
Lazy handler polling frequency	Set the Lazy handler polling frequency. The frequency is configured in minutes. The default value is 5 minutes, and the allowed values are from 3-10 minutes.
Eager handler polling frequency	Set the Eager handler polling frequency. The frequency is measured in seconds. The default value is 30 seconds, and the allowed values are from 10-300 seconds.
Send Posture Data	Set this to TRUE if you want to send posture data to Palo Alto Firewall server.
Command Control	
CoA Delay	Set the CoA Delay value. The default value is measured in seconds. The default value is 2, and the allowed values are from 0-15 seconds.
Enable SNMP Bounce Action	Set the Enable SNMP Bounce Action value. The default value is FALSE.

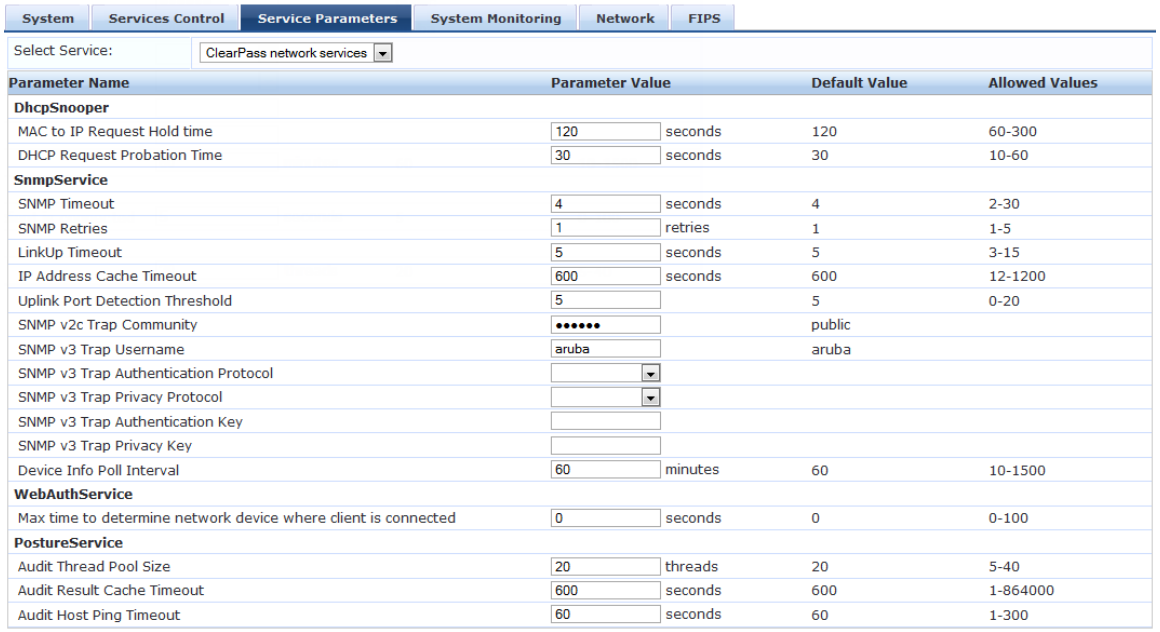
ClearPass Network Services Options

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

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

The following figure displays the **ClearPass network services** parameters in the **Service Parameters** tab:

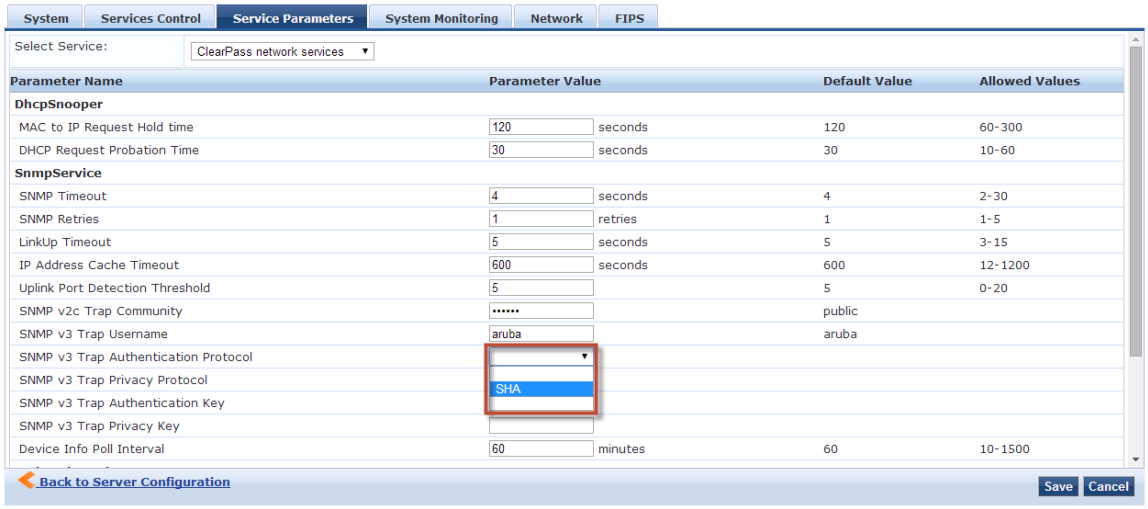
Figure 388: *ClearPass Network Services - Service Parameters Tab*



Parameter Name	Parameter Value	Default Value	Allowed Values
DhcpSnooper			
MAC to IP Request Hold time	120 seconds	120	60-300
DHCP Request Probation Time	30 seconds	30	10-60
SnmpService			
SNMP Timeout	4 seconds	4	2-30
SNMP Retries	1 retries	1	1-5
LinkUp Timeout	5 seconds	5	3-15
IP Address Cache Timeout	600 seconds	600	12-1200
Uplink Port Detection Threshold	5	5	0-20
SNMP v2c Trap Community	••••••	public	
SNMP v3 Trap Username	aruba	aruba	
SNMP v3 Trap Authentication Protocol			
SNMP v3 Trap Privacy Protocol			
SNMP v3 Trap Authentication Key			
SNMP v3 Trap Privacy Key			
Device Info Poll Interval	60 minutes	60	10-1500
WebAuthService			
Max time to determine network device where client is connected	0 seconds	0	0-100
PostureService			
Audit Thread Pool Size	20 threads	20	5-40
Audit Result Cache Timeout	600 seconds	600	1-864000
Audit Host Ping Timeout	60 seconds	60	1-300

The following figure displays the **ClearPass network services** parameters in the **Service Parameters** tab in FIPS mode:

Figure 389: *ClearPass Network Services - Service Parameters Tab FIPS Mode*



Parameter Name	Parameter Value	Default Value	Allowed Values
DhcpSnooper			
MAC to IP Request Hold time	120 seconds	120	60-300
DHCP Request Probation Time	30 seconds	30	10-60
SnmpService			
SNMP Timeout	4 seconds	4	2-30
SNMP Retries	1 retries	1	1-5
LinkUp Timeout	5 seconds	5	3-15
IP Address Cache Timeout	600 seconds	600	12-1200
Uplink Port Detection Threshold	5	5	0-20
SNMP v2c Trap Community	••••••	public	
SNMP v3 Trap Username	aruba	aruba	
SNMP v3 Trap Authentication Protocol	SHA		
SNMP v3 Trap Privacy Protocol			
SNMP v3 Trap Authentication Key			
SNMP v3 Trap Privacy Key			
Device Info Poll Interval	60 minutes	60	10-1500

The following table describes the parameters for **ClearPass network services** parameters in the **Service Parameters** tab :

Table 236: *Service Parameters - ClearPass Network Services*

Service Parameters	Description
DhcpSnooper	
MAC to IP Request Hold time	Specifies the number of seconds to wait before responding to a query to get an IP address corresponding to a MAC address. Any DHCP message received in this time period refreshes the MAC to IP binding. Typically, audit service requests for a MAC to IP mapping as soon the RADIUS request is received, but the client may take some more time receive and IP address through DHCP. This wait period takes into account the latest DHCP IP address that the client got.
DHCP Request Probation Time	Specifies the number of seconds to wait before considering the MAC to IP binding received in a DHCPREQUEST message as final. This wait handles cases where client receives a DHCPNAK for a DHCPREQUEST and receives a new IP address after going through the DHCPDISCOVER process again.
SnmpService	
SNMP Timeout	Specifies the seconds to wait for an SNMP response from the network device.
SNMP Retries	Specifies the number of retries for SNMP requests.
LinkUp Timeout	Specifies the seconds to wait before processing link-up traps. If a MAC notification trap arrives in this time, SNMP service does not try to poll the switch for MAC addresses behind a port for link-up processing.
IP Address Cache Timeout	Specifies the duration in seconds for which MAC to IP lookup response is cached.
Uplink Port Detection Threshold	Shows the limit for the number of MAC addresses found behind a port after which the port is considered an uplink port and not considered for SNMP lookup and enforcement.
SNMP v2c Trap Community	Specifies the community string that must be checked in all incoming SNMP v2 traps.
SNMP v3 Trap Username	Specifies the SNMP v3 Username to be used for all incoming traps.
SNMP v3 Trap Authentication Protocol	Specifies the SNMP v3 Authentication protocol for traps. Must be one of MD5, SHA, or empty (to disable authentication).

Table 236: *Service Parameters - ClearPass Network Services (Continued)*

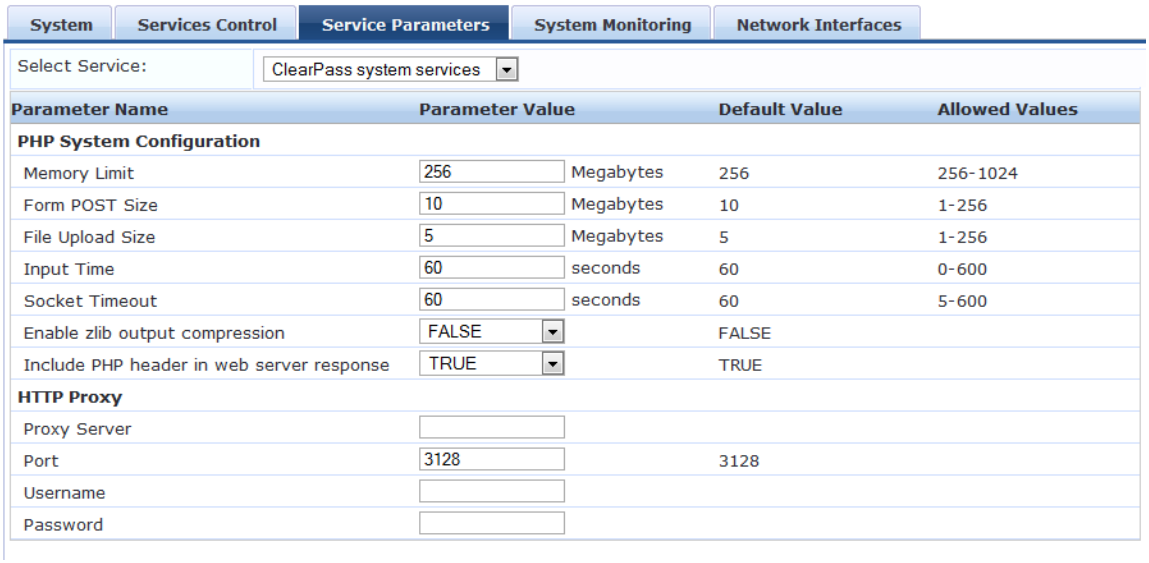
Service Parameters	Description
	NOTE: The **EAP-MD5** authentication type is not supported if you use the Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.
SNMP v3 Trap Privacy Protocol	Specifies the SNMP v3 Privacy protocol for traps. Must be one of DES_CBC, AES_128, or empty (to disable privacy). **NOTE:** The **DES_CBC** privacy protocol is not supported if you use the Dell Networking W-ClearPass Policy Manager in the **FIPS** mode.
SNMP v3 Trap Authentication Key	Specifies the SNMP v3 authentication key and privacy key for incoming traps.
SNMP v3 Trap Privacy Key	
Device Info Poll Interval	Specifies the time (in minutes) between polling for device information.
WebAuthService	
Max time to determine network device where client is connected	In some usage scenarios where the web authentication request does not originate from the network device. Policy Manager has to determine the network device to which the client is connected through an out-of-band SNMP mechanism. The network device deduction can take some time. This parameter specifies the maximum time to wait for Policy Manager to determine the network device to which the client is connected.
PostureService	
Audit Thread Pool Size	Specifies the number of threads to use for connections to audit servers.
Audit Result Cache Timeout	Specifies the time (in seconds) for which audit result entries are cached by Policy Manager.
Audit Host Ping Timeout	Specifies the number of seconds for which Policy Manager pings an end-host before giving up and deeming the host to be unreachable.

ClearPass System Services Options

You can use the ClearPass system service parameters for PHP configuration and for http traffic flowing through a proxy server. Dell Networking W-ClearPass Policy Manager relies on an http connection for Dell W-ClearPass update portal to download the latest information for posture services.

The following figure displays the **ClearPass system services** parameters in the **Service Parameters** tab:

Figure 390: *ClearPass System Services Parameters (partial view)*



The following table describes the **ClearPass system services** parameters in the **Service Parameters** tab:

Table 237: *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.

Table 237: *Service Parameters - ClearPass System Services (Continued)*

Service Parameter	Description
HTTP Proxy	
Proxy Server	Hostname or IP address of the proxy server.
Port	Port at which the proxy server listens for HTTP traffic.
Username	Username to authenticate with proxy server.
Password	Password to authenticate with proxy server.
Database Configuration	
Maximum connections	Specify a number between 300 and 2000 for a maximum number of allowed connections.
TCP Keepalive Configurations	
Keep Alive Time	Specify a value in seconds from 10-86400.
Keep Alive Interval	Specify a value in seconds from 1-3600.
Keep Alive Probes	Specify a value from 1-100 for the number of probes.
Web Server Configuration	
Maximum Clients	Specify a value from 10-20000 for the maximum number of clients allowed.
Timeout	Specify a server timeout value in seconds from 1-60.
Keep Alive	Select TRUE or FALSE to enable or disable keep alive for the web-server.
Request Wait	Specify the request wait time in seconds from 1-60. The default value is 4 seconds.

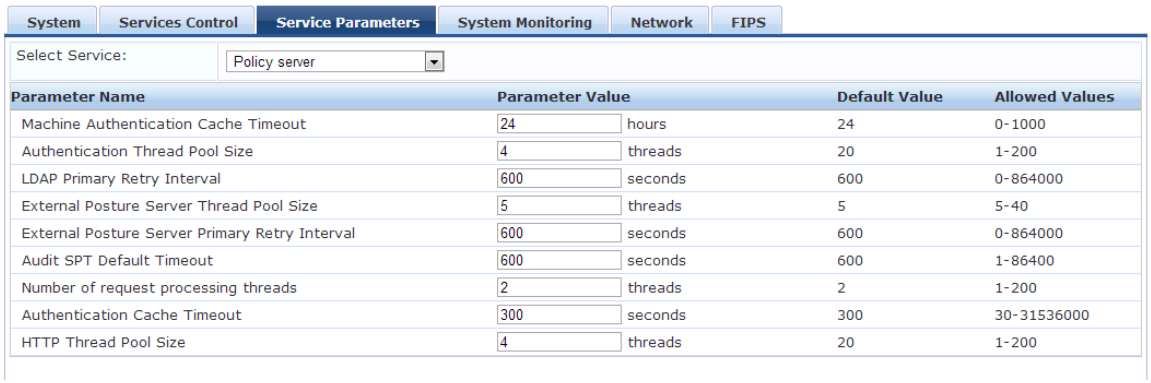
Table 237: *Service Parameters - ClearPass System Services (Continued)*

Service Parameter	Description
Maximum Requests	Specify a number between 0 and 3000 for the maximum number of requests allowed. The default value is 500.
Enable Host Header check	Specify **TRUE** or **FALSE**. The default value is **TRUE**. When you set this value to **TRUE**, the **Host Header Restriction check** is enabled and only the allowed or whitelisted host headers are allowed. When you set this value to **FALSE**, irrespective of Host Headers in the http packet, Dell Networking W-ClearPass Policy Manager redirects to https://<cppm-server>/tips.
WhiteList Host Names	When the **Enable Host Header check** value is set to **TRUE**, the web access is allowed for Whitelist Host Names, hostnames, IP addresses, and VIP addresses in Dell Networking W-ClearPass Policy Manager. The comma separated whitelist host names are allowed to support multiple hostnames. When the **Enable Host Header check** value is set to **TRUE** and the **WhiteList Host Names** field is blank, the web access is allowed only for hostnames, IP addresses, and VIP addresses in Dell Networking W-ClearPass Policy Manager.

Policy Server Options

The following figure displays the **Policy server** parameters in the **Service Parameters** tab:

Figure 391: *Policy Server Service Parameters*



The following table describes the **Policy server** parameters in the **Service Parameters** tab:

Table 238: *Service Parameters - Policy Server service*

Service Parameter	Description
Machine Authentication Cache Timeout	This specifies the time (in hours) for which machine authentication entries are cached by Policy Manager.
Authentication Thread Pool Size	This specifies the number of threads to use for LDAP/AD and SQL connections.
LDAP Primary Retry Interval	After a primary LDAP server is down, Policy Manager connects to one of the backup servers. This parameter specifies how long Policy Manager waits before it tries to connect to the

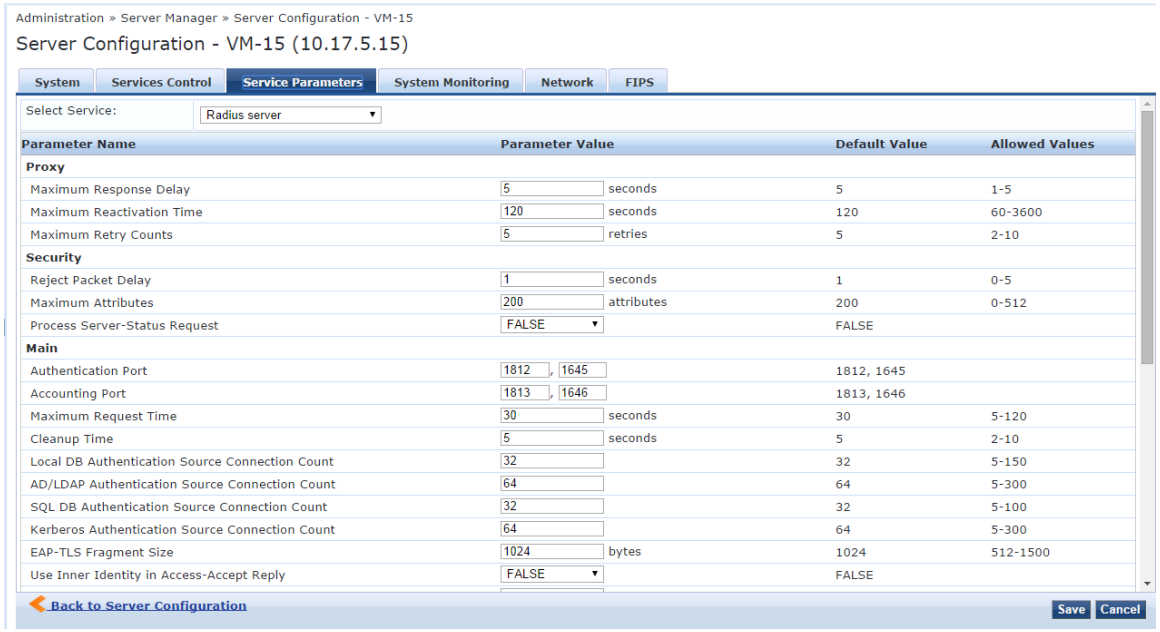
Table 238: *Service Parameters - Policy Server service (Continued)*

Service Parameter	Description
	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	After a primary posture server is down, Policy Manager connects to one of the backup servers. This parameter specifies how long Policy Manager waits before it tries to connect to the primary server again.
Audit SPT Default Timeout	Time for which Audit success or error response is cached in policy server.
Number of request processing threads	Maximum number of threads used to process requests.
Authentication Cache Timeout	Specifies the time in seconds for which authentication information is cached by Policy Manager.
HTTP Thread Pool Size	Specify the number of threads allotted for the HTTP thread pool.

Radius Server Options

The following figure displays the **RADIUS server** parameters in the **Service Parameters** tab:

Figure 392: *RADIUS Server Parameters (partial view)*



The following table describes the **RADIUS server** parameters in the **Service Parameters** tab:

Table 239: *Service Parameters - Radius Server Service*

Service Parameter	Description
Proxy	
Maximum Response Delay	Time delay before retrying a proxy request, if the target server has not responded.
Maximum Reactivation Time	Time to elapse before retrying a dead proxy server.
Maximum Retry Counts	Maximum number of times to retry a proxy request if the target server doesn't respond.
Security	
Reject Packet Delay	Delay time before sending an actual RADIUS Access-Reject after the server decides to reject the request.
Maximum Attributes	Maximum number of RADIUS attributes allowed in a request.
Process Server-Status Request	Send replies to Status-Server RADIUS packets.
Main	
Authentication Port	Ports on which radius server listens for authentication requests. Default values are 1645, 1812.
Accounting Port	Ports on which radius server listens for accounting requests. Default values are 1646, 1813.
Maximum Request Time	Maximum time allowed for processing a request after which it is considered timed out.
Cleanup Time	Time to cache the response sent to a RADIUS request after sending it. If the RADIUS server gets a duplicate request for which the response is already sent, the cached response is resent if the duplicate request arrives within this time period.
Local DB Authentication Source Connection Count	Maximum number of Local DB connections opened.
AD/LDAP Authentication	Maximum number of AD/LDAP connections opened.

Table 239: *Service Parameters - Radius Server Service (Continued)*

Service Parameter	Description
Source Connection Count	
SQL DB Authentication Source Connection Count	Maximum number of SQL DB.
Kerberos Authentication Source Connection Count	Maximum number of Kerberos connections opened.
EAP - TLS Fragment Size	Maximum allowed size for the EAP-TLS fragment.
Use Inner Identity in Access-Accept Reply	Specify TRUE to use the inner identity in the Access-Accept replies. Else, specify FALSE.
Reject if OCSP response does not have Nonce	Specify TRUE to reject an OCSP response without a nonce. Else, specify FALSE.
Include Nonce in OCSP request	Specify TRUE or FALSE. This determines whether OCSP request should have nonce or not. If the OCSP server does not support the nonce, then set the value as FALSE for this parameter to avoid the EAP-TLS authentication failure. The default value is TRUE.
Enable signing for OCSP Request	Specify TRUE or FALSE. This determines whether ClearPass should sign an OCSP request with a RADIUS server certificate. The default value is FALSE.
Check the validity of all certificates in the chain against CRLs	Specify TRUE to check the validity of all certificates in the chain against CRLs. Else, specify FALSE.
ECDH Curve	Select one of the following ECDH curve options from the drop-down list: • X9.62/SECG curve over a 256 bit prime field • NIST/SECG curve over a 384 bit prime field
Re-attempt AD login with different Username formats	Specify TRUE to re-attempt AD login with different Username formats. Else, specify FALSE.
TLS Session Cache Limit	Number of TLS sessions to cache before purging the cache (used in TLS based 802.1X EAP Methods).

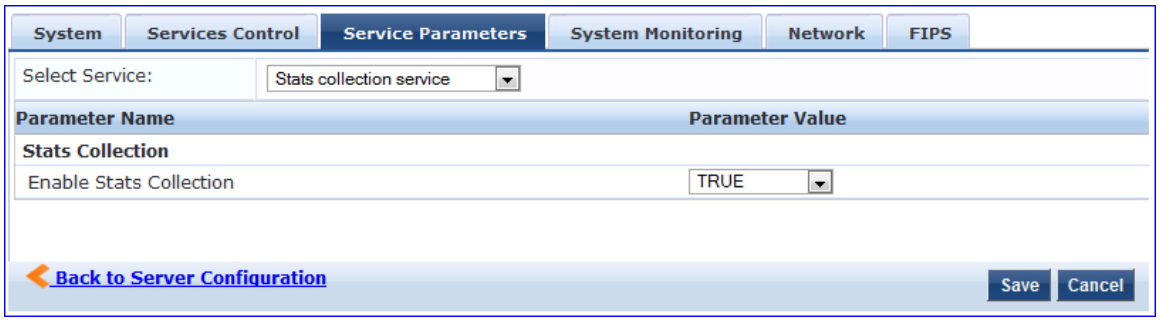
Table 239: *Service Parameters - Radius Server Service (Continued)*

Service Parameter	Description
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.
AD (Active Directory) Errors	**AD (Active Directory) Errors**
Window Size	Enter a duration during which Active Directory errors are accumulated for possible action. The default is 5 minutes.
Number of Errors	Enter a number. If this number of Active Directory errors occurs within the defined Window Size, the self-healing Recovery Action is taken. The default is 150.
Recovery Action	Select one of the following recovery actions from the drop-down list: • None - To initiate no self-recovery action [Default]. • Exit - To restart the RADIUS server (Monitoring daemon will restart it). • Restart Domain Service - To restart the Domain service.
EAP-FAST	
Master Key Expire Time	Specify the lifetime of a generated EAP-FAST master key.
Master Key Grace Time	Specify the grace period for an EAP-FAST master key after its lifetime. If a client presents a PAC that is encrypted using the master key in this period after its TTL, it is accepted and a new PAC encrypted with the latest master key is provisioned on the client.
PACs are valid across cluster	Select true if PACs generated by this server are valid across the cluster. Else, select false.
Accounting	
Log Accounting Interim-Update Packets	Select TRUE to store the Interim-Update packets in session logs. Else, select FALSE.

Stats Collection Service Options

The following figure displays the **Stats Collection service** parameters in the **Service Parameters** tab:

Figure 393: *Stats Collection Service Parameters*



The following table describes the **Stats collection service** parameters in the **Service Parameters** tab:

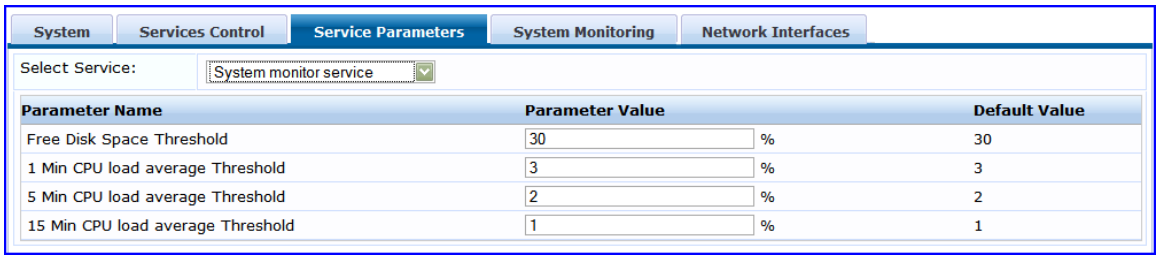
Table 240: *Service Parameters - Stats Collection Service*

Service Parameter	Description
Enable Stats Collection	This option enables or disables Stats Collection and Stats Aggregation. If this is not enabled, then stats collection and aggregation services will not run on the node. In addition, the following error message will display if the admin attempts to start these services: **Failed to start Stats collection service - Ignoring service start request as Stats Collection option is disabled on the node** **NOTE:** Enabling/disabling this parameter requires a restart of cpass-statsd-server and cpass-carbon-server.

System Monitor Service Options

The following figure displays the **System monitor service** parameters in the **Service Parameters** tab:

Figure 394: *System Monitor Service Parameters*



The following table describes the **System monitor service** parameters in the **Service Parameters** tab:

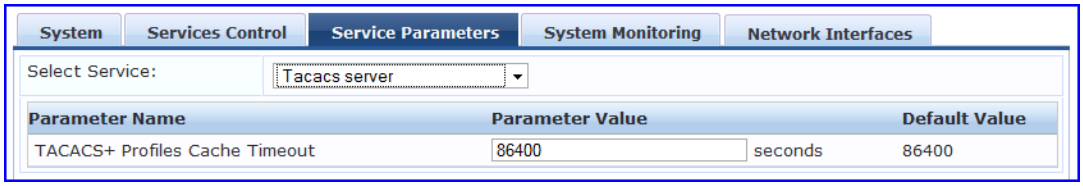
Table 241: *Services Parameters - System Monitor Service*

Service Parameter	Description
Free Disk Space Threshold	This parameter monitors the available disk space. If the available disk free space falls below the specified threshold (default 30%), then system sends SNMP traps to the configured trap servers.
1 Min CPU load average Threshold	These parameters monitor the CPU load average of the system, specifying thresholds for 1-min, 5-min and 15-min averages, respectively. If any of these loads exceed the associated maximum value, then system sends traps to the configured trap servers.
5 Min CPU load average Threshold	
15 Min CPU load average Threshold	

Tacacs Server Options

The following figure displays the **TACACS+ server** parameters in the **Service Parameters** tab:

Figure 395: *TACACS+ Service Parameters*



The following table describes the **TACACS+ server** parameters in the **Service Parameters** tab:

Table 242: *Service Parameters tab - TACACS server*

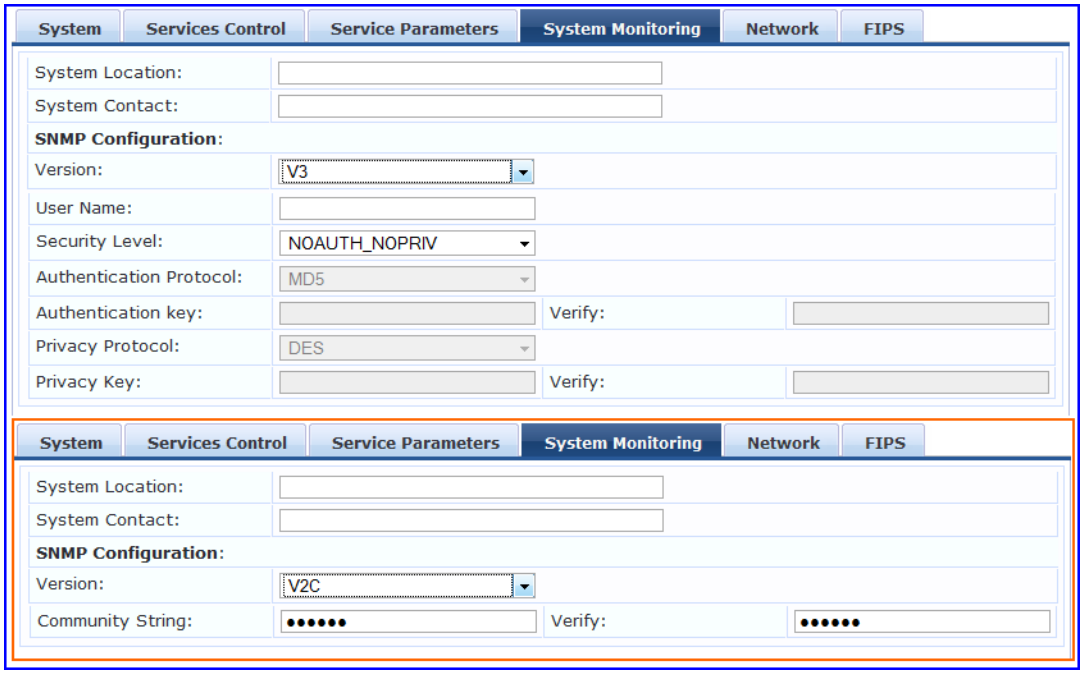
Service Parameter	Description
TACACS+ Profiles Cache Timeout	This specifies the time (in seconds) for which TACACS+ profile result entries are cached by Dell Networking W-ClearPass Policy Manager.

System Monitoring Tab

You can configure the SNMP parameters in the **System Monitoring** tab under the **Administration** > **Server Manager** > **Server Configuration** page. You can edit the system configuration of a server manager by clicking a table entry. By configuring this tab, you can ensure that external Management Information Base (MIB) browsers can browse the system level MIB objects exposed by the Dell Networking W-ClearPass Policy Manager appliance. The options in this page vary based on the SNMP version that you select.

The following figure displays the **System Monitoring** tab:

Figure 396: *System Monitoring Tab*



The following table describes the **System Monitoring** tab parameters:

Table 243: *System Monitoring tab Parameters*

Parameter	Description
System Location	Specify the location of the Dell Networking W-ClearPass Policy Manager appliance.
System Contact	Specify the contact information of the Dell Networking W-ClearPass Policy Manager appliance.
SNMP Configuration	
Version	Specify the SNMP version from the options V1, V2C, or V3. The GUI options on this page vary based on the SNMP version selected.
Community String	Enter and re-enter the community string for sending traps. This is applicable only for SNMP V1 and V2C versions
Username	Specify the user name to use for SNMP v3 communication. This field is available only if you selected the **V3** as the SNMP version in the **Version** field.
Security Level	Select any of the following options: • NOAUTH_NOPRIV (no authentication or privacy) - If you select this security level, only the **SHA** authentication protocol is available. • AUTH_NOPRIV (authenticate, but no privacy) - If you select this security level, the **MD5** and **SHA** authentication protocols are available.

Table 243: *System Monitoring tab Parameters (Continued)*

Parameter	Description
	• AUTH _PRIV (authenticate and keep the communication private) - If you select this security level, the **MD5** and **SHA** authentication protocols are available. This field is available only if you selected **V3** as the SNMP version in the **Version** field.
Authentication Protocol	Select the authentication protocol from **MD5** or **SHA**. These protocols vary depends on the security level that you selected in the **Security Level** field. This field is available only if you selected **V3** as the SNMP version in the **Version** field. **NOTE:** The **MD5** authentication protocol is not supported in the **FIPS** mode.
Authentication key	Enter and re-enter the authentication key. This field is available only if you selected **V3** as the SNMP version in the **Version** field.
Privacy Protocol	Select the privacy protocol from **DES** or **AES**. This field is available only if you selected **V3** as the SNMP version in the **Version** field.
Privacy Key	Enter the privacy key. This field is available only if you selected **V3** as the SNMP version in the **Version** field.

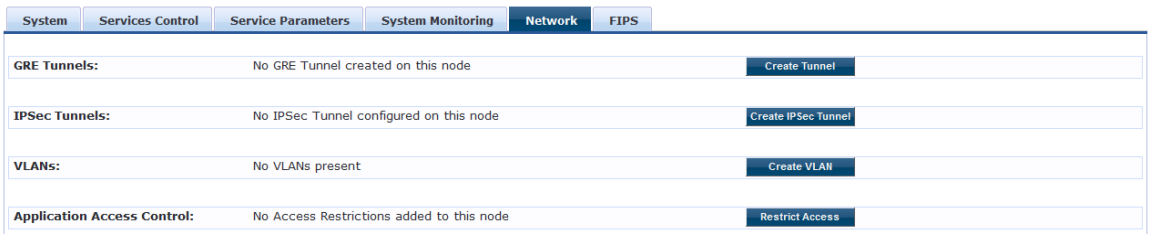
Network Tab

You can navigate to the **Network** tab and perform the following tasks:

- Create GRE Tunnels on page 425
- Create IPSec Tunnel on page 427
- on page 427
- Define Access Restrictions on page 429

The following figure displays the **Network** tab:

Figure 397: *Network Interfaces Tab*

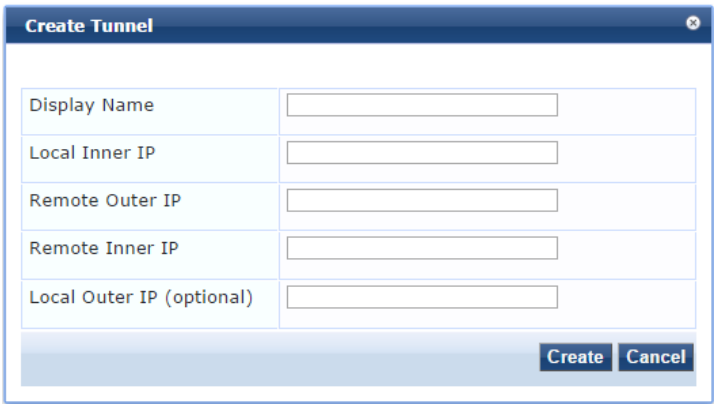


Create GRE Tunnels

You can navigate to the **Network** tab and click **Create Tunnel** to create a GRE tunnel. This protocol can be used to create a virtual point-to-point link over standard IP network or the internet.

The following figure displays the **Create Tunnel** pop-up:

Figure 398: *Create Tunnel*



The following table describes the **Create Tunnel** parameters:

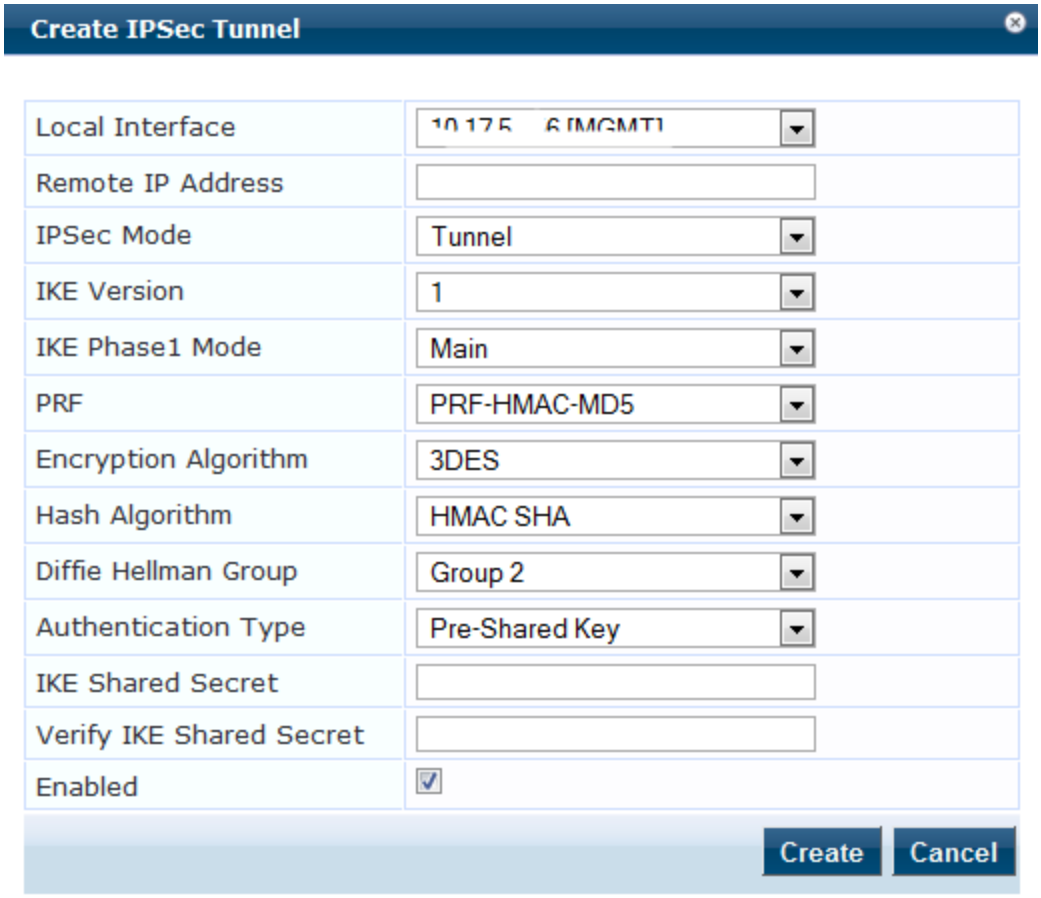
Table 244: *Create Tunnel Parameters*

Parameter	Description
Display Name	Specify the name for the tunnel interface. This name is used to identify the tunnel in the list of network interfaces.
Local Inner IP	Local IP address of the tunnel network interface.
Remote Outer IP	IP address of the remote tunnel endpoint.
Remote Inner IP	Remote IP address of the tunnel network interface. Enter a value here to automatically create a route to this address through the tunnel.
Local Outer IP (Optional)	Local IP address of the tunnel endpoint.
Create/Cancel	Commit or dismiss changes.

Create IPSec Tunnel

Navigate to the **Network** tab and click **Create VLAN** to create VLAN interfaces. The following figure displays the **Create IPSec Tunnel** pop-up:

Figure 399: *Create IPSec Tunnel*



The following table describes the **Create IPSec Tunnel** parameters:

Table 245: *Create IPSec Tunnel Parameters*

Parameter	Description
Local Interface	Specify the local (management) port.
Remote IP Address	Shows the IP address of the remote host.
IPSec Mode	Select the IPSec mode from the options: Tunnel or Transport.
IKE Version	Specify the version of the Internet Key Exchange (IKE) protocol from the options: 1 or 2.
IKE Phase 1 Mode	Specify the mode of the IKE phase from the options: Main or Aggressive.
PRF	Specify the pseudorandom function (PRF) from the following options:

Table 245: *Create IPSec Tunnel Parameters (Continued)*

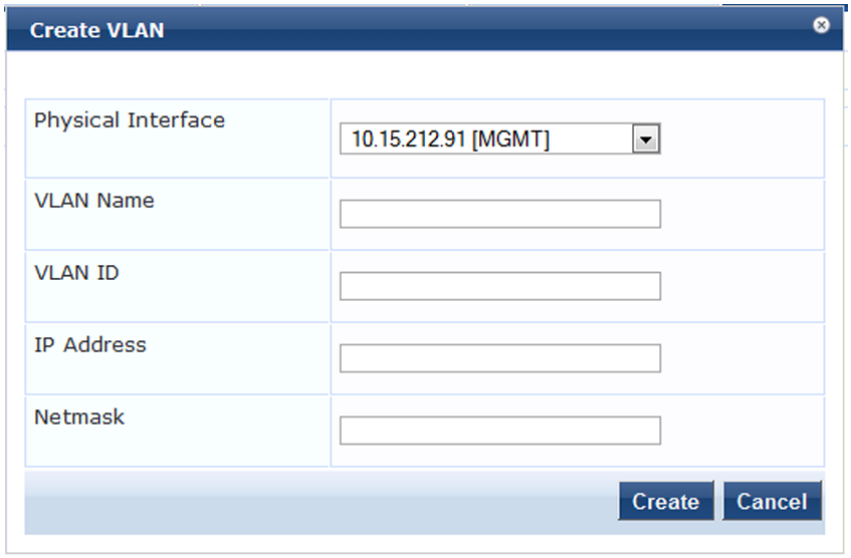
Parameter	Description
	• PRF-HMAC-MD5 • PRF-HMAC-SHA1 • PRF-HMAC-SHA256 • PRF-HMAC-SHA384
Encryption Algorithm	Select encryption algorithm to use from the following: • 3DES • AES128 • AES192 • AES256
Hash Algorithm	Select hash algorithm to use from the following: • HMAC SHA • HMAC-SHA256 • HMAC-SHA384 • HMAC-MD5
Diffie Hellman Group	Select the Diffie Hellman group from the following: • Group 1 • Group 2 • Group 5 • Group 14 • Group 19 • Group 20
Authentication Type	Select the authentication type from the options: Pre-Shared Key or Certificate.
IKE Shared Secret	Enter the secret key.
Verify IKE Shared Secret	Enter the secret key again to confirm.
Enabled	Specifies the IPSec tunnel is enabled or not.

Create VLANs

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

The following figure displays the **Create VLAN** pop-up:

Figure 400: *Create VLAN*



The following table describes the **Create VLAN** parameters:

Table 246: *Create 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.

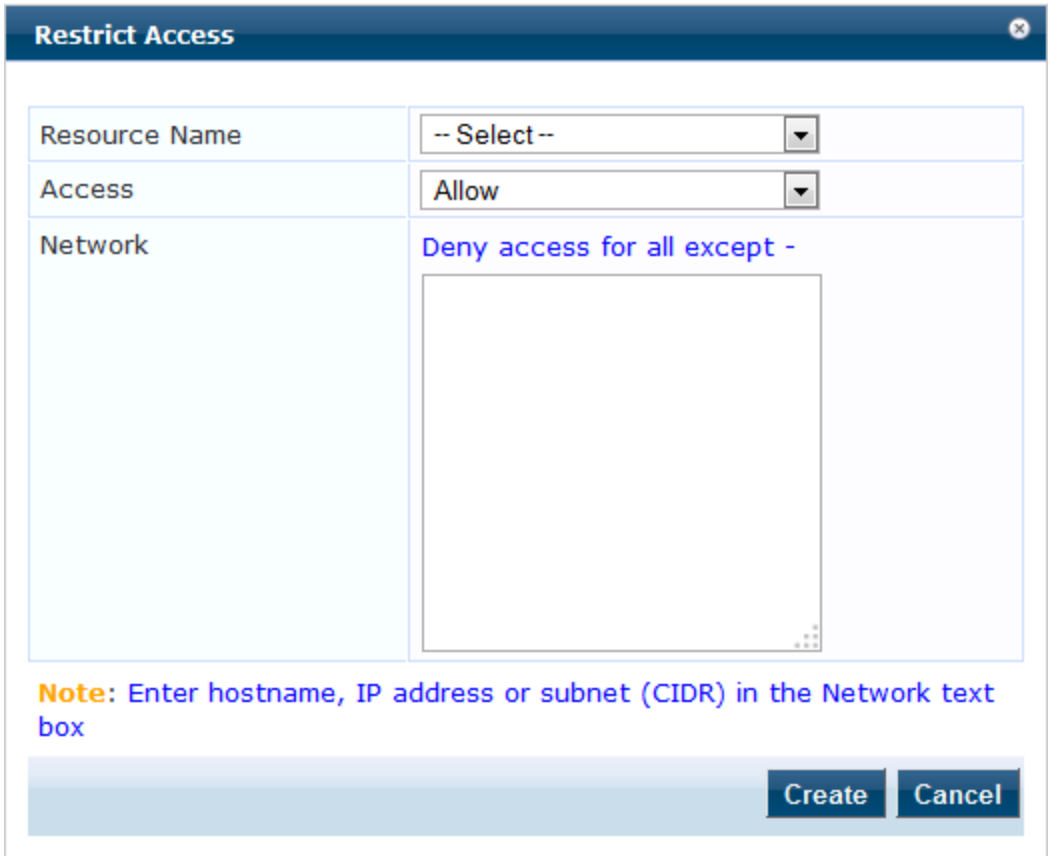
Your network infrastructure must support tagged 802.1Q packets on the physical interface selected. VLAN ID 1 is often reserved for use by certain network management components; avoid using this ID unless you know it will not conflict with a VLAN already defined in your network.

Define 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**.

The following figure displays the **Restrict Access** pop-up:

Figure 401: *Restrict Access dialog box*



The following table describes the **Restrict Access** parameters:

Table 247: *Restrict Access Parameters*

Parameter	Description
Resource Name	Select the application to which you want to allow or deny access.
Access	Select one of the access control options: • **Allow**— Allows access to the selected application. • **Deny**—Denies access to the selected application.
Network	Enter one or more hostnames, IP addresses, or IP subnets per line. The devices defined by what you enter here will be either specifically allowed or specifically denied access to the application you select.

FIPS Tab

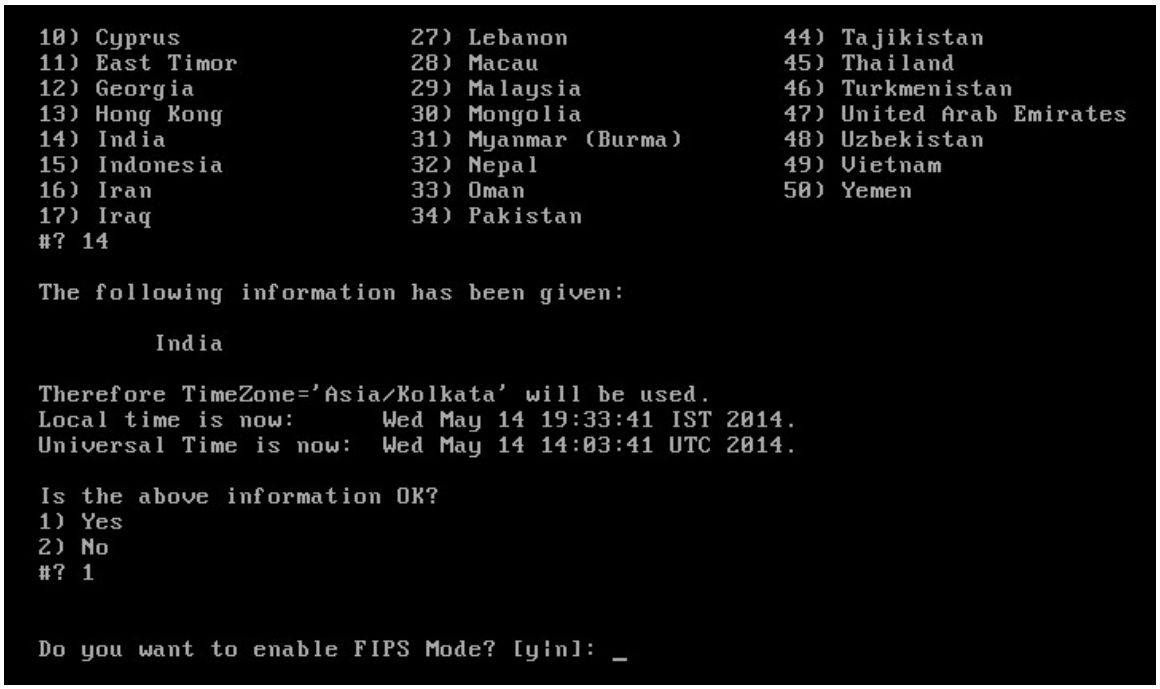
This section provides information on using ClearPass Policy Manager in Federal Information Processing Standards 140-2 (FIPS) approved mode. The United States Government developed FIPS 140-2 to define procedures, architectures, cryptographic algorithms, and other security techniques for use in government applications and networks that use cryptography. When running in FIPS Approved mode, ClearPass Policy Manager utilizes a FIPS 140-2 validated cryptographic module. Support is not available for non-approved authentication methods such as EAP-MD5 and MD5 digest algorithm.

NOTE

See http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747 for details on the FIPS 140-2 validated cryptographic module.

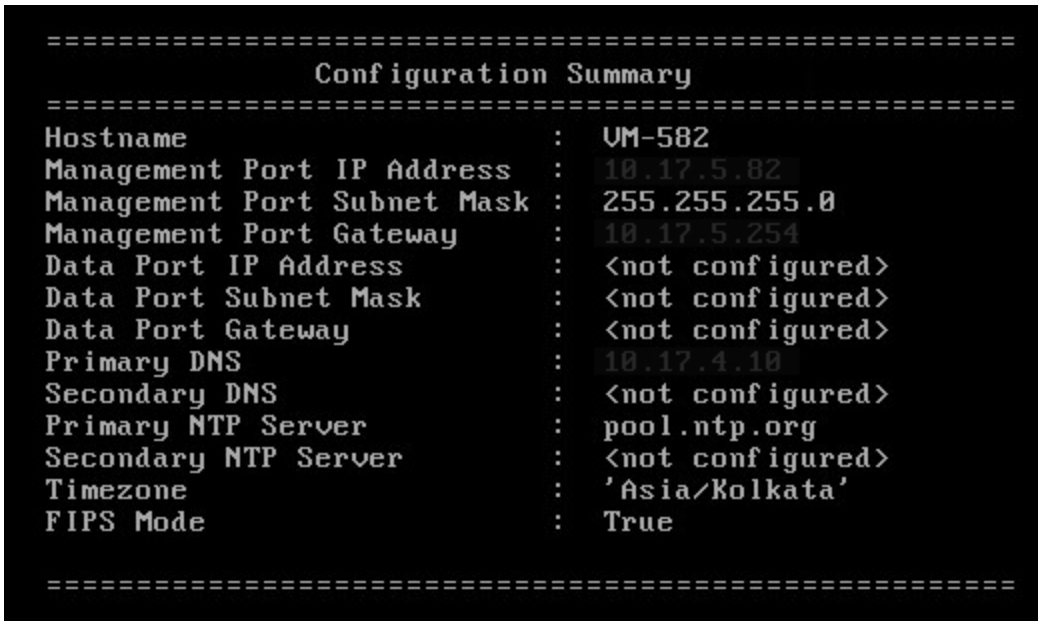
You can enable FIPS mode in ClearPass Policy Manager during installation using the CLI or post-installation using the Web UI. The following figure displays the prompt to enable FIPS Mode using the CLI:

Figure 402: *Enabling FIPS Mode*



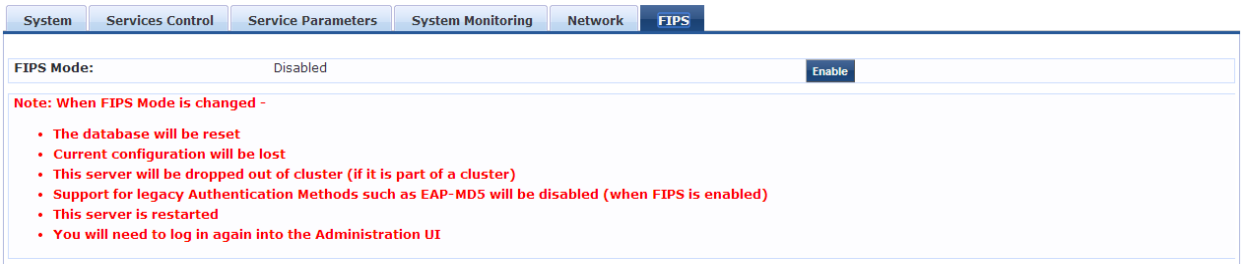
After enabling FIPS mode using the CLI commands, you can verify whether FIPS mode is enabled or not in the **Configuration Summary** page. The following figure displays the **Configuration Summary** page:

Figure 403: *FIPS Mode - Configuration Summary*



Alternatively, you can enable or disable the FIPS mode in the **Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab. The following figure displays the **Server Configuration - FIPS** tab in the Dell Networking W-ClearPass Policy Manager UI:

Figure 404: *Server Configuration - FIPS Tab*



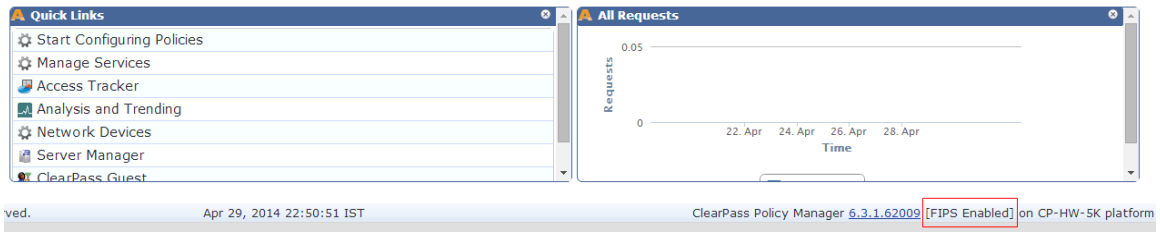
Important Points to Remember

Note the following important points, when you enable FIPS mode in Dell Networking W-ClearPass Policy Manager UI:

- The database is reset when you enable the FIPS mode in Dell Networking W-ClearPass Policy Manager. Ensure that you backed up your database before enabling FIPS mode.
- Configuration backup file from the Dell Networking W-ClearPass Policy Manager in the non-FIPS mode cannot be restored on Dell Networking W-ClearPass Policy Manager in FIPS mode. However, configuration backup file from the Dell Networking W-ClearPass Policy Manager in FIPS mode can be restored on the Dell Networking W-ClearPass Policy Manager in non-FIPS mode.
- The server will be removed from the cluster if FIPS mode is enabled.
- All nodes in a cluster must be either in FIPS or non-FIPS mode. The Dell Networking W-ClearPass Policy Manager nodes in FIPS mode cannot be connected to the cluster whose nodes are in the non-FIPS mode.
- The legacy authentication method such as EAP-MD5 and MD5 digest algorithm are not supported in FIPS mode. You cannot import the certificates that are created with the MD5 authentication type to the **Certificates Trust List** (**Administration** > **Certificates** > **Certificate Trust List**) page.
- The server reboots when you enable FIPS mode. You need to log in again to the Administration UI.

You can view the status of FIPS mode in the status bar. The following figure displays the **Status** bar with the status of FIPS mode:

Figure 405: *FIPS Status*



You can also view the status of the FIPS mode using the CLI commands. For more information, see Show Commands on page 581.

Set Date & Time

Click the **Set Date and Time** link under the **Administration > Server Manager > Server Configuration** page to access the **Change Date and Time** pop-up where can set the date and time for the server.

The **Change Date and Time** pop-up has the following two tabs:

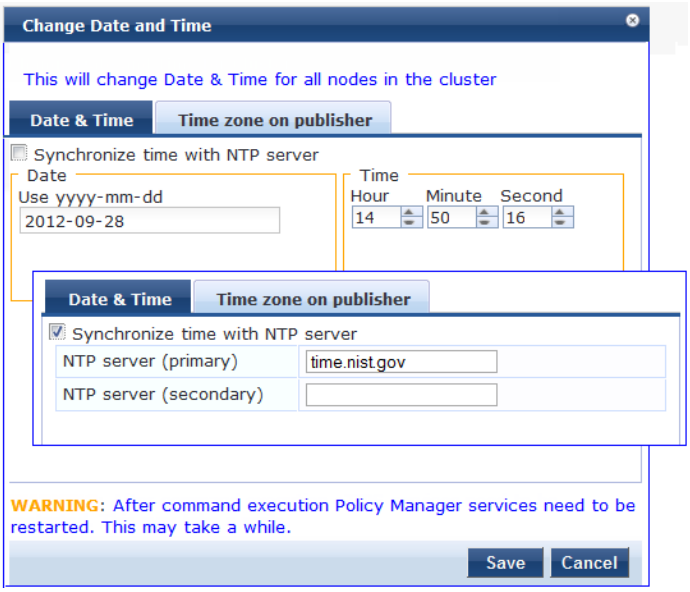
- Set Date & Time on page 432

- Time Zone on Publisher Tab on page 433

Date & Time Tab

You can set the date and time for the server using this tab. The following figure displays the **Date & Time** tab of the **Change Date and Time** pop-up:

Figure 406: *Change Date and Time - Date & Time tab*



The following table describes the **Date and Time** tab parameters:

Table 248: *Change Date and Time - Date & Time tab Parameters*

Parameter	Description
Date in yyyy-mm-dd format	To specify date and time, use the indicated syntax. This is available only when Synchronize time with NTP server is unchecked.
Time in hh:mm:ss format	
Synchronize Time With NTP Server	To synchronize with a Network Time Protocol Server, enable this check box and specify the NTP servers. You can specify one primary and one secondary server.
NTP Server (primary)	Specify the primary NTP server.
NTP Server (secondary)	Specify the secondary NTP server.

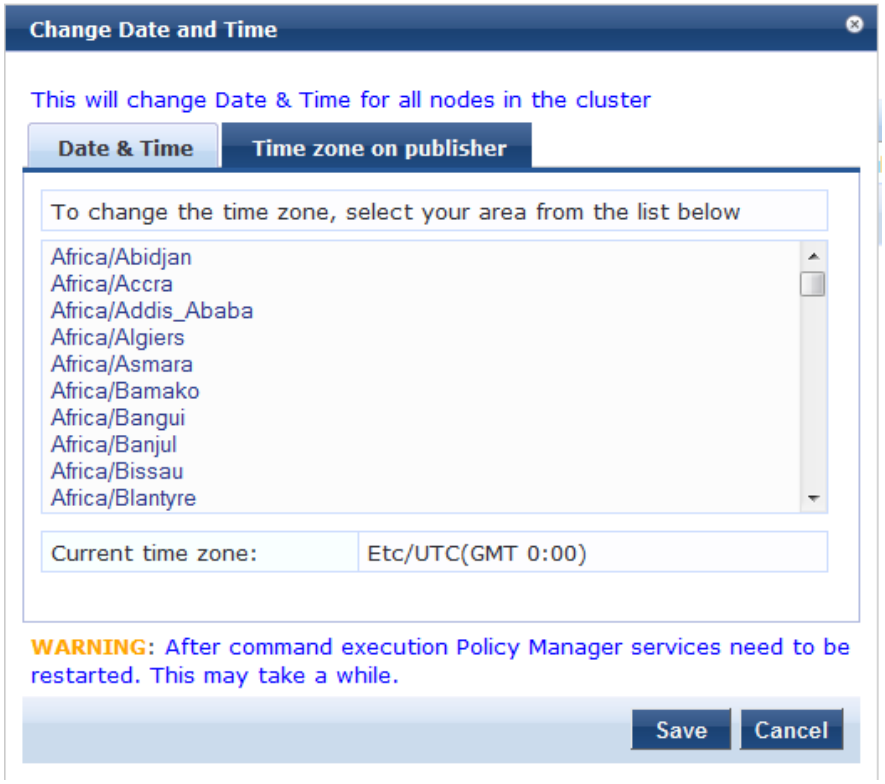
Time Zone on Publisher Tab

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

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

The following figure displays the **Time zone on publisher** tab of the **Change Date and TIme** pop-up:

Figure 407: *Time zone on publisher tab*



Change Cluster Password

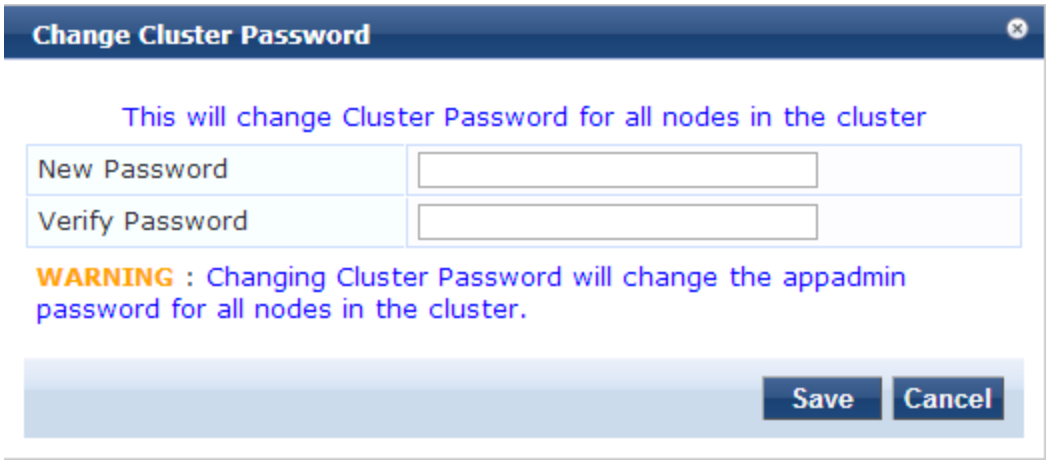
To change the cluster-wide password, follow the procedure below:

1. Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Change Cluster Password** link. The **Change Cluster password** pop-up appears.
2. Enter the new password, then verify the password.
3. Click **Save**.

Changing this password changes the password for the CLI user *appadmin* as well.

The following figure displays the **Change Cluster Password** pop-up:

Figure 408: *Change Cluster Password Dialog*



Policy Manager Zones

CPPM shares a distributed cache of runtime state across all nodes in a cluster. These runtime states include:

- Roles and Postures of connected entities
- Connection status of all endpoints running OnGuard
- Endpoint details gathered by OnGuard Agent

CPPM uses this runtime state information to make policy decisions across multiple transactions.

In a deployment where a cluster spans WAN boundaries and multiple geographic zones, it is not necessary to share all of this runtime state across all nodes in the cluster.

For example, when endpoints present in one geographical area are not likely to authenticate or be present in another area, it is more efficient from a network bandwidth usage and processing perspective to restrict the sharing of such runtime state to a given geographical area.

You can configure Zones in Dell Networking W-ClearPass Policy Manager to match with the geographical areas in your deployment. There can be multiple Zones per cluster, and each Zone has a number of Dell Networking W-ClearPass Policy Manager nodes that share runtime state.

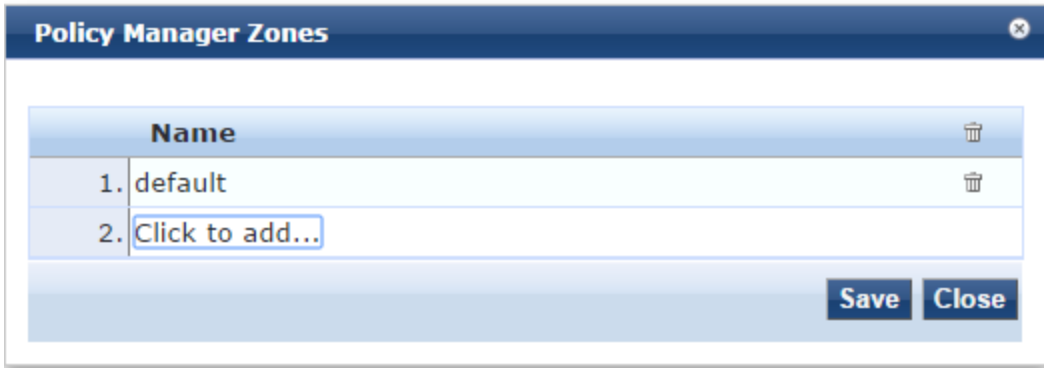
Manage Policy Manager Zones

To add or delete a Policy Manager Zone:

1. Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Manage Policy Manager Zones** link.
2. Click **Click to add...** and enter the Policy Manager Zone to be added.
3. Click **Save** to add the Policy Manager Zone.
4. Click the trashcan icon to delete a zone.

The following figure displays the **Policy manager Zones** pop-up:

Figure 409: *Policy Manager Zones*



NetEvents Targets

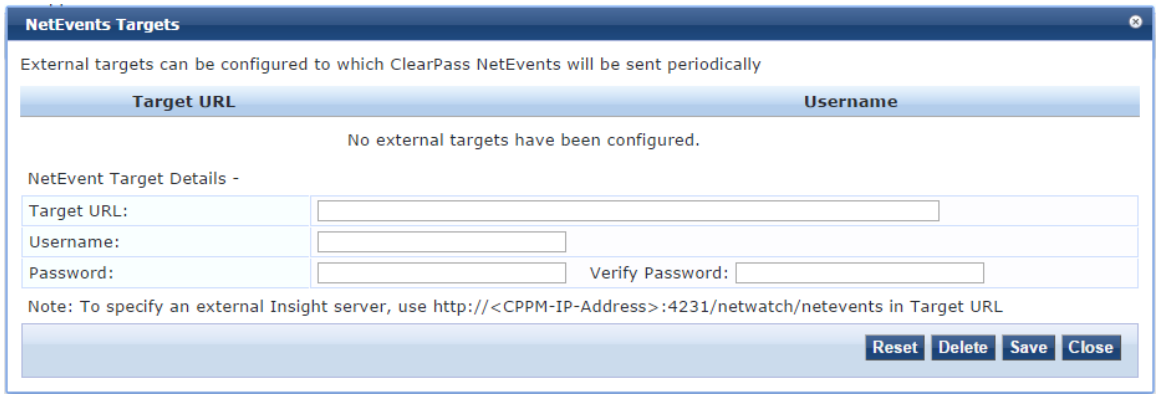
NetEvents are a collection of details for various Dell Networking W-ClearPass Policy Manager users, endpoints, guests, authentications, accounting details, and so on. This information is periodically posted to a server that is configured as the NetEvents target.

If the ClearPass Insight feature is enabled on a Dell Networking W-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.

To configure Netevents Target, navigate to the **Administration > Server Manager > Server Configuration** page and click the **NetEvents Targets** link.

The following figure displays the **NetEvents Targets** pop-up:

Figure 410: *NetEvents Targets*



The following table describes the **NetEvents Targets** parameters:

Table 249: *NetEvents targets*

Parameter	Description
Target URL	HTTP URL for the service that support POST and requires Authentication using Username / Password. **NOTE:** To specify an external Insight server, use http://<CPPM-IP-Address>:4231/netwatch/netevents in Target URL.
Username/Password	Credentials configured for authentication for the HTTP service that is provided in the Target URL.
Reset	Resets the values entered in the pop-up.
Delete	Deletes the selected Target URL.

Virtual IP Settings

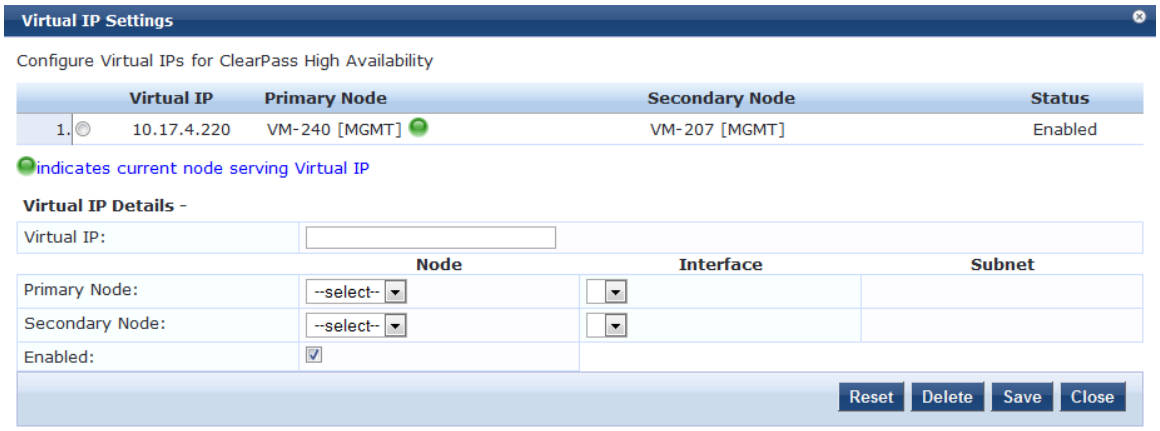
You can configure two nodes in a cluster to share a Virtual IP address. The Virtual IP address is bound to the primary node by default. The secondary node takes over when the primary node is unavailable.

In a virtual machine deployment of Dell Networking W-ClearPass Policy Manager, enable forged transmits on the VMWare distributed virtual switch for the Virtual IP feature to be effective.

To configure a virtual IP address, navigate to the **Administration > Server Manager > Server Configuration** page and click the **Virtual IP Settings** link.

The following figure displays the **Virtual IP Settings** pop-up:

Figure 411: *Virtual IP Settings*



The following table describes the **Virtual IP Settings** parameters:

Table 250: *Virtual IP Settings Parameters*

Parameter	Description
Virtual IP	Enter the IP address you want to define as the virtual IP address.
Primary Node	Select the servers to use as the primary node.
Secondary Node	Select the servers to use as the secondary node.
Interface	Select an interface on each server to which the virtual IP address is bound.
Subnet	This value is automatically filled after selecting the interface.
Enabled	Select the check box to enable the Virtual IP address.

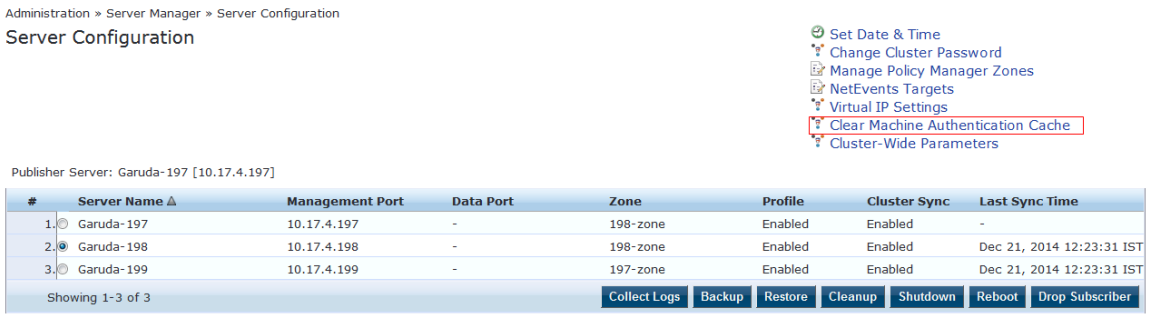
Clear Machine Authentication Cache

To clear machine authentication cache on all the nodes in a cluster:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration** page and click the **Clear Machine Authentication Cache** link.
2. Click **Yes** to confirm. The following message appears:
   Machine authentication cache cleared from all nodes

The following figure displays the **Server Configuration** page:

Figure 412: *Server Configuration - Clear Machine Authentication Cache*

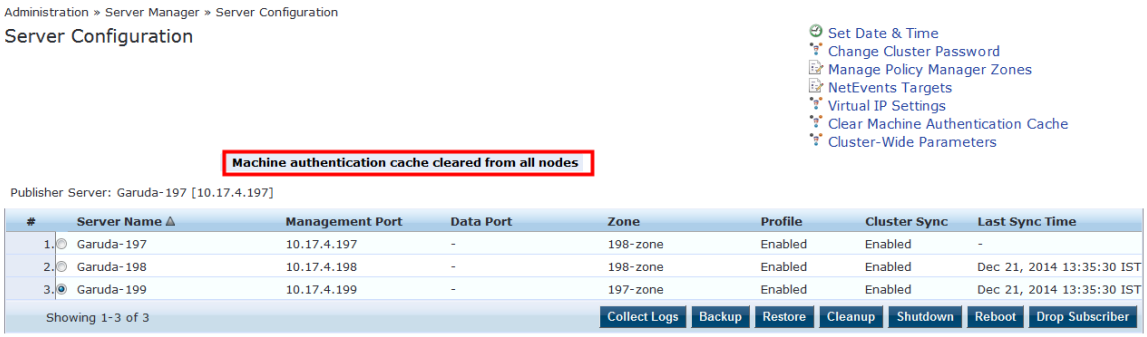


The following figure displays the confirmation prompt for clearing the machine authentication cache:

Figure 413: *Clear Machine Authentication Cache Prompt*

The following figure displays the message displayed after clearing the Machine authentication cache successfully :

Figure 414: *Clear Machine Authentication Cache Success Message*



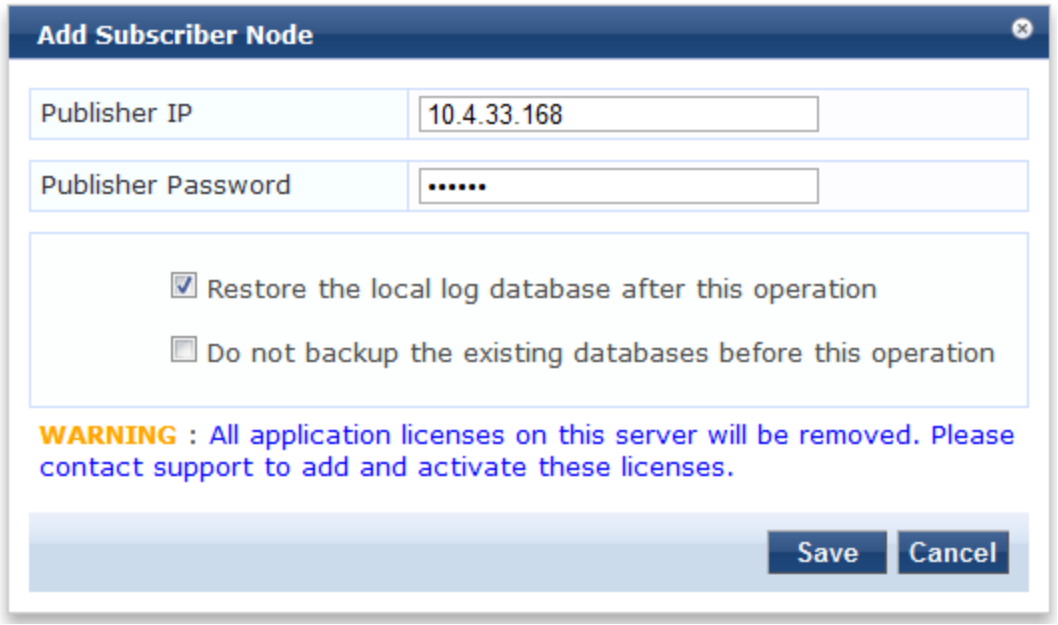
Make Subscriber

In the Policy Manager cluster environment, the publisher node acts as master. A Policy Manager cluster can contain only one publisher node. Administration, configuration, and database write operations may occur only on this master node.

The Policy Manager appliance defaults to a publisher node unless it is made a subscriber node. Cluster commands can be used to change the state of the node, hence the publisher can be made a subscriber. When it is a subscriber, you will not see this link.

To add a subscriber, navigate to the **Administration > Server Manager > Server Configuration** page, and click the **Make Subscriber** link. The following figure displays the **Add Subscriber Node** pop-up:

Figure 415: *Add Subscriber Node*



The following table describes the **Add Subscriber Node** parameters:

Table 251: *Add Subscriber Node*

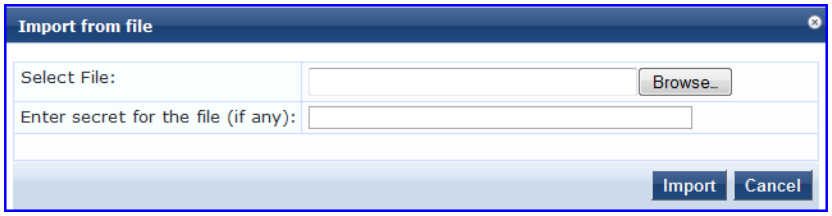
Parameter	Description
Publisher IP	Specify publisher address and password. **NOTE:** The password specified here is the password for the CLI user *appadmin*
Publisher Password	
Restore the local log database after this operation	Select the check box to restore the log database following addition of a subscriber node.
Do not backup the existing databases before this operation	Select the check box only if you do not require a backup to the existing database.

Upload Nessus Plugins

To upload a Nessus plugins, navigate to the **Administration > Server Manager > Server Configuration** page, and click the **Upload Nessus Plugins** link.

The following figure displays the **Upload Nessus Plugins** pop-up:

Figure 416: *Upload Nessus Plugins*



The following table describes the **Upload Nessus Plugins** parameters:

Table 252: *Upload Nessus Plugins*

Parameter	Description
Select File	Click **Browse** and select the plugin files with the extension tar.gz.
Enter secret for the file (if any)	Always leave this blank.
Import/Cancel	Load the plugins, or dismiss. **NOTE:** If there are a large number of plugins, the load time can be in the order of minutes.

Cluster-Wide Parameters

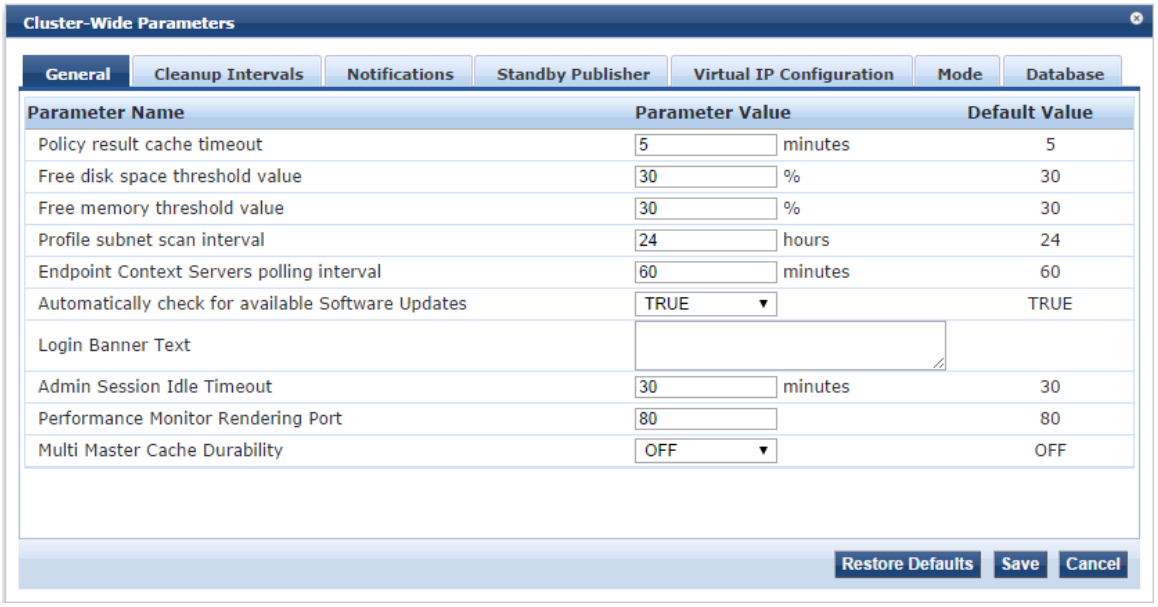
You can configure the parameters that apply to all the nodes in a cluster by clicking the **Cluster-Wide Parameters** link in the **Administration > Server Manager > Server Configuration** page. Cluster-wide parameters include Cache timeouts, Cleanup intervals, Auto backup, System alert notification, Virtual AP and so on.

The **Cluster-Wide Parameters** pop-up contains the following tabs:

General

The following figure displays the **General** tab of **Cluster-Wide Parameters**:

Figure 417: *Cluster-Wide Parameters - General Tab*



The following table describes the **General** tab parameters of **Cluster-Wide Parameters**:

Table 253: *Cluster-Wide Parameters - General Tab Parameters*

Parameter	Description
Policy result cache timeout	Specifies the duration allowed in minutes to store the role mapping and posture results derived by the policy engine during a policy evaluation. This result can then be used in subsequent evaluation of policies associated with a service, if the **Use cached Roles and Posture attributes from previous sessions** option is turned on for the service. A value of 0 disables caching. **NOTE:** The value of the **Policy result cache timeout** field must be greater than the highest value set in the **Health Check Interval (in hours)** fields. For example, if you have created the profiles Student-Enforcement-Profile and Staff-Enforcement-Profile with health check interval configured, then the value of the **Policy result cache timeout** field must be greater than the highest value of the **Health Check Quiet Period (in hours)** value configured among the following profiles: • Global Agent Settings • Student-Enforcement-Profile • Staff-Enforcement-Profile
Free disk space threshold value	Specifies the percentage below which disk usage warnings are issued in the Monitoring > Event Viewer page. For example, a value of 30% indicates that a warning is issued only when the available disk space is 30% or lower. The error message similar to the following may appear in the **System Event Details** pop-up: '**System is running with low disk space. Aggressive cleanup will be initiated when the available disk space falls below 80%. Current available disk space = 75%**'.
Free memory threshold value	Specifies the percentage below which RAM usage warnings are issued in the Policy Manager Event Viewer. For example, a value of 30 indicates that a warning is issued only when the available RAM is 30% or lower.
Profile subnet scan interval	Specify the profile subnet scan interval in hours. The default value is 24 hours.
Endpoint Context Servers polling interval	Enter the interval in minutes between polling of endpoint context servers. The default interval is 60 minutes.
Automatically check for available Software Updates	Select the check box to enable automatic check for

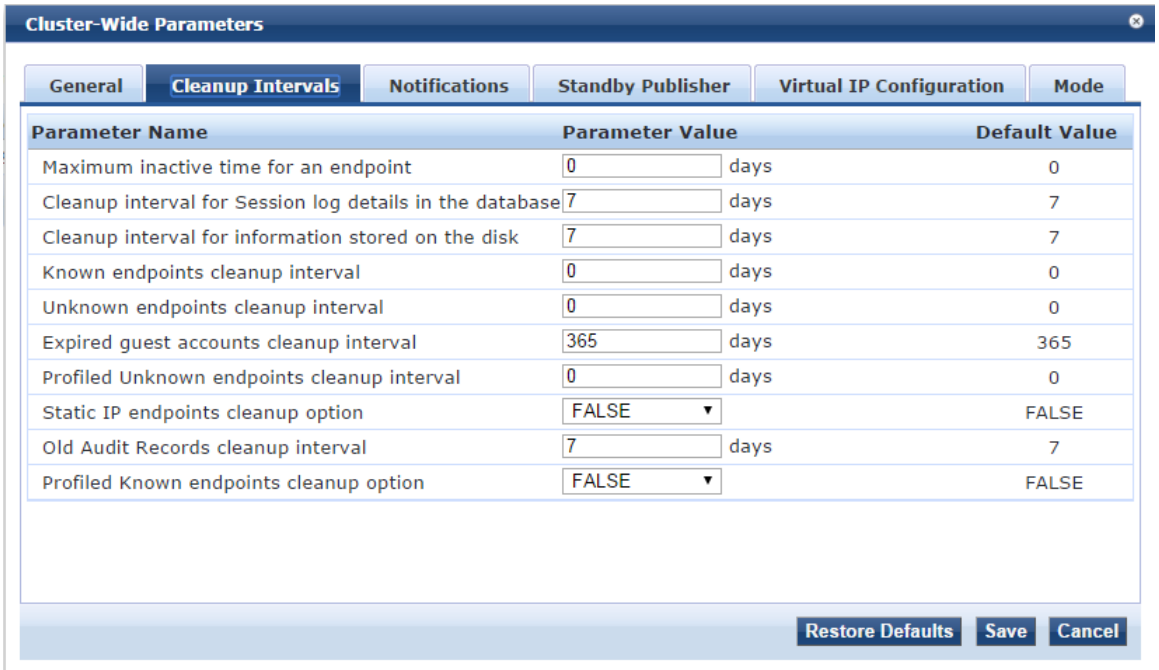
Table 253: *Cluster-Wide Parameters - General Tab Parameters (Continued)*

Parameter	Description
	available software updates.
Login Banner Text	Customize the banner text that appears on the ClearPass login screen and CLI access. You may use the banner to warn users of restrictions to access the website.
Admin Session Idle Timeout	Specify the maximum idle time permitted for the admin users beyond which the session times out. The default value is 30 minutes. The allowed range is 5–1440 minutes.
Multi Master Cache Durability	Set this to **Normal** or **Full** for the Multi Master Cache to survive most abrupt shutdowns. The default value is **OFF**. **NOTE:** Enabling this feature may result in some performance drop.

Cleanup Intervals

The following figure displays the **Cleanup Interval** tab of **Cluster-Wide Parameters**:

Figure 418: *Cluster-Wide Parameters - Cleanup Interval Tab*



The following table describes the **Cleanup Interval** tab parameters of **Cluster-Wide Parameters**:

Table 254: *Cluster-Wide Parameters - Cleanup Interval Tab Parameters*

Parameter	Description
Maximum inactive time for an endpoint	Specifies the duration in number of days to which an endpoint is retained in the endpoints table since its last authentication. If the endpoint is not authenticated for this period, the entry is removed from the endpoint table. 0 specifies no time limit configured.
Cleanup interval for Session log details in the database	Specify the duration in number of days to keep the following data in the Policy Manager DB: • session logs (found on **Access Tracker** page) • event logs (found on **Event Viewer** page) • machine authentication cache The default value is 7 days.
Cleanup interval for information stored on the disk	Specify the duration in number of days to keep log files that are written to the disk. The default value is 7 days.
Known endpoints cleanup interval	Specify the duration in number of days that ClearPass uses to determine when to start deleting known or disabled entries from the Endpoint repository. Known entries are deleted based on the last **Added At** value for each Endpoint. For example, if this value is 7, then known Endpoints that do not have the **Added At** value within the last 7 days are deleted. The default value is 0 days. This indicates that no cleanup interval is specified.
Unknown endpoints cleanup interval	Specify the duration in number of days that ClearPass uses to determine when to start deleting unknown entries from the Endpoint repository. Unknown entries are deleted based on the last **Updated At** value for each Endpoint. For example, if this value is 7, then unknown Endpoints that do not have the **Updated At** value within the last 7 days (stale endpoints) are deleted. The default value is 0 days. This indicates that no cleanup interval is specified.
Expired guest accounts cleanup interval	Specify the cleanup interval for expired guest accounts. This indicates the number of days after expiry that the cleanup occurs. 0 specifies no expired guest accounts cleanup interval. The default value is 365 days.
Profiled Unknown endpoints cleanup interval	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting profiled unknown entries from the Endpoint repository. Profiled unknown entries are deleted based on their last **Updated At** value for each Endpoint. For example, if this value is 7, then the Profiled Unknown Endpoints that do not have an **Updated At** value within the last 7 days are deleted. The default value is 0.

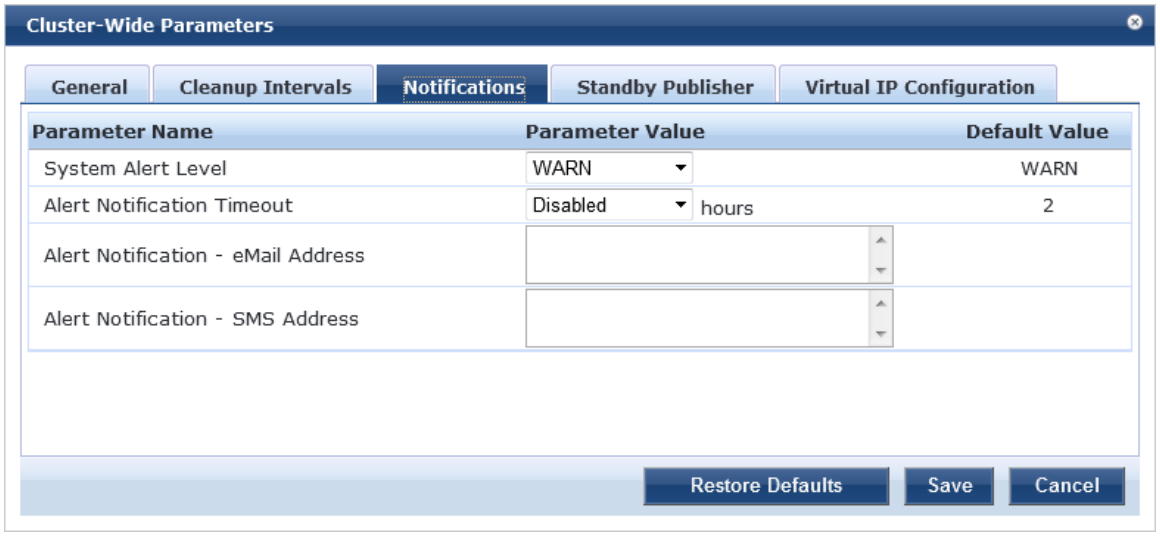
Table 254: *Cluster-Wide Parameters - Cleanup Interval Tab Parameters (Continued)*

Parameter	Description
Static IP endpoints cleanup option	Specify whether to enable the option to cleanup static IP endpoints. You can select TRUE or FALSE. The default options is FALSE.
Old Audit Records cleanup interval	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting old audit records from the **Audit Viewer** page. The default value is 7 days.
Profiled Known endpoints cleanup option	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting profiled known entries from the Endpoint repository. The default value is FALSE.

Notifications

The following figure displays the **Notifications** tab of **Cluster-Wide Parameters**:

Figure 419: *Cluster-Wide Parameters - Notifications Tab*



The following table describes the **Notifications** tab parameters of **Cluster-Wide Parameters**:

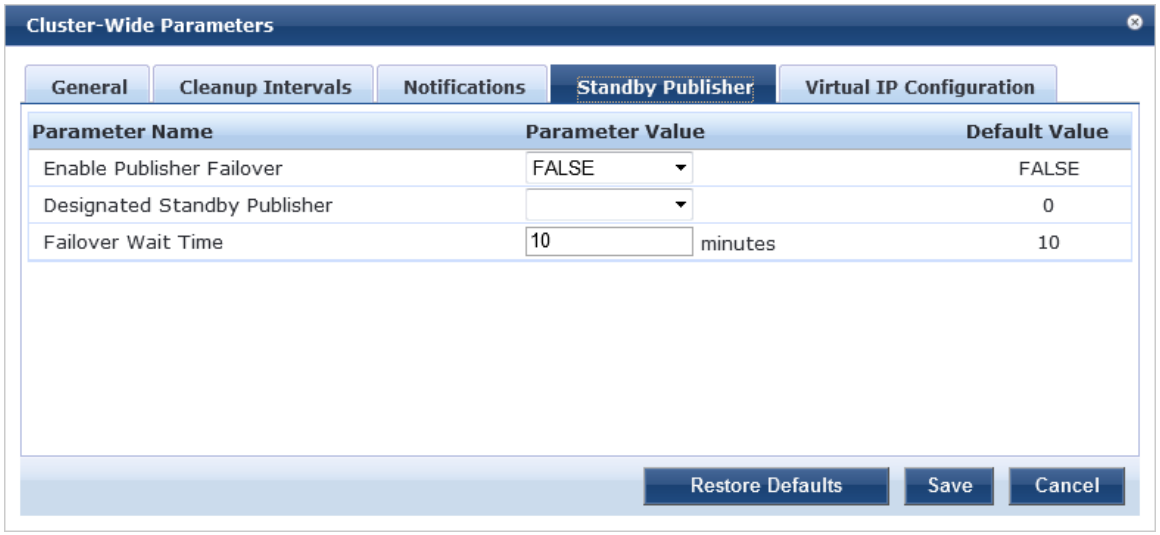
Table 255: *Cluster-Wide Parameters - Notifications Tab Parameters*

Parameter	Description
System Alert Level	Specify the alert notifications that are generated for system events logged at this level or higher. If you select **INFO,** alerts for INFO, WARN, and ERROR messages are generated. If you select **WARN**, alerts for WARN and ERROR messages are generated. If you select **ERROR**, then alerts for ERROR messages are only generated. The default value is **WARN**.
Alert Notification Timeout	Indicates the timeout in hours that determines how often alert messages are generated and sent out. If you select the **Disabled** option, the alert generation is disabled. The default value is 2 hours.
Alert Notification - eMail Address	Specify comma separated list of email addresses to which alert messages are sent.
Alert Notification - SMS Address	Specify comma separated list of SMS addresses to which alert messages are sent.

Standby Publisher

The following figure displays the **Standby Publisher** tab of **Cluster-Wide Parameters**:

Figure 420: *Cluster-Wide Parameters - Standby Publisher Tab*



The following table describes the **Standby Publisher** tab parameters of **Cluster-Wide Parameters**:

Table 256: *Cluster-Wide Parameters - Standby Publisher Tab Parameters*

Parameter	Description
Enable Publisher Failover	Select **TRUE** to authorize a node in a cluster on the system to act as a publisher if the primary publisher fails. The default value is **FALSE**.
Designated Standby Publisher	Select the server in the cluster to act as the standby publisher. The default value is 0. **NOTE:** If the Standby Publisher is on a different subnet from the Publisher, then ensure that a reliable connection between the two sub-nets is available to avoid unwanted network segmentation and potential data loss from false failover.
Failover Wait Time	The time (in minutes) for which the secondary node waits before it acquires a Virtual IP address after the primary node fails . The default failover wait time is 10 minutes. This avoids the secondary node from taking over when the primary node is temporarily unavailable during restart.

Virtual IP Configuration

The following figure displays the **Virtual IP Configuration** tab of **Cluster-Wide Parameters**:

Figure 421: *Cluster-Wide Parameters - Virtual IP Configuration Tab*

The following table describes the **Virtual IP Configuration** tab parameters of **Cluster-Wide Parameters**:

Table 257: *Cluster-Wide Parameters - Virtual IP Configuration Tab*

Parameter	Description
Failover Wait Time	Enter the number of seconds for the secondary node to wait after primary node failure before it acquires the Virtual IP Address. The default failover wait time is 10 seconds so the secondary node takes over and respond quickly to authentication access and requests.

You can define a virtual IP address only with a primary server without a secondary server, if required. This can be used to add an additional IP address to the Dell Networking W-ClearPass Policy Manager server without any redundancy.

Mode

The **Mode** tab in **Cluster-Wide Parameters** pop-up allows you to enable or disable **High Capacity Guest** mode. The **High Capacity Guest** mode addresses the high volume licensing requirements in the Public Facing Enterprises (PFE) environment, where a large volume of unique endpoints need wireless access.

The licensing scheme in the **High Capacity Guest** mode supports high volume of user traffic in the following PFEs where the count of endpoints keep changing everyday:

- Transportation—Airports and Rail Stations
- Hospitality—Hotels, Casinos, and Resorts
- Healthcare—Hospitals, Clinics, and Health Centers
- Retail—Shopping Malls
- Large Public Venues—Stadiums, Convention Centers, and Theaters
- Restaurants and Coffee Shops—Quick-Serve Restaurants

In enterprise deployments, the CPPM licensing accumulates the unique endpoint count for 7 days, which can cause the number of licenses to exceed. To address this license limit in the PFE environment, you can enable the **High Capacity Guest** mode on a cluster. In the **High Capacity Guest** mode, the count of unique endpoints is reset everyday instead of accumulating the count for 7 days. In the **High Capacity Guest** mode, only you can view the supported guest authentication methods such as PAP, CHAP, MSCHAP, EAP_MD5, MAC_AUTH, AUTHORIZE, and EAP_PEAP_in the **Authentication Methods** page.

You cannot enable the RADIUS services with the following authentication methods when the **High Capacity Guest** mode is enabled:

- EAP-FAST
- EAP-GTC
- EAP-MSCHAPv2
- EAP-PEAP
- EAP-TLS
- EAP-TTLS

Licensing

You can add only guest licenses to the **High Capacity Guest** mode and this mode is intended to handle only high volume of guest users in PFE environment. After enabling the **High Capacity Guest** mode, you cannot add enterprise licenses.

If the number of licenses used exceeds the number of licenses purchased, a warning message appears four months after the number is exceeded. The number of licenses used is based on the daily moving average. In the **High Capacity Guest** mode, a maximum of 2x licenses are allowed. For example, if you use the CP-HW-5K platform that supports 5k licenses, a maximum of 10k licenses are allowed in the **High Capacity Guest** mode.

Restrictions

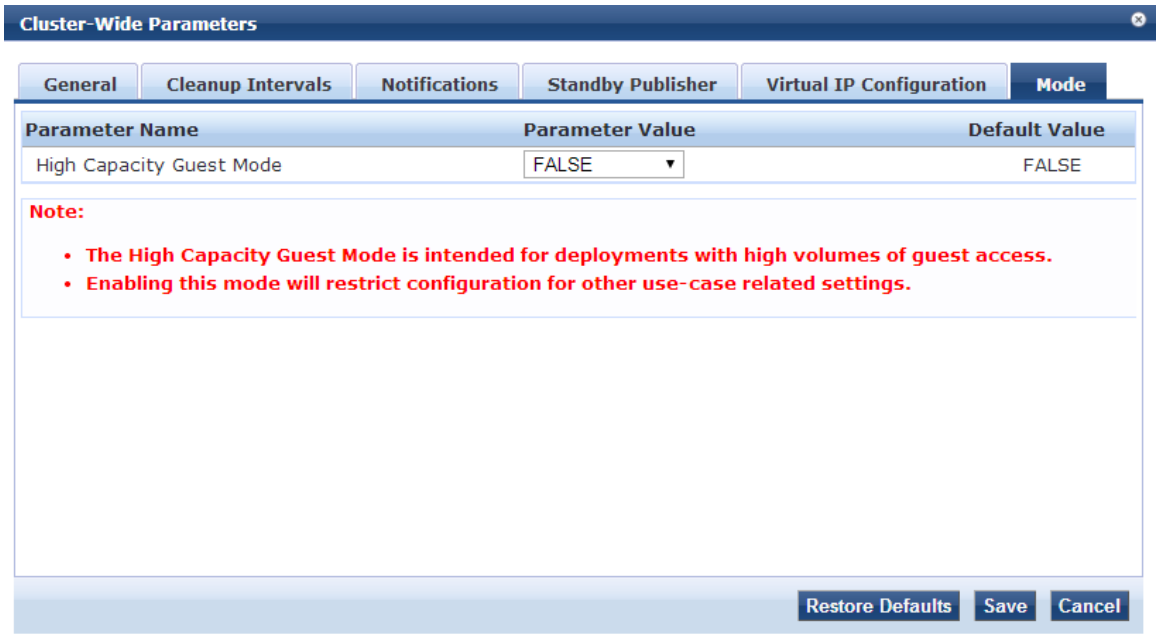
When the **High Capacity Guest** mode is enabled in a cluster, the following restrictions apply:

- Configuration settings cannot be moved from one cluster to another cluster that operates in the **High Capacity Guest** mode.
- Restoring configuration is allowed only with the backup files from the **High Capacity Guest** mode enabled servers.
- The **High Capacity Guest** mode is intended only for high volumes of guest access.
- Use-case related settings other than the **High Capacity Guest** mode are restricted.

- OnGuard and OnBoard access are restricted.
- Default cleanup interval values are reset.
- Only guest application licenses are allowed.

The following figure displays the **Mode** tab of **Cluster-Wide Parameters**:

Figure 422: *Cluster-Wide Parameters - Mode Tab*



The following table describes the **Mode** tab parameters of **Cluster-Wide Parameters**:

Table 258: *Cluster-Wide Parameters - Mode Tab*

Parameter	Description
High Capacity Guest Mode	Select **TRUE** or FALSE to enable or disable the **High Capacity Guest** mode. By default, the **High Capacity Guest** mode is disabled.

The following table describes the default cleanup interval values when the **High Capacity Guest** mode is enabled:

Table 259: *Cleanup Interval Values in the **High Capacity Guest** Mode*

Parameter	Description
Cleanup interval for Session log details in the database	The default value is 3 days.
Known endpoints cleanup interval	The default value of the known endpoints cleanup interval is 3 days.
Unknown endpoints cleanup interval	The default value of the unknown endpoints cleanup interval is 3 days.

Table 259: *Cleanup Interval Values in the High Capacity Guest Mode (Continued)*

Parameter	Description
Expired guest accounts cleanup interval	The default value of the Expired guest accounts cleanup interval is 10 days.
Profiled endpoints cleanup interval	The default value of the Profiled endpoints cleanup interval is 3 days.
Old Audit Records cleanup interval	The default value of the Old Audit Records cleanup interval is 10 days.
Profiled Known endpoints cleanup option	Specify the cleanup interval in number of days that ClearPass uses to determine when to start deleting profiled known entries from the Endpoint repository. The default value is TRUE.

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

- ClearPass Admin Access (Active Directory)
- ClearPass Admin SSO Login (SAML SP Service)
- ClearPass Identity Provider (SAML IdP Service)
- Encrypted Wireless Access via 802.1X Public PEAP method
- Guest Access
- Guest Access - Web Login
- Guest MAC Authentication
- OAuth2 API User Access

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

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

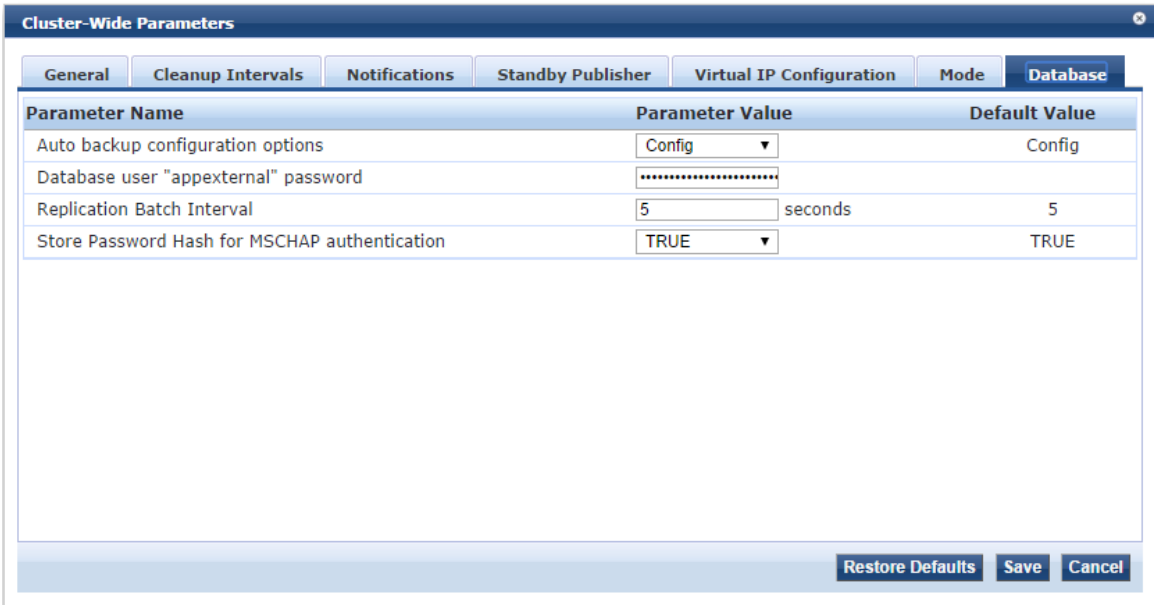
The following authentication methods are used in service templates in the HCG mode:

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

Database

The following figure displays the **Database** tab of **Cluster-Wide Parameters**:

Figure 423: *Cluster-Wide Parameters - Database Tab*



The following table describes the **Database** tab parameters of **Cluster-Wide Parameters**:

Table 260: *Cluster-Wide Parameters - Database Tab Parameters*

Parameter	Description
Auto backup configuration options	Select any of the following auto backup configuration options: • **Off** - Select this to not to perform periodic backups. **NOTE:** Select **Off** before upgrading Dell Networking W-ClearPass Policy Manager to avoid the interference between Auto backup and migration process. • **Config** - Perform a periodic backup of the configuration database only. This is the default auto backup configuration option. • **Config|SessionInfo** - Perform a backup of the configuration database and the session log database. **NOTE:** It is recommended that you set this option to **Off** or **Config** before starting an upgrade. This ensures the Auto Backup process does not interfere with migration post upgrade. If required, you may change this setting back to **Config|SessionInfo** 24 hours after upgrade completion.
Database user "appexternal" password	Enter the password for the **appexternal** username for this connection to the database.
Replication Batch Interval	Configure the time interval at which the subscribers

Table 260: *Cluster-Wide Parameters - Database Tab Parameters (Continued)*

Parameter	Description
	synchronize with the publisher. The default value is 5 seconds. The allowed range is 1–60 seconds.
Store Password Hash for MSCHAP authentication	Set this to TRUE to store passwords for admin and local users to Hash and NTLM hash formats which enables RADIUS MSCHAP authentications against admin or local repositories. If you set this to FALSE, the following warning message is displayed: **Changing the Cluster-wide Parameter "Store Password Hash for MSCHAP" to FALSE removes NTLM hashes for local and admin users. This means RADIUS MSCHAP auths against those auth sources is no longer possible, and this is not "reversible" by just reverting the cluster-wide parameter value. To revert you need to set the parameter back to TRUE and reset the passwords for all admin/local users.**

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. Navigate to **Administration > Server Manager > Server Configuration**,
2. Click **Collect Logs**. The **Collect Logs** pop-up appears.
3. Enter an output filename and add the .tar.gz extension to the filename.
4. Select the types of logging information you want to collect. The types of logging are:
   - System Logs
   - Logs from all Policy Manager services
   - Capture network packets Duration of dump

Use this option only when you want to debug a problem. System performance can be severely impacted.

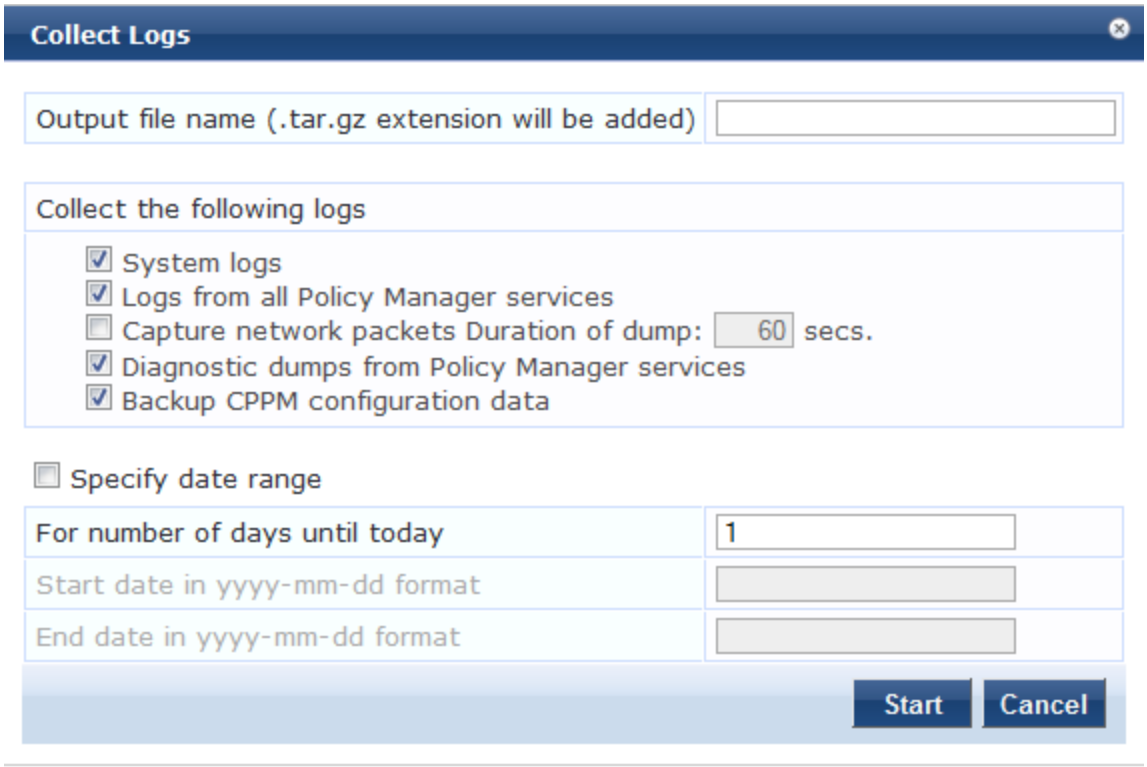
   - Diagnostic dumps from Policy Manager services
   - Backup CPPM Configuration data
5. Enter the time period for which you want to collect the information.
   - Specify a number to collect logs for the number of days until the current day.
   - Select the **Specify date range** check box and enter a start date and end date in yyyy.mm.dd format in the respective fields to collect logs for the specified time period.
6. Click **Start**. You'll see the progress of the information collection.
7. Click **Close** to finish or click **Download File** to save the log file to your computer.

NOTE

If you are attempting to open a capture file (.cap or .pcap) using WireShark, untar or unzip the file (based on the file extension). When the entire file is extracted, navigate to the PacketCapture folder. In this folder, you will find a file with a .cap extension. WireShark can be used to open this file and study the network traffic.

The following figure displays the **Collect Logs** pop-up:

Figure 424: *Collect Logs*

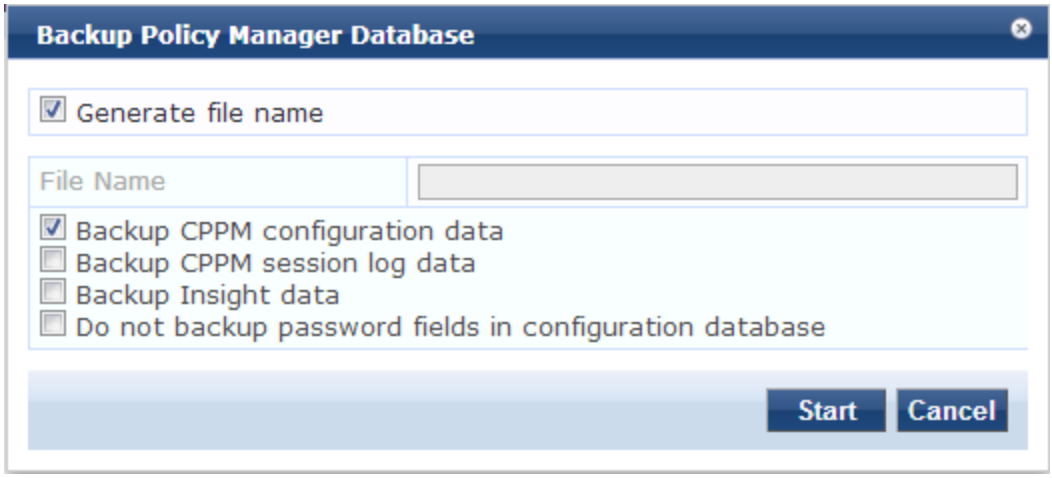


Backup

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Back Up** button.

The following figure displays the **Backup Policy Manager Database** pop-up:

Figure 425: *Backup Popup*



The following table describes the **Backup Policy Manager Database** parameters:

Table 261: *Backup Policy Manager Database*

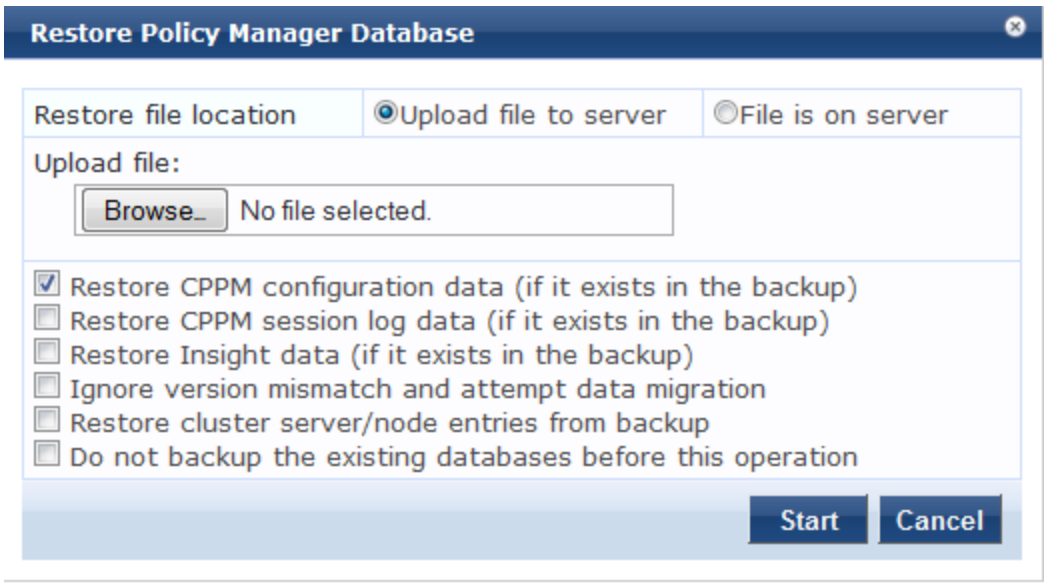
Parameter	Description
Generate filename	Select the check box to enable Policy Manager to generate a filename; otherwise, specify a filename. Backup files are in the gzipped tar format (tar.gz extension). The backup file is automatically placed in the *Shared Local Folder* under folder type *Backup Files* (See Local Shared Folders).
Filename	
Do not backup log database	Select the check box if you do not want to backup the log database.
Do not backup password fields in configuration database	Select the check box if you do not want to backup password fields in configuration database.
Backup databases for installed applications	Select the check box if you want the backup to include databases for installed applications.

Restore

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Restore** button to restore Dell Networking W-ClearPass Policy Manager configuration data.

The following figure displays the **Restore Policy Manager Database** pop-up:

Figure 426: *Restore Policy Manager Database*



The following table describes the **Restore Policy Manager Database** parameters:

Table 262: *Restore Policy Manager Database*

Parameter	Description
Restore file location	Select either **Upload file to server** or **File is on server**.
Upload file path	Browse to select name of backup file. **NOTE:** This option is available only when the **Upload file to server** option is selected.
Shared backup files present on the server	If the files is on a server, select a file from the files in the local shared folders. (See Local Shared Folders.) **NOTE:** This is displayed only when the **File on server** option is selected.
Restore CPPM configuration data (if it exists in the backup)	Select the check box to include an existing configuration data in the restore.
Restore CPPM session log data (if it exists in the backup).	Select the check box to include the log data in the restore.
Restore Insight data (if it exists in the backup)	Select the check box to include Insight reporting data in the restore.
Ignore version mismatch and attempt data migration	Select the check box if you are migrating configuration and/or log data from a backup file that was created with a previous compatible version.
Restore cluster server/node entries from backup.	Select the check box to include the cluster server/node entries in the restore.
Do not backup the existing databases before this operation.	Select the check box if you do not want to backup the existing databases before performing a restore.

Cleanup

You can perform a system cleanup operation to purge the following records:

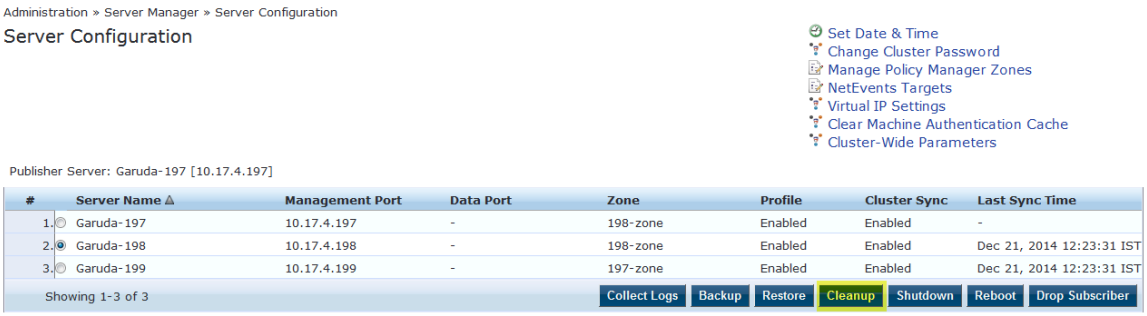
- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

To perform a system cleanup:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration** page and click the **Cleanup** button. The **Force Cleanup Files** pop-up is displayed.
2. Enter a number to cleanup files that are older than the specified number of days. The allowed range is 0-15.
3. Click **Start** to initiate the cleanup process.

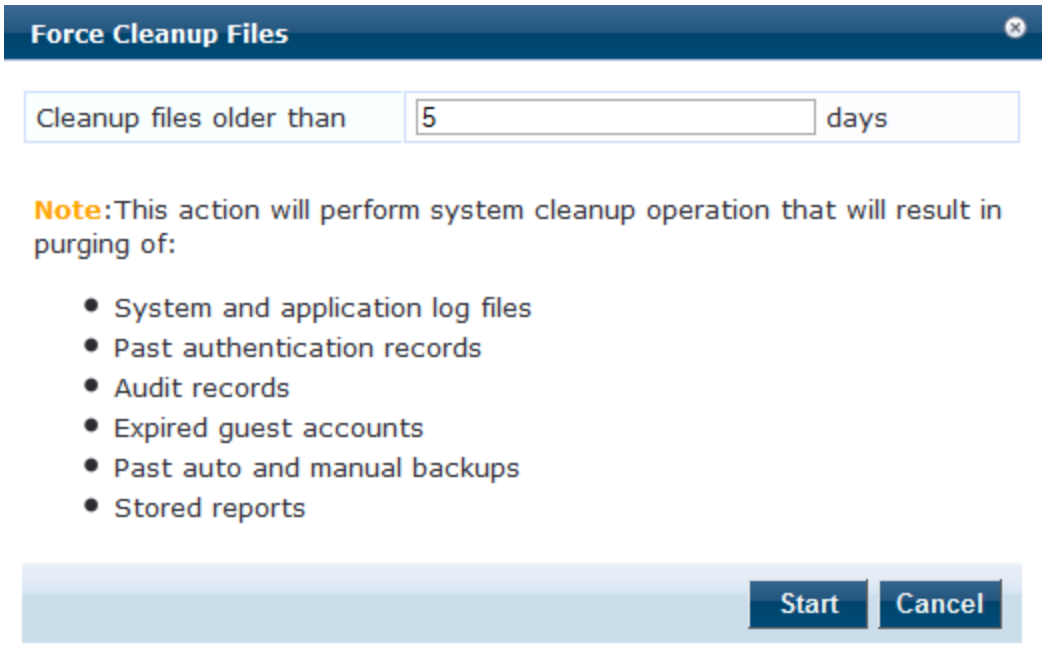
The following figure displays the **Cleanup** option in the **Server Configuration** page:

Figure 427: *Server Configuration - Cleanup*



The following figure displays the **Force Cleanup Files** pop-up:

Figure 428: *Force Cleanup Files*



The following figure displays the cleanup progress:

Figure 429: *Cleanup Progress Screen*

Shutdown/Reboot

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Shutdown** or **Reboot** buttons to shutdown or reboot the node.

Drop Subscriber

Navigate to the **Administration > Server Manager > Server Configuration** page and click the **Drop Subscriber** button to drop a subscriber from the cluster.

This option is not available in a single node deployment.

Log Configuration

Navigate to the **Adminitration > Server Manager > Log Configuration** page to configure logs for services and system level.

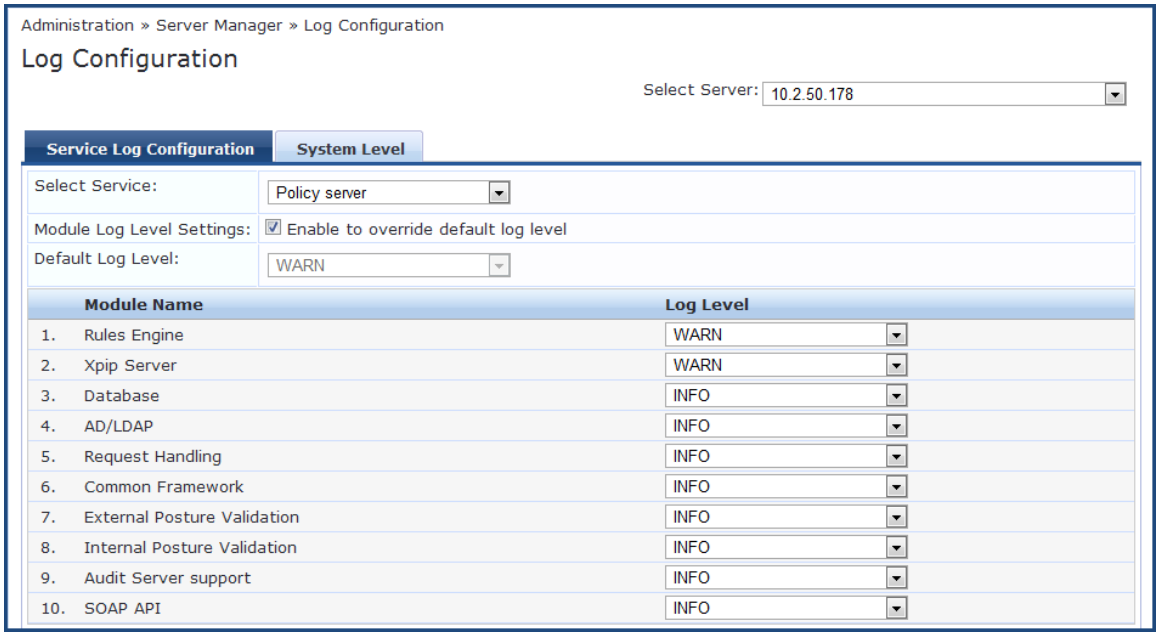
The **Log Configuration** page contains the following tabs:

- Service Log Configuration on page 458
- System Level on page 459

Service Log Configuration

The following figure displays the **Service Log Configuration** tab:

Figure 430: *Log Configuration - Service Log Configuration Tab*



The following table describes the **Service Log Configuration** tab parameters:

Table 263: *Log Configuration - Service Log Configuration tab Parameters*

Parameter	Description
Select Server	Specify the server for which you want to configure logs. All nodes in the cluster appear in the drop-down list.
Select Service	Specify the service for which you want to configure logs.
Module Log Level Settings	Select the check box to set the log level for each module individually (listed in decreasing level of verbosity. For optimal performance you must run Policy Manager with log level set to ERROR or FATAL): • DEBUG • INFO • WARN • ERROR • FATAL If this option is disabled, then all module level logs are set to the default log level.
Default Log Level	This drop-down list is available if the **Module Log Level Settings** option is disabled. This sets the default logging level for all modules. Available options include the following: • DEBUG • INFO • WARN • ERROR • FATAL

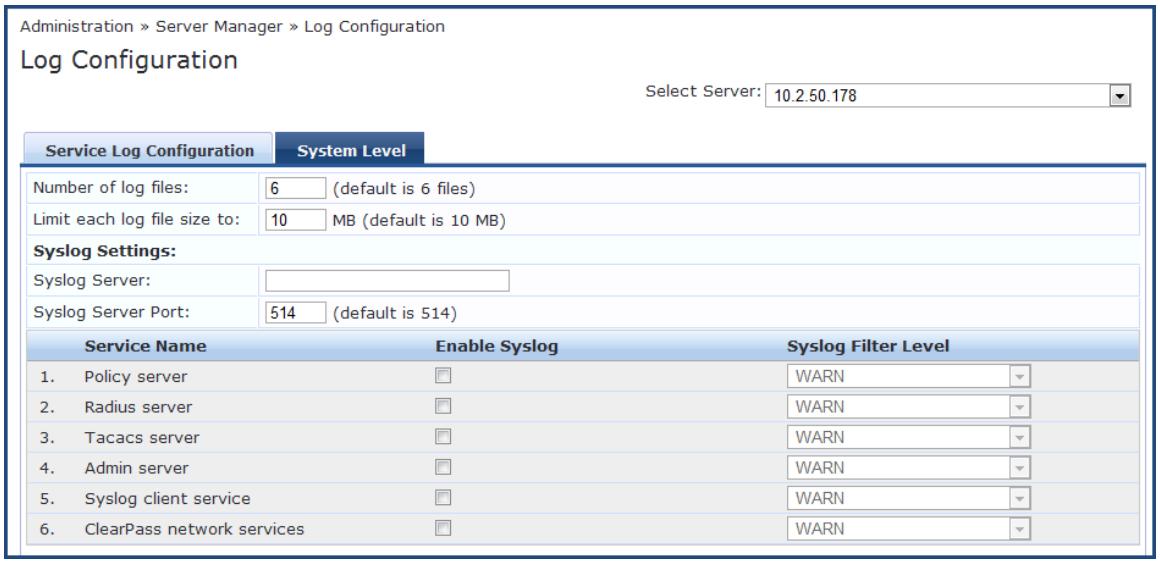
Table 263: *Log Configuration - Service Log Configuration tab Parameters (Continued)*

Parameter	Description
	NOTE: Set this option first, and then override any modules as necessary.
Module Name & Log Level:	If the **Module Log Level Settings** option is enabled, select log levels for each available module (listed in decreasing level of verbosity): • DEBUG • INFO • WARN • ERROR • FATAL
Restore Defaults/Save	Click **Save** to save changes or **Restore Defaults** to restore default settings.

System Level

The following figure displays the **System Level** tab:

Figure 431: *Log Configuration - System Level tab*



The following table describes the **System Level** tab parameters:

Table 264: *Log Configuration - System Level tab Parameters*

Parameter	Description
Select Server	Specify the server for which you want 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 the number of log files exceeds the specified value, Policy Manager overwrites the oldest file.
Limit each log file size to	Limit each log file to this size, before the log rolls over to the next file. The default value is 50 MB.
Syslog Server Syslog Port	Specify the syslog server and port number. Policy Manager sends the configured module logs to this syslog server.
Service Name Enable Syslog Syslog Filter Level	For each service, you can select the **Enable Syslog** check box and then override the Syslog Filter level. The current Syslog Filter level is based on the default log level specified on the **Service Log Configuration** tab.
Restore Defaults/Save	Click **Save** to save changes or **Restore Defaults** to restore default settings.

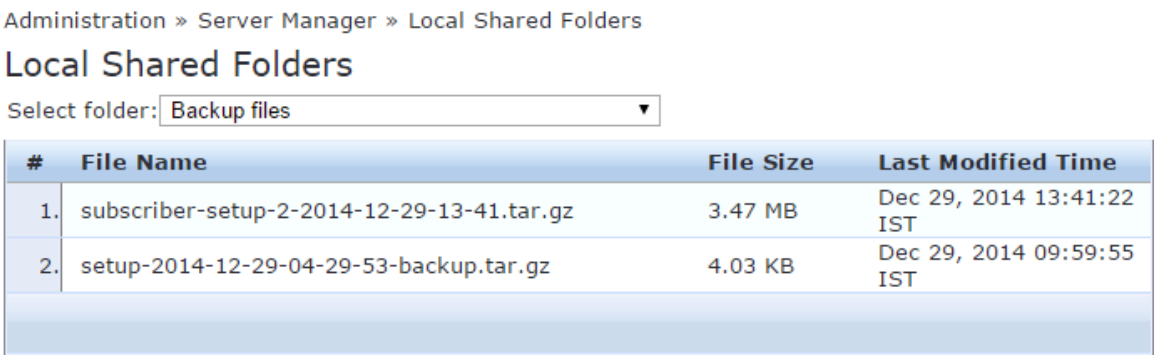
Local Shared Folders

To download a local shared folder, navigate to **Administration > Server Manager > Local Shared Folders**. Choose a file type from the **Select folder** drop-down list. The browser download box appears. Currently supported folder types are listed below:

- **Backup files** - Database backup files backed up manually
- **Log files** - Log files backed up via the Collect Logs on page 452 mechanism
- **Automated Backup files** - Database backup files backed up automatically on a daily basis

The following figure displays the **Local Shared Folders** page:

Figure 432: *Local Shared Folders Page*



License Management

The **Licensing** page shows all the licenses that is activated for the entire Dell Networking W-ClearPass Policy Manager cluster. You must have a Dell Networking W-ClearPass Policy Manager base license for every instance of the product.

NOTE

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

This section describes the following topics:

NOTE

On a VM instance of CPPM, the permanent license must be entered.

Licensing Main Page

To manage licenses, navigate to **Administration > Server Manager > Licensing**. The **Licensing** page has the following tabs:

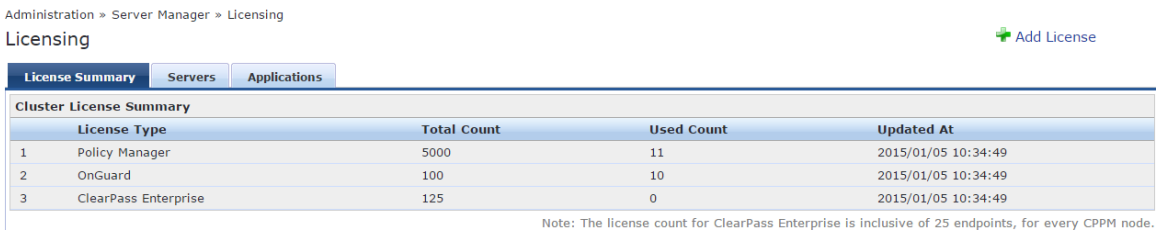
NOTE

The **Applications** tab gets activated on adding an application license like OnGuard, Guest, or Onboard.

License Summary Tab

You can add and activate OnGuard, Guest, Onboard, and Enterprise licenses. The **License Summary** tab displays the number of purchased licenses for Policy Manager, OnGuard, Guest, Onboard, and ClearPass Enterprise. The following figure displays the **License Summary** tab:

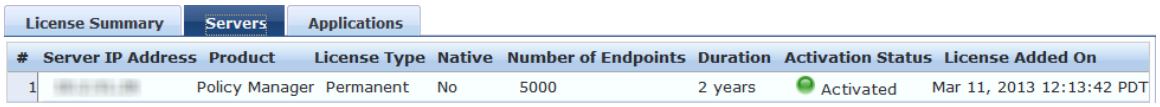
Figure 433: *License Summary Tab*



Servers Tab

The **Servers** tab displays the Policy Manager server IP address, the product type, license type, license activation status, and many more parameters. The following figure displays the **Servers** tab:

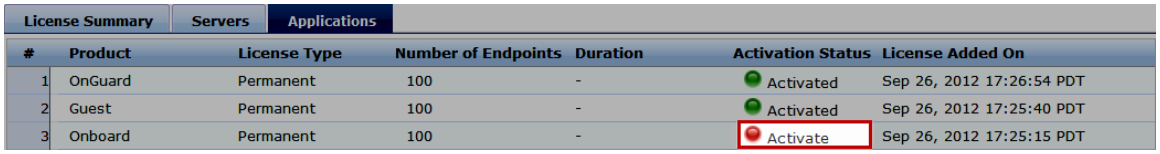
Figure 434: *Servers Tab*



Applications Tab

The **Applications** tab displays the Dell Networking W-ClearPass Policy Manager application license details like product type, license type, license activation status, and many more. The following figure displays the **Applications** tab:

Figure 435: *Applications Tab*



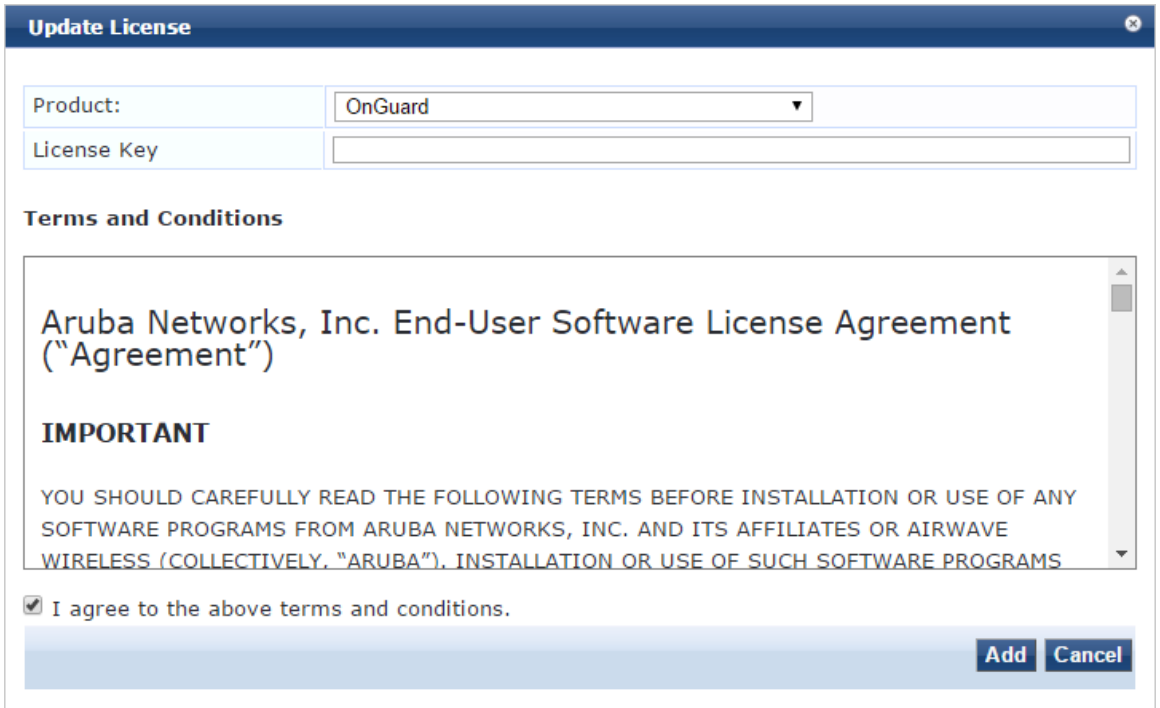
Adding an Application License

To add an application license:

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Add License** link on the top right section of the page. The **Update License** pop-up appears.
3. Choose a product from the **Product** drop-down list.
4. Enter the license key.
5. Click the **I agree to the above terms and conditions.** check box.
6. Click **Add**.

The following figure displays the **Update License** pop-up:

Figure 436: *Update License Pop-up*



Activating a Server License

You must activate a server license only once, when you first install Policy Manager on a server. To activate a server license:

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Servers** tab. Servers that are not activated have the keyword **Activate** next to the red dot in the **Activation Status** field heading.
3. Click **Activate** next to the red dot in the **Activation Status** field heading. The **Activate License** pop-up appears.
4. In the **Online Activation** section of the **Activate License** pop-up, click **Activate Now**.

If you are not connected to the Internet, follow the instructions in the **Offline Activation** section. Download an activation request token from the Policy Manager server and email the file to Dell support. You will receive an activation key that you can upload.

The following figure displays the **Activate License** pop-up:

Figure 437: *Activate License Pop-up*

Activating an Application License

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

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Applications** tab. Applications that are not activated have the keyword **Activate** next to the red dot in the **Activation Status** field heading.
3. Click **Activate** next to the red dot in the **Activation Status** field heading. The **Activate License** pop-up appears.
4. In the **Online Activation** section of the **Activate License** pop-up, click **Activate Now**.

If you are not connected to the Internet, follow the instructions in the **Offline Activation** section. Download an activation request token from the Policy Manager server and email the file to Dell support. You will receive an activation key that you can upload.

The following figure displays the **Activate License** pop-up:

Figure 438: *Activate License Pop-up*

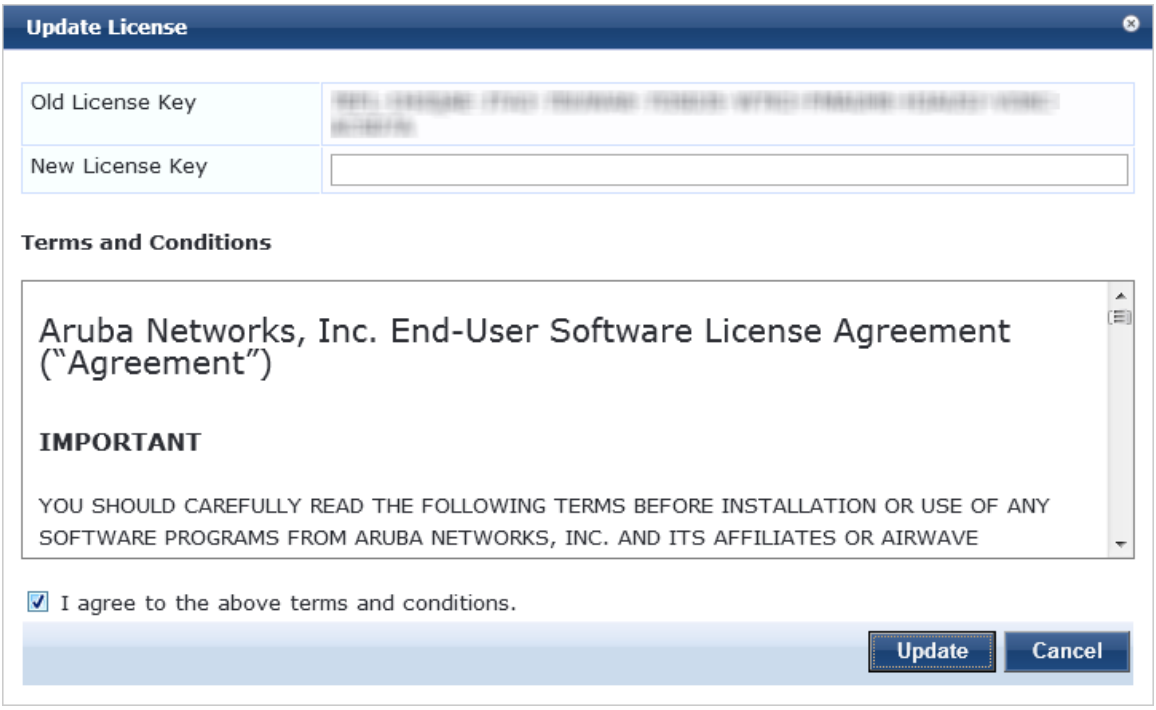
Updating a Server License

Licenses typically require updating after they expire, for example, after the evaluation license expires, or when capacity exceeds its licensed amount. To update a server license:

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Servers** tab.
3. Click anywhere on a server entry except the **Activation Status** field entry. The **Update License** pop-up appears.
4. Enter the new license key.
5. Click the **I agree to the above terms and conditions.** check box.
6. Click **Update**.

The following figure displays the **Update License** pop-up:

Figure 439: *Update License Pop-up*



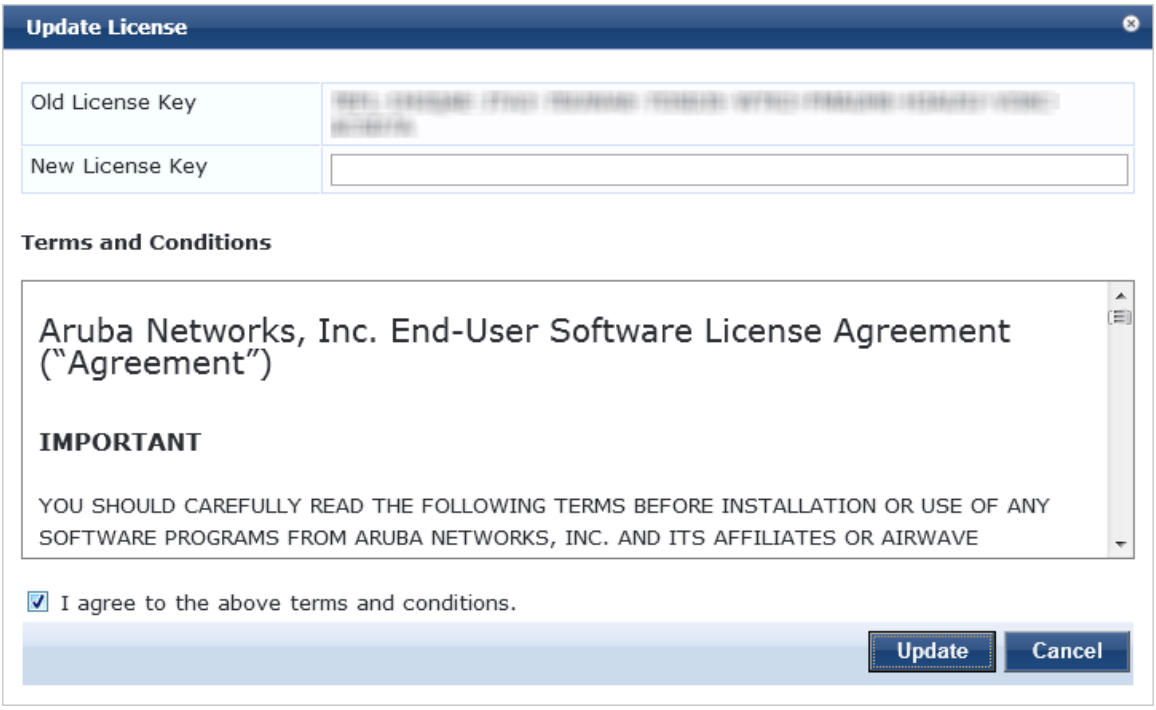
Updating an Application License

Licenses typically require updating after they expire, for example, after the evaluation license expires, or when capacity exceeds its licensed amount. To update an application license:

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Applications** tab.
3. Click anywhere on an application entry except the **Activation Status** field entry. The **Update License** pop-up appears.
4. Enter the new license key.
5. Click the **I agree to the above terms and conditions.** check box.
6. Click **Update**.

The following figure displays the **Update License** pop-up:

Figure 440: *Update License Pop-up*



SNMP Trap Receivers

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

- **System up-time**— Provides 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 the set limit. The value can be in percentage 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 sends a trap to the configured destination.
- **Memory usage**— Report the memory usage of the system.

This section describes the following topics:

SNMP Trap Receivers Main Page

To view a list of SNMP trap receivers configured on the Dell Networking W-ClearPass Policy Manager server, navigate to **Administration > External Servers > SNMP Trap Receivers**.

The following figure displays the **SNMP Trap Receivers** page:

Figure 441: *SNMP Trap Receivers Page*

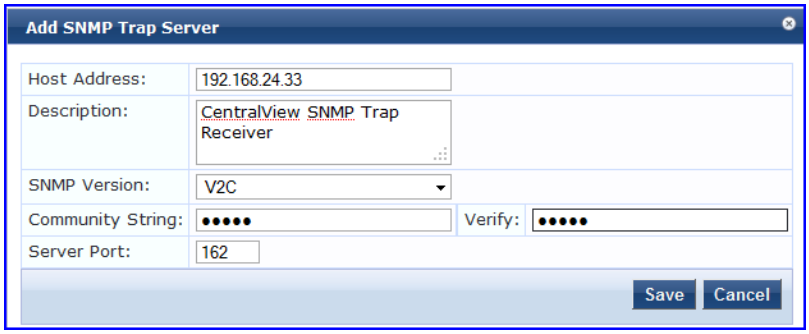
Adding an SNMP Trap Server

To add an SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Click the **Add** link on the top right section of the page. Enter the details based on Table 265.
3. Click **Save**.

The following figure displays the **Add SNMP Trap Server** pop-up:

Figure 442: *Add SNMP Trap Server Pop-up*



The following table describes the **Add SNMP Trap Server** parameters:

Table 265: *Add SNMP Trap Server Parameters*

Parameter	Description
Host Address	Enter the trap destination hostname or IP address. **NOTE:** This server must have an SNMP trap receiver or trap viewer installed.
Description	Enter a short description of the SNMP trap server.
SNMP Version	Select the SNMP version.

Table 265: *Add SNMP Trap Server Parameters (Continued)*

Parameter	Description
Community String / Verify	Enter and re-enter the community string for sending the traps.
Server Port	Port number for sending the traps. By default, the port number is 162. **NOTE:** Configure the trap server firewall for traffic on this port.

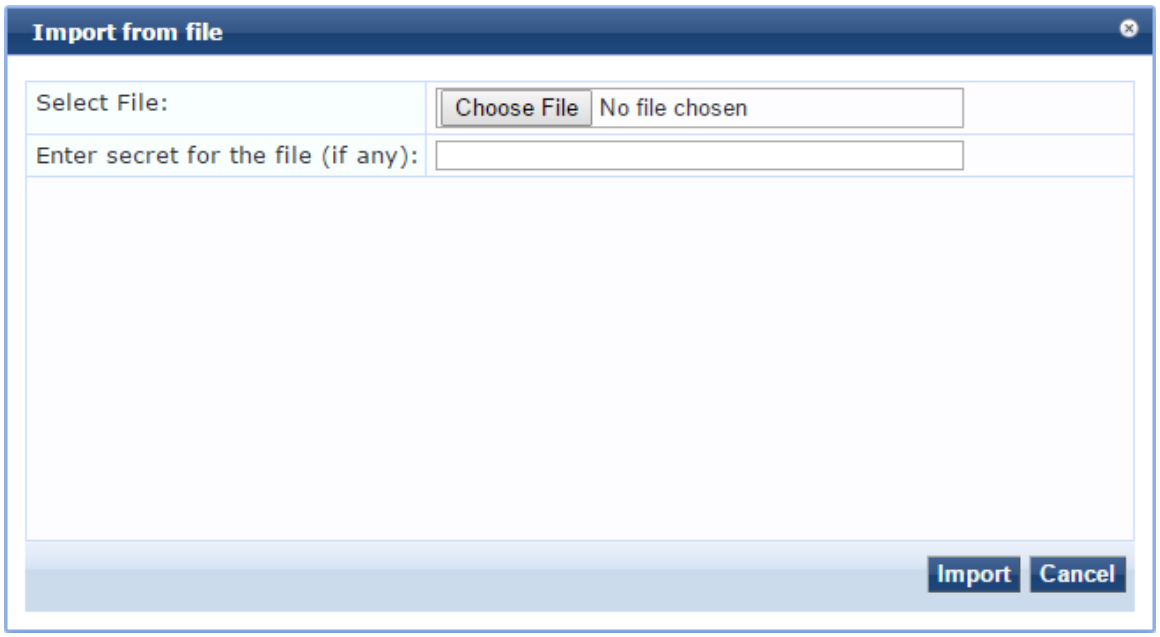
Importing an SNMP Trap Server

To import an SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Click the **Import** link on the top right section of the page. Enter the details based on Table 266.
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 443: *Import from file Pop-up*



The following table describes the **Import from file** parameters:

Table 266: *Import from file Parameters*

Parameter	Description
Select File	Browse to the SNMP Trap Server configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the secret key here.

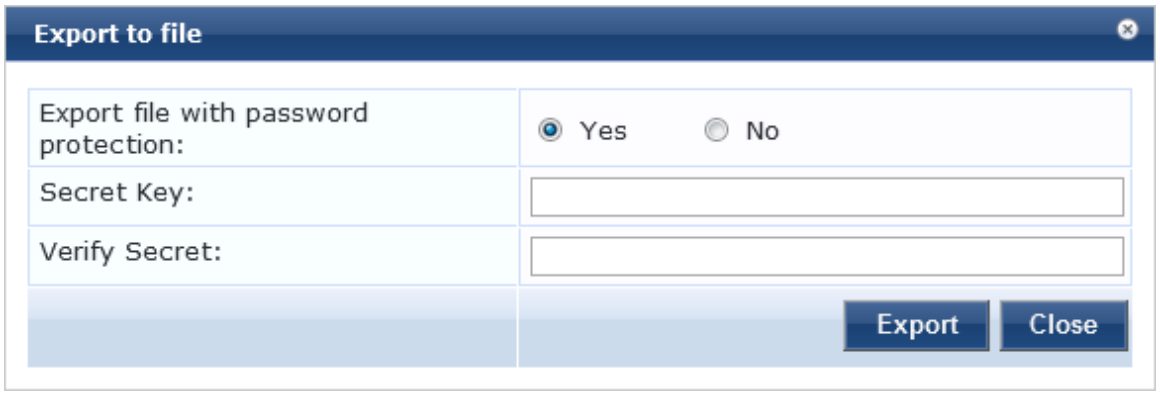
Exporting All SNMP Trap Servers

This link exports all configured SNMP Trap Receivers. To export all SNMP trap servers:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Click the **Export All** link on the top right section of the page. Enter the details based on Table 267.
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 444: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 267: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose **Yes** to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

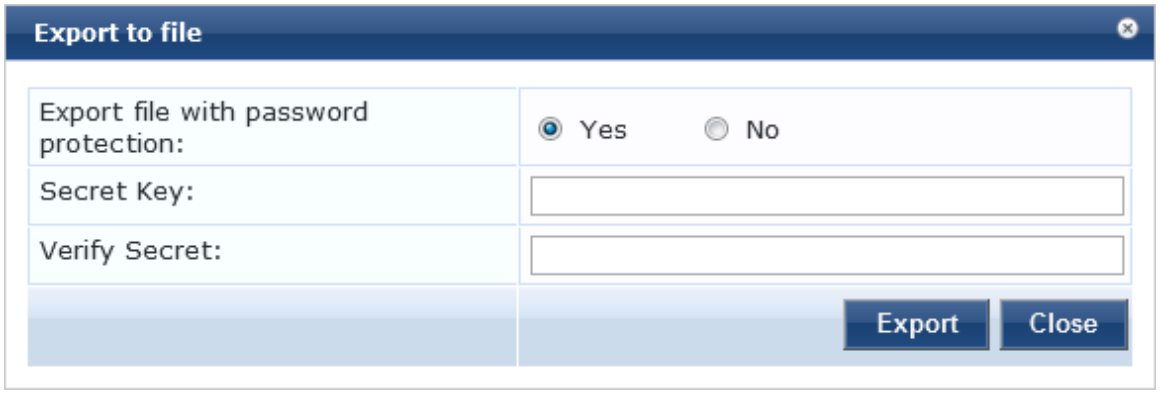
Exporting an SNMP Trap Server

To export a single SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Select the **Host Address** from the list of check boxes and click **Export**. Enter the details based on Table 268.
3. Enter the name of the XML file in the **Save As** dialog.
4. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 445: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 268: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose **Yes** to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Deleting an SNMP Trap Server

To delete a single SNMP trap server:

1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.
2. Click the check box next to the **Host Address** entry and click **Delete**.
3. Click **Yes**.

Syslog Targets

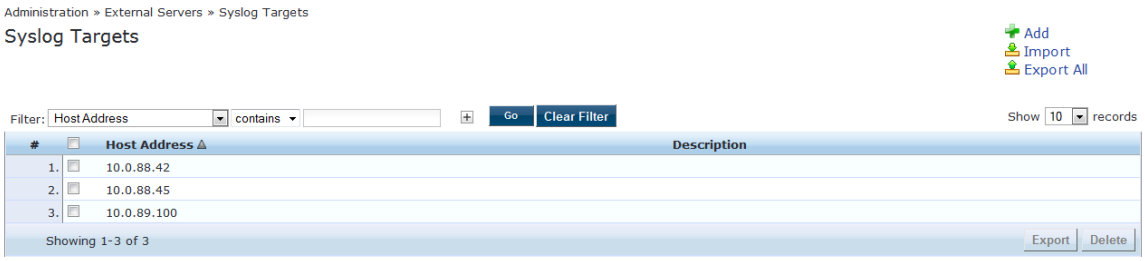
Dell Networking W-ClearPass Policy Manager can export session data (see Live Monitoring: Access Tracker on page 43), audit records (see Audit Viewer on page 75) and event records (see Event Viewer on page 77). This information can be sent to one or more syslog targets (servers). You configure syslog targets from this page. To configure syslog target, navigate to **Administration > External Servers > Syslog Targets**.

This section describes the following topics:

Syslog Targets Main Page

The following figure displays the **Syslog Targets** page:

Figure 446: *Syslog Targets Page*



The following table describes the **Syslog Targets** parameters:

Table 269: *Syslog Targets Parameters*

Parameter	Description
Add	Opens the **Add Syslog Target** pop-up.
Import	Opens the **Import from file** pop-up. You can import the syslog target from a file.
Export All	Opens the **Export to file** pop-up. You can export all the syslog target entries to a file.
Export	Opens the **Export to file** pop-up. With this option, you can export individual syslog targets.
Delete	Deletes a syslog target server.

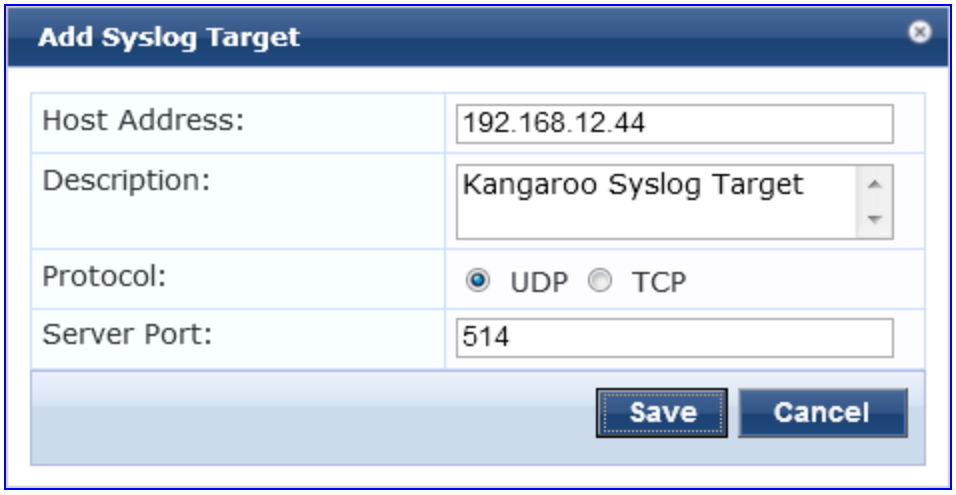
Adding a Syslog Target

To add a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the **Add** link on the top right section of the page. Enter the details based on Table 270.
3. Click **Save**.

The following figure displays the **Add Syslog Target** pop-up:

Figure 447: *Add Syslog Target Pop-up*



The following table describes the **Add Syslog Target** parameters:

Table 270: *Add Syslog Target Parameters*

Parameter	Description
Host Address	Syslog server hostname or IP address.
Description	Enter a short description of the syslog server.
Protocol	Select one of the following options: • **UDP**: This option reduces overhead and latency. • **TCP**: this option provides error checking and packet delivery validation.
Server Port	Port number for sending the syslog messages. Default port number is 514.

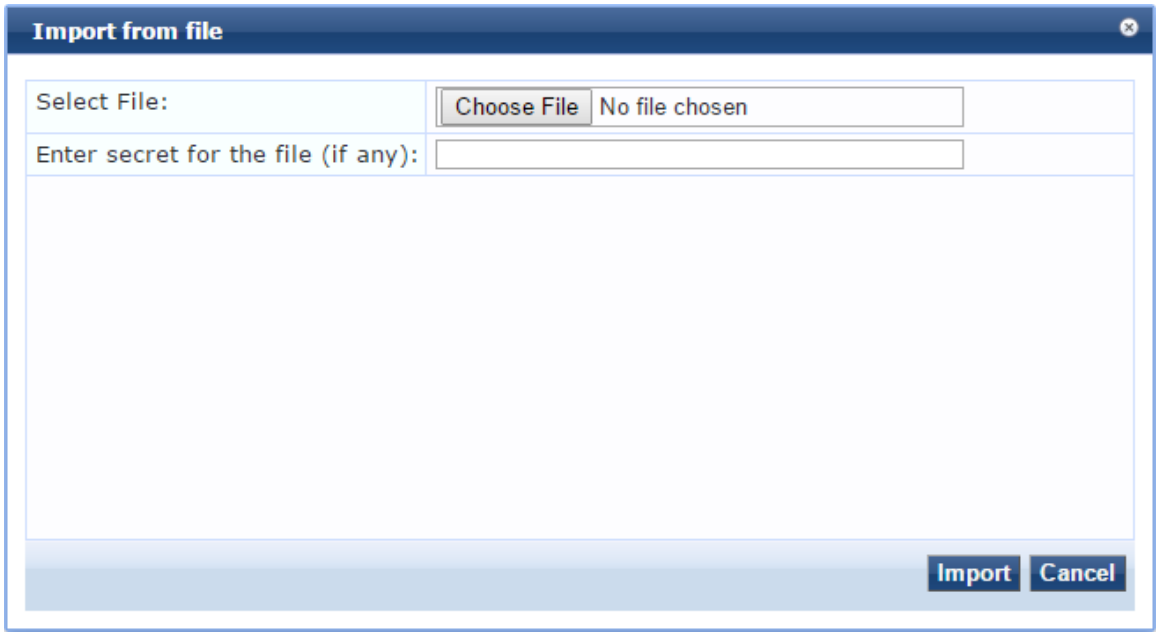
Importing a Syslog Target

To import a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the **Import** link on the top right section of the page. Enter the details based on Table 271.
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 448: *Import from file Pop-up*



The following table describes the **Import from file** parameters:

Table 271: *Import from file Parameters*

Parameter	Description
Select File	Browse to the Syslog Target configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.

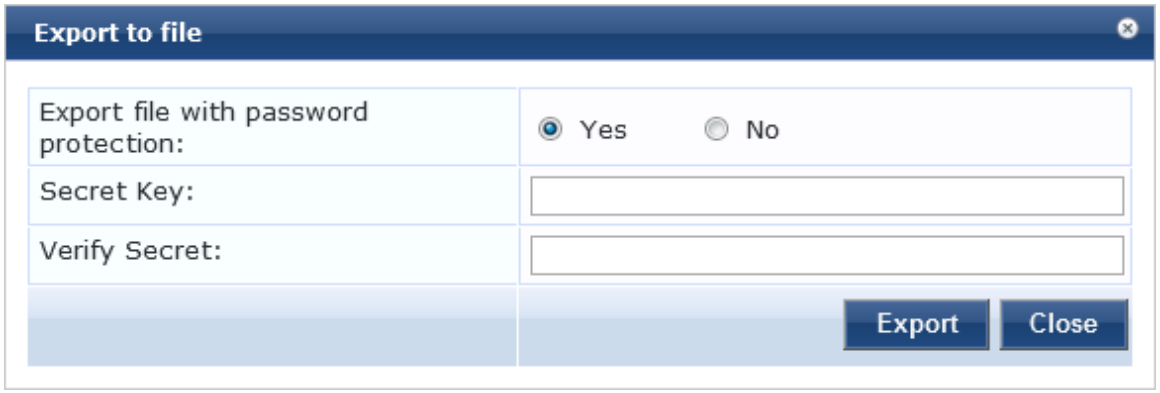
Exporting All Syslog Target

To export all syslog targets:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the **Export All** link on the top right section of the page. Enter the details based on Table 272.
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 449: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 272: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose **Yes** to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

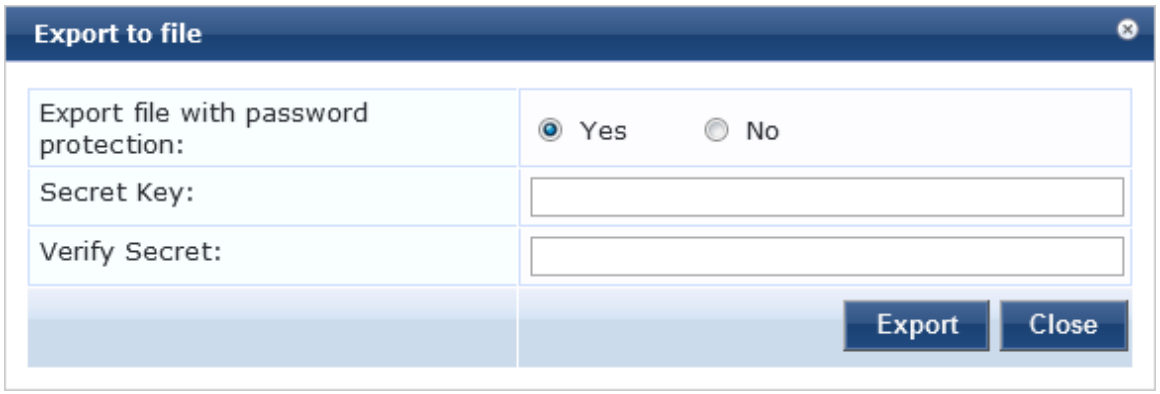
Exporting a Syslog Target

To export a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Select the **Host Address** from the list of check boxes and click **Export**. Enter the details based on Table 272.
3. Enter the name of the XML file in the **Save As** dialog.
4. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 450: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 273: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose **Yes** to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Deleting a Syslog Target

To delete a syslog target:

1. Navigate to **Administration > External Servers > Syslog Targets**.
2. Click the check box next to the **Host Address** entry and click **Delete**.
3. Click **Yes**.

Syslog Export Filters

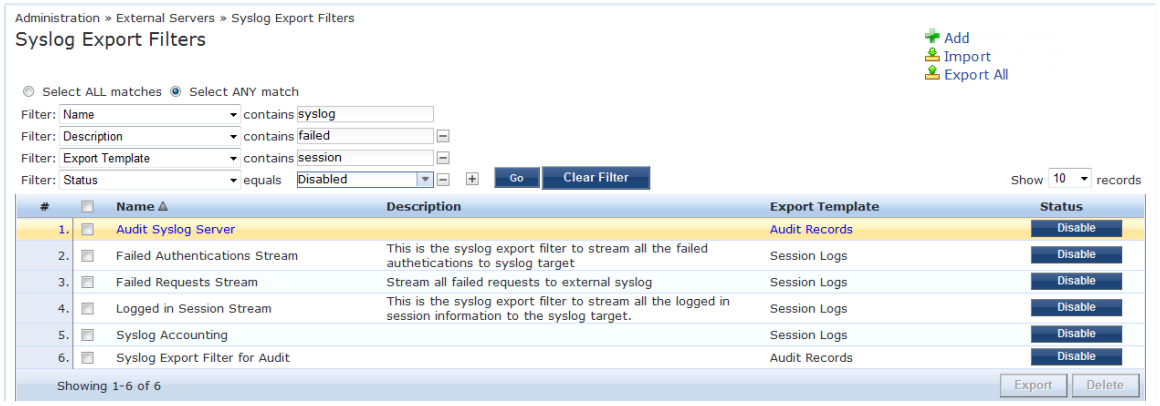
Policy Manager can export session data (see Live Monitoring: Access Tracker on page 43), audit records (see Audit Viewer on page 75) and event records (see Event Viewer on page 77). You configure syslog export filters to instruct Policy Manager where to send this information, and what kind of information should be sent through data filters. To configure syslog export filters, navigate to **Administration > External Servers > Syslog Export Filters**.

This section describes the following topics:

Syslog Export Filters Main Page

The following figure displays the **Syslog Export Filters** page:

Figure 451: *Syslog Export Filters Page*



The following table describes the **Syslog Export Filters** parameters:

Table 274: *Syslog Export Filters Page Parameters*

Parameter	Description
Add	Add a syslog export filter.
Import	Opens **Import from file** pop-up. You can import the syslog export filters from a file.
Export All	Opens **Export to file** pop-up. You can export all the syslog export filter entries to a file.
Enable/Disable	Enable or disable the syslog filter.
Export	Opens the **Export to file** pop-up. With this option, you can export individual syslog export filters.
Delete	Deletes a syslog export filter.

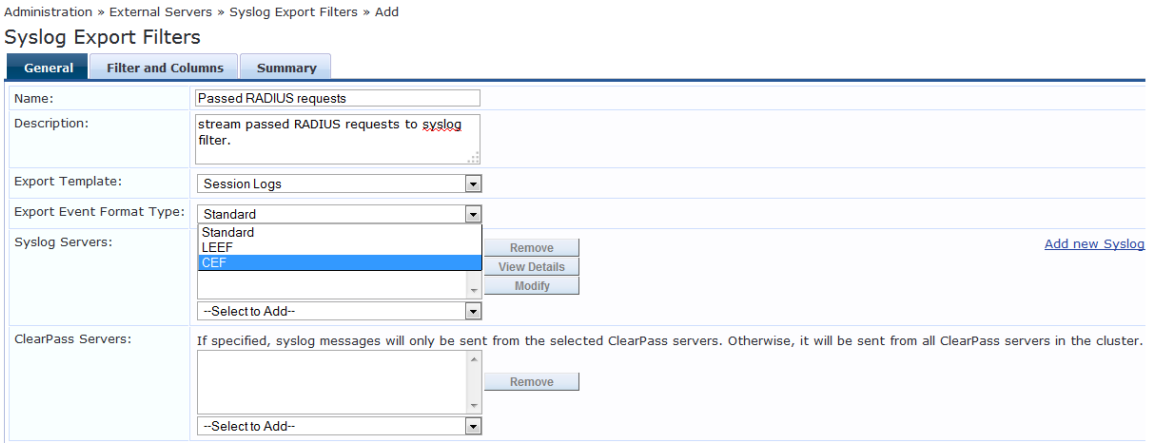
Adding a Syslog Export Filter

To add a syslog export filter, follow the instructions described below.

General Tab

This section describes the parameters in the **General** tab of the **Administration > External Servers > Syslog Export Filters > Add** page. The following figure displays the **Syslog Export Filters - General** tab:

Figure 452: *Syslog Export Filters - General Tab*



NOTE

The **Filter and Columns** tab shown in the figure above is only visible if you select **Insight Logs** or **Session Logs** as the export template in the **General** tab. For more information, see Filter and Columns Tab on page 481.

The following table describes the **Syslog Export Filters - General** tab parameters:

Table 275: *Syslog Export Filters - General Tab Parameters*

Parameter	Description
Name	Enter the name of the syslog export filter.
Description	Enter the description that provides additional information about the syslog export filter.
Export Template	Select any one of the templates from the following options: • **Audit Records** • **Insight Logs** • **Session Logs** • **System Events** **NOTE:** If you select **Insight Logs** or **Session Logs**, the **Filter and Columns** tab is enabled. For more information, see Filter and Columns Tab on page 481.

Table 275: *Syslog Export Filters - General Tab Parameters (Continued)*

Parameter	Description
Export Event Format Type	Select any one of the export event formats from the following options: • **Standard** – Select this event format type to send the event types in raw syslog format. This is the default event format type. • **LEEF** - Select this event format type to send the event types in Log Enhanced Event Format (LEEF). • **CEF** - Select this event format type to send the event types in Common Event Format (CEF). For sample event format types, see Export Event Format Types - Examples on page 478.
Syslog Servers	Syslog servers define the receivers of syslog messages sent by servers in the ClearPass cluster. • To add a syslog server, select it from the **--Select to Add--** drop-down list. • To view details about a syslog server, select the syslog server, then click **View Details**. • To change details about a syslog server, select the syslog server, then click **Modify**. For information about syslog server details, see Adding a Syslog Target on page 471 • To remove a syslog server (from receiving syslog messages), select the syslog server, then click **Remove**. If the syslog server does not appear in the drop-down list, you can click **Add new Syslog target**. For more information about syslog target, see Adding a Syslog Target on page 471 for more information.
ClearPass Servers	You can designate syslog messages to be sent from exactly one server in the ClearPass cluster or from all of them. • To add a ClearPass server, select it from the **Select to Add** drop-down list. • To remove the ClearPass server, select the ClearPass server, then click **Remove**. **NOTE:** When no servers are listed, syslog messages are sent from all servers in the cluster.

Export Event Format Types - Examples

This section shows few examples of Standard, LEEF, and CEF event format types for the syslog export filter templates.

The following example describes the Standard event format type for the **Audit Events** syslog export filter template:

```
Mar 20 21:18:56 10.17.5.228 2015-01-19 21:19:50,118 10.17.5.228 Audit Logs 96 1 0
TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,User=clusteradmin,Category=Endpoint,Action=ADD,EntityName=34a39527afc0,src=10.17.5.
228,Timestamp=Jan 19, 2015 21:18:54 IST
Mar 20 21:20:56 10.17.5.228 2015-01-19 21:21:50,111 10.17.5.228 Audit Logs 97 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,User=admin,Category=Cluster-wide
Parameter,Action=MODIFY,EntityName=Endpoint Context Servers polling
interval,src=10.17.5.228,Timestamp=Jan 19, 2015 21:20:22 IST
Mar 21 09:28:59 10.17.5.228 2015-01-20 09:29:54,3 10.17.5.228 Audit Logs 99 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,User=admin,Category=Network
Device,Action=REMOVE,EntityName=1.1.1.1,src=10.17.5.228,Timestamp=Jan 20, 2015 09:29:13 IST
```

The following example describes the Standard event format type for the **System Events** syslog export filter template:

```
Mar 21 16:46:29 10.17.5.228 2015-01-20 16:47:23,880 10.17.5.228 System Events 0 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,Description=User: arubasupport\nClient IP Address:
10.20.23.178,Category=Logged in,Action=None,Level=INFO,src=10.17.5.228,Component=Support
Shell,Timestamp=Jan 20, 2015 16:45:59 IST
Mar 21 16:49:10 10.17.5.228 2015-01-20 16:50:05,210 10.17.5.228 System Events 1 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,Description='Failed to start ClearPass Virtual IP
```

```
service',Category=start,Action=Failed,Level=WARN,src=10.17.5.228,Component=ClearPass Virtual
IP service,Timestamp=Jan 20, 2015 16:48:53 IST
2015-01-20 16:50:05,210 [pool-6-thread-1] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2015-
01-20 16:50:05,210 10.17.5.228 System Events 2 1 0 TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,Description=Performed action stop on cpass-domain-server_
CPATS,Category=stop,Action=Success,Level=INFO,src=10.17.5.228,Component=cpass-domain-server_
CPATS,Timestamp=Jan 20, 2015 16:48:57 IST
2015-01-20 16:50:05,211 [pool-6-thread-1] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2015-
01-20 16:50:05,211 10.17.5.228 System Events 3 1 0 TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,Description=Performed action start on cpass-domain-server_
CPATS,Category=start,Action=Success,Level=INFO,src=10.17.5.228,Component=cpass-domain-server_
CPATS,Timestamp=Jan 20, 2015 16:49:00 IST
```

The following example describes the Standard event format type for the **Session Events** syslog export filter template:

```
Mar 21 16:31:49 10.17.5.211 2015-01-20 16:32:41,552 10.17.5.211 Radius Session Logs 4 1 0
Common.NAS-IP-Address=10.17.4.7,RADIUS.Acct-Delay-Time=null,RADIUS.Acct-Framed-IP-
Address=null,RADIUS.Auth-Source=AD:win2008R2-64bit.bangalore.avendasys.com,RADIUS.Acct-
Timestamp=null,RADIUS.Acct-Authentic=null,RADIUS.Auth-Method=EAP-PEAP,EAP-
MSCHAPv2,Common.Host-MAC-Address=58a2b5d05ac9,RADIUS.Acct-Termination-Cause=null,RADIUS.Acct-
Service-Name=null,RADIUS.Acct-Session-Time=null,TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,RADIUS.Acct-NAS-Port=null,Common.Username=test1,RADIUS.Acct-Session-
Id=null,RADIUS.Acct-Called-Station-Id=null,RADIUS.Acct-NAS-Port-
Type=null,src=10.17.5.211,RADIUS.Acct-NAS-IP-Address=null,Common.Service=Test Post
Authentication Rules,RADIUS.Acct-Input-Pkts=null,RADIUS.Acct-Status-Type=null,RADIUS.Acct-
Calling-Station-Id=null,Common.Request-Timestamp=2015-01-20 16:31:46+05:30,RADIUS.Acct-Output-
Pkts=null,RADIUS.Acct-Output-Octets=null,RADIUS.Acct-Username=null,RADIUS.Acct-Input-
Octets=null
Mar 21 16:31:49 10.17.5.211 2015-01-20 16:32:41,550 10.17.5.211 Radius Session Logs 3 2 0
Common.NAS-IP-Address=10.17.4.7,RADIUS.Acct-Delay-Time=0,RADIUS.Acct-Framed-IP-
Address=10.17.4.148,RADIUS.Auth-Source=AD:win2008R2-64bit.bangalore.avendasys.com,RADIUS.Acct-
Timestamp=2015-01-20 16:31:50+05:30,RADIUS.Acct-Authentic=RADIUS,RADIUS.Auth-Method=EAP-
PEAP,EAP-MSCHAPv2,Common.Host-MAC-Address=e0f8471a5450,RADIUS.Acct-Termination-
Cause=null,RADIUS.Acct-Service-Name=null,RADIUS.Acct-Session-Time=null,TimestampFormat=yyyy-
MM-dd HH:mm:ss,S,RADIUS.Acct-NAS-Port=0,Common.Username=test1,RADIUS.Acct-Session-
Id=test1E0F8471A5450-54BE336C,RADIUS.Acct-Called-Station-Id=000B8661CD70,RADIUS.Acct-NAS-Port-
Type=Wireless-802.11,src=10.17.5.211,RADIUS.Acct-NAS-IP-Address=10.17.4.7,Common.Service=Test
Post Authentication Rules,RADIUS.Acct-Input-Pkts=null,RADIUS.Acct-Status-
Type=Start,RADIUS.Acct-Calling-Station-Id=E0F8471A5450,Common.Request-Timestamp=2015-01-20
16:31:45+05:30,RADIUS.Acct-Output-Pkts=null
Mar 21 16:35:58 10.17.5.228 2015-01-20 16:36:52,346 10.17.5.228 Tacacs authetnications 2 1 0
TACACS.Request-Type=TACACS_AUTHORIZATION,TACACS.Enforcement-Profiles=[TACACS Super
Admin],TACACS.Acct-Flags=null,TACACS.Authen-Service=AUTHEN_SVC_NONE,TACACS.Acct-Session-
Id=null,TACACS.Remote-Address=10.20.23.178,Common.Request-Timestamp=2015-01-20
16:34:54.647+05:30,TimestampFormat=yyyy-MM-dd HH:mm:ss,S,TACACS.Authen-Action=,TACACS.Authen-
Method=AUTHEN_METH_TACACSPLUS,Common.Username=a,TACACS.Authen-Type=AUTHEN_TYPE_
PAP,TACACS.Auth-Source=[Local User Repository],src=10.17.5.228,TACACS.Privilege-
Level=1,Common.Service=[Policy Manager Admin Network Login Service]
Mar 21 16:35:58 10.17.5.228 2015-01-20 16:36:52,346 10.17.5.228 Tacacs authetnications 3 1 0
TACACS.Request-Type=TACACS_AUTHENTICATION,TACACS.Enforcement-Profiles=[TACACS Super
Admin],TACACS.Acct-Flags=null,TACACS.Authen-Service=AUTHEN_SVC_NONE,TACACS.Acct-Session-
Id=null,TACACS.Remote-Address=10.20.23.178,Common.Request-Timestamp=2015-01-20
16:34:54.647+05:30,TimestampFormat=yyyy-MM-dd HH:mm:ss,S,TACACS.Authen-Action=AUTHEN_ACTION_
LOGIN,TACACS.Authen-Method=AUTHEN_METH_TACACSPLUS,Common.Username=a,TACACS.Authen-Type=AUTHEN_
TYPE_PAP,TACACS.Auth-Source=[Local User Repository],src=10.17.5.228,TACACS.Privilege-
Level=1,Common.Service=[Policy Manager Admin Network Login Service]
```

The following example describes the Standard event format type for the **Session Events** syslog export filter template:

```
Mar 21 16:59:12 10.17.5.211 2015-01-20 17:00:04,745 10.17.5.211 Insight Events 0 1 0
Auth.Username=keerthi,Auth.Request-Timestamp=2015-01-20 16:56:17+05:30,Auth.Source=Bangalore
AD,Auth.Auth-Username=keerthi,Auth.Protocol=RADIUS,Auth.Request-Id=R0000000b-01-
54be3b58,Auth.NAS-Port=null,Auth.SSID=cppm-dot1x-test,TimestampFormat=yyyy-MM-dd
HH:mm:ss,S,Auth.NAS-Port-Type=19,Auth.Roles=[User Authenticated],Auth.Service=Test Post
```

```
Authentication Rules,Auth.NAS-IP-
Address=10.17.4.7,src=10.17.5.211,Auth.CalledStationId=000B8661CD70,Auth.NAS-
Identifier=ClearPassLab3600
Mar 21 16:57:24 10.17.5.228 2015-01-20 16:58:18,909 10.17.5.228 Test Syslogs 0 1 0
TimestampFormat=yyyy-MM-dd HH:mm:ss,S,Endpoint.Status=null,Endpoint.Device-Name=Mac OS
X,Endpoint.Device-Family=Apple Mac,Endpoint.Device-Category=Computer,Endpoint.MAC-
Address=e0f8471a5450,src=10.17.5.228,Endpoint.Hostname=apples-air,Endpoint.Added-At=2015-01-19
17:06:51+05:30,Endpoint.MAC-Vendor=Apple,Endpoint.Fingerprint={"dhcp": {"option55":
["1,3,6,15,119,95,252,44,46"], "options": ["53,55,57,61,50,51,12"]}},Endpoint.Updated-At=2015-
01-20 16:55:37+05:30
```

The following example describes the LEEF event format type for the **Insight Logs** syslog export filter template:

```
Dec 03 2014 16:50:44.085 IST 10.17.4.208 LEEF:1.0|Dell|ClearPass|6.5.0.69058|0-1-
0|Auth.Username=host/Asif-Test-PC2 Auth.Authorization-Sources=null Auth.Login-Status=216
Auth.Request-Timestamp=2014-12-03 16:48:41+05:30 Auth.Protocol=RADIUS Auth.Source=null
Auth.Enforcement-Profiles=[Allow Access Profile] Auth.NAS-Port=null Auth.SSID=cppm-dot1x-test
TimestampFormat=MMM dd yyyy HH:mm:ss.SSS z Auth.NAS-Port-Type=19 Auth.Error-Code=216
Auth.Roles=null Auth.Service=Test Wireless Auth.Host-MAC-Address=6817294b0636
Auth.Unhealthy=null Auth.NAS-IP-Address=10.17.4.7 src=10.17.4.208
Auth.CalledStationId=000B8661CD70 Auth.NAS-Identifier=ClearPassLab3600
```

The following example describes the CEF event format type for the **Insight Logs** syslog export filter template:

```
Dec 03 2014 16:31:28.861 IST 10.17.4.208 CEF:0|Dell|ClearPass|6.5.0.69058|0-1-0|Insight
Logs|0|Auth.Username=host/Asif-Test-PC2 Auth.Authorization-Sources=null Auth.Login-Status=216
Auth.Request-Timestamp=2014-12-03 16:28:20+05:30 Auth.Protocol=RADIUS Auth.Source=null
Auth.Enforcement-Profiles=[Allow Access Profile] Auth.NAS-Port=null Auth.SSID=cppm-dot1x-test
TimestampFormat=MMM dd yyyy HH:mm:ss.SSS zzz Auth.NAS-Port-Type=19 Auth.Error-Code=216
Auth.Roles=null Auth.Service=Test Wireless Auth.Host-MAC-Address=6817294b0636
Auth.Unhealthy=null Auth.NAS-IP-Address=10.17.4.7 src=10.17.4.208
Auth.CalledStationId=000B8661CD70 Auth.NAS-Identifier=ClearPassLab3600
```

The following example describes the CEF event format type for the **Audit Logs** syslog export filter template:

```
Nov 19 2014 18:22:40.700 IST 10.17.4.221 CEF:0|Dell|ClearPass|6.5.0.68754|13-1-0|Audit
Records|5|cat=Role timeFormat=MMM dd yyyy HH:mm:ss.SSS zzz rt=Nov 19, 2014 18:21:13 IST
src=Test Role 10 act=ADD usrName=admin
```

The following example describes the LEEF event format type for the **Audit Logs** syslog export filter template:

```
Nov 19 2014 14:31:10.422 IST 10.17.4.221 LEEF:1.0|Dell|ClearPass|6.5.0.68754|0-1-0|cat=Syslog
Export Data devTime=Nov 19, 2014 14:30:35 IST action=ADD src=Audit Events - LEEF usrName=admin
devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z
```

The following example describes the CEF event format type for the **System Events** syslog export filter template:

```
Nov 19 2014 17:15:52.348 IST 10.17.4.221 CEF:0|Dell|ClearPass|6.5.0.68754|0-1-0|System
Events|10|cat=WebService Error level=ERROR description=No valid subscription ID\nCheck
Subscription ID, Network Connectivity, http_proxy credentials.\nClick on 'Check Status Now'
after correcting the configuration. timeFormat=MMM dd yyyy HH:mm:ss.SSS zzz rt=Nov 19, 2014
17:15:12 IST src=ClearPass Firmware Update Checker act=None
```

The following example describes the LEEF event format type for the **System Events** syslog export filter template:

```
Dec 02 2014 20:38:40.901 IST 10.17.4.206 LEEF:1.0|Dell|ClearPass|6.5.0.68878|295-1-0|cat=start
devTime=Dec 02, 2014 20:38:12 IST level=WARN description='Failed to start ClearPass Virtual IP
service' action=Failed src=ClearPass Virtual IP service devTimeFormat=MMM dd yyyy HH:mm:ss.SSS
z
```

The following example describes the CEF event format type for the **Session Logs** syslog export filter template:

```
Dec 01 2014 15:28:40.540 IST 10.17.4.206 CEF:0Dell|ClearPass|6.5.0.68878|1604-1-0|Session
Logs|0|RADIUS.Acct-Calling-Station-Id=00:32:b6:2c:28:95 RADIUS.Acct-Framed-IP-
Address=192.167.230.129 RADIUS.Auth-Source=AD:10.17.4.130 RADIUS.Acct-Timestamp=2014-12-01
15:26:43+05:30 RADIUS.Auth-Method=PAP RADIUS.Acct-Service-Name=Authenticate-Only RADIUS.Acct-
Session-Time=3155 TimestampFormat=MMM dd yyyy HH:mm:ss.SSS zzz RADIUS.Acct-NAS-Port=0
RADIUS.Acct-Session-Id=R00001316-01-547c3b5a RADIUS.Acct-NAS-Port-Type=Wireless-802.11
RADIUS.Acct-Output-Octets=578470212 RADIUS.Acct-Username=A_user2 RADIUS.Acct-NAS-IP-
Address=10.17.6.124 RADIUS.Acct-Input-Octets=786315664
```

The following example describes the LEEF event format type for the **Session Logs** syslog export filter template:

```
Dec 02 2014 15:35:14.944 IST 10.17.4.206 LEEF:1.0Dell|ClearPass|6.5.0.68878|1309854-1-
0|RADIUS.Acct-Calling-Station-Id=00:88:57:2d:12:a4 RADIUS.Acct-Framed-IP-
Address=192.167.203.170 RADIUS.Auth-Source=AD:10.17.4.130 RADIUS.Acct-Timestamp=2014-12-02
15:32:47+05:30 RADIUS.Auth-Method=PAP RADIUS.Acct-Service-Name=Authenticate-Only RADIUS.Acct-
Session-Time=565 TimestampFormat=MMM dd yyyy HH:mm:ss.SSS z RADIUS.Acct-NAS-Port=0
RADIUS.Acct-Session-Id=R000a5038-01-547d8e47 RADIUS.Acct-NAS-Port-Type=Wireless-802.11
RADIUS.Acct-Output-Octets=412895267 RADIUS.Acct-Username=A_user706 RADIUS.Acct-NAS-IP-
Address=10.17.6.124 RADIUS.Acct-Input-Octets=665942581
```

Filter and Columns Tab

This section describes the parameters in the **Filter and Columns** tab of the **Administration > External Servers > Syslog Export Filters > Add** page. This tab provides two methods for configuring data filters and is only visible if you select **Insight Logs** or **Session Logs** as the export template in the **General** tab.

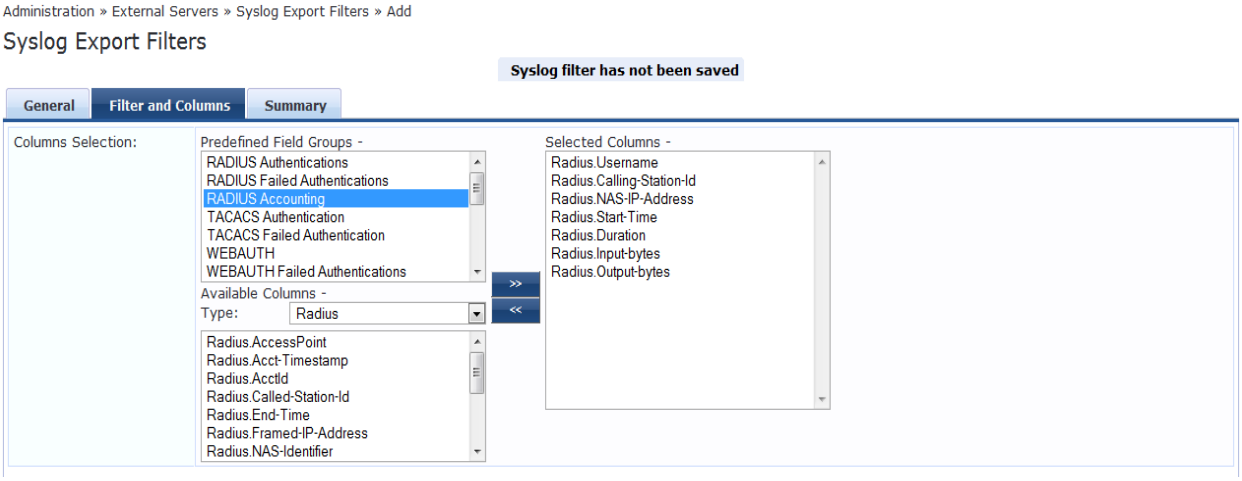
Insight Logs

This section describes the options if you select **Insight Logs** as the export template in the **General** tab.

The **Insight Logs** option is enabled only if the **Enable Insight** check box is selected from the **Administration** > **Server Manager** > **Server Configuration** > **System** tab.

The following figure displays the **Syslog Export Filters - Filter and Columns (Insight Logs)** tab.

Figure 453: *Syslog Export Filters - Filter and Columns (Insight Logs) Tab*



The data collection interval for Insight logs is -4 to -2 minutes from the current time.

The following table describes the **Syslog Export Filters - Filter and Columns (Insight Logs)** tab parameters:

Table 276: *Syslog Export Filters - Filter and Columns (Insight Logs) Tab Parameters*

Parameter	Description
Columns Selection	Determine the group of reports that you want to include in the syslog filters. The column selection limits the type of records sent to the syslog filters. **NOTE:** You can add only the Insight reports that are already created in Insight. You cannot create a new data filter for Insight logs.
Predefined Field Groups	Select the predefined Insight reports that are grouped for a quick addition.
Available Columns	Displays the reports specific to the group selected in the **Columns Selection** field.
Type	Select the type of records from the drop-down list to filter the records. This provides additional filtering option based on the type of records.
Selected Columns	After you select an entry from the **Available Columns** list, click **>>** to add the selected entry to the **Selected Columns** list. Click **<<** to remove an entry from the **Selected Columns** list.

Session Logs

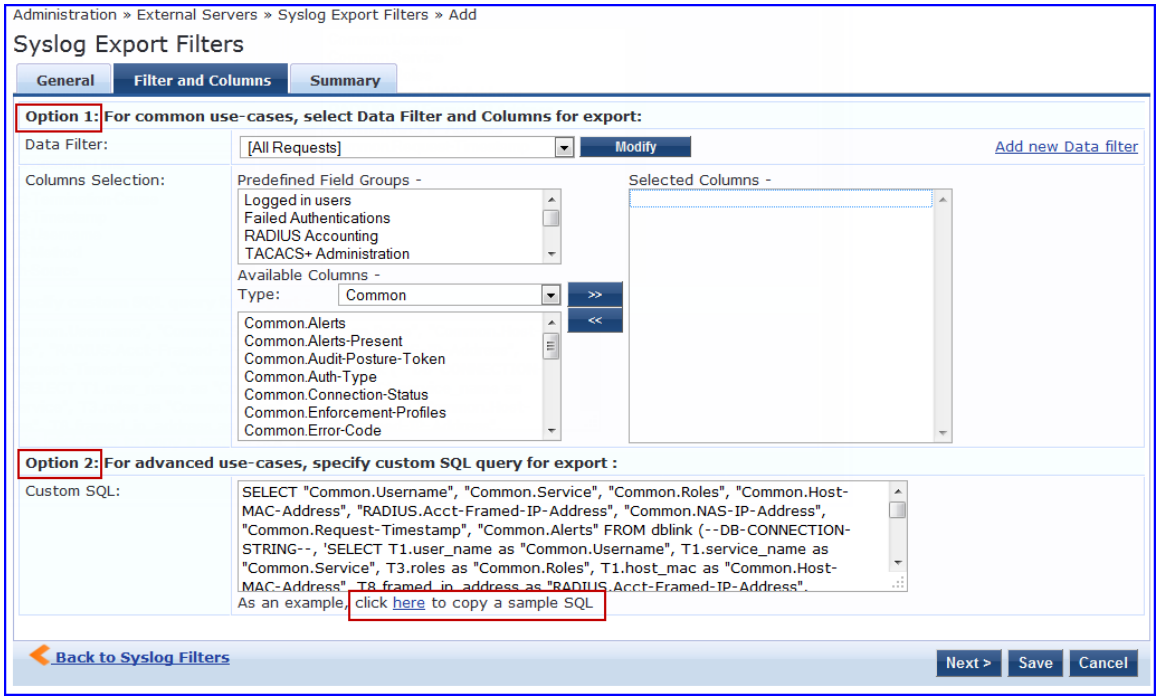
This section describes the options if you select **Session Logs** as the export template in the **General** tab. On selecting **Session Logs**, the following options are available:

- **Option 1** allows you to choose from pre-defined field groups and to select columns based on the Type.
- **Option 2** allows you to create a custom SQL query. You can view a sample template for the custom SQL by clicking the link below the text entry field.

It is recommended to contact support if you choose the option 2. Support can assist you with entering the correct information in this template.

The following figure displays the **Syslog Export Filters - Filter and Columns (Session Logs)** tab.

Figure 454: *Syslog Export Filters - Filter and Columns (Session Logs) Tab*



The following table describes the **Syslog Export Filters - Filter and Columns (Session Logs)** tab parameters:

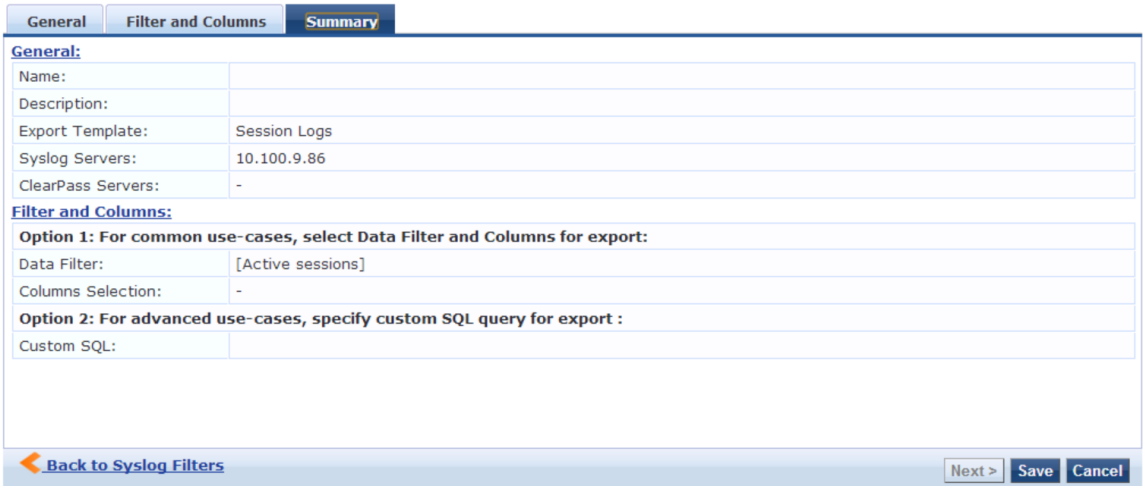
Table 277: *Syslog Export Filters - Filter and Columns (Insight Logs) Tab Parameters*

Parameter	Description
Data Filter	Specify the data filter. The data filter limits the type of records sent to the syslog target.
Modify/ Add new Data filter	Modify the selected data filter, or add a new one. Specifying a data filter filters the rows that are sent to the syslog target. You may also select the columns that are sent to the syslog target. For more information on adding a data filer, see Adding a Filter on page 80.
Columns Selection	The column selection limits the type of columns sent to the syslog target. There are predefined field groups, which are column names grouped together for quick addition to the report. For example, *Logged in users* field group has seven predefined columns. When you click *Logged in users* the seven columns automatically appear in the **Selected Columns** list. Additional fields are available to add to the reports. You can select the type of attributes (which are the different table columns available in the session database) from the **Available Columns Type** drop down list. Policy Manager populates these column names by extracting the column names from existing sessions in the session database. After you select an entry from the **Available Columns** list, click **>>** to add the selected entry to the **Selected Columns** list. Click **<<** to remove an entry from the **Selected Columns** list.
Custom SQL	Specify custom SQL query for export. This option is for advanced use cases. **NOTE:** It is recommended to contact support if you choose this option. Support can assist you with entering the correct information in this template.

Summary Tab

This section describes the parameters in the **Summary** tab of the **Administration > External Servers > Syslog Export Filters > Add** page. The following figure displays the **Syslog Export Filters - Summary** tab.

Figure 455: *Syslog Export Filters - Summary Tab*



The following table describes the **Syslog Export Filters - Summary** tab parameters:

Table 278: *Syslog Export Filters - Summary Tab Parameters*

Parameter	Description
General	
Name	Displays the name of the syslog export filter.
Description	Displays the description that provides additional information about the syslog export filter.
Export Template	Displays the template selected as the export template.
Syslog Servers	Displays the IP address of the syslog server selected during configuration.
ClearPass Servers	Displays the IP address of the ClearPass servers selected during configuration.
Filter and Columns	
Data Filter	Displays the data filter selected when configuring option 1 in the **Filter and Columns** tab.
Columns Selection	Displays the predefined field groups and available columns type selected when configuring option 1 in the **Filter and Columns** tab.
Custom SQL	Displays the SQL query selected when configuring option 2 in the **Filter and Columns** tab.

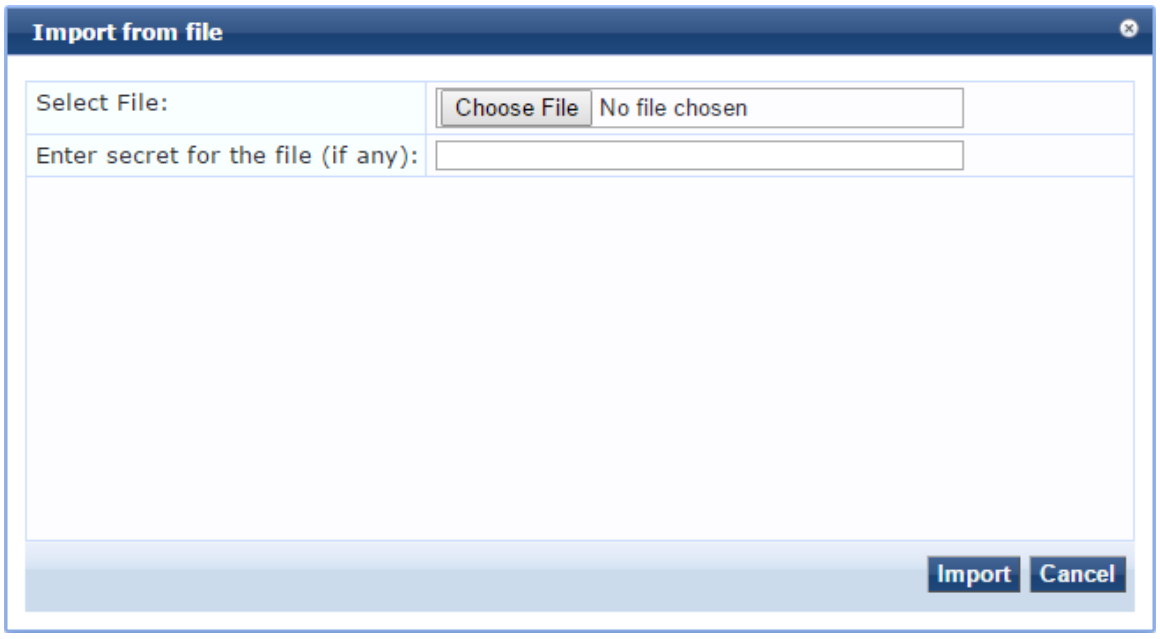
Importing a Syslog Filter

To import a syslog target:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Click the **Import** link on the top right section of the page. Enter the details based on Table 279.
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 456: *Import from file Pop-up*



The following table describes the **Import from file** parameters:

Table 279: *Import from file Parameters*

Parameter	Description
Select File	Browse to the Syslog Filter configuration file to be imported.
Enter secret for the file (if any)	If the file was exported with a secret key for encryption, enter the same key here.

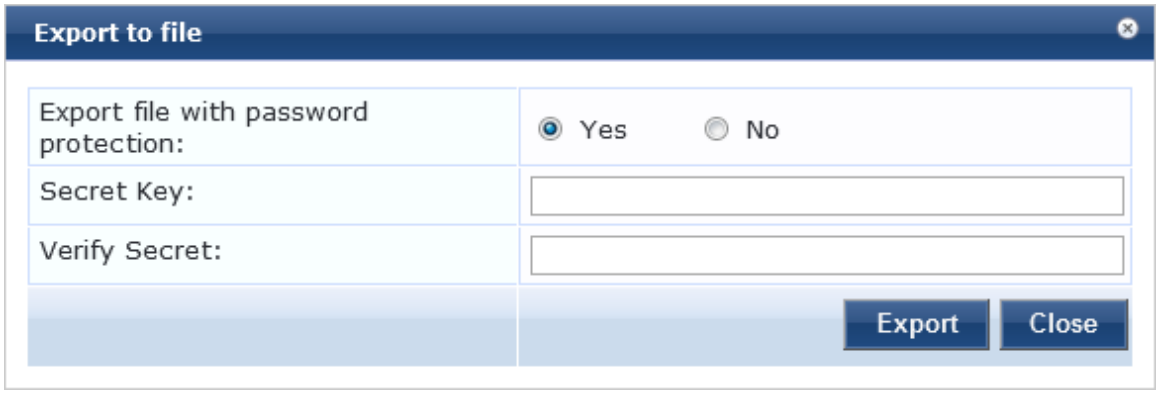
Exporting All Syslog Filter

To export all syslog filters:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Click the **Export All** link on the top right section of the page. Enter the details based on Table 280.
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 457: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 280: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose **Yes** to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

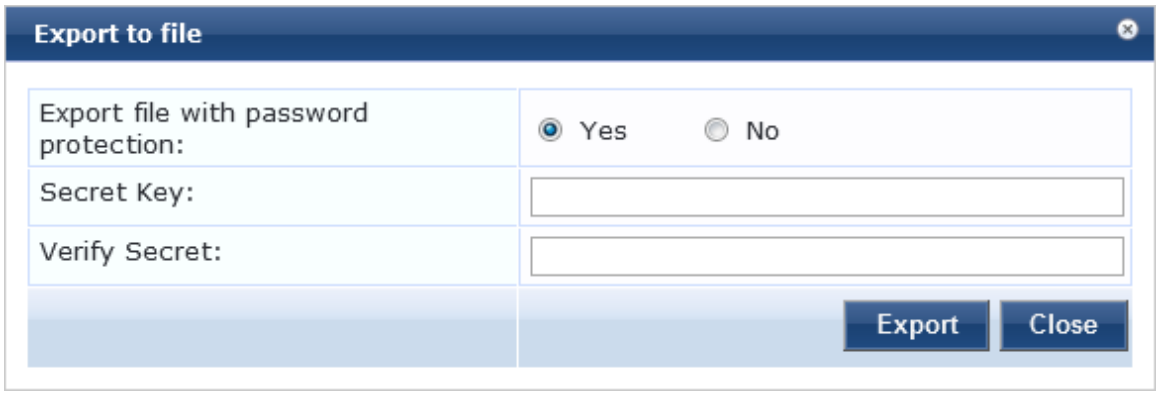
Exporting a Syslog Filter

To export a syslog filter:

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Select the **Host Address** from the list of check boxes and click **Export**. Enter the details based on Table 281.
3. Enter the name of the XML file in the **Save As** dialog.
4. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 458: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 281: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose **Yes** to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Deleting a Syslog Filter

To delete a syslog filter:

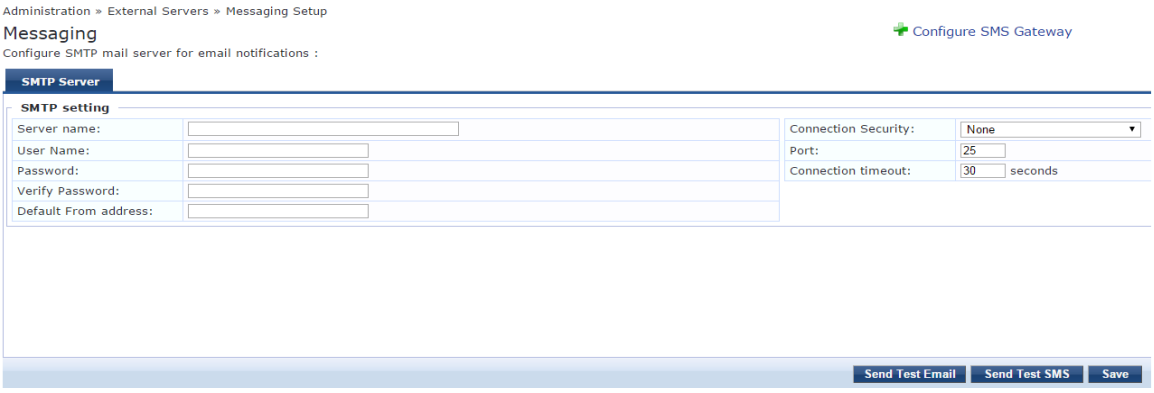
1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Click the check box next to the syslog filter entry and click **Delete**.
3. Click **Yes**.

Messaging Setup

The messaging setup provides an interface to configure the Simple Mail Transfer Protocol (SMTP) server for email and SMS notifications. To configure messaging, navigate to **Administration > External Servers > Messaging Setup**. Click the **Configure SMS Gateway** link at the top right section of the page to configure a new SMS gateway using the ClearPass Guest portal.

The following figure displays the **Messaging - SMTP Server** tab:

Figure 459: *Messaging - SMTP Server Tab*



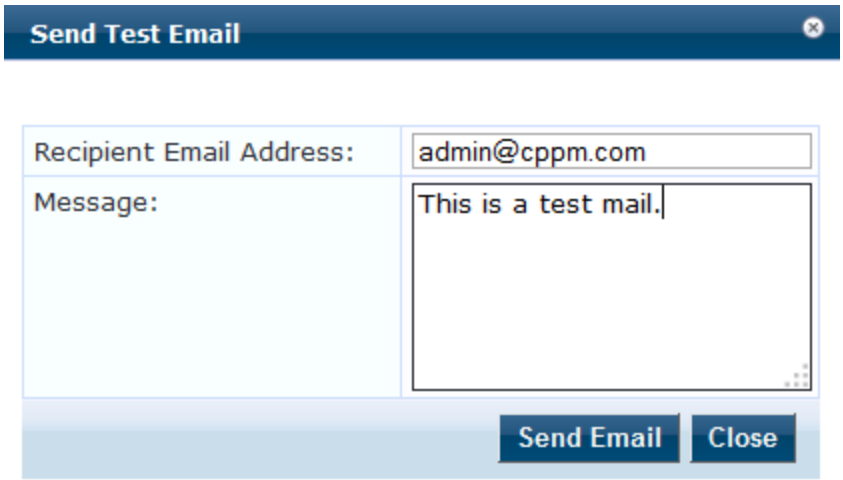
The following table describes the **Messaging - SMTP Server** tab parameters:

Table 282: *Messaging - SMTP Server Tab Parameters*

Parameter	Description
Server name	Enter the Fully Qualified Domain Name (FQDN) or the IP address of the SMTP server.
User Name	Enter the username if your email server requires authentication for sending email messages.
Password	Enter the password for the specified username.
Verify Password	Re-enter the password.
Default From address	Enter the email address that must to be displayed as sender's address in the message.
Connection Security	To establish the communication with the server, select from one of the following options: • **None** - Select this option to disable secure communication with the server. • **SSL** - Select this option to have a Secured Socket Layer communication with the server. • **Start TLS** - Select this option to have a Transport Layer Security communication with the server.
Port	Enter the TCP port number that the SNMP server listens on. The default value of the port is 25.
Connection timeout	Enter the timeout value for connection to the server (in seconds). The default value is 30 seconds.

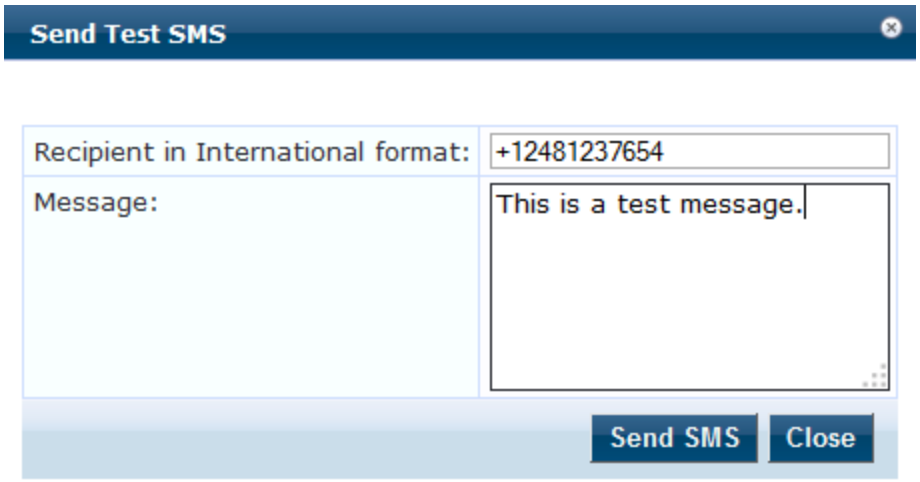
Click **Send Test Email** to send a test mail to the preferred email address. The following figure displays the **Send Test Email** pop-up:

Figure 460: *Send Test Email Pop-up*



Click **Send Test SMS** to send a test SMS message to the preferred mobile phone number. The following figure displays the **Send Test SMS** pop-up:

Figure 461: *Send Test SMS Pop-up*



The recipient's mobile number must be entered in the international format consisting of a + sign, followed by the country code and the mobile phone number (without the first '0' of the number). Number must be entered without spaces and only numbers (with an exception of the + sign) are allowed. For example, the US number (248) 123-7654 is entered as +12481237654. The number 1 is the country code for the US.

Endpoint Context Servers

Policy Manager provides the ability to collect endpoint profile information from different types of Dell W-Series IAPs and RAPs via Aruba Activate. Policy Manager supports AirWatch, Aruba Activate, AirWave, Google Admin Console, Generic HTTP, JAMF, Maas360, MobileIron, Palo Alto Networks Firewall and Panorama, SAP Afaria, SOTI, and XenMobile.

The mobile device management platforms run on MDM servers. These servers provision mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

To configure endpoint context servers, navigate to **Administration > External Servers > Endpoint Context Servers**.

This section describes the following topics:

Endpoint Context Servers Main Page

The following figure displays the **Endpoint Context Servers** page:

Figure 462: *Endpoint Context Servers Page*

The following table describes the **Endpoint Context Servers** parameters:

Table 283: *Endpoint Context Servers Parameters*

Parameter	Description
Server Name	Displays the name of the endpoint context server.
Server Type	Displays the type of the endpoint context server. For example, Generic HTTP, airwatch, or SAP Afaria.
Status	Displays the status of the endpoint context server: Enabled or Disabled. For non MDM servers, the status is always displayed as 'Disabled'.
Trigger Poll	Click this button to poll an endpoint context server.

Adding an Endpoint Context Server

To add an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Click the **Add** link on the top right section of the page.
3. In the **Add Endpoint Context Server** pop-up, enter the details based on Table 284.
4. Click **Save**.

The following table describes the **Add Endpoint Context Servers** parameters:

Table 284: *Add Endpoint Context Servers Parameters*

Parameter	Description
Select Server Type	Choose one of the server types from the following options. The server type you select determines the configuration parameters. For example, if you select the **airwatch** server type, you must enter an **API Key** parameter. Click each server type link below for more information on configuration parameters. • AirWatch • Aruba Activate • AirWave • Google Admin Console • Generic HTTP • JAMF • MaaS360 • MobileIron • Palo Alto Networks Firewall • Palo Alto Networks Panorama • SAP Afaria • SOTI • XenMobile **NOTE:** You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

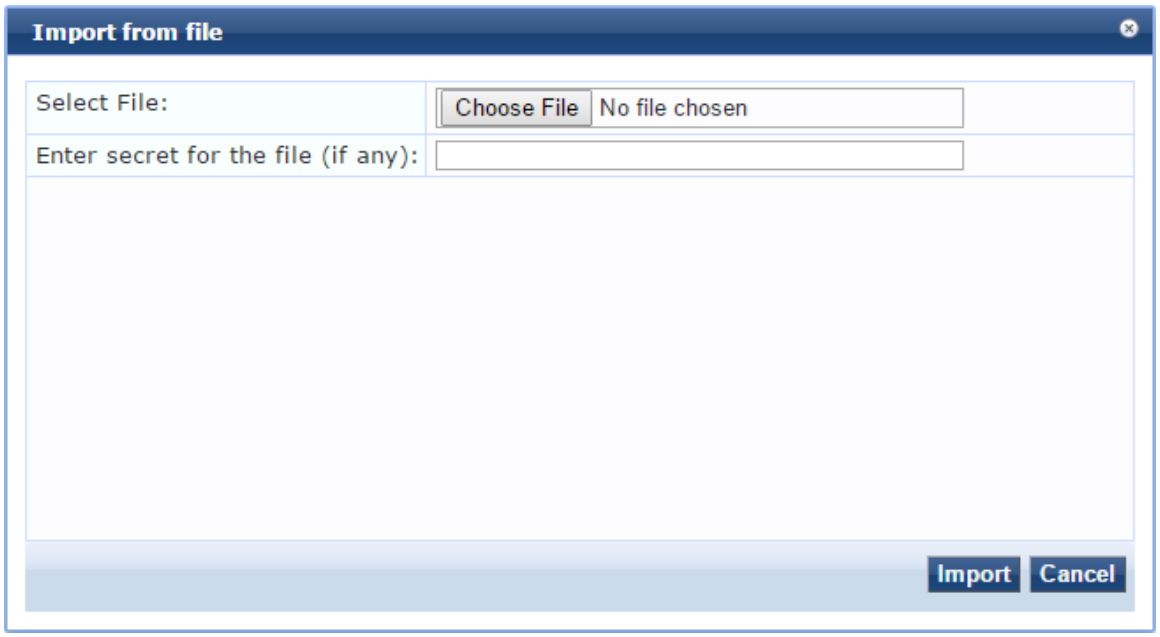
Importing an Endpoint Context Server

To import an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Click the **Import** link on the top right section of the page. Enter the details based on Table 285.
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 463: *Import from file Pop-up*



The following table describes the **Import from file** parameters:

Table 285: *Import from file Parameters*

Parameter	Description
Select File	Browse to the Endpoint Context 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.

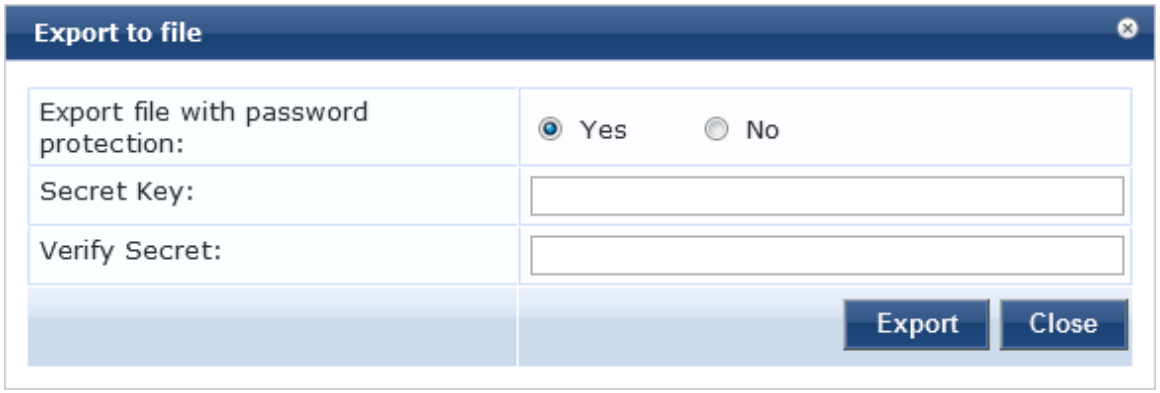
Exporting All Endpoint Context Servers

To export all endpoint context servers:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Click the **Export All** link on the top right section of the page. Enter the details based on Table 286.
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

The following figure displays the **Export to file** pop-up:

Figure 464: *Export to file Pop-up*



The following table describes the **Export to file** parameters:

Table 286: *Export to file Parameters*

Parameter	Description
Export file with password protection	Choose **Yes** to export the file with password protection.
Secret Key	Enter the secret key.
Verify Secret	Re-enter the secret key.

Modifying an Endpoint Context Server

To modify an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. In the **Endpoint Context Servers** main page, click the desired server name entry.
3. In the **Modify Endpoint Context Server** pop-up, enter the details based on Table 284.
4. Click **Update**.

The **Modify Endpoint Context Server** pop-up contains the following tabs:

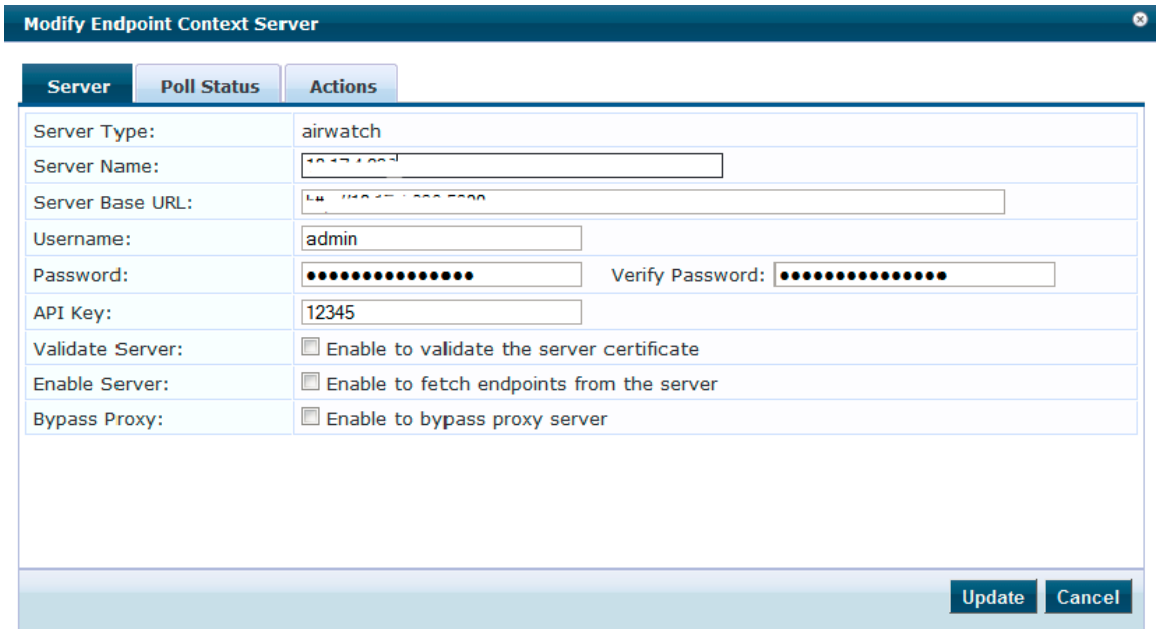
- Endpoint Context Servers
- Poll Status Tab
- Actions Tab
- Certificates Tab

The tabs appear when you add or modify an endpoint context server will vary depends on the endpoint context server selected.

Server Tab

Use the **Server** tab to modify the server name, Server base URL, and API key. You can also use this tab to validate the server certificate and to bypass proxy servers. The following figure displays the **Modify Endpoint Context Server** pop-up:

Figure 465: *Modify Endpoint Context - Server Pop-up*



The following table describes the **Modify Endpoint Context - Server** parameters:

Table 287: *Modify Endpoint Context - Server Parameters*

Parameter	Description
Server Type	Select the type of the endpoint context server. For example, airwatch, MobileIron, or SAP Afaria.
Server Name	Enter the name of the server or host.
Server Base URL	Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter the password.
API Key	Enter the API key that was provided by the vendor. This field is not displayed for all endpoint context servers.

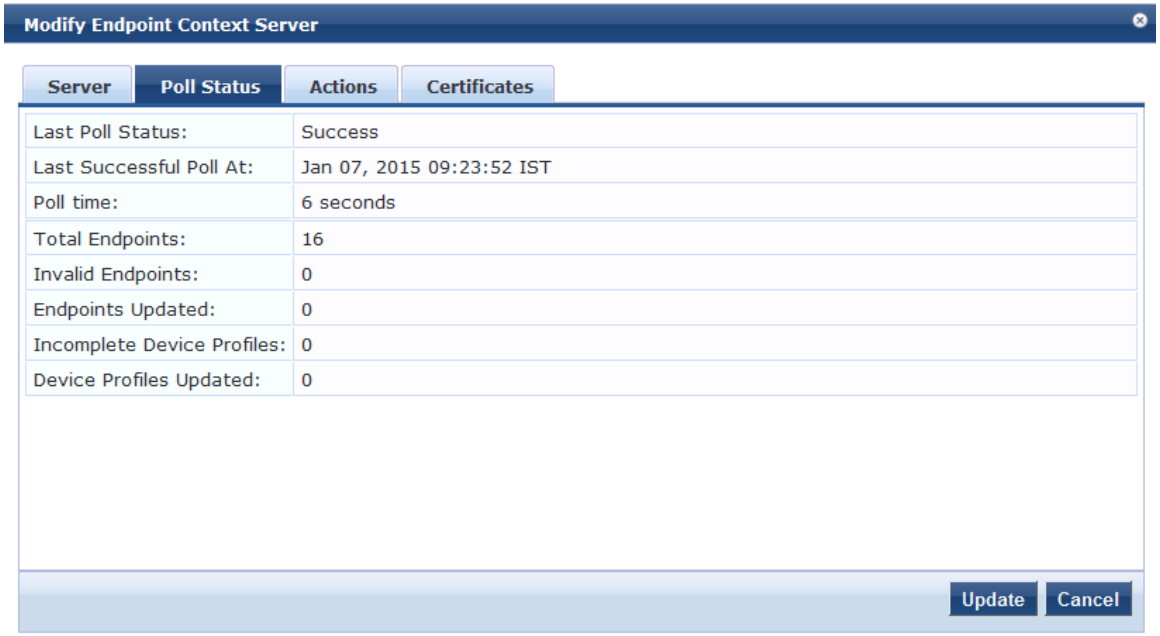
Table 287: *Modify Endpoint Context - Server Parameters (Continued)*

Parameter	Description
Validate Server	Select the **Enable to validate the server certificate** check box to validate. By default, this field is disabled. Checking this option enables the **Certificate** tab.
Enable Server	Select the **Enable to fetch endpoints from the server** check box to enable the endpoint context server. By default, this field is disabled. The **Bypass Proxy** field will be enabled only if you enable this field.
Bypass Proxy	Select the **Enable to bypass proxy server** check box to bypass the proxy server. An administrator can select this option to specify that the endpoint context server should not use the configured proxy settings (if a proxy is used). ClearPass then bypass the proxy for functions such MDM API, Endpoint Context Server Actions, or Generic HTTP outbound enforcement. When this field is enabled, the proxy servers configured in the **Administration** > **Server Manager** > **Server Configuration** > **Service Parameters** tab > **ClearPass system services** service page will be bypassed. The server discovery occurs without any issues even when the proxy servers are bypassed. By default, this field is disabled. You must enable the **Enable Server** field to enable this field.

Poll Status Tab

Use the **Poll Status** tab to view the status of the polling: Success or Failure. The parameters appear in the **Poll Status** tab will vary depends on the success or failure. A minimum of one successful polling should have occurred to view the 'Success' polling status from the **Poll Status** tab. The following figure displays the successful poll status in the **Poll Status** tab:

Figure 466: *Modify Endpoint Context - Poll Status Tab with Success Status*



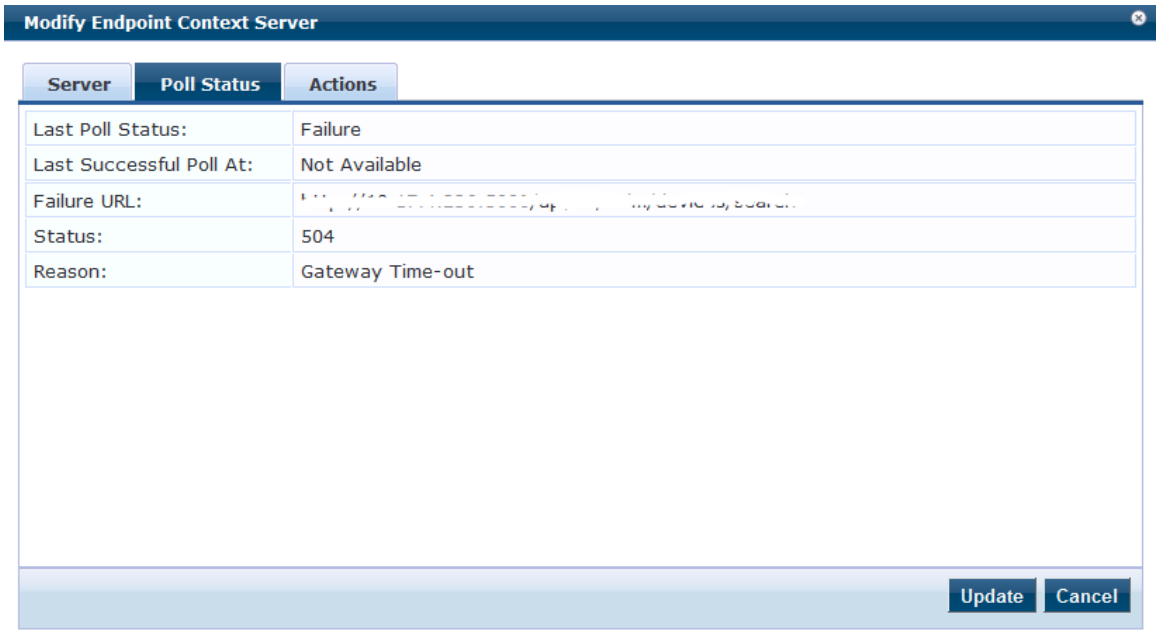
The following table describes the **Modify Endpoint Context - Poll Status** parameters with the 'Success' polling status:

Table 288: *Modify Endpoint Context - Poll Status Parameters with Success Status*

Parameter	Description
Last Poll Status	Displays the last polling status: Success or Failure. In this case, Success.
Last Successful Poll At	Displays the date and time at which the polling was triggered.
Poll time	Specifies the time duration in seconds to complete the polling.
Total Endpoints	Specifies the total number of endpoints triggered for polling.
Invalid Endpoints	Specifies the number of invalid endpoints triggered for polling.
Endpoints Updated	Specifies the number of endpoints updated after polling.
Incomplete Device Profiles	Displays the incomplete device profiles after polling.
Device Profiles Updated	Specifies the number of device profiles updated after polling.

The following figure displays a failed poll status in the **Poll Status** tab:

Figure 467: *Modify Endpoint Context - Poll Status Tab with Failure Status*



The following table describes the **Modify Endpoint Context - Poll Status** parameters with the 'Failure' polling status:

Table 289: *Modify Endpoint Context - Poll Status Parameters*

Parameter	Description
Last Poll Status	Displays the last polling status: Success or Failure. In this case, Failure.
Last Successful Poll At	Displays the date and time at which the polling was triggered.
Failure URL	Specifies the URL in which the failure occurred.
Status	Displays the error code for the failure.
Reason	Displays the reason for the failure. For example,Gateway Time-out.

Actions Tab

Use the Actions tab to view the server action that is performed on endpoints and description. The following figure displays the **Modify Endpoint Context - Actions** tab:

Figure 468: *Modify Endpoint Context - Actions Tab*

The following table describes the **Modify Endpoint Context - Actions** parameters:

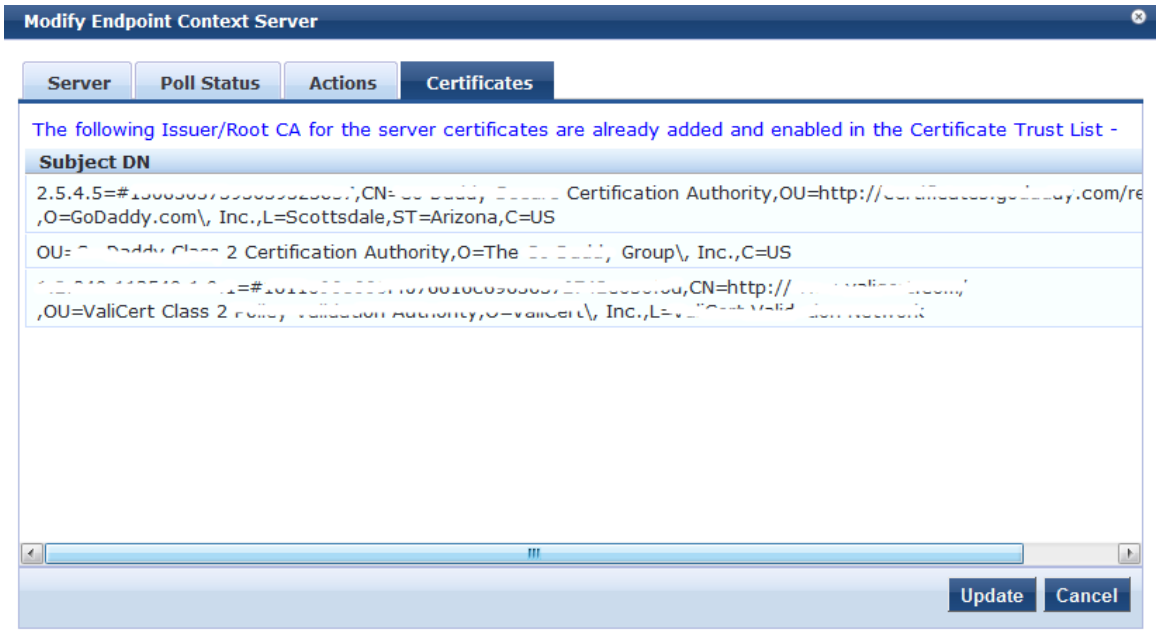
Table 290: *Modify Endpoint Context - Actions Parameters*

Parameter	Description
Clear Passcode	Reset passcode on the device.
Enterprise Wipe	Deletes only stored corporate information.
Get Apps	Gets Apps related information for the device.
Lock Device	Locks the associated device.
Remote Wipe	Deletes all stored information.
Send Message	Sends message to the device.
Send Message (Parameterized)	Sends message with the configured parameters to the device.

Certificates Tab

The **Certificates** tab displays the server certificates added and enabled in the **Certificate Trust List** page. The following figure displays the **Modify Endpoint Context - Certificates** tab:

Figure 469: *Modify Endpoint Context - Certificates Tab*



Polling an Endpoint Context Server

To poll an endpoint context server:

NOTE

You can poll only one server at a time. You cannot poll multiple server name entries.

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. In the **Endpoint Context Servers** main page, click the check box next to the server name entry.
3. Click **Trigger Poll**.

Deleting an Endpoint Context Server

Deleting an endpoint context server removes the configuration information from the Policy Manager server. To add it again, export the servers before you delete it and save the configuration so that you can import it in future.

To delete an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Click the check box next to the server name entry and click **Delete**.
3. Click **Yes**.

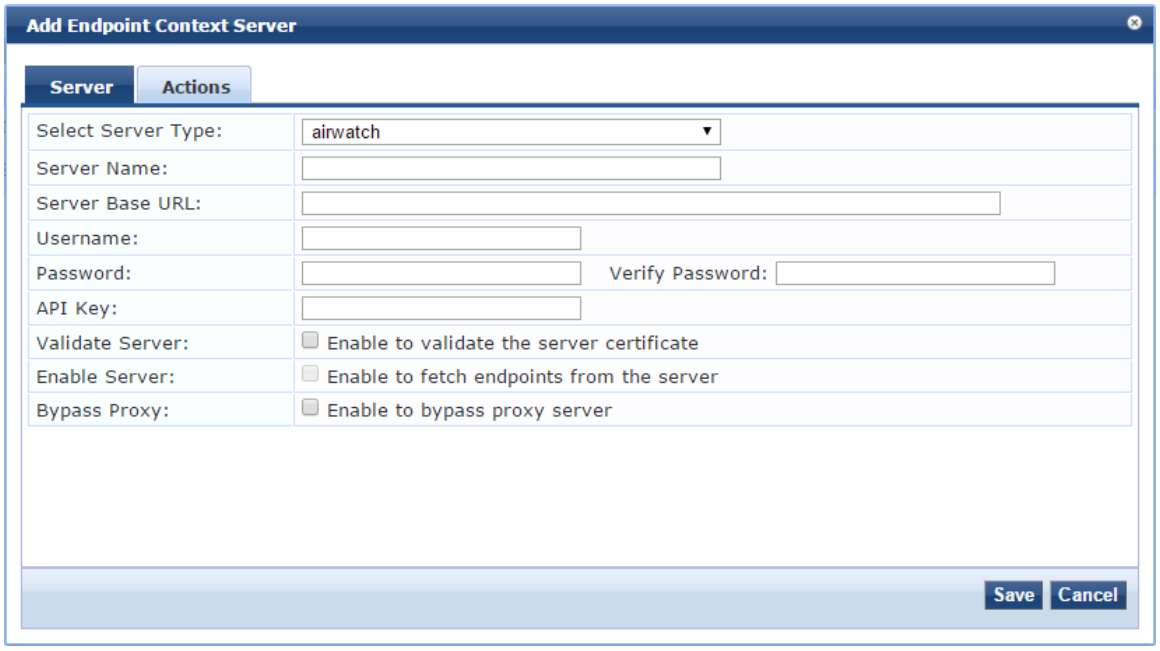
Adding an AirWatch Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (AirWatch) tab:

Figure 470: *Add Endpoint Context Server - Server (AirWatch) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table displays the **Add Endpoint Context Server - Server** (AirWatch) tab parameters:

Table 291: *Add Endpoint Context Server - Server (AirWatch) Tab Parameters*

Parameter	Description
Select Server Type	Choose AirWatch from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
API Key	Enter the API key that is provided by the vendor.
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Select the **Enable to fetch endpoints from the server** check box to enable the endpoint context server. By default, this field is disabled. The **Bypass Proxy** field will be enabled only if you enable this field.
Bypass Proxy	Select the **Enable to bypass proxy server** check box to bypass the proxy server. When this field is enabled, the proxy servers configured in the **Administration** > **Server Manager** > **Server Configuration** > **Service Parameters** tab > **ClearPass system services** service page will be bypassed. The server discovery occurs without any issues even when the proxy servers are bypassed. By default, this field is disabled. You must enable the **Enable Server** field to enable this field.

Actions Tab

The following figure displays the **Add Endpoint Context Server - Actions** (AirWatch) tab:

Figure 471: *Add Endpoint Context Server - Actions (AirWatch) Tab*

The following table describes the **Add Endpoint Context Server - Actions** (AirWatch) tab parameters:

Table 292: *Add Endpoint Context Server - Actions (AirWatch) Tab Parameters*

Parameter	Description
Clear Passcode	Reset passcode on the device.
Enterprise Wipe	Delete only stored corporate information.
Get Apps	Get application information for the device.
Lock Device	Lock the associated device.
Remote Wipe	Delete all stored information.
Send Message	Send message to the device.
Send Message (Parameterized)	Send message with parameters to the device.

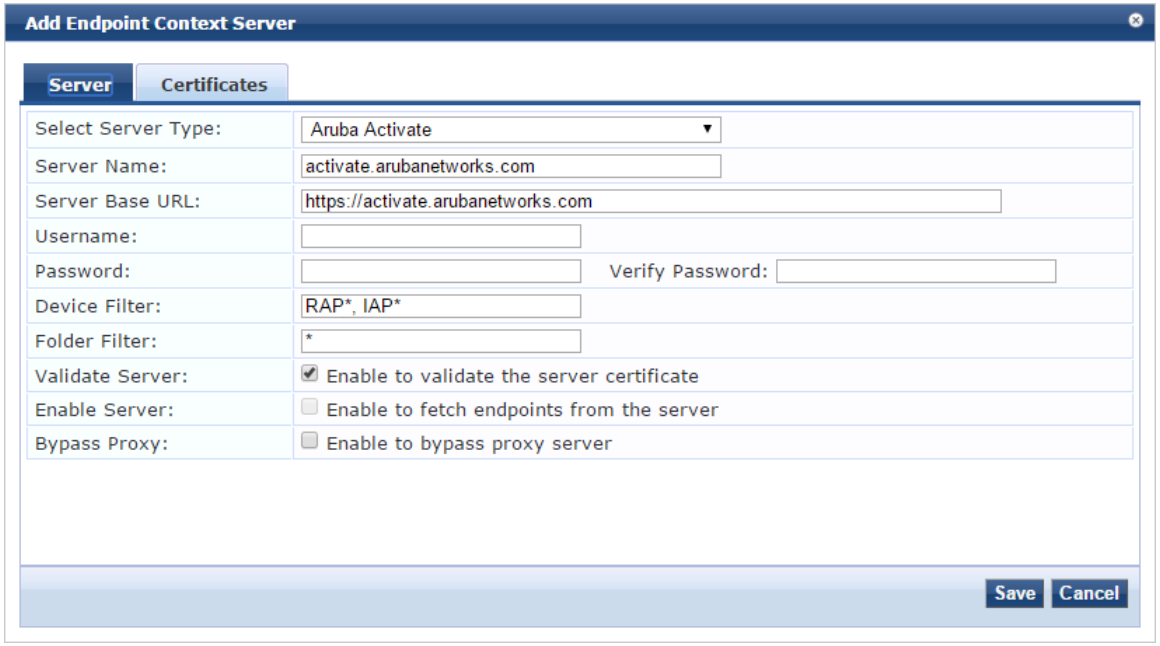
Adding an Aruba Activate Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (Aruba Activate) tab:

Figure 472: *Add Endpoint Context Server - Server (Aruba Activate) Tab*



The following table describes the **Add Endpoint Context Server - Server** (Aruba Activate) tab parameters:

Table 293: *Add Endpoint Context Server - Server (Aruba Activate) Tab Parameter*

Parameter	Description
Select Server Type	Choose Aruba Activate from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Device Filter	This field is populated with a default regex to retrieve only the information of RAP and IAP information.
Folder Filter	This field is set to "*" by default.
Validate	Enable to validate the server certificate. Checking this option enables the **Certificate** tab. For

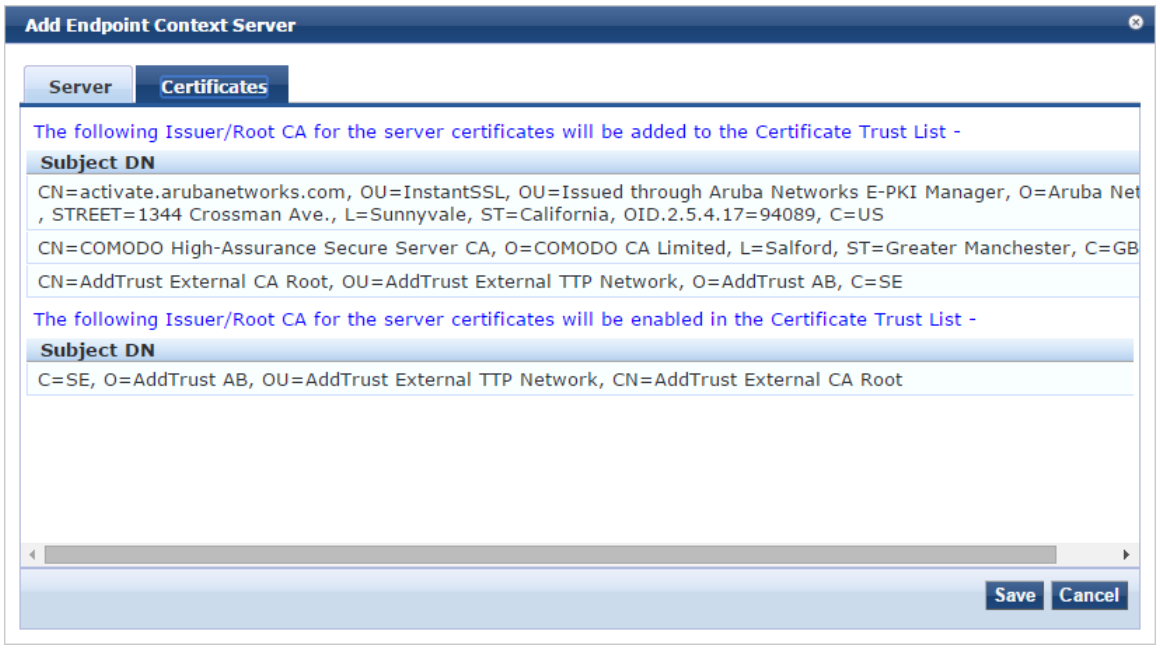
Table 293: *Add Endpoint Context Server - Server (Aruba Activate) Tab Parameter (Continued)*

Parameter	Description
Server	more information on certificate, see Certificates Tab on page 503.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Certificates Tab

The following figure displays the **Add Endpoint Context Server - Certificates** (Aruba Activate) tab:

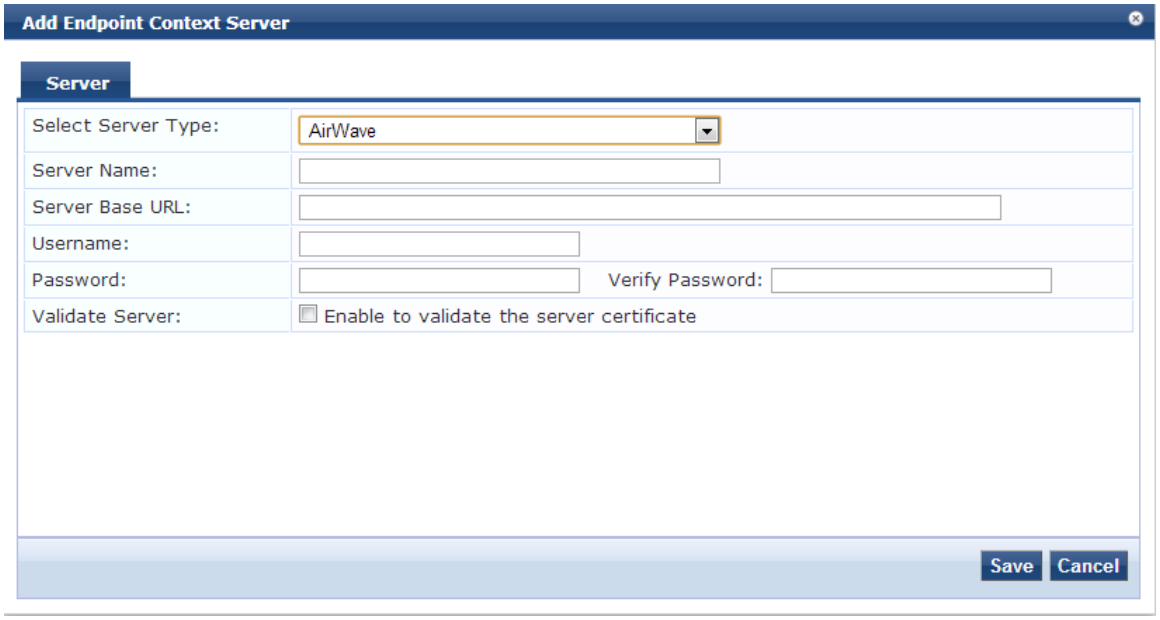
Figure 473: *Add Endpoint Context Server - Certificates (Aruba Activate) Tab*



Adding an AirWave Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (AirWave) tab:

Figure 474: *Add Endpoint Context Server - Server (AirWave) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (AirWave) tab parameters:

Table 294: *Add Endpoint Context Server - Server (AirWave) Tab Parameters*

Parameter	Description
Select Server Type	Choose AirWave from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Bypass Proxy	Enable to bypass proxy server.

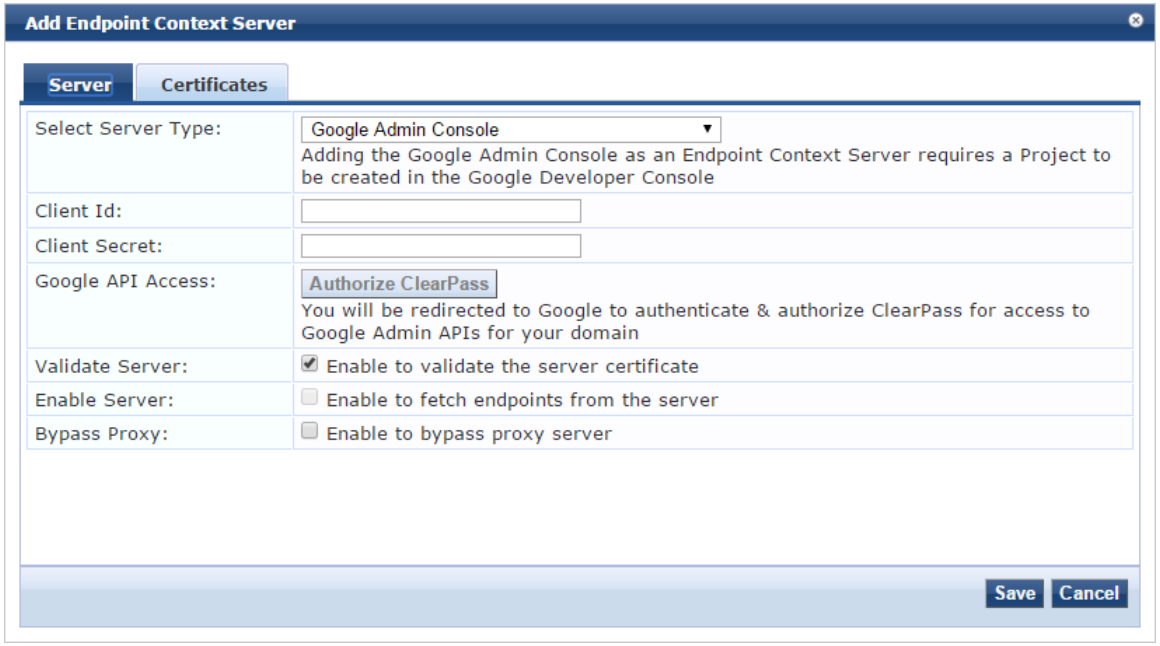
Adding a Google Admin Console Endpoint Context Server

Consult Google Developer documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (Google Admin Console) tab:

Figure 475: *Add Endpoint Context Server - Server (Google Admin Console) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (Google Admin Console) tab parameters:

Table 295: *Add Endpoint Context Server - Server (Google Admin Console) Tab Parameters*

Parameter	Description
Select Server Type	Choose Google Admin Console from the drop-down list.
Client Id	Enter the client ID. For example, **9169879216kpl50kxuaq6q6qqwe0i.apps.googleusercontent.com.**
Client Secret	Enter the client secret. For example, **gMcfg342ePaKgx1ZlXK**.
Google API Access	Authenticate and authorize ClearPass for access to Google Admin APIs for your domain.

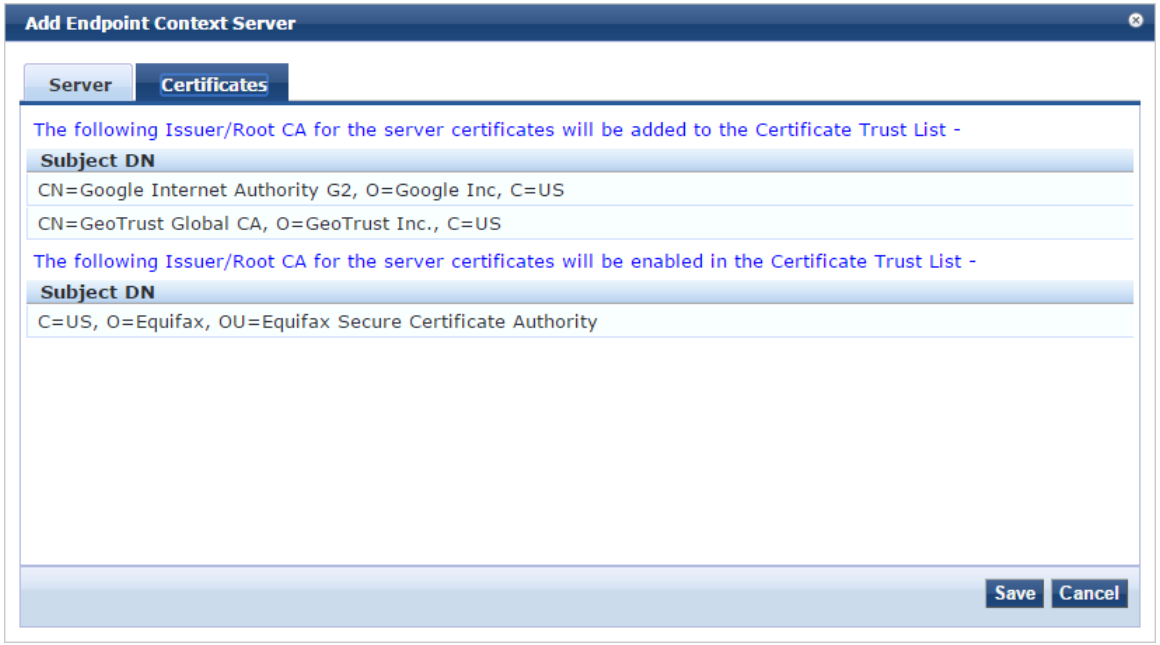
Table 295: *Add Endpoint Context Server - Server (Google Admin Console) Tab Parameters (Continued)*

Parameter	Description
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab. For more information on certificate, see Certificates Tab on page 506.
Enable Server	Enable this field to fetch endpoints from the server.
Bypass Proxy	Select the **Enable to bypass proxy server** check box to bypass the proxy server. When this field is enabled, the proxy servers configured in the **Administration** > **Server Manager** > **Server Configuration** > **Service Parameters** tab > **ClearPass system services** service page will be bypassed. The server discovery occurs without any issues even when the proxy servers are bypassed. By default, this field is disabled.

Certificates Tab

The following figure displays the **Add Endpoint Context Server - Certificates** (Google Admin Console) tab:

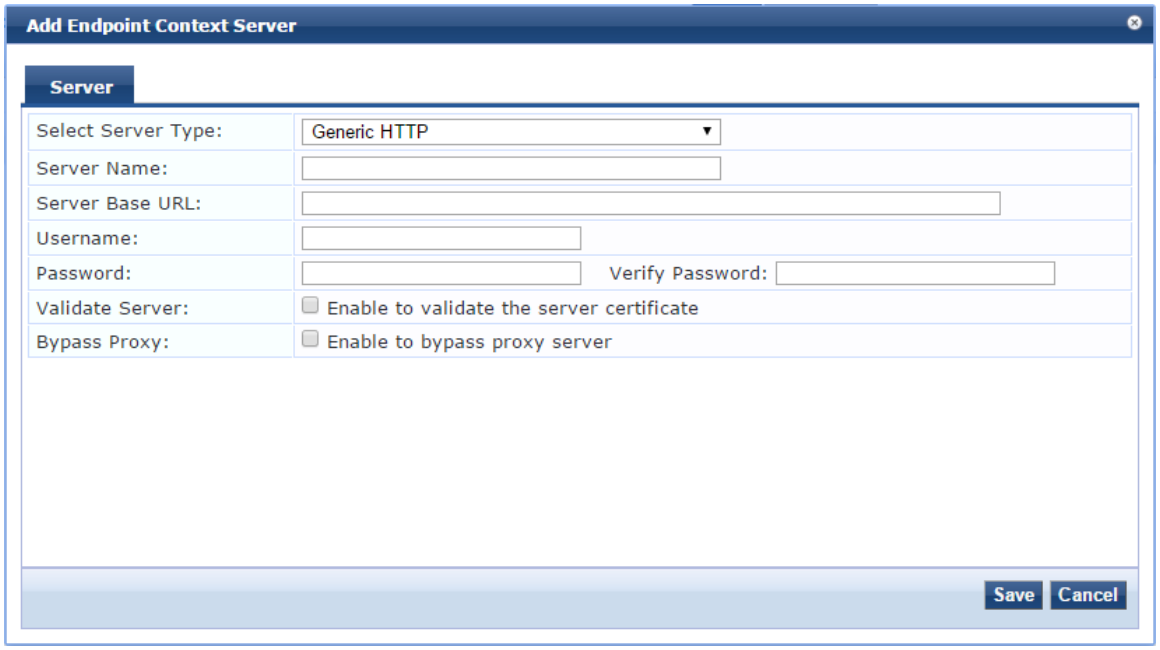
Figure 476: *Add Endpoint Context Server - Certificates (Google Admin Console) Tab*



Adding a Generic HTTP Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (Generic HTTP) tab:

Figure 477: *Add Endpoint Context Server - Server (Generic HTTP) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (Generic HTTP) tab parameters:

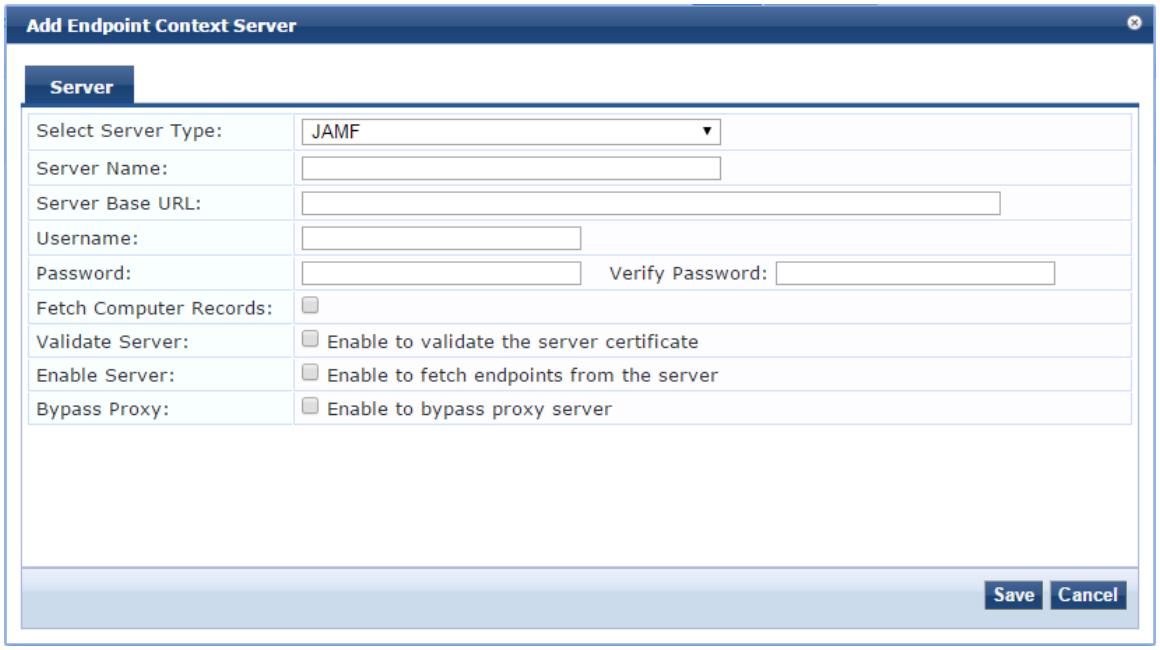
Table 296: *Add Endpoint Context Server - Server (Generic HTTP) Tab Parameters*

Parameter	Description
Select Server Type	Choose Generic HTTP from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Bypass Proxy	Enable to bypass proxy server.

Adding a JAMF Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (JAMF) tab:

Figure 478: *Add Endpoint Context Server - Server (JAMF) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (JAMF) tab parameters:

Table 297: *Add Endpoint Context Server - Server (JAMF) Tab Parameters*

Parameter	Description
Select Server Type	Choose JAMF from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Fetch Computer Records	Enable to fetch computer records.

Table 297: *Add Endpoint Context Server - Server (JAMF) Tab Parameters (Continued)*

Parameter	Description
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

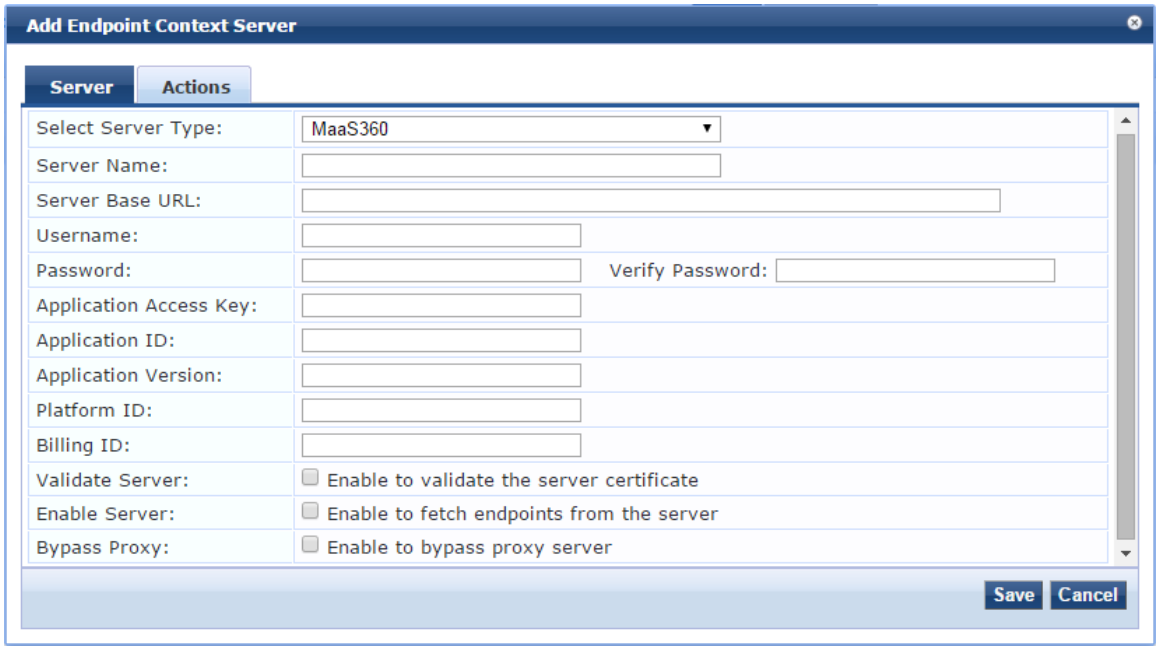
Adding a MaaS360 Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (MaaS360) tab:

Figure 479: *Add Endpoint Context Server - Server (MaaS360) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (MaaS360) tab parameters:

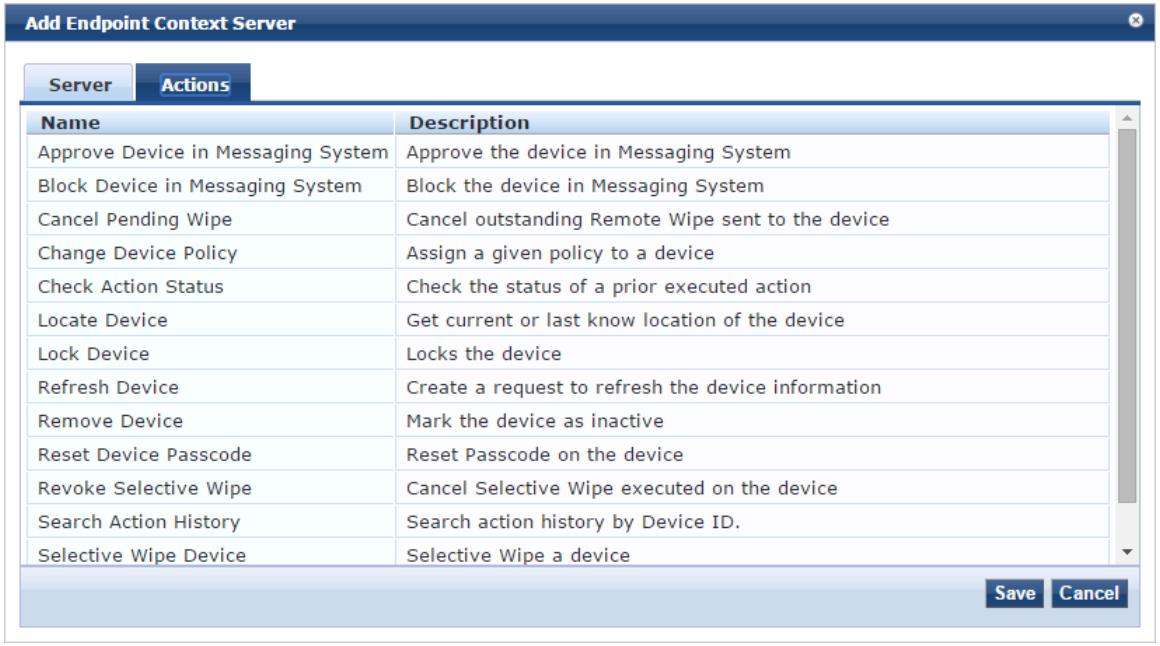
Table 298: *Add Endpoint Context Server - Server (MaaS360) Tab Parameters*

Parameter	Description
Select Server Type	Choose MaaS360 from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Application Access Key	Enter the application access key (API key).
Application ID	Enter the application ID.
Application Version	Enter the application version number.
Platform ID	Enter the platform version number.
Billing ID	Enter the billing ID.
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Actions Tab

The following figure displays the **Add Endpoint Context Server - Actions** (MaaS360) tab:

Figure 480: *Add Endpoint Context Server - Actions (MaaS360) Tab*



The following table describes the **Add Endpoint Context Server - Actions** (MaaS360) tab parameters:

Table 299: *Add Endpoint Context Server - Actions (MaaS360) Tab Parameters*

Parameter	Description
Approve Device in Messaging System	Approve the device in Messaging System.
Block Device in Messaging System	Block the device in Messaging System.
Cancel Pending Wipe	Cancel outstanding Remote Wipe sent to the device.
Change Device Policy	Assign a given policy to a device.
Check Action Status	Check the status of a prior executed action.
Locate Device	Get current or last know location of the device.
Lock Device	Lock the device.
Refresh Device	Create a request to refresh the device information.
Remove Device	Mark the device as inactive.
Reset Device Passcode	Reset the pass code on the device.

Table 299: *Add Endpoint Context Server - Actions (MaaS360) Tab Parameters (Continued)*

Parameter	Description
Revoke Selective Wipe	Cancel Selective Wipe executed on the device.
Search Action History	Search action history by Device ID.
Selective Wipe Device	Execute a Selective Wipe on a device.
Wipe Device	Delete all information stored on a device.

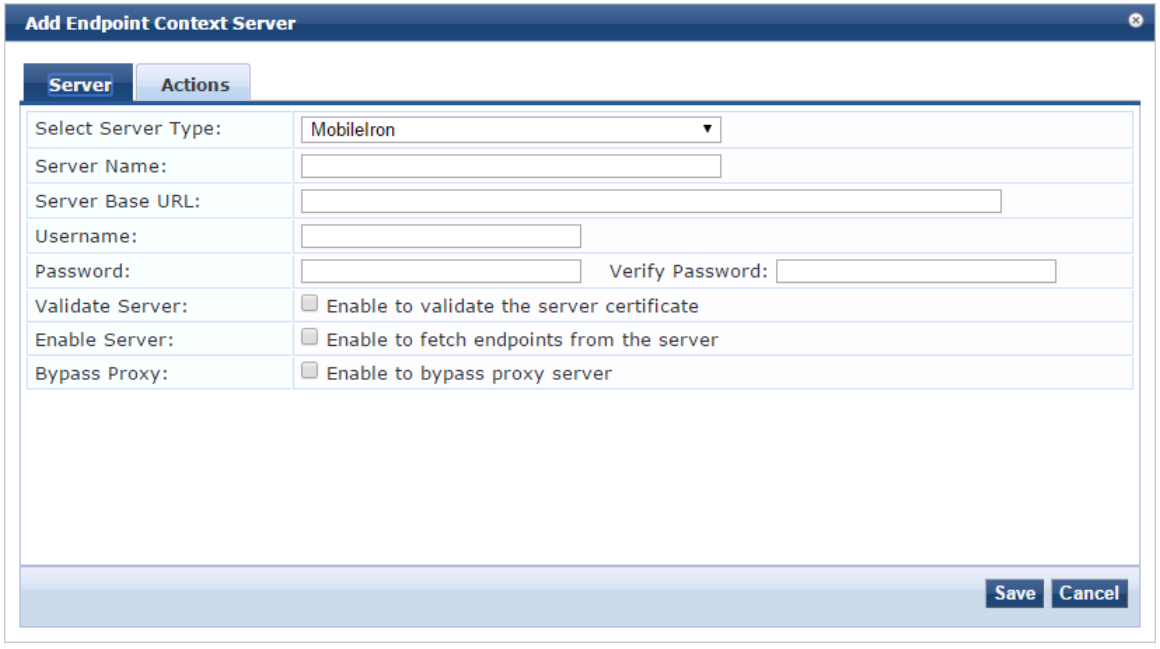
Adding a MobileIron Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (MobileIron) tab:

Figure 481: *Add Endpoint Context Server - Server (MobileIron) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (MobileIron) tab parameters:

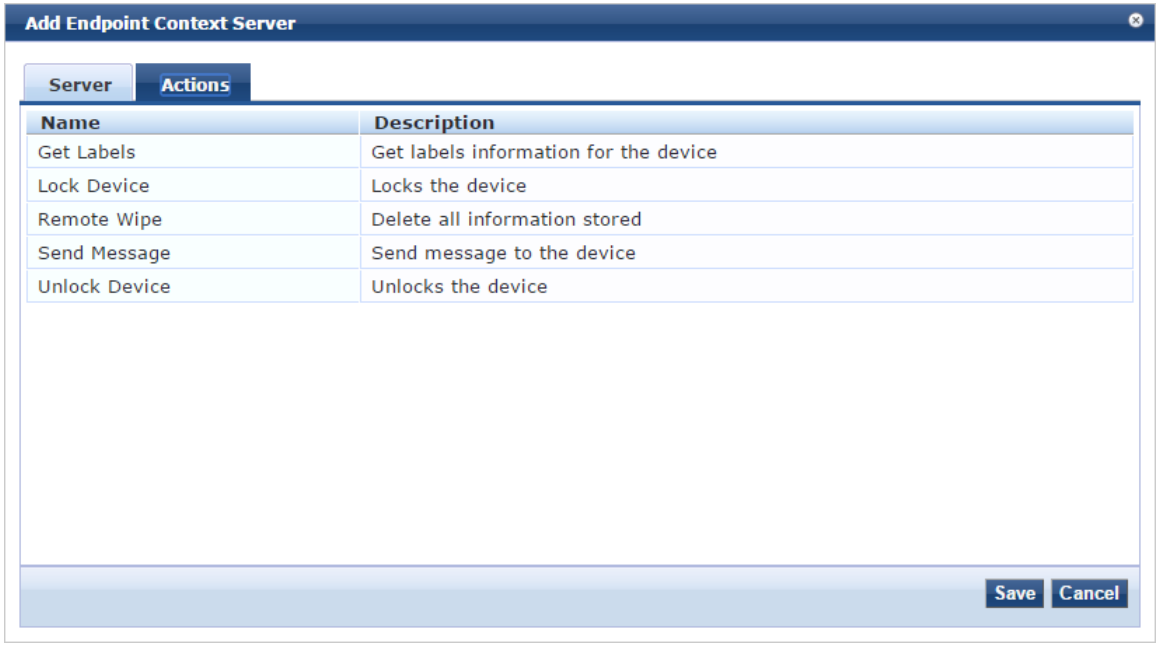
Table 300: *Add Endpoint Context Server - Server (MobileIron) Tab Parameters*

Parameter	Description
Select Server Type	Choose MobileIron from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Actions Tab

The following figure displays the **Add Endpoint Context Server - Actions** (MobileIron) tab:

Figure 482: *Add Endpoint Context Server - Actions (MobileIron) Tab*



The following table describes the **Add Endpoint Context Server - Actions** (MobileIron) tab parameters:

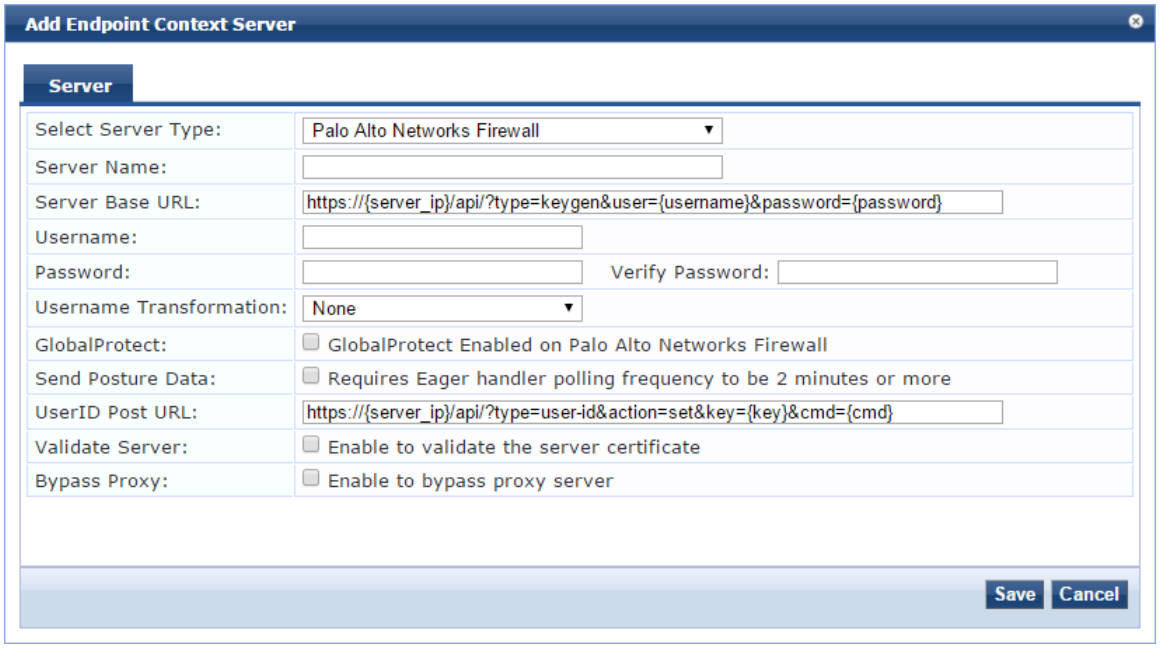
Table 301: *Add Endpoint Context Server - Actions (MobileIron) Tab Parameters*

Parameter	Description
Get Labels	Get label information of the device.
Lock Device	Lock the device.
Remote Wipe	Delete all information stored on the device.
Send Message	Send message to the device.
Unlock Device	Unlock the device.

Adding a Palo Alto Networks Firewall Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (Palo Alto Networks Firewall) tab:

Figure 483: *Add Endpoint Context Server - Server (Palo Alto Networks Firewall) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (Palo Alto Networks Firewall) tab parameters:

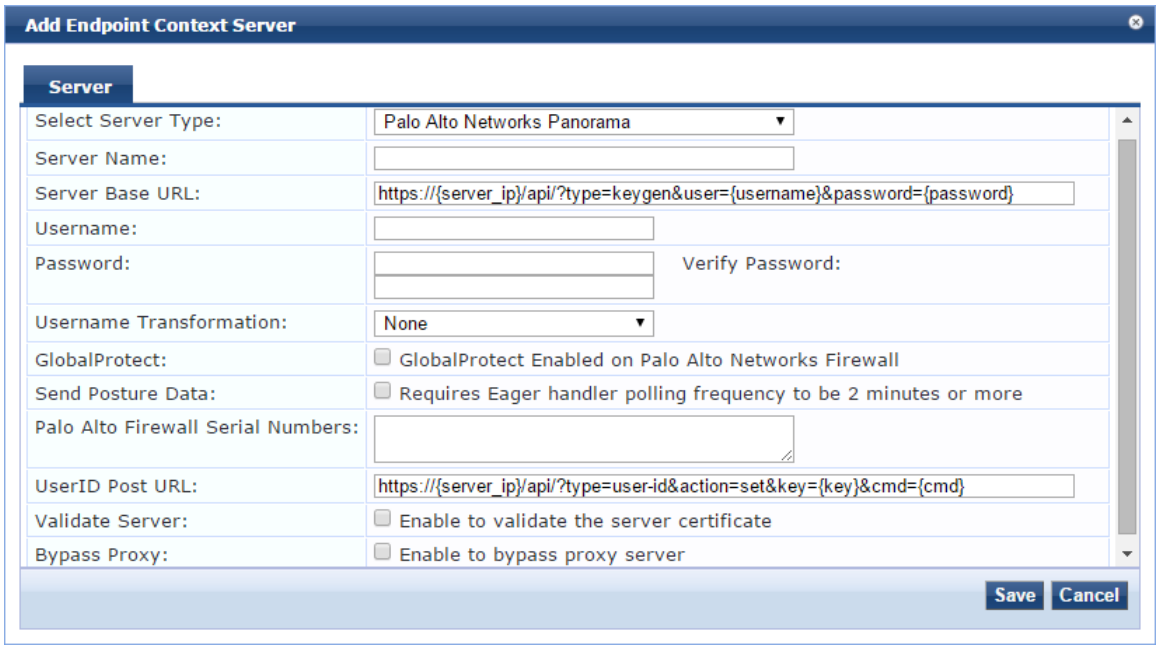
Table 302: *Add Endpoint Context Server - Server (Palo Alto Networks Firewall) Tab Parameters*

Parameter	Description
Select Server Type	Choose Palo Alto Networks Firewall from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the server base URL in the following format: https://{server_ip} /api/?type=keygen&user={username}&password={password}
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Username Transformation	Choose one of the following options: • **None** - Do not use any username transformation. • **Prefix NETBIOS name** - Prefix NETBIOS name in UID updates. • **Use Full Username** - Use full username in UID updates.
GlobalProtect	Enable to send HIP report to firewall. GlobalProtect license should be enabled on firewall for this to work.
Send Posture Data	Enable to send posture data on Palo Alto Networks firewall after authentication. This option can be resource-intensive, the eager handler-polling interval must be two minutes or more. Enabling this field verifies whether the polling frequency is set to 2 minutes and then send the posture data to Palo Alto Networks firewall. These posture data can be verified in **Access Tracker** page.
UserID Post URL	Enter the user ID post URL in the following format: https://{server_ip} /api/?type=user-id&action=set&key={key}&cmd={cmd}
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Bypass Proxy	Enable to bypass proxy server.

Adding a Palo Alto Networks Panorama Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (Palo Alto Networks Panorama) tab:

Figure 484: *Add Endpoint Context Server - Server (Palo Alto Networks Panorama) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (Palo Alto Networks Panorama) tab parameters:

Table 303: *Add Endpoint Context Server - Server (Palo Alto Networks Panorama) Tab Parameters*

Parameter	Description
Select Server Type	Choose Palo Alto Networks Panorama from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the server base URL in the following format: https://{server_ip} /api/?type=keygen&user={username}&password={password}
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Username Transformation	Choose one of the following options: • **None** - Do not use any username transformation. • **Prefix NETBIOS name** - Prefix NETBIOS name in UID updates. • **Use Full Username** - Use full username in UID updates.
GlobalProtect	Enable to send HIP report to firewall. GlobalProtect license should be enabled on firewall for this to work.

Table 303: *Add Endpoint Context Server - Server (Palo Alto Networks Panorama) Tab Parameters (Continued)*

Parameter	Description
Send Posture Data	Enable to send posture data on Palo Alto Networks firewall after authentication. This option can be resource-intensive, the eager handler-polling interval must be two minutes or more. Enabling this field verifies whether the polling frequency is set to 2 minutes and then send the posture data to Palo Alto Networks firewall. These posture data can be verified in **Access Tracker** page.
Palo Alto Firewall Serial Numbers	Enter the Palo Alto firewall serial numbers.
UserID Post URL	Enter the user ID post URL in the following format: https://{server_ip} /api/?type=user-id&action=set&key={key}&cmd={cmd}
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Bypass Proxy	Enable to bypass proxy server.

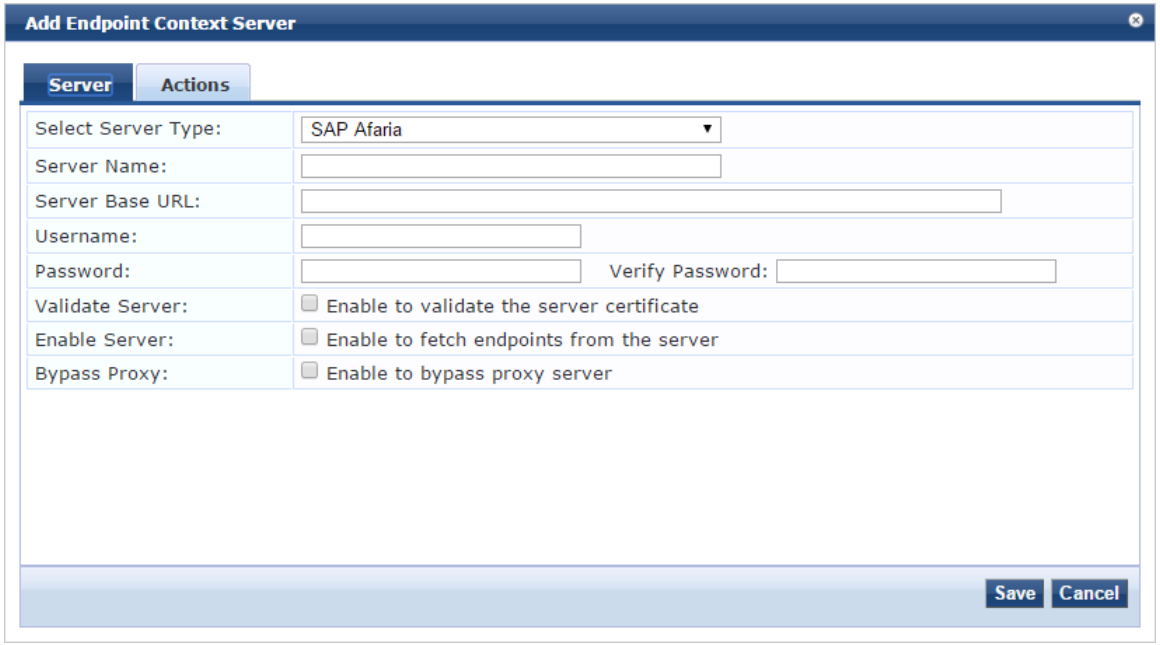
Adding an SAP Afaria Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint.

Server Tab

The following figure displays the **Add Endpoint Context Server - Server** (SAP Afaria) tab:

Figure 485: *Add Endpoint Context Server - Server (SAP Afaria) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (SAP Afaria) tab parameters:

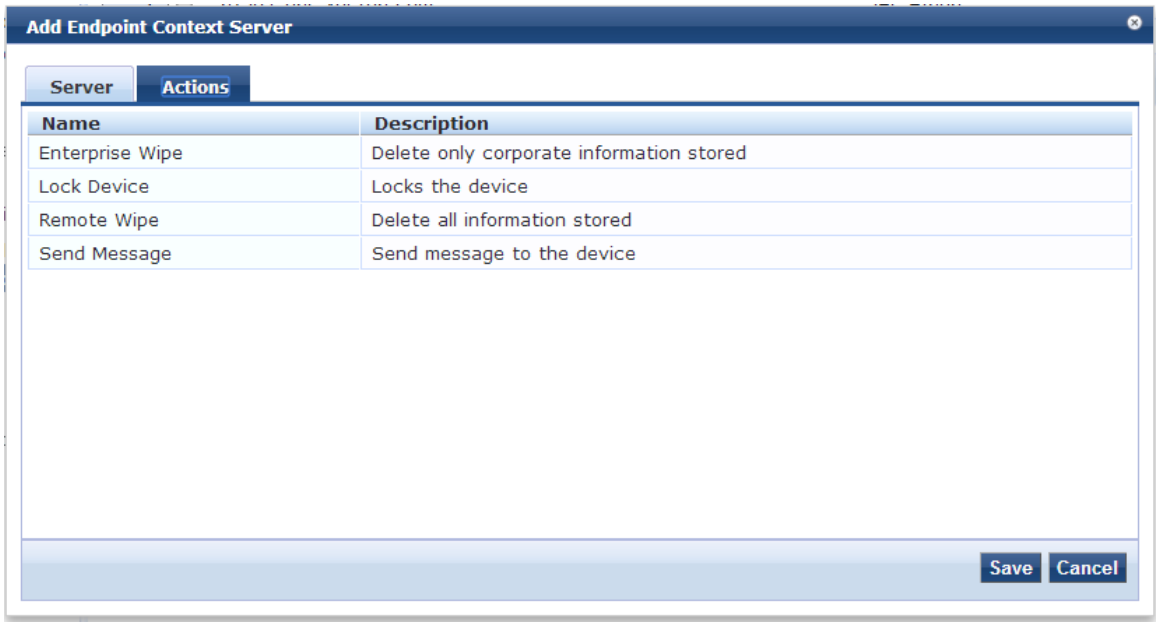
Table 304: *Add Endpoint Context Server - Server (SAP Afaria) Tab Parameters*

Parameter	Description
Select Server Type	Choose SAP Afaria from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	Enter the full URL for the server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber.
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Actions Tab

The following figure displays the **Add Endpoint Context Server - Actions** (SAP Afaria) tab:

Figure 486: *Add Endpoint Context Server - Actions (SAP Afaria) Tab*



The following table describes the **Add Endpoint Context Server - Actions** (SAP Afaria) tab parameters:

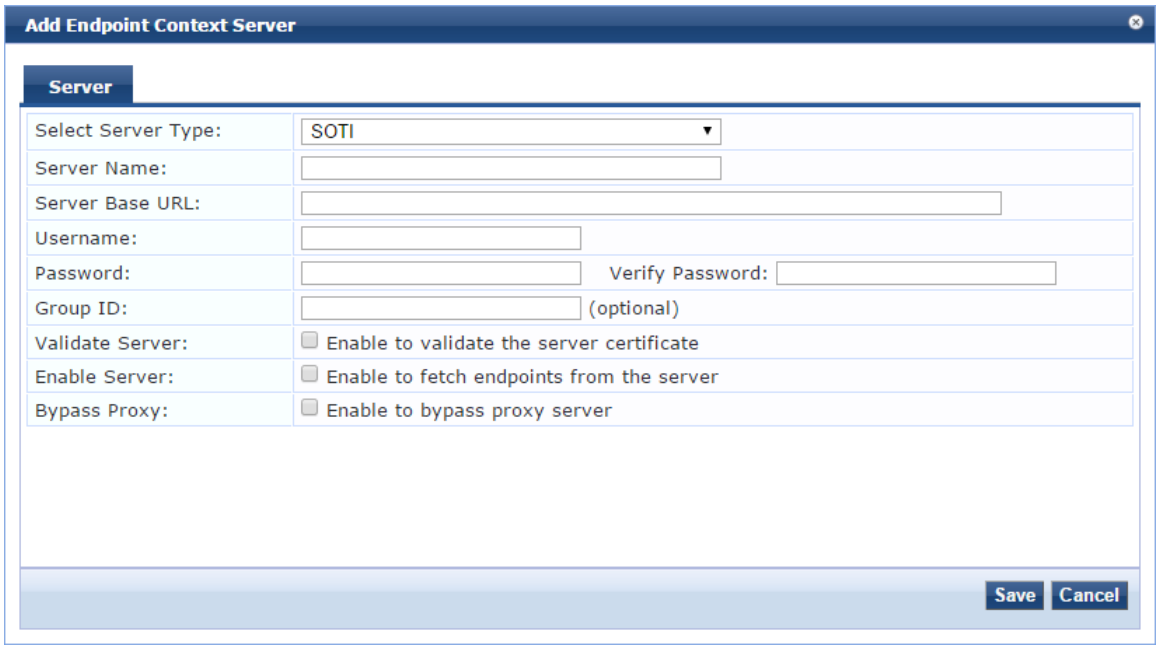
Table 305: *Add Endpoint Context Server - Actions (SAP Afaria) Tab Parameters*

Parameter	Description
Enterprise Wipe	Delete corporate information related data.
Lock Device	Lock the associated device.
Remote Wipe	Delete all stored information.
Send Message	Send message to the device.

Adding an SOTI Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (SOTI) tab:

Figure 487: *Add Endpoint Context Server - Server (SOTI) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (SOTI) tab parameters:

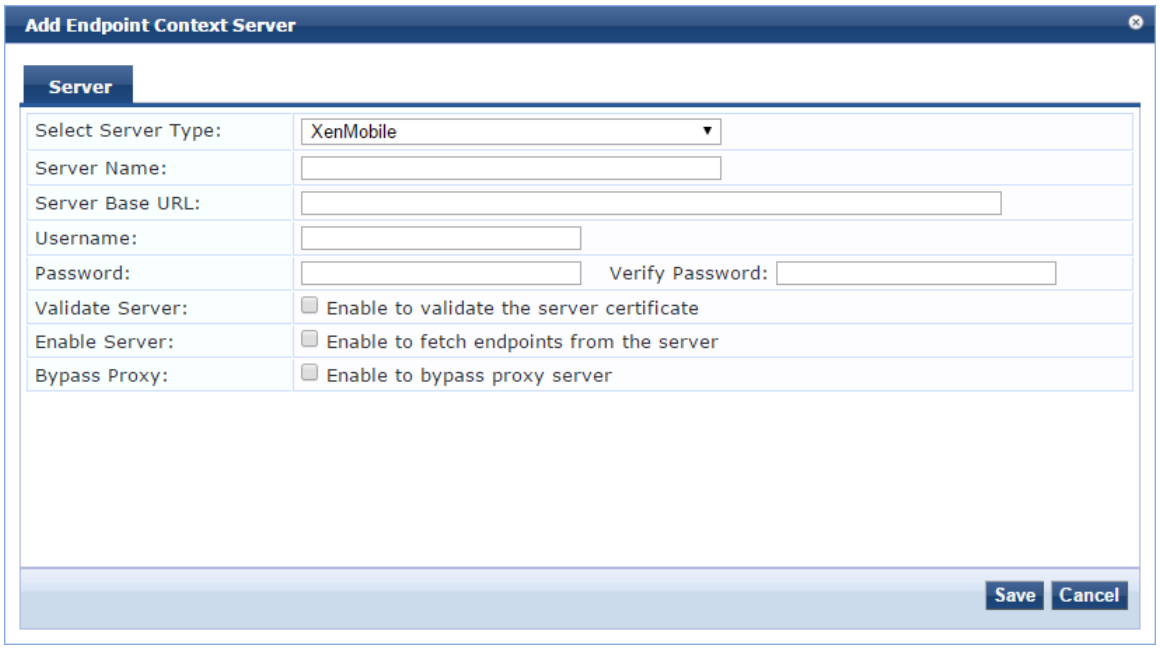
Table 306: *Add Endpoint Context Server - Server (SOTI) Tab Parameters*

Parameter	Description
Select Server Type	Choose SOTI from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the server base URL in the following format: https://{server_ip} /api/?type=keygen&user={username}&password={password}
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Group ID	Enter the group ID. This parameter is optional.
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

Adding a XenMobile Endpoint Context Server

Consult the endpoint manufacturer's documentation for information about the parameters that you must enter to configure this endpoint. The following figure displays the **Add Endpoint Context Server - Server** (XenMobile) tab:

Figure 488: *Add Endpoint Context Server - Server (XenMobile) Tab*



NOTE

You can add more than one endpoint context server of the same type. For example, you can add more than one AirWatch endpoint context server.

The following table describes the **Add Endpoint Context Server - Server** (XenMobile) tab parameters:

Table 307: *Add Endpoint Context Server - Server (XenMobile) Tab Parameters*

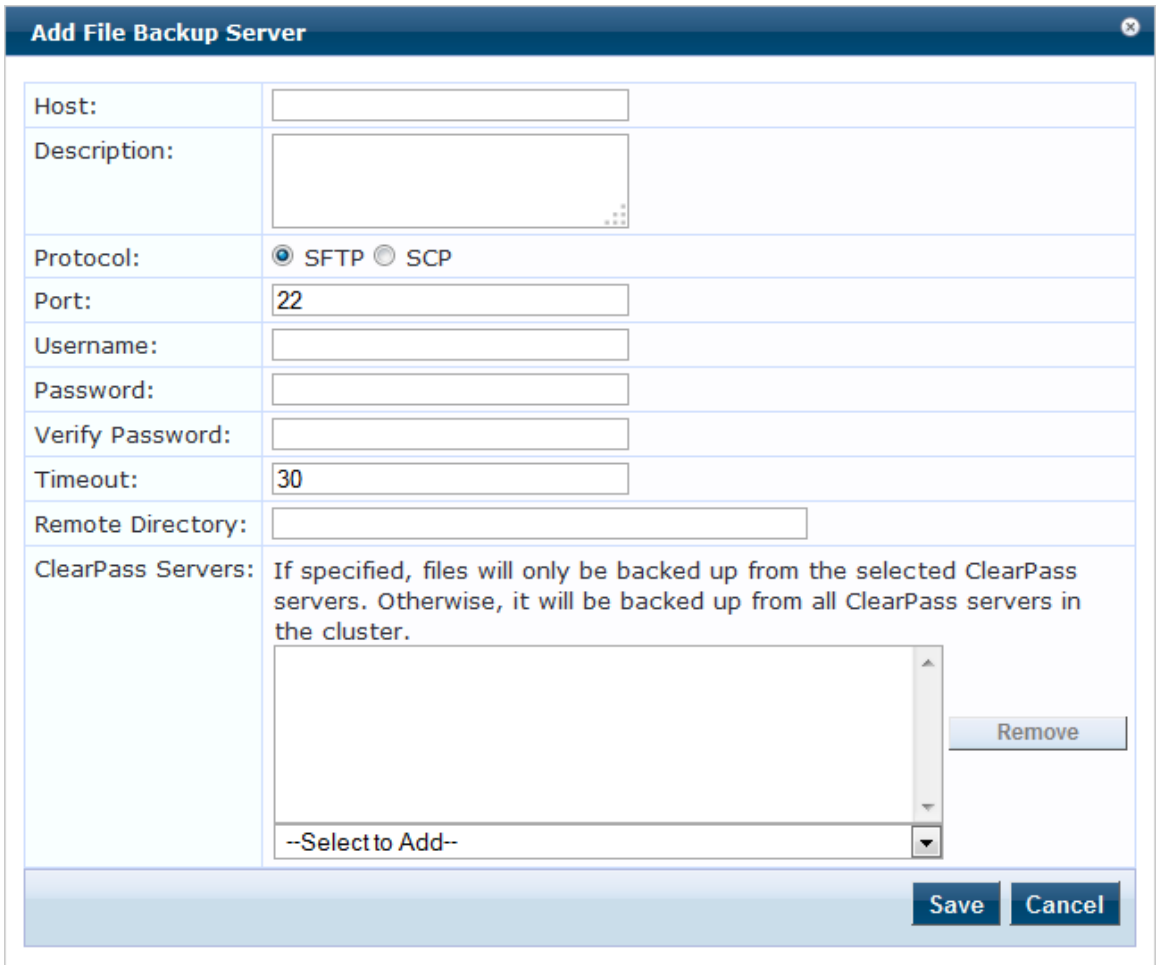
Parameter	Description
Select Server Type	Choose XenMobile from the drop-down list.
Server Name	Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	Enter the server base URL in the following format: https://{server_ip} /api/?type=keygen&user={username}&password={password}
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

File Backup Servers

Dell Networking W-ClearPass Policy Manager provides the ability to push scheduled data securely to an external server. You can push the data using the SFTP and SCP protocols. Navigate to the **Administration** > **External Servers** > **File Backup Servers** page and click the **Add** link at the top-right corner. The **Add File Backup Server** page opens.

The following figure displays the **Add File Backup Server** page:

Figure 489: *File Backup Servers - Add File Backup Server Page*



The following table describes the **Add File Backup Server** page parameters:

Table 308: *Add File Backup Server Page Parameters*

Parameter	Description
Host	Enter the name or IP address of the host.
Description	Enter the description that provides additional information about the File Backup server.
Protocol	Specify the protocol to be used to upload the generated reports to an external server. You can select from the following protocols: • SFTP (SSH File Transfer Protocol) • SCP (Session Control Protocol)

Table 308: *Add File Backup Server Page Parameters (Continued)*

Parameter	Description
Port	Specify the port number. The default port is 22.
Username	Enter the user name and password of the host server.
Password	Enter the user name of the host server.
Verify Password	Enter the password of the host server.
Timeout	Specify the timeout value in seconds. The default value is 30 seconds.
Remote Directory	Specify the location in this field to which the files to be copied. A folder will be automatically created in the file path that you specify based on the selected ClearPass servers in the **ClearPass Servers** field.
ClearPass Servers	Specify the ClearPass servers. If a servers are specified, files will only be backed up from the selected ClearPass servers. Otherwise, it will be backed up from all ClearPass servers in the cluster. You can select the servers from the **Select to Add** drop-down list.

Server Certificate

The **Server Certificate** page depends if the RADIUS Server Certificate type or the HTTPS Service Certificate type is assigned to the selected server. To configure the server certificate, navigate to **Administration > Certificates > Server Certificate**.

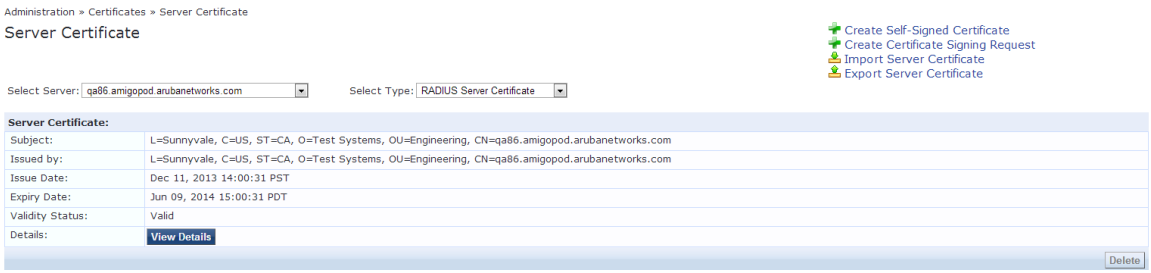
This section describes the following topics:

- Server Certificate Main Page on page 523
- Server Certificate Type on page 524

Server Certificate Main Page

The following figure displays the Server Certificate page:

Figure 490: *Server Certificate Page*



The following table describes the **Server Certificate** parameters:

Table 309: *Server Certificate Parameters*

Parameter	Description
Create Self-Signed Certificate	Opens the **Create Self-Signed Certificate** page where you can create and install a Self-Signed Certificate. For more information, see Creating a Self-Signed Certificate on page 529.
Create Certificate Signing Request	Opens the **Create Certificate Signing Request** page where you can create and install a Certificate Signing Request. For more information, see Creating a Certificate Signing Request on page 526.
Import Server Certificate	Opens the **Import Server Certificate** page where you can import a certificate that has been exported previously. For more information, see Importing a Server Certificate on page 534.
Export Server Certificate	On clicking this link, the self-signed certificate is downloaded. For more information, see Exporting a Server Certificate on page 534.
Select Server	Select a server in the cluster for server certificate operations.
Select Type	Select a certificate type. The options are **RADIUS Server Certificate** or **HTTPS Server Certificate**. The availability of two certificate types (internally signed and publicly signed) can provide deployment flexibility.
View Details	Click to view the certificate details.

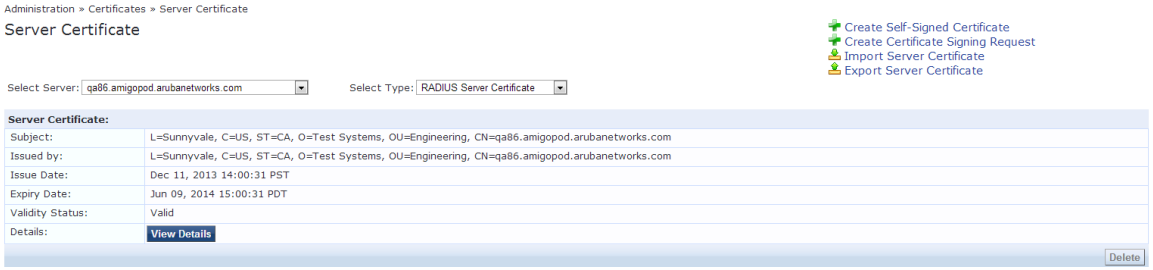
Server Certificate Type

Dell Networking W-ClearPass Policy Manager provides two types of server certificates.

RADIUS Server Certificate

This page displays the parameters configured when a self-signed certificate with a RADIUS Server Certificate is created and installed. The following figure displays the RADIUS **Server Certificate** page:

Figure 491: *RADIUS Server Certificate Page*



The following table describes the RADIUS **Server Certificate** parameters:

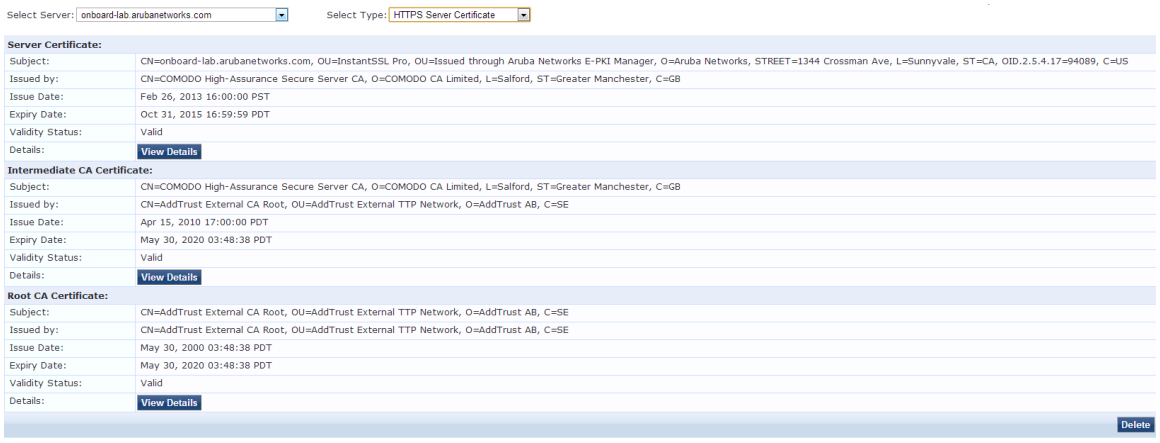
Table 310: *RADIUS Server Certificate Parameters*

Parameter	Description
Subject	Displays Organization and Common Name.
Issued by	Displays Organization and Common Name.
Issue Date	Displays the date the self-signed certificate is installed.
Expiry Date	Displays the date (in days) when the self-signed certificate expires.
Validity Status	Displays the validity status of the self-signed certificate.
Details	Click the **View Details** button to view details about the certificate, such as Signature Algorithm, Subject Public Key Info, and more.

HTTPS Server Certificate

The page displays the parameters configured after a self-signed certificate with an HTTPS Server Certificate is created and installed. The page contains data about the Server Certificate, Intermediate CA Certificate and Root CA Certificate. Click the **View Details** button for each section to see details about Signature Algorithm, Public Key Info, and more. The following figure displays the HTTPS **Server Certificate** page:

Figure 492: *HTTPS Server Certificate Page*



The following table describes the HTTPS **Server Certificate** parameters:

Table 311: *HTTPS Server Certificate Parameters*

Parameter	Description
Subject	Displays Organization and Common Name.
Issued by	Displays Organization and Common Name.
Issue Date	Displays the date the self-signed certificate is installed.

Table 311: *HTTPS Server Certificate Parameters (Continued)*

Parameter	Description
Expiry Date	Displays the date (in days) when the self-signed certificate expires.
Validity Status	Displays the validity status of the self-signed certificate.
Details	Click the **View Details** button to view details about the certificate, such as Signature Algorithm, Subject Public Key Info, and more.

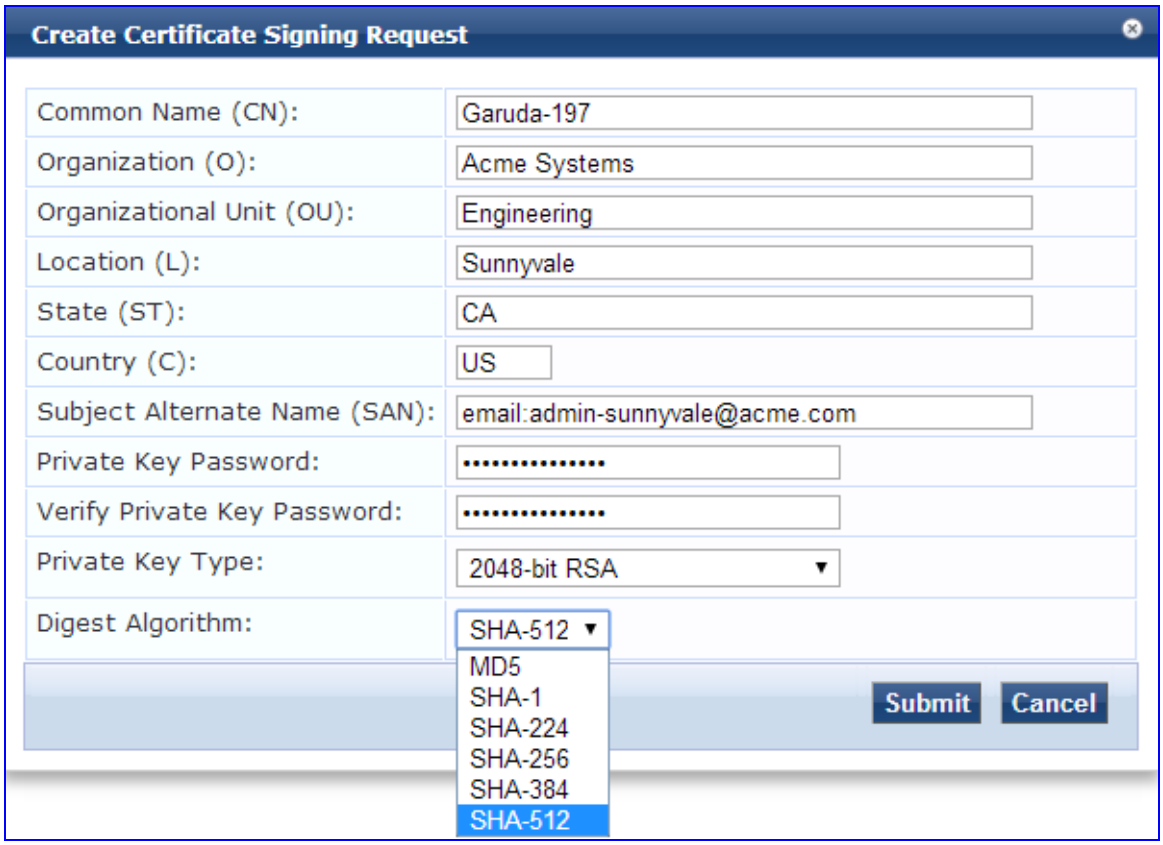
Creating a Certificate Signing Request

After you select a server and a certificate type, you can create a certificate signing request. This task creates a self-signed certificate to be signed by a CA. To create a certificate signing request:

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Select a server, for example, localhost.
3. Click the **Create Certificate Signing Request** link. Configure the parameters based on Table 312.
4. Click **Submit**.

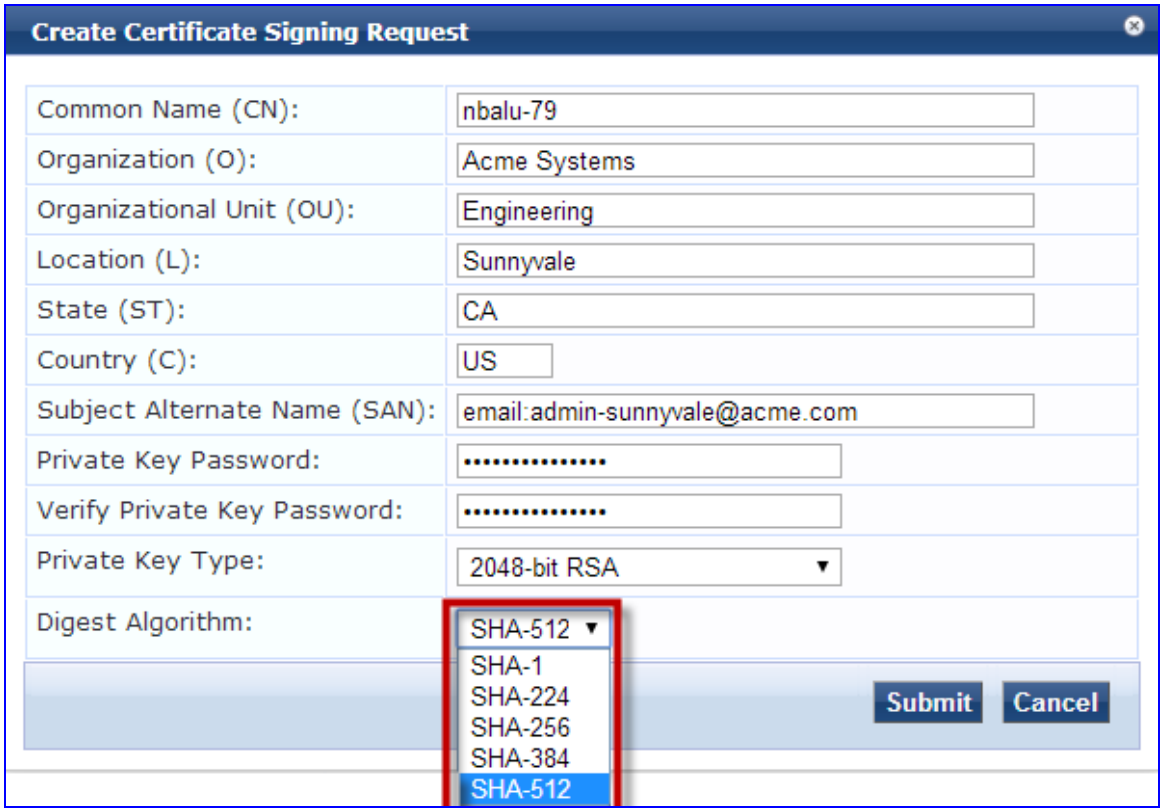
The following figure displays the **Create Certificate Signing Request** pop-up:

Figure 493: *Create Certificate Signing Request Pop-up*



The following figure displays the **Create Certificate Signing Request** page in the FIPS mode pop-up:

Figure 494: *Create Certificate Signing Request - FIPS Mode Pop-up*



The following table describes the **Create Certificate Signing Request** parameters:

Table 312: *Create Certificate Signing Request Parameters*

Parameter	Description
Common Name (CN)	Enter the name associated with this entity. This can be a host name, IP address, or other name. The default is the fully-qualified domain name (FQDN). This field is mandatory.
Organization (O)	Enter the name of the organization. This field is optional.
Organizational Unit (OU)	Enter the name of the department, division, section, or other meaningful name. This field is optional.
Location (L)	Enter the name of the location, state, country, and/or other meaningful name. These fields are optional.
State (ST)	
Country (C)	
Subject Alternate	Enter the alternative names for the specified Common Name. **NOTE:** Enter the SAN in the following formats:

Table 312: *Create Certificate Signing Request Parameters (Continued)*

Parameter	Description
Name (SAN)	• email: *email_address* • URI: *uri* • IP: *ip_address* • dns: *dns_name* • rid: *id* This field is optional.
Private Key Password	Enter and re-enter the Private Key password.
Verify Private Key Password	
Private Key Type	Select the length for the generated private key types from the following options: • 1024-bit RSA • 2048-bit RSA • 4096-bit RSA • X9.62/SECG curve over a 256 bit prime field • NIST/SECG curve over a 384 bit prime field The default private key type is **2048-bit RSA.**
Digest Algorithm	Select the message digest algorithm from the following options: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 **NOTE:** The MD5 algorithm is not available in the **FIPS** mode.

After you create a **Certificate Signing Request** form and click **Submit**, the generated certificate signing request is displayed. Copy the certificate and paste it into the Web form as part of the enrollment process. You can click **Download CSR and Private Key Files** to save the Certificate Signing Request file and the private key password file. The following figure displays the **Create Certificate Signing Request** pop-up:

Figure 495: *Create Certificate Signing Request Pop-up*

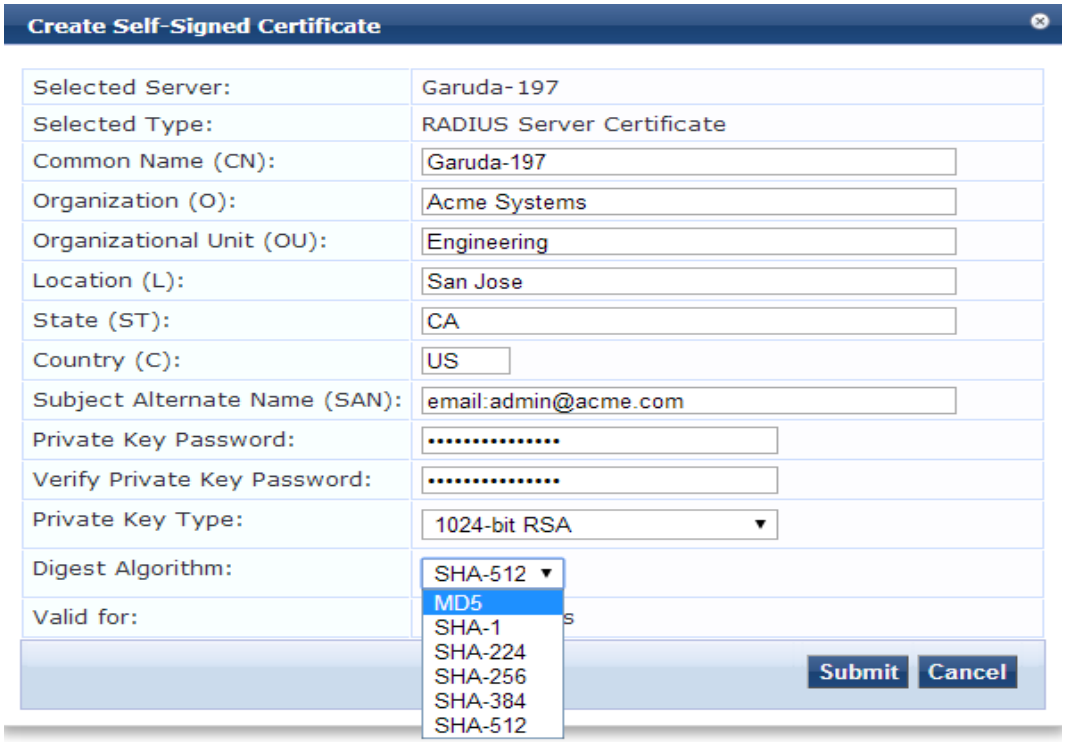
Creating a Self-Signed Certificate

After you select a server and a certificate type, you can create and install a self-signed certificate. To create a self-signed certificate:

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Select a server, for example, localhost.
3. Click the **Create Self-Signed Certificate** link. Configure the parameters based on Table 313.
4. Click **Submit**.
5. To install a self-signed certificate, see Installing a Self-Signed Certificate on page 532.

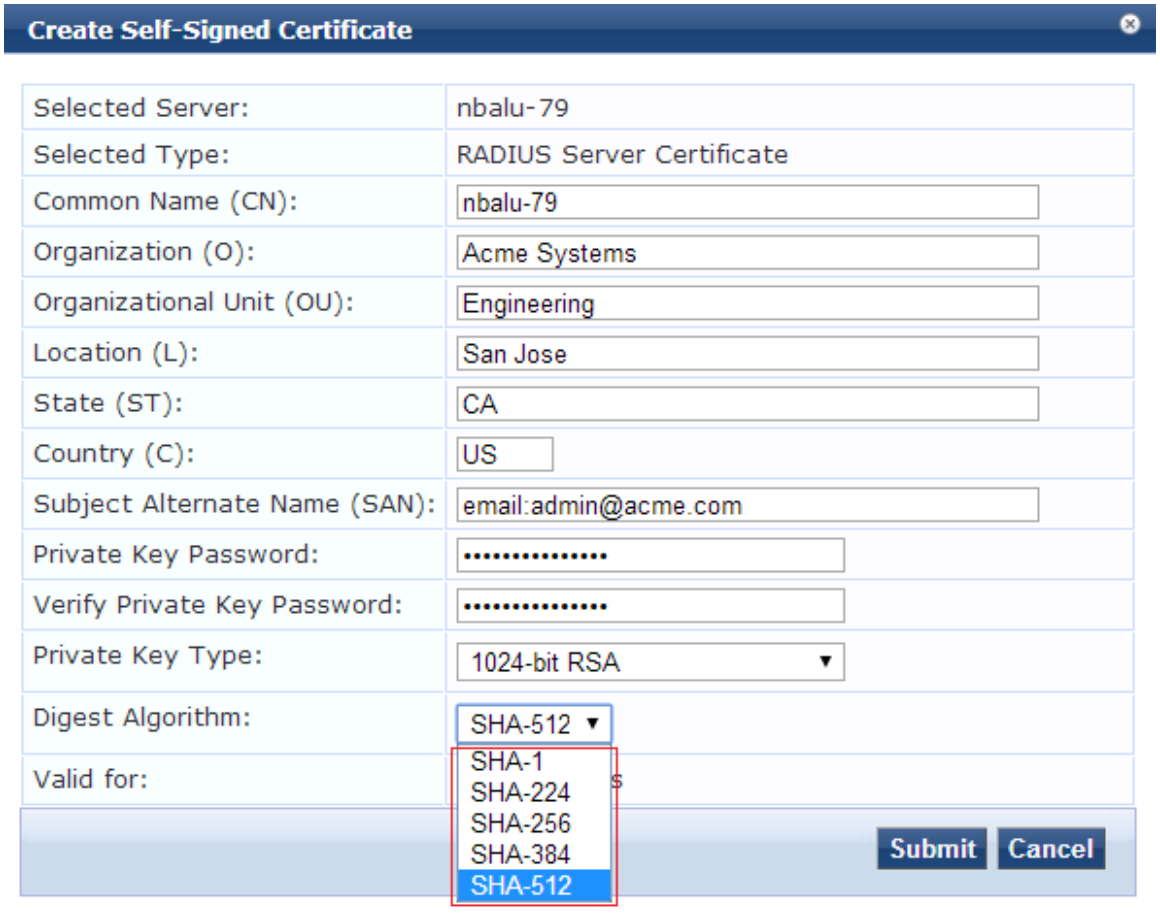
The following figure displays the **Create Self-Signed Certificate** pop-up:

Figure 496: *Create Self-Signed Certificate Pop-up*



The following figure displays the **Create Self-Signed Certificate** page in the FIPS mode pop-up:

Figure 497: *Create Self-Signed Certificate Page - FIPS Mode Pop-up*



The following table describes the **Create Self-Signed Certificate** parameters:

Table 313: *Create Self-Signed Certificate Parameters*

Parameter	Description
Selected Server	Displays the name of the selected server on the **Server Certificate** page.
Selected Type	Displays the selected certificate type for the server on the **Server Certificate** page.
Common Name (CN)	Enter the name associated with this entity. This can be a host name, IP address, or other meaningful name. This field is mandatory.
Organization (O)	Enter the name of the organization. This field is optional.
Organizational Unit (OU)	Enter the name of the department, division, section, or other meaningful name. This field is optional.

Table 313: *Create Self-Signed Certificate Parameters (Continued)*

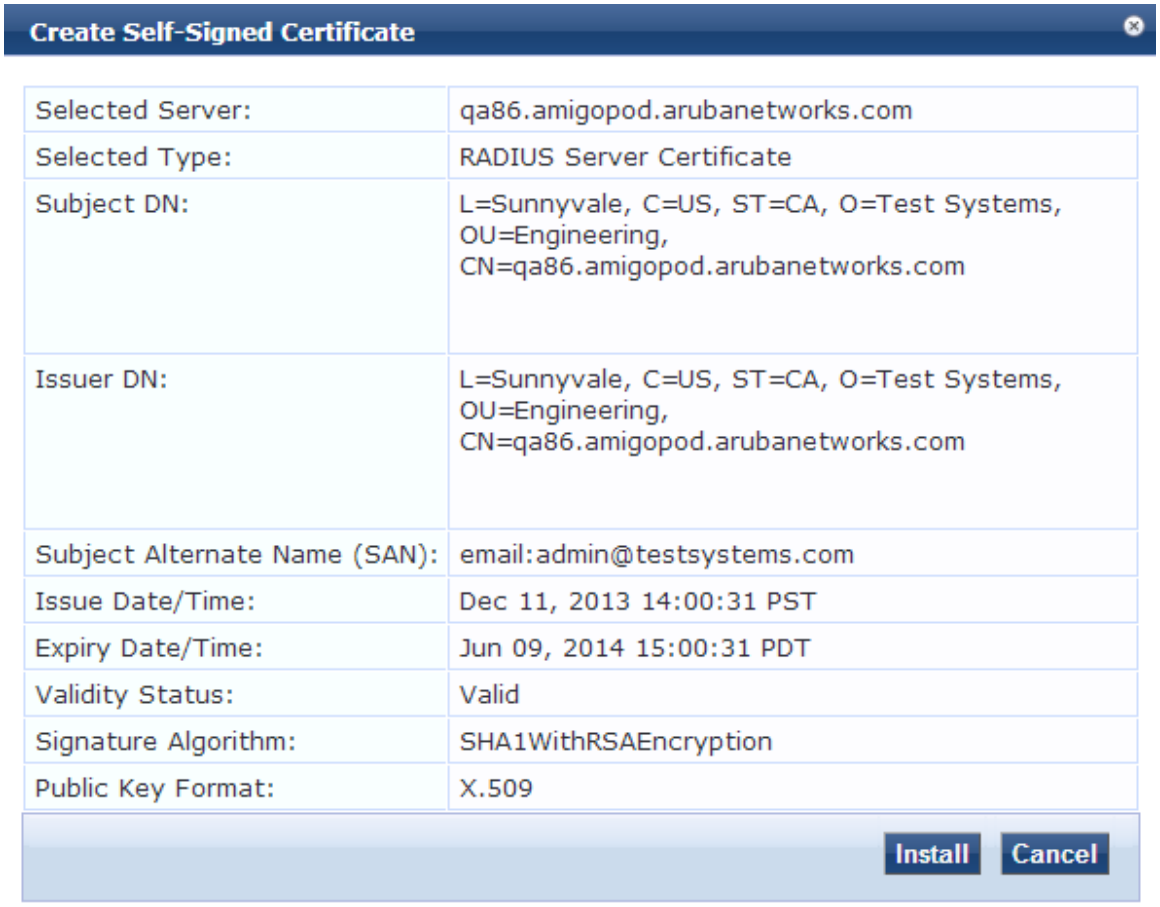
Parameter	Description
Location (L)	Enter the name of the location, state, country, and/or other meaningful name. These fields are optional.
State (ST)	
Country (C)	
Subject Alternate Name (SAN)	Enter the alternative names for the specified Common Name. **NOTE:** Enter the SAN in the following formats: • email: *email_address* • URI: *uri* • IP: *ip_address* • dns: *dns_name* • rid: *id* This field is optional.
Private Key Password	Enter and re-enter the Private Key password.
Verify Private Key Password	
Private Key Type	Select the length for the generated private key types from the following options: • 1024-bit RSA • 2048-bit RSA • 4096-bit RSA • X9.62/SECG curve over a 256 bit prime field • NIST/SECG curve over a 384 bit prime field The default private key type is **2048-bit RSA.**
Digest Algorithm	Select the message digest algorithm from the following options: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 **NOTE:** The **MD5** algorithm is not available in the **FIPS** mode.
Valid for	Enter the duration in number of days.

Installing a Self-Signed Certificate

Once you click **Submit**, you are prompted to install the self-signed certificate. This page displays a summary of the values selected in the **Create Self-Signed Certificate** page. Click **Install** to install the self-signed certificate.

The following figure displays the **Create Self-Signed Certificate** pop-up.

Figure 498: *Create Self-Signed Certificate Pop-up*



The following table describes the **Create Self-Signed Certificate** parameters configured:

Table 314: *Self-Signed Certificate Parameters*

Parameter	Description
Selected Server	Displays the name of the server selected on the **Server Certificate** page.
Selected Type	Displays the selected certificate type for the server.
Subject DN	Displays information about the organization, common name, and location of the Subject DN.
Issuer DN	Displays information about the organization, common name, and location of the Subject DN.
Subject Alternate Name (SAN)	Displays the SAN defined during certificate creation.
Issue Date/Time	Displays the certificate issue date and time.
Expire Date/Time	Displays the certificate expiration date and time.

Table 314: *Self-Signed Certificate Parameters (Continued)*

Parameter	Description
Validity Status	Displays the validity status of the certificate.
Signature Algorithm	Displays the **Digest Algorithm** and **Private Key Type** selected during certificate configuration.
Public Key Format	Displays the public key format in use for the self-signed server certificate.

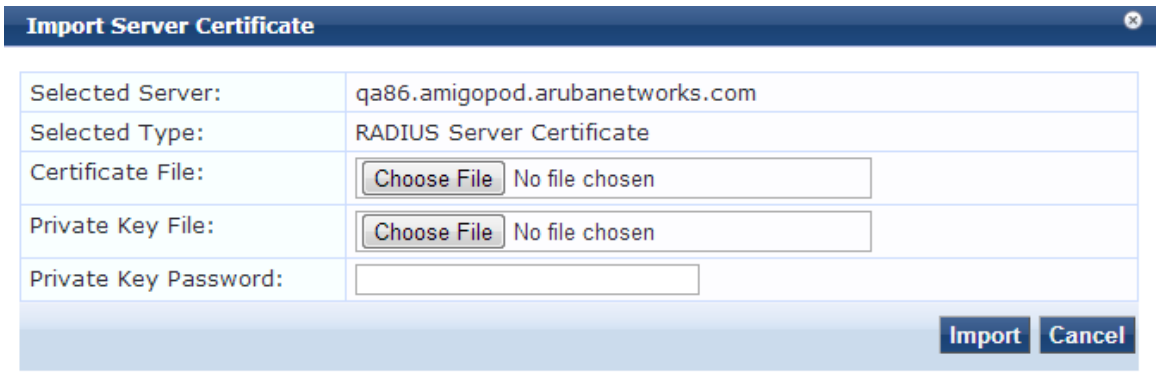
Exporting a Server Certificate

Navigate to **Administration > Certificates > Server Certificates**, and click the **Export Server Certificate** link. The default location for an exported certificate is **C:/ <user>/Downloads/<HTTPSServerCertificate.zip> or <RADIUSServerCertificate.zip>**. The zip file has the server certificate (.crt file) and the private key (.pvk file).

Importing a Server Certificate

Navigate to **Administration > Certificates > Server Certificates**, and select the **Import Server Certificate** link. The following figure displays the **Import Server Certificate** pop-up:

Figure 499: *Import Server Certificate Pop-up*



NOTE

For security reasons, certificate signed using SHA1RSA is not recommended. It is recommended to import certificates signed with stronger keys such as RSA with length more than 1024 bits.

The following table describes the **Import Server Certificate** parameters:

Table 315: *Import Server Certificate Parameters*

Parameter	Description
Selected Server	Displays the name of the selected server on the **Server Certificate** page.
Selected Type	Displays the selected certificate type for the server on the **Server Certificate** page.
Certificate File	Browse to the certificate file to be imported.

Table 315: *Import Server Certificate Parameters (Continued)*

Parameter	Description
Private Key File	Browse to the private key file to be imported.
Private Key Password	Specify the private key password that was entered when the server certificate was configured.

Certificate Trust List

The Certificate Trust List page displays a list of trusted Certificate Authorities (CA). On this page, you can add, view, or delete a certificate.

This section describes the following topics:

NOTE

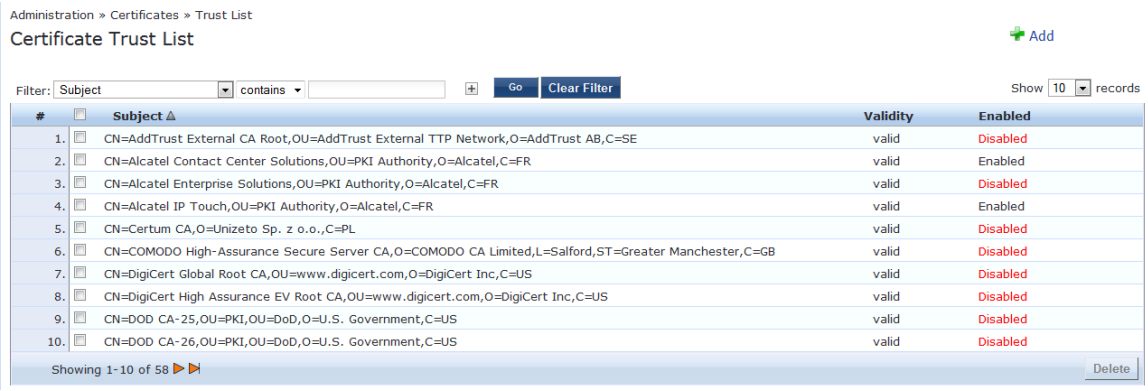
You cannot import the certificates that are created with the **MD5** digest algorithm to the **Certificate Trust List** in the **FIPS** mode.

Certificate Trust List Main Page

To display a list of trusted Certificate Authorities (CA), navigate to **Administration > Certificates > Trust List**.

The following figure displays the **Certificate Trust List** page:

Figure 500: *Certificate Trust List Main Page*



The **Certificate Trust List** (**Administration** > **Certificates** > **Trust List**) page can include the following certificates:

- DoD (Department of Defense) certificates - These are disabled by default. To enable this certificate, select a DoD certificate and click **Enable** in the **View Certificate Details** pop-up. A DoD certificate allows a browser to trust Web sites whose secure communications are authenticated by a DoD agency.
- Alcatel root certificate - These are disabled by default. To enable this certificate, select a DoD certificate and click **Enable** in the **View Certificate Details** pop-up. An Alcatel root certificate allows Alcatel Lucent IP phones to authenticate using EAP-TLS.

The following table describes the **Certificate Trust List** parameters:

Table 316: *Certificate Trust List Parameters*

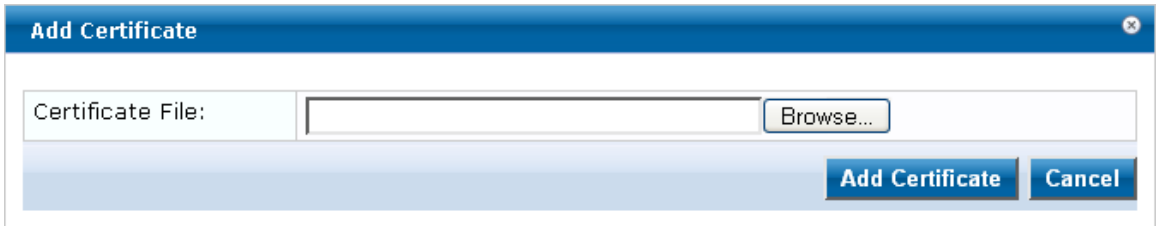
Parameter	Description
Subject	Displays the Distinguished Name (DN) of the subject field in the certificate.
Validity	Indicates whether the CA certificate is valid or expired.
Enabled	Indicates whether the CA certificate is enabled or disabled.

Adding a Certificate

1. Navigate to **Administration > Certificates > Trust List**.
2. Click the **Add** link on the top right section of the page.
3. On the **Add Certificate** pop-up, click **Choose File** to browse the certificate file.
4. Click **Add Certificate**.

The following figure displays the **Add Certificate** pop-up:

Figure 501: *Add Certificate Pop-up*



The following table describes the **Add Certificate** parameters:

Table 317: *Add Certificate Parameters*

Parameter	Description
Certificate File	Click **Choose File** to browse the certificate file.

Viewing a Certificate Detail

To view the details of a certificate, click any one of the entries from the certificate trust list. From the **View Certificate Details** pop-up, clicking the **Enable** button enables the CA certificate. When you enable a CA certificate, Policy Manager considers the entity whose certificate is signed by this CA to be trusted.

Deleting a Certificate

To delete a certificate:

1. Navigate to **Administration > Certificates > Trust List**.
2. Select the check box to the left of the certificate.
3. Click **Delete**.

Certificate Revocation Lists

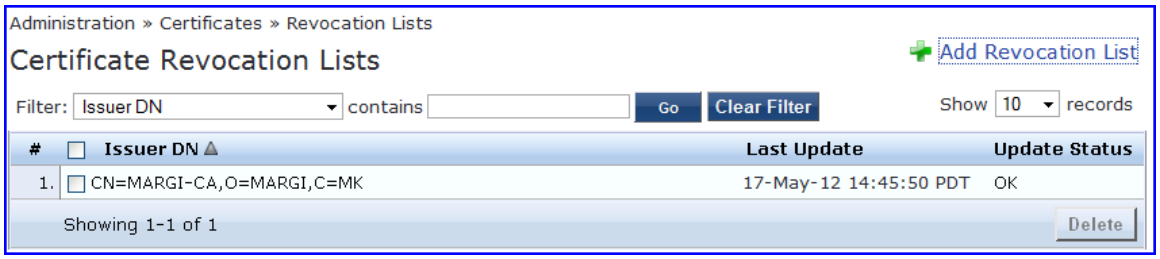
To add a revocation list, click **Add Revocation List**. To delete a revocation list, select the check box to the left of the list and then click **Delete.**

This section describes the following topics:

Certificate Revocation Lists Main Page

To display available Revocation Lists, navigate to **Administration > Certificates > Revocation Lists**. The following figure displays the **Certificate Revocation Lists** page:

Figure 502: *Certificate Revocation Lists Page*



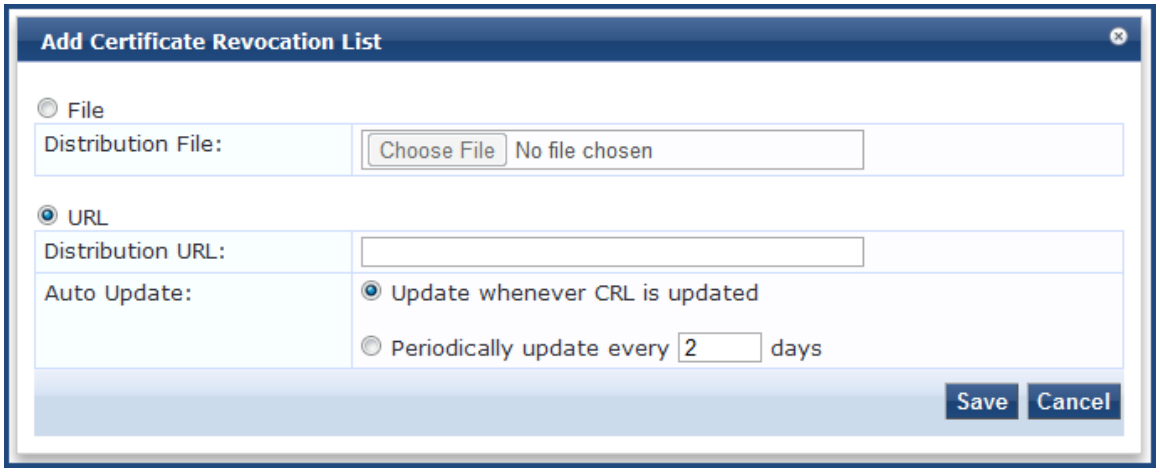
Adding a Certificate Revocation List

To add a certificate revocation list:

1. Navigate to **Administration > Certificates > Revocation Lists**.
2. Click the **Add** link on the top right section of the page. Configure the parameters based on Table 318.
3. Click **Save**.

The following figure displays the **Add Certificate Revocation List** pop-up:

Figure 503: *Add Certificate Revocation List Pop-up*



The following table describes the **Add Certificate Revocation List** parameters:

Table 318: *Add Certificate Revocation List Parameters*

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

Deleting a Certificate Revocation List

To delete a certificate revocation list:

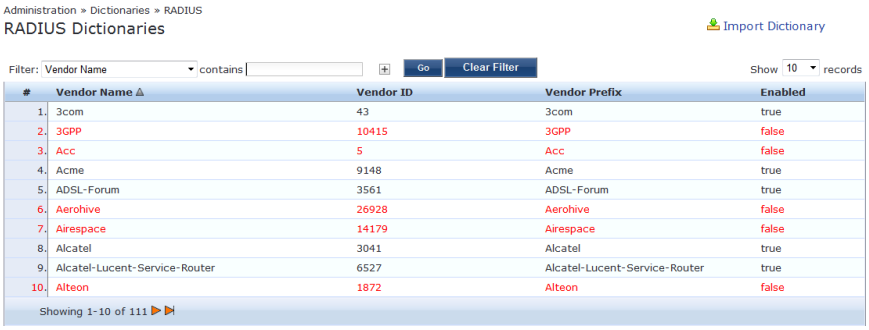
1. Navigate to **Administration > Certificates > Revocation Lists**.
2. Select the check box to the left of the certificate revocation list.
3. Click **Delete.**

RADIUS Dictionary

This page includes the list of available vendor dictionaries. To configure RADIUS dictionaries, navigate to **Administration > Dictionaries > RADIUS**.

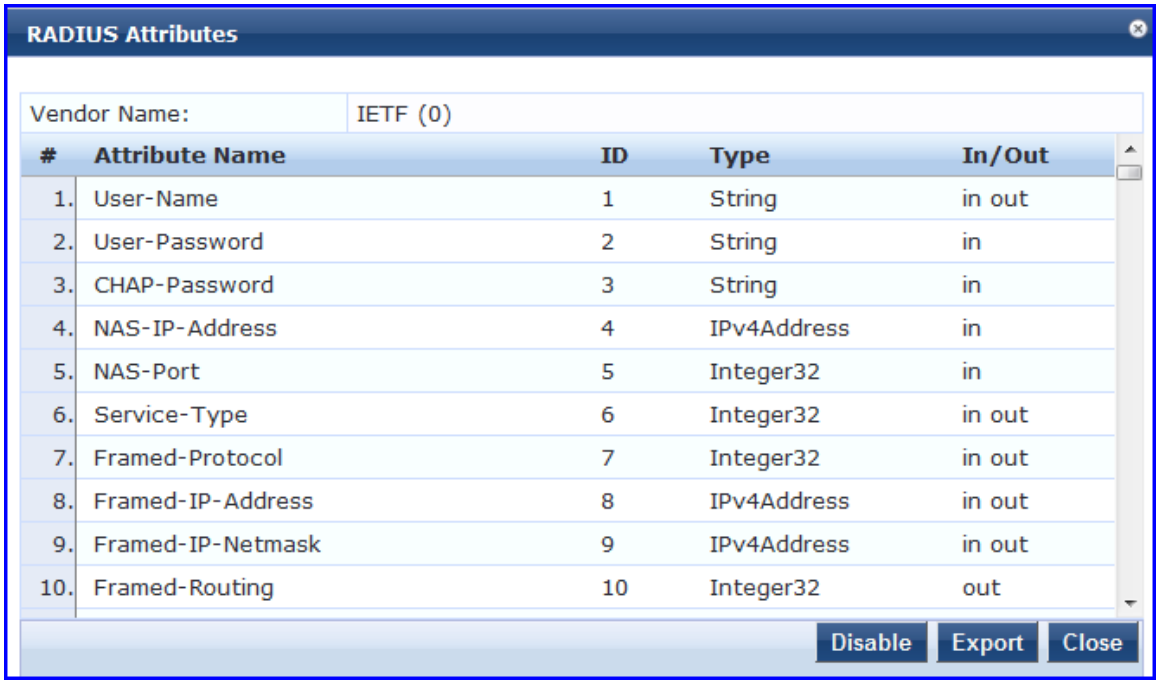
The following figure displays the **RADIUS Dictionaries** page:

Figure 504: *RADIUS Dictionaries*



Click on a row view the dictionary attributes, to enable or disable the dictionary, and to export the dictionary. For example, click on vendor IETF to see all IETF attributes and their data type. The following figure displays the RADIUS IETF dictionary attributes pop-up:

Figure 505: *RADIUS Attributes Pop-up*



The following table describes the **RADIUS Attributes** parameters:

Table 319: *RADIUS Dictionary Attributes Parameters*

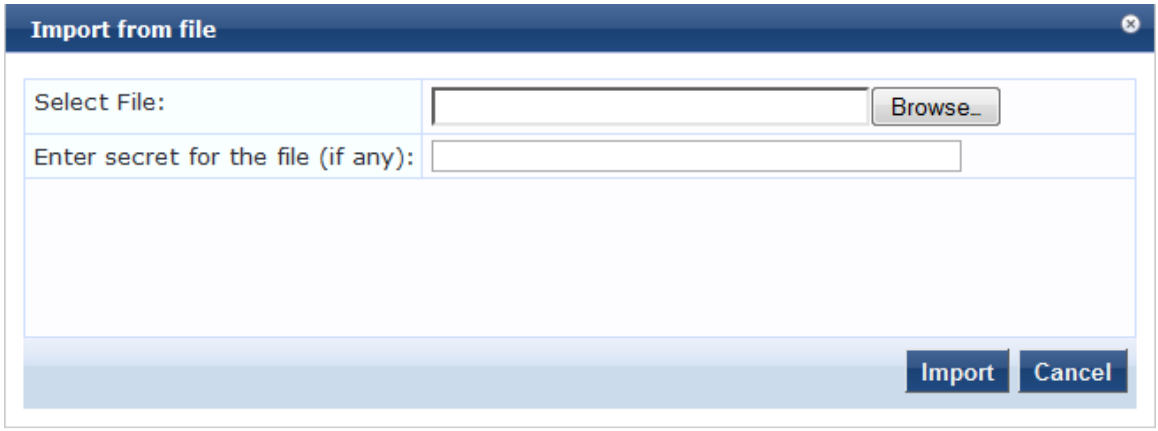
Parameter	Description
Export	Click to save the dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.
Enable/Disable	Enable or disable this dictionary. Enabling a dictionary makes it appear in the Policy Manager rules editors (Service rules, Role mapping rules, etc.).

Import RADIUS Dictionary

You can add additional dictionaries using the Import too. To add a new vendor dictionary, navigate to **Administration > Dictionaries > RADIUS**, and click the **Import** link. To edit an existing dictionary, export an existing dictionary, edit the exported XML file, and then import the dictionary. To view the contents of the RADIUS dictionary, sorted by Vendor Name, Vendor ID, or Vendor Prefix, navigate to **Administration > Dictionaries > RADIUS**.

The following figure displays the **Import from file** pop-up:

Figure 506: *Import RADIUS Dictionary Pop-up*



The following table describes the **Import from file** parameters:

Table 320: *Import from file Parameters*

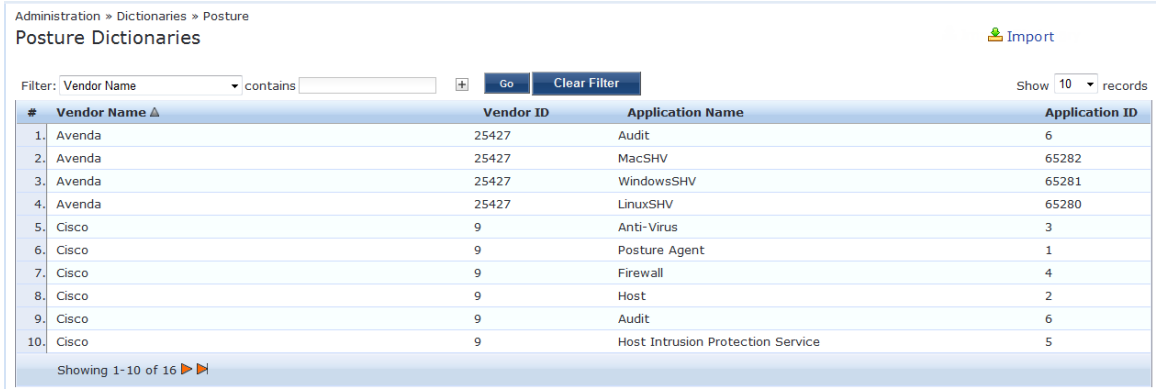
Parameter	Description
Select File	Browse to select the file that you want to import.
Enter secret for the file (if any)	If the file that you want to import is password protected, enter the secret here.

Posture Dictionary

To add a vendor posture dictionary, click on **Import**. To edit an existing dictionary, export an existing dictionary, edit the exported XML file, and then import the dictionary. To view the contents of the Posture dictionary, navigate to **Administration > Dictionaries > Posture** and sort by Vendor Name, Vendor ID, Application Name, or Application ID.

The following figure displays the **Posture Dictionaries** page:

Figure 507: *Posture Dictionaries*



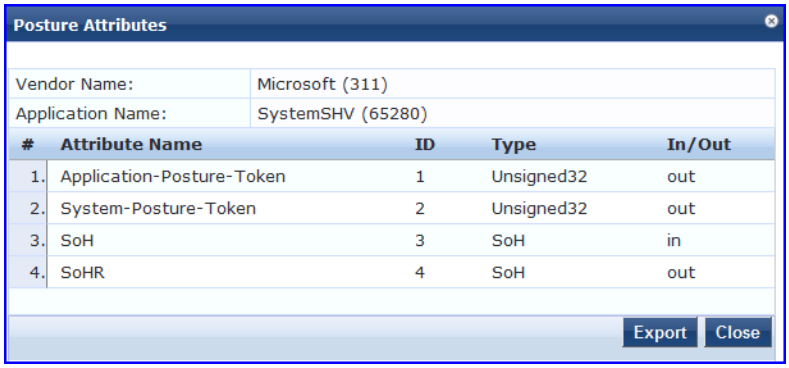
The following table describes the **Posture Dictionaries** parameters:

Table 321: *Posture*

Parameter	Description
Import	Click to open the **Import Dictionary** pop up.

Click 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. The following figure displays the **Posture Attributes** pop-up.

Figure 508: *Posture Attributes Pop-up*



The following table describes the **Posture Attributes** parameters:

Table 322: *Posture Attributes Parameters*

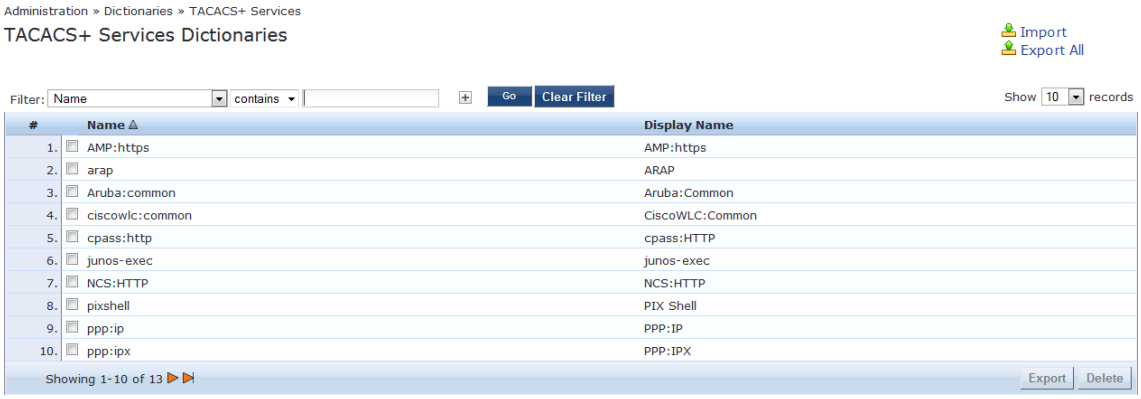
Parameter	Description
Export	Click to save the posture dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.

TACACS+ Services Dictionary

To view the contents of the TACACS+ service dictionary, navigate to **Administration > Dictionaries > TACACS+ Services** and sort by Name or Display Name. To add a new TACACS+ service dictionary, click the **Import** link. To add or modify attributes in an existing service dictionary, select the dictionary, export it, make edits to the XML file, and import it back into Policy Manager.

The following figure displays the **TACACS+ Services Dictionaries** page:

Figure 509: *TACACS+ Services Dictionaries Page*



The following table describes the **TACACS+ Services Dictionaries** parameters:

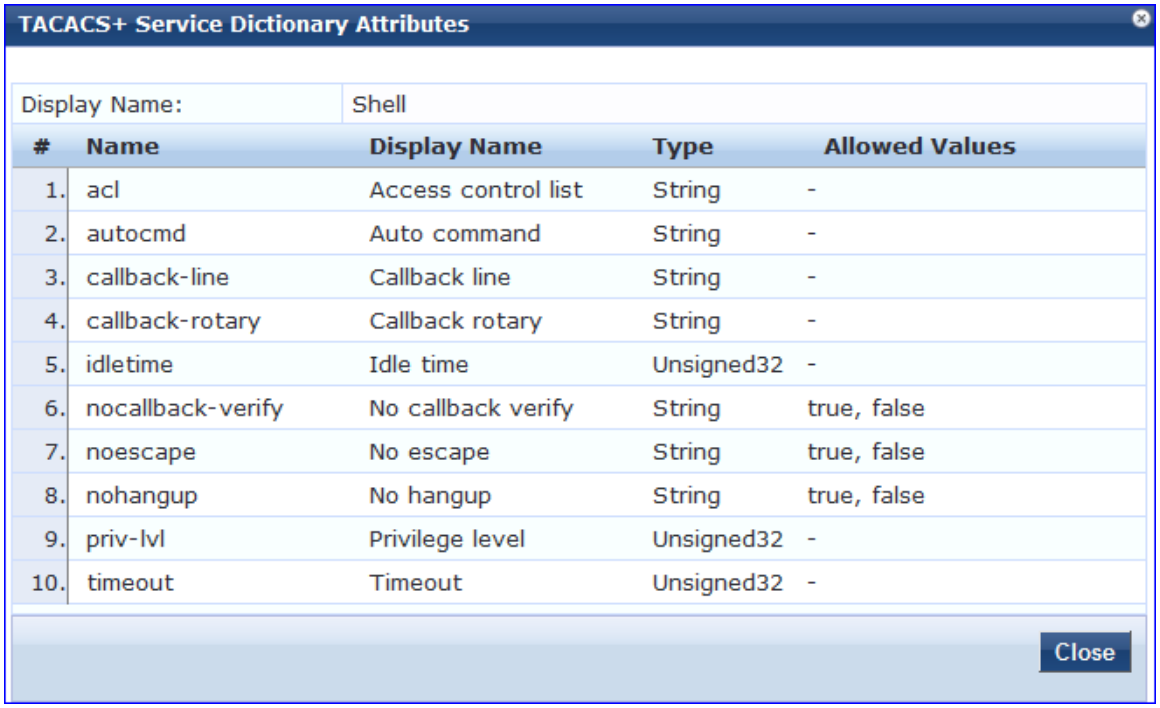
Table 323: *TACACS+ Services Dictionaries Parameters*

Parameter	Description
Import	Click to open the **Import Dictionary** pop up. Import the dictionary (XML file).
Export All	Export all TACACS+ services into one XML file containing multiple dictionaries.

To export a specific service dictionary, select a service and click **Export**. To see all the attributes and their data types, click a service row. For example, click shell service to see all shell service attributes and their data type.

The following figure displays the **TACACS+ Service Dictionary Attributes** pop-up:

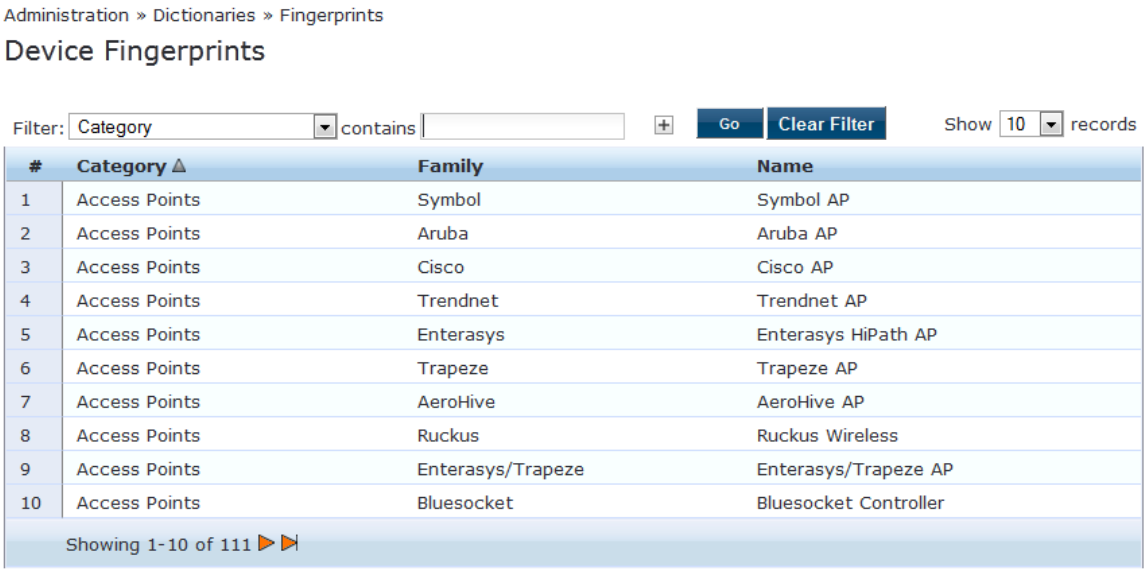
Figure 510: *TACACS+ Service Dictionary Attributes Pop-up*



Fingerprints Dictionary

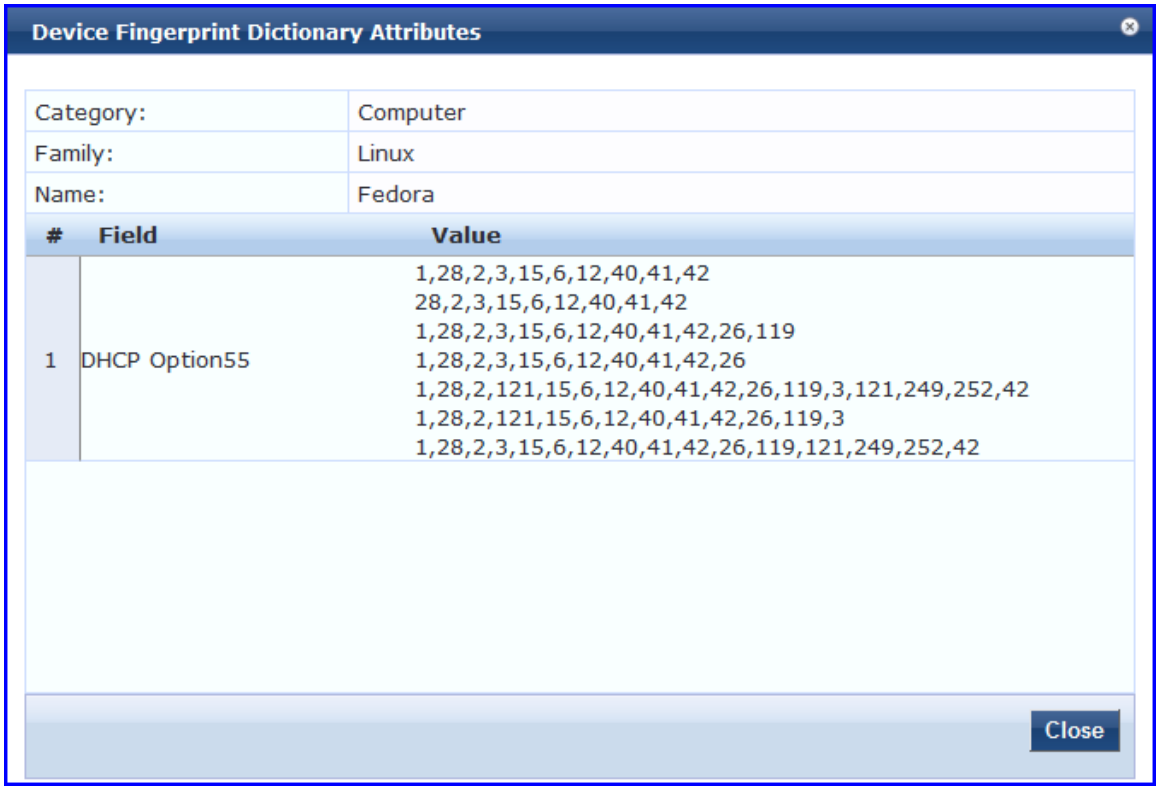
The **Device Fingerprints** page shows a listing of all the device fingerprints recognized by the Profile module. These fingerprints are updated from the Dell W-ClearPass Update Portal (see Software Updates on page 556 for more information). To view the contents of the fingerprints dictionary, navigate to **Administration > Dictionaries > Fingerprints**. The following figure displays the **Device Fingerprints** page.

Figure 511: *Device Fingerprints Page*



You can click on a line in the Device Fingerprints list to drill down and view additional details about the category. The following figure displays the **Device Fingerprint Dictionary Attributes** pop-up.

Figure 512: *Device Fingerprint Dictionary Attributes Pop-up*

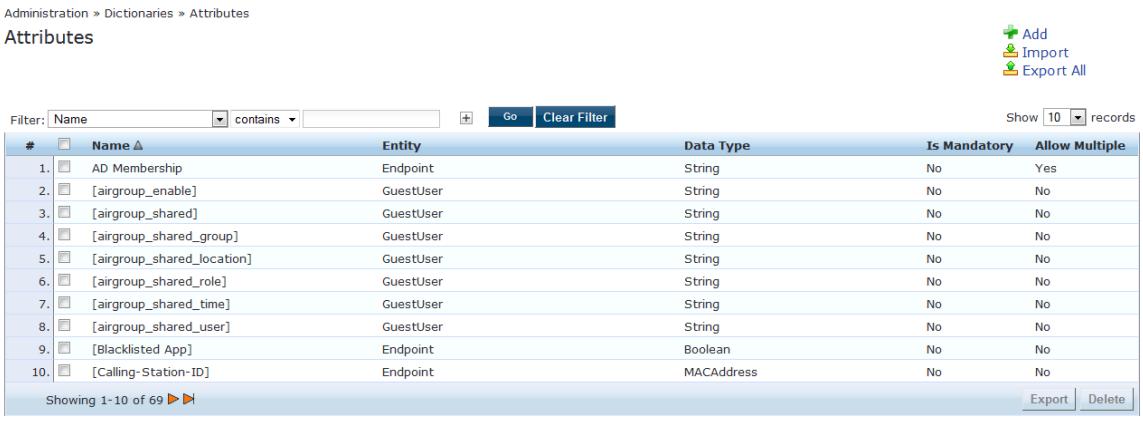


Attributes

The **Attributes** dictionary page allows you to specify unique sets of criteria for Local Users, Guest Users, Endpoints, and Devices. This information can then be with role-based device policies for enabling appropriate network access. To view the contents of the attributes dictionary, navigate to **Administration > Dictionaries > Attributes**.

The following figure displays the **Attributes** dictionary page:

Figure 513: *Attributes page*



The following table describes the **Attributes** dictionary parameters:

Table 324: *Attributes Dictionary Parameters*

Parameter	Description
Filter	Use the drop-down list to create a search based on the available Name, Entity, Data Type, Is Mandatory, or Allow Multiple settings.
Name	The name of the attribute.
Entity	Shows whether the attribute applies to a Local User, Guest User, 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.

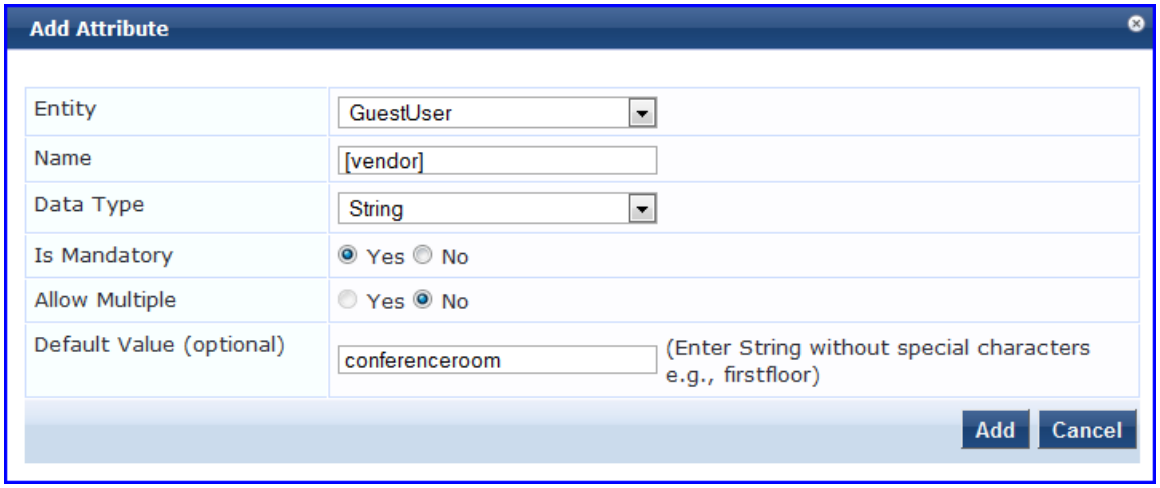
The **Attributes** dictionary page provides the following interfaces for configuration:

- Add Attributes on page 545
- Import Attributes on page 546
- Export Attributes on page 547
- Export on page 547

Add Attributes

To add an attribute dictionary, select **Add** in the upper right section of the page. The following figure displays the **Add Attribute** pop-up:

Figure 514: *Add Attributes Pop-up*



Enter the 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**.

The following table describes the **Add Attribute** parameters:

Table 325: *Attribute Setting Parameters*

Parameter	Description
Entity	Specify whether the attribute applies to a Local User, Guest User, Device, or Endpoint.
Name	Enter a unique ID for this attribute.
Data Type	Specify whether the data type is boolean, date, date-time, day, IPv4 address, integer, list, MAC address, string, text, or time of day.
Is Mandatory	Specify whether the attribute is required for a specific entity.
Allow Multiple	Specify whether multiple attributes are allowed for an entity. **NOTE:** Multiple attributes are not permitted if **Is Mandatory** is specified as **Yes**.
Default Value (optional)	Enter the default attribute value. This field is optional.

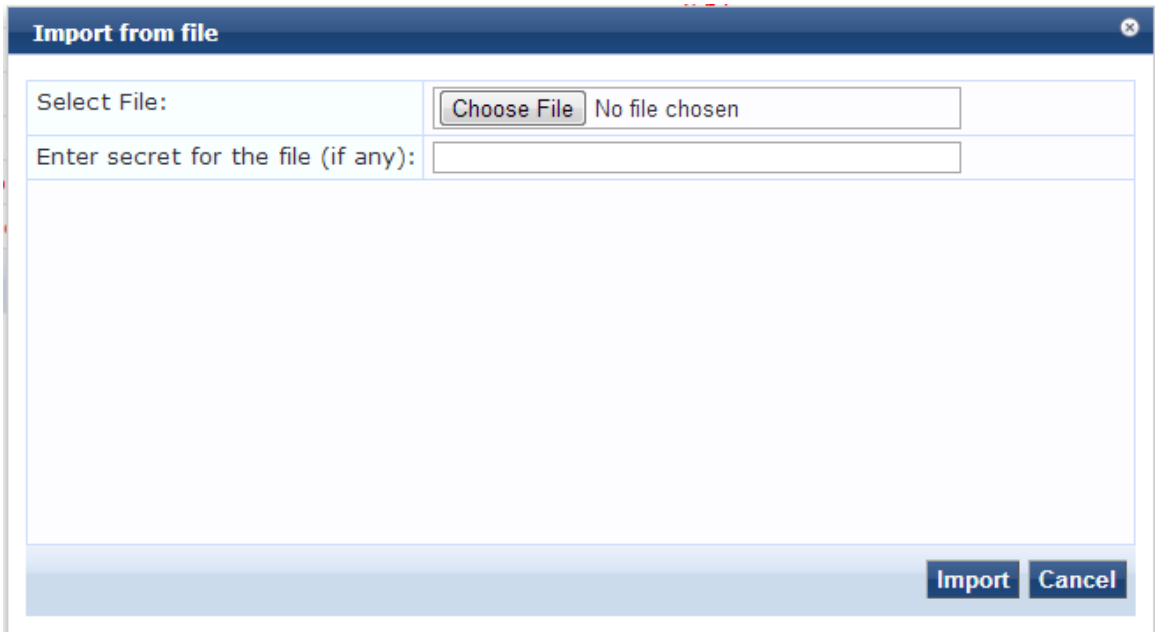
Import Attributes

Select **Import** on the top right section 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.

The following figure displays the **Import from file** pop-up:

Figure 515: *Import from file Pop-up*



The following table describes the **Import from file** parameters:

Table 326: *Import From File Setting Parameters*

Parameter	Description
Select File	Browse to select the file that you want to import.
Enter secret for the file	If the file that you want to import is password protected, enter the secret here.

Export Attributes

Select **Export All** on the upper right section of the page to export all attributes. The **Export Attributes** button saves the **Attributes.zip** file. The zip file consists of the server certificate (.crt file) and the private key (.pvk file).

Export

On the **Attributes** dictionary page, select an attribute entry. Thereafter, click the **Export** button on the lower right section of the page. To export just one attribute, select it (check box at left) and click **Export.** Your browser will display its normal **Save As** dialog, in which to enter the name of the XML file to contain the export.

Applications Dictionaries

Application dictionaries define the attributes of the Onboard Policy Manager application and the type of each attribute. When Policy Manager is used as the Policy Definition Point (PDP), it uses the information in these dictionaries to validate the attributes and data types sent in a WEB-AUTH request. To view the contents of the application dictionary, navigate to **Administration > Dictionaries > Applications**.

The **Application Dictionaries** page provides the following interfaces for configuration:

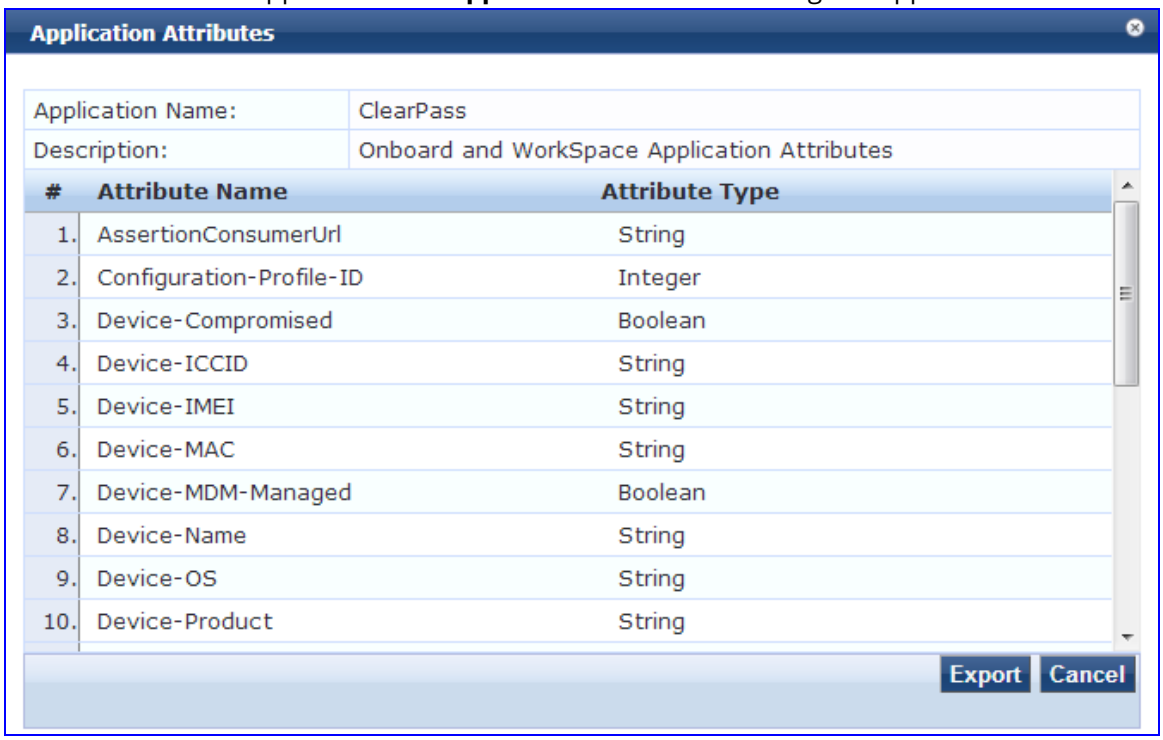
- Viewing an Application Dictionary on page 547
- Deleting an Application Dictionary on page 548
- Importing on page 35
- Exporting on page 36

Viewing 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.



Deleting an Application Dictionary

In general, there is no need to delete an application dictionary. They have no effect on Policy Manager performance. To delete an application dictionary:

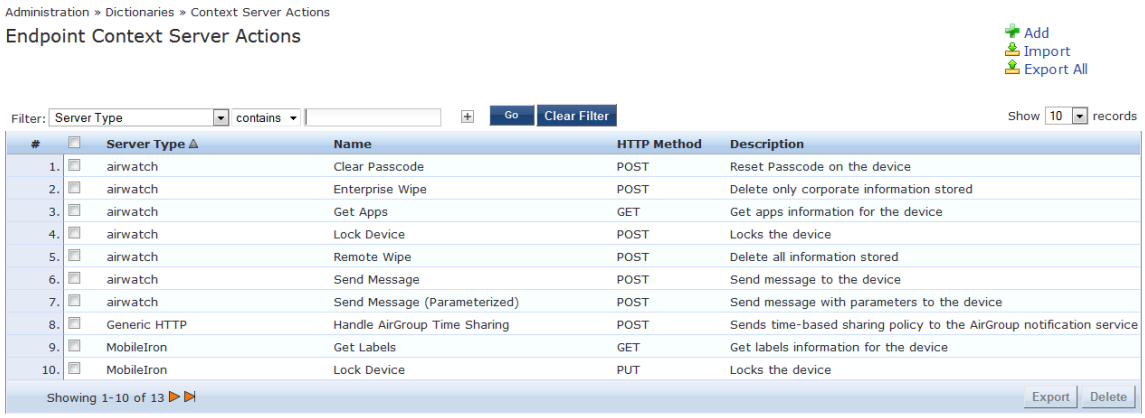
1. Go to **Administration > Dictionaries > Applications**.
2. Click the check box next to an application name.
3. Click **Delete**.

Endpoint Context Server Actions

Use the **Endpoint Context Server Actions** page to configure actions that are performed on endpoints, such as locking a device, triggering a remote, or enterprise wipe, and so on. The **Context Server Actions** page displays the report that shows information about all configured Endpoint Context Server Actions. To view the contents of the endpoint context server actions, navigate to **Administration > Dictionaries > Context Server Actions** > **Endpoint Context Server Actions** page.

The following figure displays the **Endpoint Context Server Actions** page:

Figure 516: *Endpoint Context Server Actions Page*



The following table describes the **Endpoint Context Server Actions** parameters:

Table 327: *Endpoint Context Server Actions Parameters*

Parameter	Description
Server Type	Specifies the server type configured when the server action was configured.
Action Name	Specifies the name of the action such as Enterprise Wipe, Lock Device, and so on.
HTTP Method	Specifies the HTTP method selected when the server action was configured.
Description	Specifies the description of the action. For example, you can provide a description as **Delete all stored information** if the configured action is **Remote Wipe**.

Adding an Endpoint Context Server Action Item

Enter information in the tabs described in the following table. Click **Add** after providing the required information. To modify existing Endpoint Context Server Details, select a row and change detail, make any necessary changes, and then click **Save**. The **Endpoint Context Server Details - Action** page contains the following tabs:

- Action Tab on page 550
- Header Tab on page 551
- Content Tab on page 552
- Attributes Tab on page 553

Action Tab

Use the **Action** tab to specify the server type, action name, HTTP method, and URL for the server action. The following figure displays the **Endpoint Context Server Details - Action** tab:

Figure 517: *Endpoint Context Server Details - Action Tab*

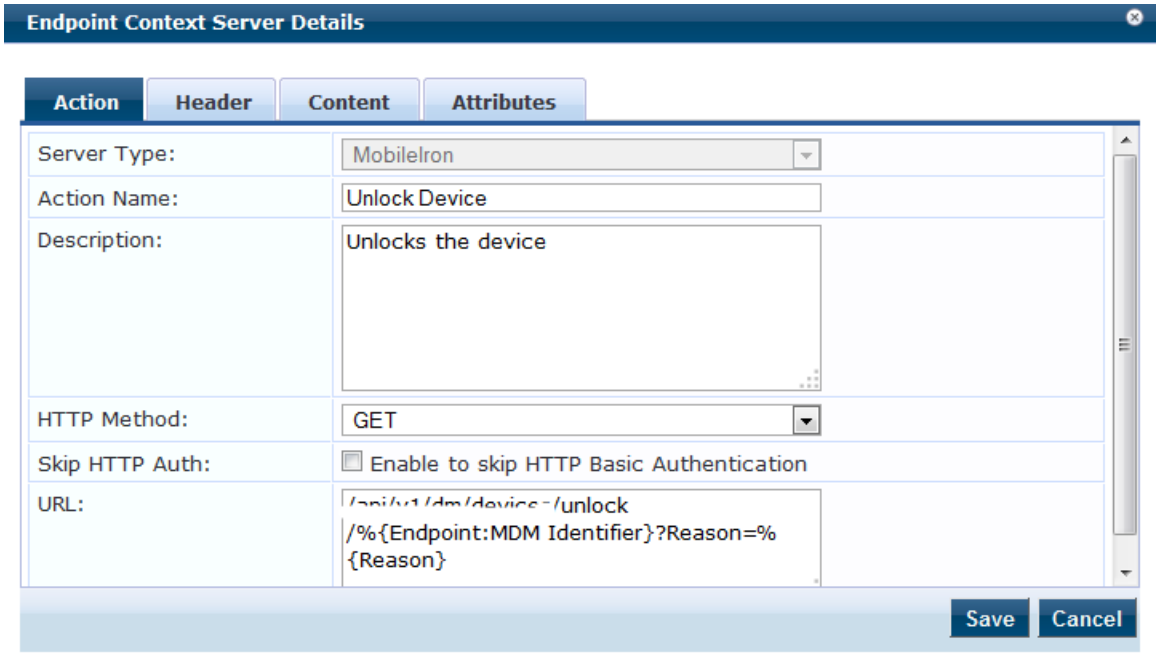


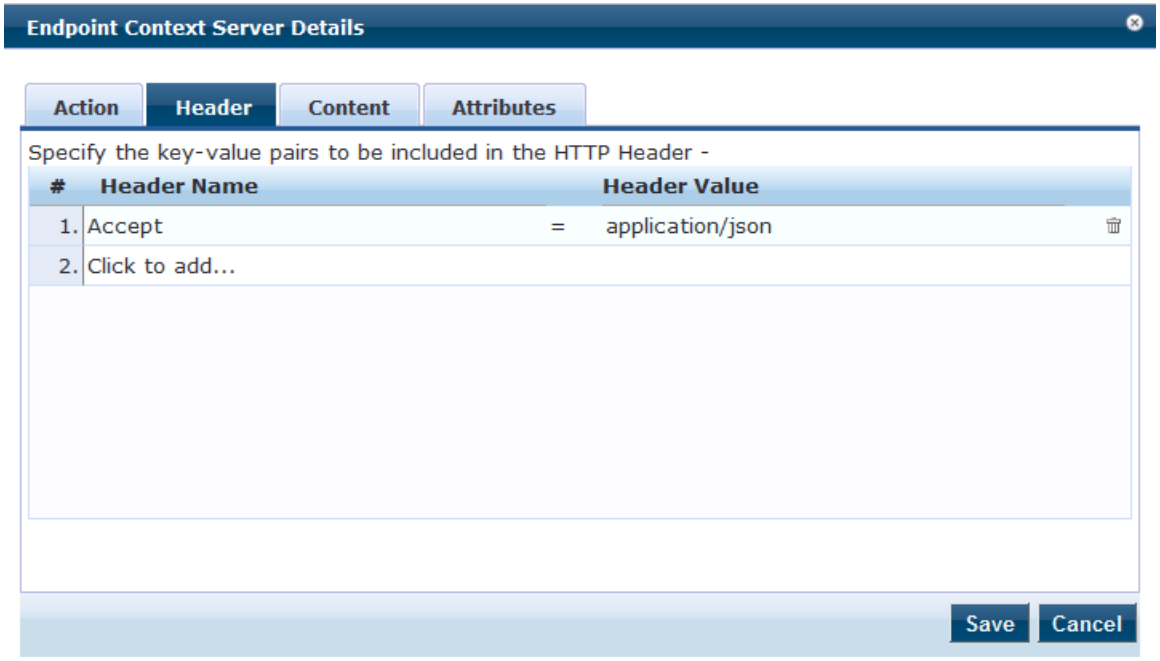
Table 328: *Endpoint Context Server Details - Action Tab Parameters*

Parameter	Description
Server Type	Specifies the server type configured when the server action was configured. You can select the server type from the drop-down list.
Server Name	Lists the context servers specific to the server type selected in the **Server Type** field. This field is visible only if you selected the service type **Generic HTTP**.
Action Name	Specifies the name of the action configured.
Description	Provides additional information about the action specified.
HTTP Method	Specifies the HTTP method selected when the server action was configured.
Skip HTTP Auth	Select this check box to disable the HTTP basic authentication for endpoint context server actions. This exposes the context server attributes such as Username, Password, and Server Name to be used in context server actions.
URL	Specifies the URL for the selected HTTP method.

Header Tab

Use the **Header** tab to specify the key-value pairs to be included in the HTTP header. The following figure displays the **Header** tab:

Figure 518: *Endpoint Context Server Details - Header Tab*



The following table describes the **Endpoint Context Server Details - Header** parameters:

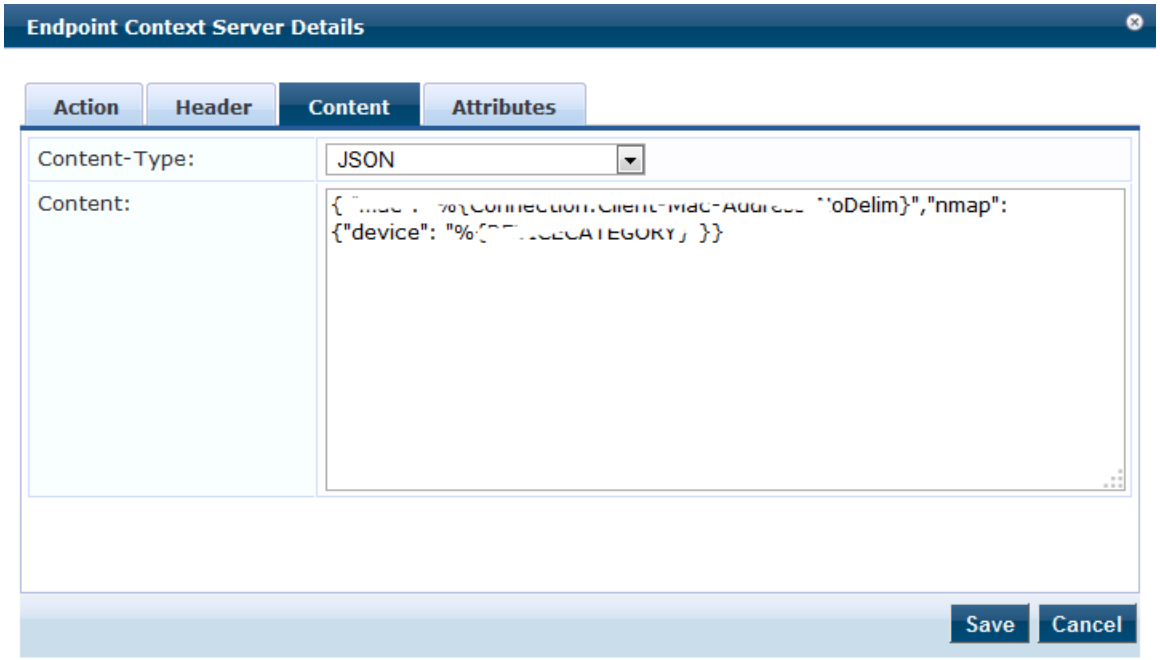
Table 329: *Endpoint Context Server Details - Header Tab Parameters*

Parameter	Description
Header Name	Specify the name of the header to be included in the HTTP header.
Header Value	Specify the value of the header specific to the name to be included in the HTTP header.

Content Tab

Use the **Content** tab to specify a content type. The following figure displays the **Endpoint Context Server Details - Content** tab:

Figure 519: *Endpoint Context Server Details - Content Tab*



The following table describes the **Endpoint Context Server Details - Content** parameters:

Table 330: *Endpoint Context Server Details - Content Tab Parameters*

Parameter	Description
Content-Type	Specify the type of the content. Select from the following options: • CUSTOM • HTML • JSON • PLAIN • XML
Content	Specify the content. For example, { "mac": "%{Connection:Client-Mac-Address-NoDelim} ","nmap": {"device": "%{DEVICECATEGORY}"}}.

Attributes Tab

Use **Attributes** tab to specify the mapping for attributes used in the content to parametrized values from the request. The following figure displays the **Endpoint Context Server Details - Attributes** tab:

Figure 520: *Endpoint Context Server Details - Attributes Tab*

The following table describes the **Endpoint Context Server Details - Attributes** parameters:

Table 331: *Endpoint Context Server Details - Attributes Tab Parameters*

Parameter	Description
Attribute Name	Enter attribute names and assign values to those names. These name/value pairs are included in context server actions.
Attribute Value	Enter the value for the selected name in the **Attribute Name** field.

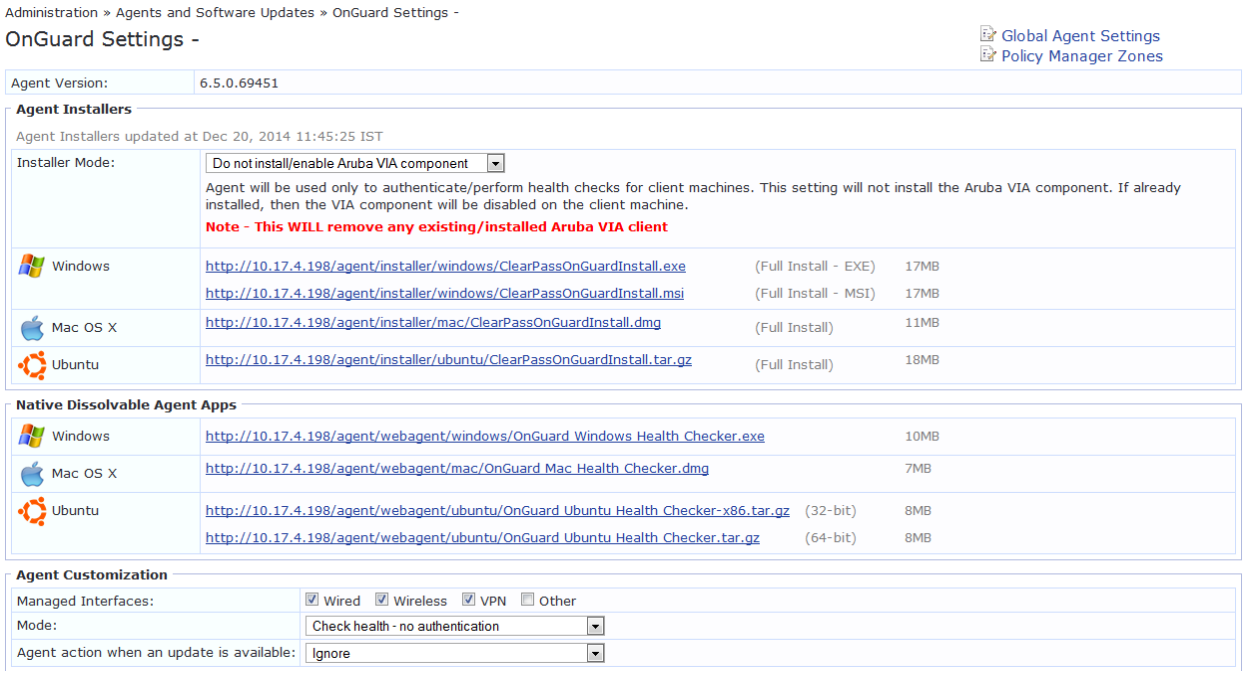
OnGuard Settings

Use the **OnGuard Settings** page to configure the agent deployment packages. Once the configuration is saved, agent deployment packages are created for Windows and Mac OS X operating systems and provided at a fixed URL on the Dell Networking W-ClearPass Policy Manager appliance. This URL can then be published to the user community. The agent deployment packages can also be downloaded to another location.

OnGuard Settings Main Page

Navigate to **Administration** > **Agents and Software Updates** > **OnGuard Settings**. The following figure displays the **OnGuard Settings** page:

Figure 521: *OnGuard Settings*



The following table describes the **OnGuard Settings** parameters:

Table 332: *OnGuard Settings Parameters*

Parameter	Description
Global Agent Settings	Configure the global parameters for OnGuard agents. For more information on configuring global agent settings, see Global Agent Settings on page 1.
Policy Manager Zones	Configure the network (subnet) for a Policy Manager Zone. For more information on configuring Policy Manager zones, see Policy Manager Zones on page 1.
Agent Version	Specifies the current agent version.
Agent Installers	
Installer Mode	Specify the action to be taken from the following options when the Dell VIA component is used to provide VPN-based access: • **Do not install/enable VIA component** • **Install and enable VIA Component**
Windows	Use the download link to download OnGuard Agent for Windows.This binary file is in .exe and .msi formats.
Mac OS X	Use the download link to download OnGuard Agent for Mac OS X. This binary file is in .DMG format.

Table 332: *OnGuard Settings Parameters (Continued)*

Parameter	Description
Ubuntu	Use the download link to download Ubuntu Agent for Linux. This binary file is in .tar.gz format.
Native Dissolvable Agent Apps	
Windows	Click the URL to download Native Dissolvable Agent for Windows.
Mac OS X	Click the URL to download Native Dissolvable Agent for Mac OS X.
Ubuntu	Click the URL to download Native Dissolvable Agent for Ubuntu. You can download the .tar.gz files specific to 32-bit and 64-bit systems.
Agent Customization	
Managed Interfaces	Select the type(s) of interfaces that OnGuard will manage on the endpoint. Select from the following options: • **Wired** • **Wireless** • **VPN** • **Other**
Mode	Select one of the following options: • **Authenticate - no health checks** - OnGuard collects username/password but does not perform health checks on the endpoint. • **Check health - no authentication** - OnGuard does not collect username/password. • **Authenticate with health checks** - OnGuard collects username/password and also performs health checks on the endpoint. Username/Password Text: The label for the username/password field on the OnGuard agent. This setting is not valid for the **Check health - no authentication** mode.
Username text	The label for the username field on the OnGuard agent. This setting is not valid for the **Check health - no authentication** mode.
Password text	Enter the password field on the OnGuard agent. This setting is not valid for the **Check health - no authentication** mode.
Agent action when an update is available	Determines what the agent does when an update is available. Select one of the following options: • **Ignore** - Dell Networking W-ClearPass Policy Manager ignores the available update. • **Notify User** - Dell Networking W-ClearPass Policy Manager notifies the user that an update is available. • **Download and Install** - Dell Networking W-ClearPass Policy Manager automatically downloads and installs an update is available.

Software Updates

This section describes the Dell Networking W-ClearPass Policy Manager server software update process.

Use the **Software Updates** page to register for and to receive live updates for:

- Posture updates, including Antivirus, Antispyware, and Windows Updates
- Profile data updates, including Fingerprint
- Software upgrades for the ClearPass family of products
  - Patch binaries, including Onboard, Guest Plugins, and Skins

You can also:

- Reinstall a patch in the event the previous installation attempt fails.
- Uninstall a skin, translation, or plug-in.

The Dell Networking W-ClearPass Policy Manager checks for available updates to the ClearPass webservice server. The administrator can download and install these updates directly from the **Software Updates** page. The first time the Subscription ID is saved, Dell Networking W-ClearPass Policy Manager performs the following:

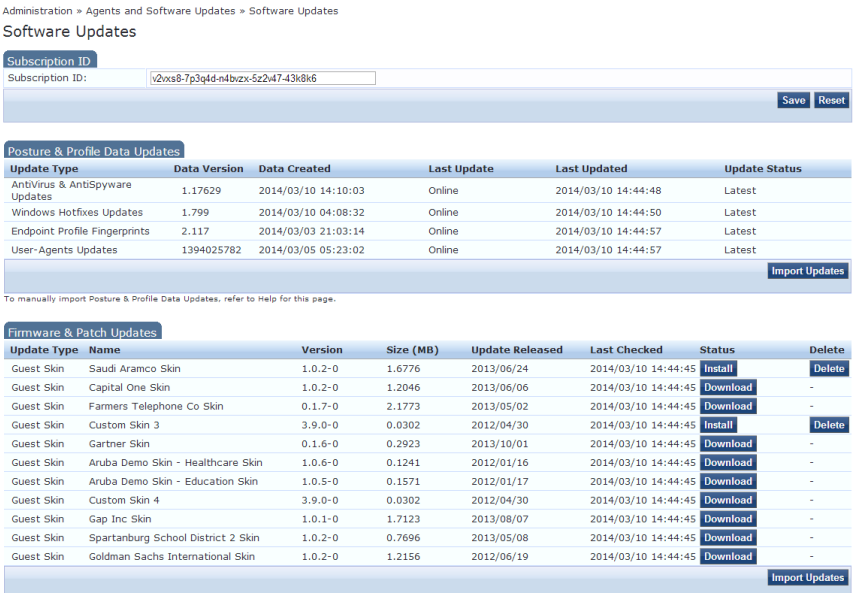
- Contacts the webservice to download the latest Posture & Profile Data updates.
- Checks for any available firmware and patch updates.

This section describes the following topics:

Software Updates Main Page

Navigate to **Administration > Agents and Software Updates > Software Updates**. The following figure displays the **Software Updates** main page:

Figure 522: *Software Updates Page*



The following table describes the **Software Updates** parameters:

Table 333: *Software Updates Parameters*

Parameter	Description
Subscription ID	
Subscription ID	Enter the Subscription ID provided to you. This text box is enabled only on a Publisher node. You can opt out of automatic downloads at any time by saving an empty Subscription ID.
Posture & Profile Data Updates	
Import Updates	If this Dell Networking W-ClearPass Policy Manager server is not able to reach the webservice server, use **Import Updates** to import (upload) the Posture and Profile Data into this server. You can download the data from the webservice server by accessing the following URL: *https://clearpass.dell-pcw.com/cppm/appupdate/cppm_apps_updates.zip* When prompted, enter the provided Subscription ID for the username and the password. **NOTE:** In a cluster, the **Import Updates** option is available on the Publisher node only.
Firmware & Patch Updates	
Import Updates	If the server is not able to reach the webservice server, click **Import Updates** to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server. These patch binaries will appear in the table and can be installed by clicking on the **Install** button. When logged in as *appadmin*, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands: • **system update** (for patches) • **system upgrade** (for upgrades) If a patch requires a prerequisite patch, that patchs' **Install** button will not be enabled until the prerequisite patch is installed.
Install	The **Install** button appears after the update has been downloaded. When you click **Install**, the installation of the update starts and the Install Update dialog box displays, showing the log messages being generated.
Re-Install	Click **Re-Install** to reinstall a patch in the event the previous attempt to install fails. Reinstalling a patch is available only for the last installed patch.
Uninstall	Click **Uninstall** to uninstall a skin, translation, or plugin.
Needs Restart	The **Needs Restart** link appears when an update needs a reboot of the server in order to complete the installation. Clicking this link displays the **Install Update** dialog box, which shows the log messages generated during the installation.
Installed	The **Installed** link appears when an update has been successfully installed. Clicking this link displays the **Install Update** dialog box, which shows the log messages generated during the installation.

Table 333: *Software Updates Parameters (Continued)*

Parameter	Description
Install Error	This link appears when an update install encounters an error. Clicking this link displays the **Install Update** dialog box, which shows the log messages generated during the install.
Other	
Check Status Now	Click this button to perform an on-demand check for available updates. **Check Status Now** applies to updates only on a publisher node, as well as Firmware & Patch Updates.
Delete	Use this option to delete a downloaded update.

The Firmware & Patch Updates table shows only the data that is known to webservice or imported using the **Import Updates** button.

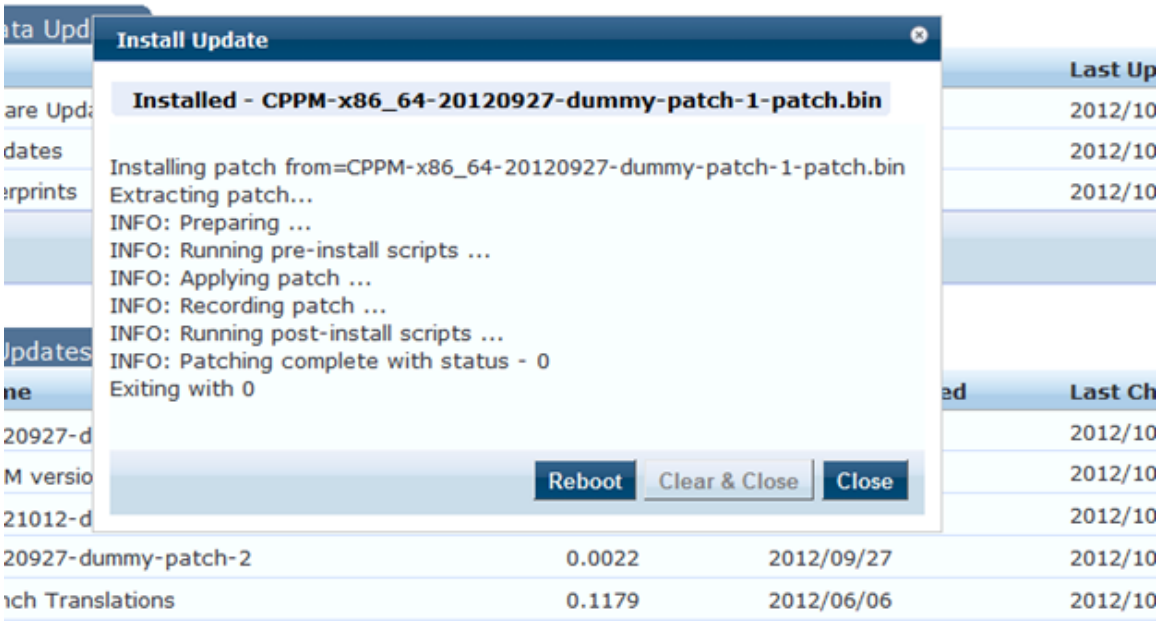
Install Update Dialog Box

The **Install Update** dialog box shows the log messages generated during the installation of an update. This popup appears when you click the **Install** button.

If the popup is closed, you can bring it up again by clicking the **Install in progress...** link while the installation is in progress, or by clicking the **Installed**, **Install Error**, or **Needs Restart** link when the installation is completed.

The following figure displays the **Install Update** pop-up:

Figure 523: *Install Update Pop-up*



The following table describes the **Install Update** parameters:

Table 334: *Install Update Parameters*

Parameter	Description
Reboot	The **Reboot** button appears only for updates that require a reboot to complete the installation. To initiate a reboot of the server, click **Reboot**.
Clear & Close	Click this button to delete the log messages and close the popup. **Clear & Close** also removes the corresponding row from the Firmware & Patch Updates table.
Close	Click this button to close the dialog box.

To delete the log messages from a failed installation, use the **Clear & Close** button on the **Install Update** dialog box. After the log messages are cleared, attempt the installation again.

System Events (as seen on the **Monitoring > Event Viewer** page) show records for events, such as communication failures with webservice, successful or failed download of updates, and successful or failed installation of updates.

The Dell Networking W-ClearPass Policy Manager server contacts the webservice server every hour in the background to download any newly available Posture & Profile Data updates. The current list of firmware and patch updates is queried from webservice every day at a random minute between 4:00 a.m and 5:00 a.m.

Any new list of firmware and update patches that are available are noted by the Policy Manager server automatically and shown in the UK that they are available for download and installation. The webservice itself is refreshed with the Antivirus and Antispyware data hourly, with Windows Updates daily. Fingerprint data and Firmware & Patches are refreshed as and when new ones are available.

An event is generated and displayed in the **Event Viewer** with the list of new updates that are available. If the event affects an SMTP server, Alert Notification email addresses are configured, and an email from the Publisher is sent with the list of downloaded images.

Reinstalling a Patch

The Reinstall Patch feature allows the administrator to reinstall a patch in the event the previous attempt to install fails. You can only reinstall the last installed patch, which is indicated by a "!" symbol next to it in the Firmware & Patch Updates table on the **Administration > Agents and Software Updates > Software Updates** page.

To reinstall a patch or software update:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware & Patch Updates** section, observe the **Status** column.
3. To bring up the dialog that shows the logs, click the **Installed**, **Install Error**, or **Needs Restart** link.
4. To reinstall the patch or software update, click **Re-Install**.

   The **Install Update** screen closes and the re-installation process begins. A pop-up displays, showing the installation progress via log messages.

Uninstalling a Skin, Translation, or Plugin

The administrator can uninstall a Skin, Translation, or Plugin.

To uninstall one of these elements:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.

2. In the **Firmware & Patch Updates** section, observe the **Status** column.
3. To bring up the dialog that shows the logs, click the **Installed** link.
4. To uninstall the patch or software update, click **Uninstall**.

   The **Install Update** screen closes and the software is uninstalled.

Updating the Policy Manager Software

In the background, the Policy Manager Publisher node acts as master. Administration, configuration, and database write operations are allowed only on this master node. The Policy Manager appliance defaults to a Publisher node unless it is made a Subscriber node. A Policy Manager cluster can contain only one Publisher node. Cluster commands can be used to change the state of the node, hence the Publisher can be made a Subscriber.

MySQL is supported in versions 6.0 and newer. Dell does not ship MySQL drivers by default. If you require MySQL, contact Dell support to get the required patch. This patch does not persist across upgrades, so customers using MySQL should contact support before they upgrade.

This section describes the following topics:

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 Dell Networking W-ClearPass Policy Manager UI, navigate to **Administration > Agents and Software Updates > Software Updates**.
   - If a Subscription ID is entered, the server can communicate with the Web service. Available upgrades will be listed in the Firmware & Patches table. Download and install the upgrade, and then reboot the server.
   - If the Subscription ID is not entered, or if the appliance cannot communicate with the Web service, click **Import Updates** to upload the upgrade image that you received from Support (or through other means). Imported updates appears in the table and can be installed by clicking the **Install** button. The upgrade file is now available and can be specified in the **system upgrade** CLI command.

Alternatively, transfer the image file to a Policy Manager external machine and make it available via http or SSH.

1. Login to the Policy Manager appliance as *appadmin* user.
2. Use the **system upgrade** command, which upgrades your second partition, then reboot. Policy Manager boots with the upgraded image.

If you access the appliance via serial console, you should also be able to boot with the previous image by choosing that image in the Grub boot screen.

3. Verify that all configuration and session logs are restored and all services are running. Also verify that node-specific configuration such as the server certificate, log configuration and server parameters are also restored.

Upgrade the Image on all Appliances

Perform these steps to upgrade the image on all appliances in a Policy Manager cluster:

1. Upgrade the publisher Policy Manager first, and reboot with 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. In short, no configuration changes are possible on subscribers in this state.

NOTE

You can add a subscriber to the cluster from the User Interface: **Administration > Server Manager > Server Configuration > Make Subscriber**.

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 Dell Networking W-ClearPass Policy Manager UI and verify that the node is replicating and **Cluster Sync** is set to true.

NOTE

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**.

Contact Support

The **Administration > Support > Contact Support** page provides you with information on how to contact Dell Support.

The following figure displays the **Contact Support** page:

Figure 524: *Contact Support Page*

Remote Assistance

The Remote Assistance feature enables the Dell Networking W-ClearPass Policy Manager administrator to allow an Aruba Networks support engineer to remotely log in using Secured Shell (SSH) to the ClearPass Policy Manager server and also view the Dell Networking W-ClearPass Policy Manager UI to debug any issues customer is facing or to perform pro-active monitoring of the server.

This section describes the following topics:

Remote Assistance Process Flow

This topic describes the Remote Assistance process flow.

1. Administrator schedules a Remote Assistance session for a specific duration.
2. The Aruba Networks support contact receives an email with instructions and credentials to login to the remote system.
3. The session is terminated at the end of the specified duration.
4. The administrator can terminate a session before its stipulated duration from Dell Networking W-ClearPass Policy Manager UI.
5. The support contact can terminate the session before the time expires.

Configuring a Remote Assistance session through a CLI can be used if the Dell Networking W-ClearPass Policy Manager UI at the customer site is inaccessible.

The following figure displays the **Remote Assistance** session page:

Figure 525: *Remote Assistance Session Page*

The following table describes the **Remote Assistance** session parameters:

Table 335: *Remote Assistance Session Parameters*

Parameter	Description
Name	Name of the session.
Type	Indicates if the session is a one-time session or a periodic session. Move the cursor over the entry to view the schedule of the session.
Support Contact	The email address of the support contact.
Status	Provides the session state. Available states are: • Saving • Scheduled • Initiated • Running • Terminated • Failed

Table 335: *Remote Assistance Session Parameters (Continued)*

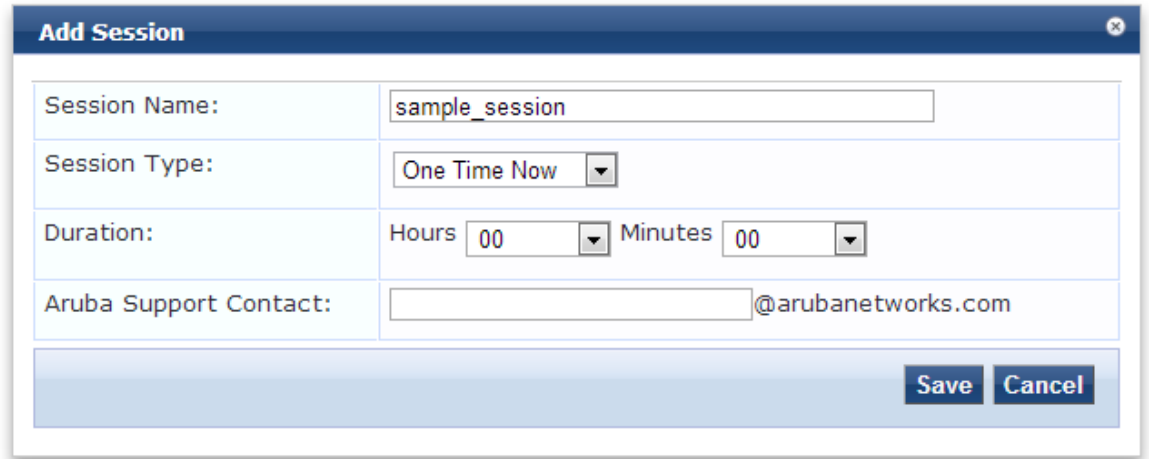
Parameter	Description
	NOTE: A session in any of Scheduled, Terminated, and Failed states can be edited and saved. Only a session in Running state can be terminated by selecting that session and clicking **Terminate**. A session in any of Scheduled, Terminated and Failed states can be deleted by selecting that session and clicking **Delete**. If a session fails, the Event Viewer indicates the cause of the failure.
Timestamp	The server time when the status was last updated.

Adding a Remote Assistance Session

The administrator can click the **Add Session** link to create a session on a Dell Networking W-ClearPass Policy Manager server in the cluster. Sessions can only be saved and deleted from the Publisher in a cluster. Sessions can be terminated from a Publisher or from Subscribers in a cluster.

To set up a session, click **Add Session**. The following figure displays the **Add Session** pop-up:

Table 336: *Add Session Pop-up*



The following table describes the **Add Session** parameters:

Table 337: *Add Session Parameters*

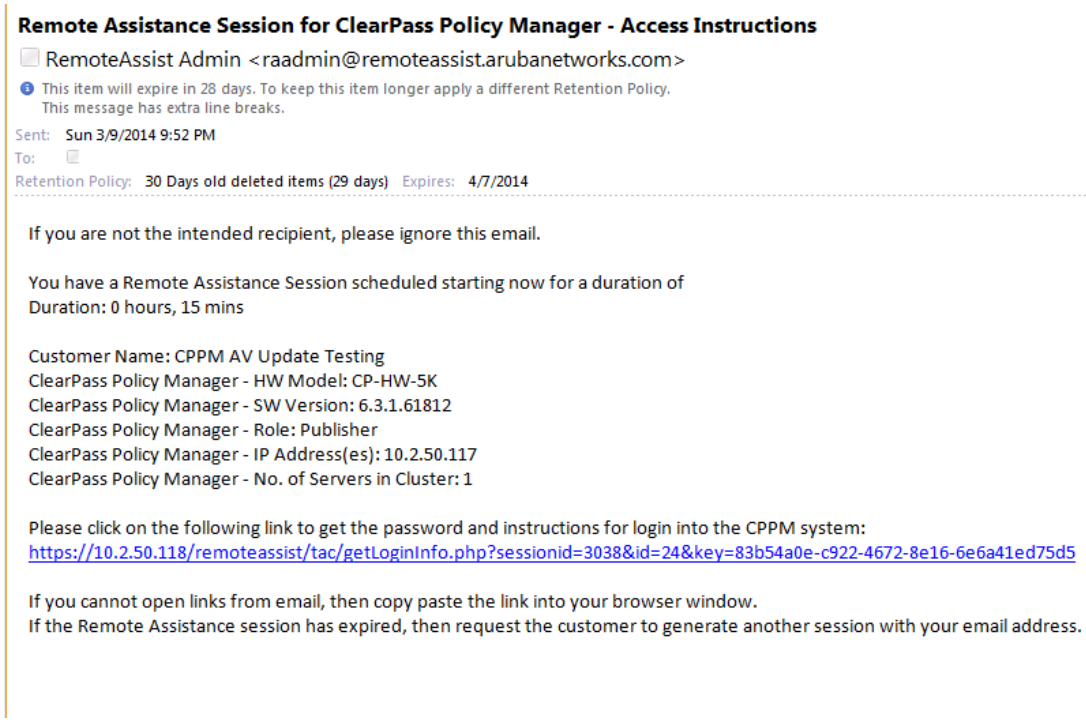
Parameter	Description
Session Name	Text name of session.
Session Type	• One Time Future (Initiates a session in future, on a selected date and time) • Weekly (Initiates a session on a selected weekday at the selected time) • Monthly (Initiates a session on a selected day of every month at the selected time)
Duration	The duration of a session is specified in Hours and Minutes. The "session begin" time saved is the time relative to server's time, and is specified in a 24-hour clock format.
Aruba	The Aruba Support Contact is just the email-id of the support contact

Table 337: *Add Session Parameters (Continued)*

Parameter	Description
Support Contact	('@arubanetworks.com' is appended to the ID).

The figure below is an example of an email that a support technician may receive after a Remote Assistance session is scheduled.

Figure 526: *Example of a Remote Assistance Session Notification Email*



Remote Assistance Session for ClearPass Policy Manager - Access Instructions

RemoteAssist Admin <raadmin@remoteassist.arubanetworks.com>

This item will expire in 28 days. To keep this item longer apply a different Retention Policy.
This message has extra line breaks.

Sent: Sun 3/9/2014 9:52 PM
To:
Retention Policy: 30 Days old deleted items (29 days) Expires: 4/7/2014

If you are not the intended recipient, please ignore this email.

You have a Remote Assistance Session scheduled starting now for a duration of
Duration: 0 hours, 15 mins

Customer Name: CPPM AV Update Testing
ClearPass Policy Manager - HW Model: CP-HW-5K
ClearPass Policy Manager - SW Version: 6.3.1.61812
ClearPass Policy Manager - Role: Publisher
ClearPass Policy Manager - IP Address(es): 10.2.50.117
ClearPass Policy Manager - No. of Servers in Cluster: 1

Please click on the following link to get the password and instructions for login into the CPPM system:
https://10.2.50.118/remoteassist/tac/getLoginInfo.php?sessionid=3038&id=24&key=83b54a0e-c922-4672-8e16-6e6a41ed75d5

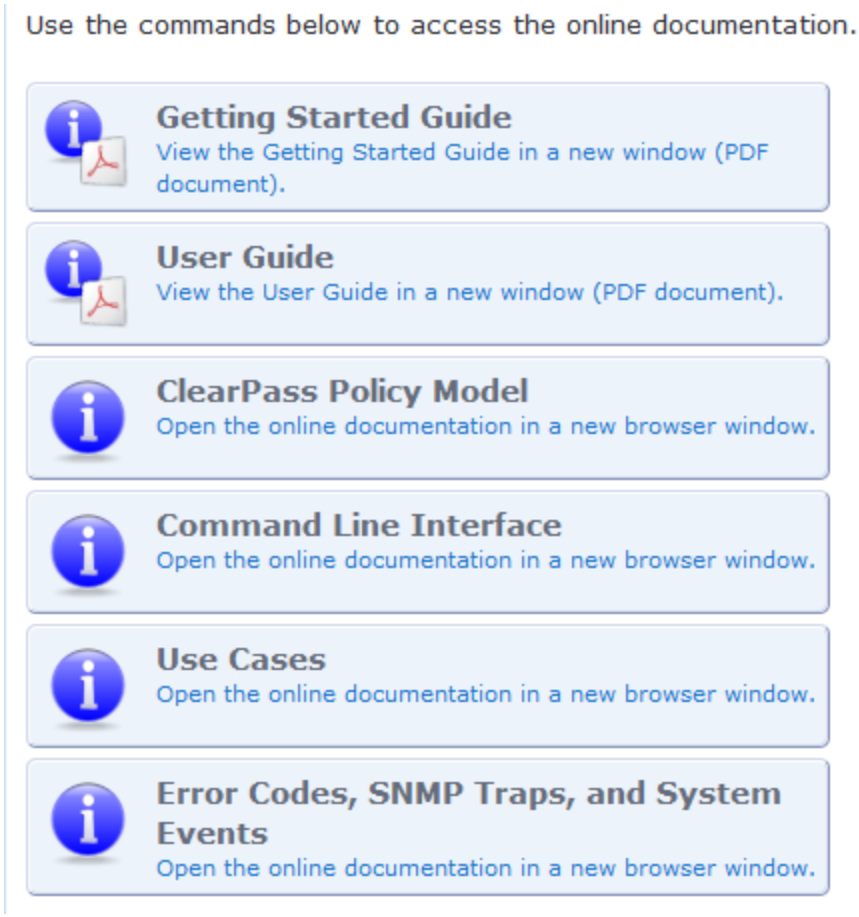
If you cannot open links from email, then copy paste the link into your browser window.
If the Remote Assistance session has expired, then request the customer to generate another session with your email address.

Documentation

The **Administration > Support > Documentation** page includes links to various sections of the Dell Networking W-ClearPass Policy Manager Online Help system. For example, to view documentation for the CLI, click the **Command Line Interface** button. This page also provides links to PDF versions of the *Dell Networking W-ClearPass Policy Manager 6.5 User Guide* and the *Dell Networking W-ClearPass Policy Manager 6.5 Getting Started Guide*.

The following figure displays the **Documentation** page:

Figure 527: *Documentation Page*



Refer to the following sections to perform various tasks using the Command Line Interface (CLI):

Cluster Commands

The Policy Manager command line interface includes the following cluster commands:

drop-subscriber

Use the **drop-subscriber** command to remove a specific subscriber node from the cluster.

Syntax

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

The following table describes the required and optional parameters for the **drop-subscriber** command:

Table 338: *Drop-Subscriber Command Parameters*

Flag/Parameter	Description
-f	Forces to drop even the nodes that are down.
-i <IP Address>	Specifies the Management IP address of the node. If this IP address is not specified and the current node is a subscriber, then Policy Manager drops the current node.
-s	Restricts resetting the database on the dropped node. By default, Policy Manager drops the current node (if a subscriber) from the cluster.

Example

The following example removes the IP address 192.xxx.1.1 from the cluster:

```
[appadmin]#   cluster drop-subscriber -f -i 192.xxx.1.1 -s
```

list

Use the **list** command to list the cluster nodes.

Syntax

```
cluster list
```

Example

The following example lists all the cluster nodes:

```
[appadmin]# cluster list
cluster list
Publisher  :
Management port IP=192.xxx.5.227

Data port IP=None [local machine]
```

make-publisher

Use the **make-publisher** command to makes a specified node as a publisher.

Syntax

```
cluster make-publisher
```

Example

The following example makes a node as a publisher:

```
[appadmin]#  cluster make-publisher
******************************************************
* WARNING: Executing this command will promote the     *
* current machine (which must be a subscriber in the   *
* cluster) to the cluster publisher. Do not close the  *
* shell or interrupt this command execution.           *
******************************************************
Continue? [y|Y]: y
```

make-subscriber

Use the **make-subscriber** command to make a node as a subscriber node.

Syntax

```
make-subscriber -i <IP Address> [-l]
```

The following table describes the required and optional parameters for the **make-subscriber** command:

Table 339: *Make-Subscriber Command Parameters*

Flag/Parameter	Description
-i <IP Address>	Specifies the publisher IP address. This field is mandatory.
-l	Restores the local log database after this operation. This field is optional.

Example

The following example makes 192.xxx.1.1 as a subscriber node:

```
[appadmin]#  cluster make-subscriber –i 192.xxx.1.1 –p !alore -l
```

reset-database

Use the **reset-database** to reset the local database and erases its configuration.

Syntax

```
cluster reset-database
```

Example

The following example reset the database:

```
[appadmin]#  cluster reset-database
******************************************************
* WARNING: Running this command will erase the Policy Manager    *
* configuration and leave the database with default     *
* configuration. You will lose all the configured data. *
* Do not close the shell or interrupt this command       *
* execution.                                           *
******************************************************
Continue? [y|Y]: y
```

set-cluster-passwd

Use the **set-cluster-passwd** to change the cluster password on all publisher nodes. If this command is executed on the publisher, the publisher prompts for the new cluster password.

Syntax

```
cluster set-cluster-passwd
```

Example

The following example changes the cluster password on publisher nodes:

```
[appadmin]#  cluster set-cluster-passwd
cluster set-cluster-passwd
Enter Cluster Passwd: santaclara
Re-enter Cluster Passwd: santaclara
INFO - Password changed on local (publisher) node
Cluster password changed
```

set-local-passwd

Use the **set-local-passwd** command to change the local password. When you execute this command locally, it prompts for the new local password.

Syntax

```
cluster sync-local-password
```

Example

The following example changes the local password:

```
[appadmin]#  cluster set-local-password
cluster sync-local-passwd
Enter Password: !alore
```

```
Re-enter Password: !alore
```

Configure Commands

The Policy Manager command line interface includes the following **configuration** commands:

date

Use the **date** command to set System Date, Time, and Time Zone.

Syntax

```
configure date -d <date> [-t <time> ] [-z <timezone>]
```

or

```
configure date -s <ntpserver> [-z <timezone>]
```

The following table describes the required and optional parameters for the **date** command:

Table 340: *Date Command Parameters*

Flag/Parameter	Description
-s <ntpserver>	Synchronizes time with the specified NTP server. This field is optional. **NOTE:** You can specify a destination node with the IPv6 address enabled.
-d <date>	Specifies the syntax: **yyyy-mm-dd**. This field is mandatory.
-t <time>	Specifies the syntax: **hh:mm:ss**. This field is optional.
-z <timezone>	Specifies the syntax. To view the list of supported timezone values, enter `show all-timezones`. This field is optional.

Example 1

The following example configures date, time, or timezone:

```
[appadmin]# configure date -d 2007-06-22 -t 12:00:31 -z America/Los_Angeles
```

Example 2

The following example synchronizes with a specified NTP server:

```
[appadmin]# -s <ntpserver>
```

dns

Use the **dns** command to configure DNS servers. Specify minimum of one DNS server and you can specify a maximum of three DNS servers.

Syntax

```
configure dns <primary> [secondary] [tertiary]
```

Example 1

The following example configures a DNS server:

```
[appadmin]# configure dns 192.168.xx.1
```

Example 2

The following example configures primary and secondary DNS servers:

```
[appadmin]# configure dns 192.168.xx.1 2001:4860:4860::8888
```

You can configure IPv6 address as described in this example.

Example 3

The following example configures primary, secondary, and tertiary DNS servers:

```
[appadmin]#  configure dns 192.168.xx.1 2001:4860:4860::8888 192.168.xx.2
```

fips-mode

Use the **fips-mode** command to enable or disable the **FIPS** mode.

Syntax

```
configure fip-smode [0|1]
```

The following table describes the required and optional parameters for the **fips-mode** command:

Table 341: *fips-mode Command Parameters*

Flag/Parameter	Description
0	Enter 0 to disable the **FIPS** mode. Read the warning message carefully before enabling or disabling the **FIPS** mode.
1	Enter 1 to enable the **FIPS** mode.

Example 1

The following example disables the **FIPS** mode:

```
[appadmin]# configure fips-mode 0
******************************************************************
*                                                                *
* WARNING: Running this command will erase the Policy Manager    *
* configuration and leave the database with default              *
* configuration. You will lose all the configured data.          *
*                                                                *
* This command will also shutdown all applications and reboot    *
* the system.                                                    *
*                                                                *
```

```
* Do not close the shell or interrupt this command execution.    *
*                                                                 *
*******************************************************************
Continue? [y|n]: y
```

Click **y** to disable the **FIPS** mode.

hostname

Use the **hostname** command to configure the hostname.

Syntax

```
configure hostname <hostname>
```

Example

The following example configures a hostname:

```
[appadmin]#  configure hostname sun.us.dellnetworks.com
```

ip

Use the **ip** command to configure IP address, netmask, and gateway.

Syntax

```
[appadmin]#  configure ip <mgmt|data> <ipaddress> netmask <netmask address> gateway <gateway address>
```

The following table describes the parameters used in the **ip** command:

Table 342: *ip Command Parameters*

Flag/Parameter	Description
ip <mgmt|data> <ip address>	Specifies the network interface type: management or data. **<ip address>** specifies the IPv4 address of the host.
netmask <netmask address>	Specifies the netmask address.
gateway <gateway address>	Specifies the gateway address.

Example

The following example configures the IP, netmask, and gateway addresses:

```
[appadmin]#  configure ip data 192.168.xx.12 netmask 255.255.255.0 gateway 192.168.xx.1
```

ip6

Use the **ip6** command to configure the IPv6 address, netmask, and gateway.

Syntax

```
configure ip6 <mgmt|data> <IPv6Address/PrefixLen> gateway <gateway address>
configure ip6 <mgmt|data> <IPv6Address> netmask <netmask address> gateway <gateway address>
```

The following table describes the parameters used in the **ip6** command:

Table 343: *ip6 Command Parameters*

Flag/Parameter	Description
ip6 <mgmt|data> <ip address>	Specifies the Network interface type: management or data. **NOTE: <ip6 address>** specifies the IPv6 address of the host.
netmask <netmask address>	Specifies the netmask address. For example, ffff:ffff:ffff:ffff:0000:0000:0000:0000.
gateway <gateway address>	Specifies the gateway address. For example, fe90:0000:0000:0000:020c:29ff:fe7e:d3a2.

Example

The following example configures the IPv6 management, netmask, and gateway:

```
[appadmin]# configure ip6 mgmt fe90:0000:0000:0000:020c:29ff:fe7e:d3e1 netmask
ffff:ffff:ffff:ffff:0000:0000:0000:0000 gateway fe90:0000:0000:0000:020c:29ff:fe7e:d3a1
```

mtu

Use the **mtu** command to set the Maximum Transmission Unit (MTU) for the management and data port interfaces.

Syntax

```
configure mtu <mgmt|data> <mtu-value>
```

The following table describes the parameters used in the **mtu** command:

Table 344: *mtu Command Parameters*

Flag/Parameter	Description
mtu <mgmt|data>	Specifies the Network interface types: management or data port.
mtu-value	Specify the MTU value in bytes. The default value is 1500 bytes.

Example 1

The following example configures the mtu management interface:

```
[appadmin] # configure mtu mgmt 1498
******************************************************
*                                                    *
* WARNING: Running this command might cause system     *
* to lose network connectivity and may require relogin.*
*                                                    *
******************************************************
Continue? [y|Y]: y
INFO: Restarting network services
INFO: Successfully applied MTU settings
```

Example 2

The following example configures the mtu data port value:

```
[appadmin]# configure mtu data 1498
******************************************************
*                                                    *
* WARNING: Running this command might cause system     *
* to lose network connectivity and may require relogin.*
```

```
*                                                    *
******************************************************
Continue? [y|Y]: y
INFO: Restarting network services
INFO: Successfully applied MTU settings
```

Example 3

The following example displays the settings of the mtu management and data port interfaces:

```
[appadmin]# show ip
==========================================
Device Type      :   Management Port
------------------------------------------
IPv4 Address     :   10.2.xx.86
Subnet Mask      :   255.255.255.0
Gateway          :   10.2.xx.1
IPv6 Address     :   2607:f0d0:1002:0011:0000:0000:0000:0002
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   2607:f0d0:1002:0011:0000:0000:0000:0001
Hardware Address :   00:0C:29:70:27:40
MTU              :   1499
==========================================
Device Type      :   Data Port
------------------------------------------
IPv4 Address     :   <not configured>
Subnet Mask      :   <not configured>
Gateway          :   <not configured>
IPv6 Address     :   fe80:0000:0000:0000:020c:29ff:fe70:274a
Subnet Mask      :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway          :   fe80:0000:0000:0000:020c:29ff:fe70:2741
Hardware Address :   00:0C:29:70:27:4A
MTU              :   1498
==========================================
DNS Information
------------------------------------------
Primary   DNS  :   10.2.xx.3
Secondary DNS  :   10.1.xx.50
Tertiary  DNS  :   10.1.xx.200
==========================================
```

timezone

Use the **timezone** command to configure time zone interactively.

Syntax

```
configure timezone
```

Example

The following example configures the timezone interactively:

```
[appadmin]#  configure timezone
configure timezone
*******************************************************
* WARNING: When the command is completed Policy Manager services *
* are restarted to reflect the changes.                *
******************************************************
Continue? [y|Y]:  y
```

Network Commands

The Policy Manager command line interface includes the following **network** commands:

ip

Use the **ip** command to add, delete, or list custom routes to the data or management interface routing table.

Syntax

```
network ip add <mgmt|data|greN> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]> [-g <ViaAddr>]
```

The following table describes the required and optional parameters for the **ip** command:

Table 345: *IP Command Parameters*

Flag/Parameter	Description
<mgmt | data| greN>	Specifies management interface, data interface or the name of the GRE tunnel. In <greN>, N specifies the GRE tunnel number ranging from 1,2,3...N.
-i <id>	Specifies the ID of the network IP rule. If this ID is not specified, the system generates an ID automatically. **NOTE:** This ID determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Specifies the IP address or network. For example, 192.168.xx.0/24 or 0/0 (for all traffic) of traffic originator. You must specify only one SrcAddr or DstAddr. This parameter is optional.
-d <DestAddr>	Specifies the destination IP address or network. For example, 192.168.xx.0/24 or 0/0 (for all traffic). You must specify only one SrcAddr or DstAddr. This parameter is optional.

Syntax

```
network ip del <-i <id>>
```

The following table describes the required and optional parameters for the **ip del <-i <id>>** command:

Table 346: *Network IP Delete Command Parameters*

Flag/Parameter	Description
-i <id>	Specifies the ID of the rule to delete.

Syntax

```
network ip list
```

This command lists all routing rules.

Syntax

```
network ip reset
```

This command reset routing table to factory default setting. All custom routes are removed. The following examples add and list the custom routes:

Example 1

The following example adds a custom route:

```
[appadmin]# network ip add data -s 192.168.xx.0/24
```

Example 2

The following example lists all custom routes:

```
[appadmin]# network ip list
================================================
            IP Rule Information
------------------------------------------------
0:      from all lookup local
10020:  from all to 10.xx.4.0/24 lookup mgmt
10040:  from 10.xx.4.200 lookup mgmt
10060:  from 10.xx.5.200 lookup data
32766:  from all lookup main
32767:  from all lookup default
================================================
```

ip6

Use the **ip6** command to add, delete, or list custom routes to the data or management interface routing table.

Syntax

```
network ip6 add <mgmt|data> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]>
```

The following table describes the required and optional parameters for the **ip6** command:

Table 347: *IP Command Parameters*

Flag/Parameter	Description
<mgmt|data>	Specifies management or data interface
-i <id>	Specifies the ID of the network ip rule. If this ID is not specified, the system generates an ID automatically. **NOTE:** This ID determines the priority in the ordered list of rules in the routing table.
-s <SrcAddr>	Specifies the source interface IPv6 address or netmask from where the network IPv6 rule is specified. For example, fe82::20c:29ff:fe7e:d3e1. The valid IPv6 address or netmask or 0/0 values are allowed. This parameter is optional.
-d <DestAddr>	Specifies the destination interface IPv6 address or netmask where the network IPv6 rule is specified. For example, fe82::20c:29ff:fe7e:d3e9. The valid IPv6 address or netmask or 0/0 values are allowed. This parameter is optional.
-g <ViaAddr>	Specifies the via or gateway IPv6 address through which the network traffic should flow. The valid IPv6 address is allowed. This parameter is optional.

Syntax

```
network ip6 del <-i <id>>
```

This command deletes a custom route.

Syntax

```
network ip6 list
```

This command lists all custom routing rules.

Syntax

```
network ip6 reset
```

This command reset routing table to factory default setting and all custom routes are removed. The following examples add and list the custom routes:

Example 1

The following example adds a custom route:

```
[appadmin]# network ip6 add data -s fe82::20c:29ff:fe7e:d3e1/d3e24
```

You can use IPv6 address when adding a custom route.

Example 2

The following example lists all custom routing rules:

```
[appadmin]# network ip6 list

================================================
IP Rule Information
------------------------------------------------
0:      from all lookup local
13000:  from all to fe82::20c:99ff:fe7e:d3e1 lookup mgmt
13001:  from all to fe82::20c:99ff:fe7e:d3e4 lookup mgmt
13002:  from all to fe82::20c:99ff:fe7e:d3e7 lookup mgmt
13003:  from all to fe82::20c:99ff:fe7e:d3e8 lookup mgmt
13004:  from all to fe82::20c:99ff:fe7e:d3e9 lookup mgmt
13005:  from all to fe82::20c:99ff:fe7e:d3ea lookup static
32766:  from all lookup main
================================================
```

nslookup

Use the **nslookup** command to get the IP address of host using DNS.

Syntax

```
nslookup -q <record-type> <host>
```

The following table describes the required and optional parameters for the **nslookup** command:

Table 348: *nslookup Command Parameters*

Flag/Parameter	Description
<record-type>	Specifies the type of DNS record. For example, A, CNAME, and PTR records.
<host>	Specifies the host or domain name to be queried.

Example 1

The following examples obtain the IPv4 and IPv6 addresses of the host or domain using DNS:

```
[appadmin]# nslookup sun.us.dellnetworks.com
[appadmin]# network nslookup 2001:4860:4860::8888
```

Example 2

The following example queries a host or domain for SRV records:

```
[appadmin]# nslookup -q SRV dellnetworks.com
```

Use the **AAAA** flag with the **-q** option to perform network nslookup with IPv6 destinations.

Syntax

```
nslookup -q  AAAA <IPv6_addr>
```

The following example performs network nslookup for the destination with IPv6 address:

Example

```
[appadmin]# network nslookup 2001::93
Server:         2001::94
Address:        2001::94#53
3.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.2.ip6.arpa        name =
ipv6test-n1.cppmipv6.com.
[appadmin]# network nslookup -q AAAA ipv6test-n1.cppmipv6.com
Server:         2001::94
Address:        2001::94#53
ipv6test-n1.cppmipv6.com        has AAAA address 2001::93
```

ping

Use the **`ping`** command to test the reachability of the network host.

Syntax

```
network ping [-i <SrcIpAddr>] [-t] <host>
```

The following table describes the required and optional parameters for the **`ping`** command:

Table 349: *Ping Command Parameters*

Flag/Parameter	Description
-i <SrcIpAddr>	Specifies the originating IP address for ping. This field is optional.
-t	Use this parameter to ping indefinitely. This field is optional.
<host>	Specifies the host to be pinged.

Example

The following example pings a network host to test the reachability:

```
[appadmin]# network ping -i 192.168.xx.10 -t sun.us.dellnetworks.com
```

ping6

Use the **`ping6`** command to test the reachability of the network host.

Syntax

```
network ping6 [-i <SrcIPv6Addr>] [-t] <host>
```

The following table describes the required and optional parameters for the **ping** command:

Table 350: *Ping6 Command Parameters*

Flag/Parameter	Description
-i <SrcIPv6Addr>	Specifies the originating IPv6 address for ping. This field is optional.
-t	Use this parameter to ping indefinitely. This field is optional.
<host>	Specifies the host to be pinged.

Example

The following example pings a network host to test the reachability:

```
[appadmin]#   network ping6 –i fe82::20c:29ff:fe7e:d3e1 –t sun.us.dellnetworks.com
```

reset

Use the **reset** command to reset the network data and management port.

Syntax

```
network reset <data/mgmt>
```

The following table describes the required and optional parameters for the **reset** command:

Table 351: *Reset Command Parameters*

Flag/Parameter	Description
data	Specifies the name of network data port to reset. This parameter is mandatory.
mgmt	Specifies the name of network management port to reset. **NOTE:** You can use this command to reset the IPv4 and IPv6 addresses.

Example

The following example reset the network data port:

```
[appadmin]# network reset data
```

traceroute

Use the **traceroute** command to print the route taken to reach the network host.

Syntax

```
network traceroute <host>
```

The following table describes the required and optional parameters for the **traceroute** command:

Table 352: *Traceroute Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of network host.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]#  network traceroute sun.us.dellnetworks.com
```

traceroute6

Use the **traceroute6** command to print the route taken to reach the network host.

Syntax

```
network traceroute6 <host>
```

The following table describes the required and optional parameters for the **traceroute** command:

Table 353: *Traceroute Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of network host. You can specify the host with IPv6 address.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]# network traceroute6 sun.us.

            dellnetworks.com
```

Service Commands

The Policy Manager CLI includes the following **service** commands:

- start
- stop
- status
- restart
- activate
- deactivate
- list

These commands in this section have identical syntax; therefore, this section presents them as variations on <action>.

<action>

Use the **<action>** command to activate the specified Policy Manager service.

Syntax

```
service <action> <service-name>
```

Where:

Table 354: *Action Command Parameters*

Flag/Parameter	Description
action	Choose an action: *activate, deactivate, list, restart, start, status,* or *stop.*
service-name	Choose a service: *tips-policy-server*, *tips-admin-server*, *tips-system-auxiliary-server*, *tips-radius-server*, *tips-tacacs-server*, *tips-dbwrite-server*, *tips-repl-server*, or *tips-sysmon-server*.

Example 1

```
[appadmin]#  service activate tips-policy-server
```

Example 2

```
[appadmin]#  service list all
service list
Policy server  [ tips-policy-server ]
Admin UI service  [ tips-admin-server ]
System auxiliary services  [ tips-system-auxiliary-server ]
Radius server  [ tips-radius-server ]
Tacacs server  [ tips-tacacs-server ]
Async DB write service  [ tips-dbwrite-server ]
DB replication service  [ tips-repl-server ]
System monitor service  [ tips-sysmon-server ]
```

Example 3

```
[appadmin]#  service status tips-domain-server
```

Show Commands

The Policy Manager command line interface includes the following **`show`** commands:

all-timezones

Use the **`all-timezones`** command to view all available timezones.

Syntax

```
show all-timezones
```

Example

The following example displays all available timezones:

```
[appadmin]#  show all-timezones
Africa/Abidjan
Africa/Accra
.....
WET
Zulu
```

date

Use the **date** command to view the System Date, Time, and Time Zone information.

Syntax

```
show date
```

Example

The following example displays the System Date, Time, and Time Zone information:

```
[appadmin]#  show date
Wed Oct 31 14:33:39 UTC 2012
```

dns

Use the **dns** command to view DNS servers.

Syntax

```
show dns
```

Example

The following example displays DNS servers:

```
[appadmin]#  show dns
show dns
================================================
          DNS Information
------------------------------------------------
Primary   DNS  :   192.xxx.5.3

Secondary DNS  :   <not configured>
Tertiary  DNS  :   <not configured>
================================================
```

domain

Use the **domain** command to view the Domain Name, IP Address, and Name Server information.

Syntax

```
show domain
```

Example

The following example displays the domain name:

```
[appadmin]#  show domain
```

fipsmode

Use the **fipsmode** command to find whether the **FIPS** mode is enabled or disabled.

Example

The following example displays that the **FIPS** mode is enabled:

```
[appadmin]# show fipsmode
FIPS Mode: Enabled
```

hostname

Use the **hostname** command to view hostname.

Syntax

```
show hostname
```

Example

The following example displays the hostname:

```
[appadmin]#  show hostname
show hostname
wolf
```

ip

Use the **ip** command to view the IPv4, IPv6, and DNS information of the host.

Syntax

```
show ip
```

Example

The following example displays the IPv4, IPv6, and DNS information of the host:

```
[appadmin]#  show ip
==========================================
Device Type       :   Management Port
------------------------------------------
IPv4 Address      :   10.2.xx.86

Subnet Mask       :   255.255.255.0
Gateway           :   10.2.xx.1

IPv6 Address      :   2607:f0d0:1002:0011:0000:0000:0000:0002
Subnet Mask       :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway           :   2607:f0d0:1002:0011:0000:0000:0000:0001
Hardware Address  :   00:0C:29:70:57:40

MTU               :   1499
==========================================
Device Type       :   Data Port
------------------------------------------
IPv4 Address      :   <not configured>
Subnet Mask       :   <not configured>
Gateway           :   <not configured>
IPv6 Address      :   fe80:0000:0000:0000:020c:29ff:fe70:274a
Subnet Mask       :   ffff:ffff:ffff:ffff:0000:0000:0000:0000
Gateway           :   fe80:0000:0000:0000:020c:29ff:fe70:2741
Hardware Address  :   00:0C:29:70:27:4A
MTU               :   1498
```

```
================================================
DNS Information
------------------------------------------------
Primary   DNS  :   10.2.xx.3

Secondary DNS  :   10.1.xx.50

Tertiary  DNS  :   10.1.xx.200

================================================
```

license

Use the **license** command to view the license key.

Syntax

```
show license
```

Example

The following example displays the license information:

```
[appadmin]#  show license
------------------------------------------------------------
Application              : PolicyManager
License key              : VWQO-MW62UO-VMVF-B7GNJT-OHUAZY-IAAM-RTQUPQ-WODIFNJI-CD7N-I5565A

License key type         : Permanent
License added on         : 2014-06-20 10:16:38
Validity                 : <not applicable>
Issued for               : 5000 users
Customer id              : JRC
Licensed features        : <not applicable>
------------------------------------------------------------
Application              : PolicyManager
License key              : VWQO-MW62UO-VMVF-B7GNJT-OHUAZY-IAAM-RTQUPQ-WODIFNJI-CD7N-I5565A
License key type         : Permanent
License added on         : 2014-06-20 10:16:38
Validity                 : <not applicable>
Issued for               : 5000 users
Customer id              : JRC
Licensed features        : <not applicable>
============================================================
```

sysinfo

Use the `sysinfo` command to view the disk and memory utilization:

Syntax

```
show sysinfo
```

Example

The following example displays the disk and memory utilization:

```
[appadmin]# show sysinfo
System Uptime :  1 day, 23:29:15.510000
================================================
Disk Utilization
------------------------------------------------
Total         :    115.48 GB
Free          :    5.42 GB (6%)
```

```
==========================================
Memory Utilization
------------------------------------------
Total          :     4.00 GB
Free           :     1.36 GB (36%)
```

timezone

Use the **timezone** command to view the current system timezone.

Syntax

```
show timezone
```

Example

The following example displays the system timezone:

```
[appadmin]#  show timezone
show timezone

Timezone is set to 'Asia/Kolkata'
```

version

Use the **Version** command to view the Policy Manager software version and the hardware model.

Syntax

```
show version
```

Example

The following example displays the Policy Manager software version and the hardware model:

```
[appadmin]#  show version
=======================================
Policy Manager software version : 2.0(1).6649
Policy Manager model number     : ET-5010
=======================================
```

System Commands

The Policy Manager command line interface (CLI) includes the following **system** commands:

- apps-access-reset
- boot-image on page 586
- System Commands
- cleanup
- gen-support-key on page 587
- install-license on page 587
- morph-vm
- refresh-license
- restart on page 589
- shutdown on page 589
- sso-reset
- start-rasession

- status-rasession
- System Commands
- update on page 590
- upgrade on page 591

apps-access-reset

Use the **apps-access-reset** command to reset the access control restrictions for Policy Manager.

Syntax

```
system apps-access-reset
```

Example

The following example reset the access control restrictions for Policy Manager:

```
[appadmin]# system apps-access-reset
Policy Manager application access is restored
```

boot-image

Use the **boot-image** to set system boot image control options.

Syntax

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

The following table describes the required and optional parameters for the **boot-image** command:

Table 355: *Boot-Image Command Parameters*

Flag/Parameter	Description
-l	Lists the boot images installed on the system.
-a <version>	Sets the active boot image version in *A.B.C.D* syntax. This field is optional.

Example

The following example sets the system boot image control options:

```
[appadmin]#  system boot-image -l
```

cleanup

Use the **cleanup** command to perform a system cleanup operation that results the purging of the records including the following:

- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

Syntax

```
system cleanup
```

Example

The following example performs cleanup operation for the system:

```
[appadmin]# system cleanup
ERROR - Insufficient arguments to proceed
System Cleanup (CLI) Usage:
system cleanup <num days>
Where, <num days>   --  Cleanup interval specifying the number of days to retain the data
[appadmin]# system cleanup 4

******************************************************
*                                                    *
* WARNING: This command will perform system cleanup  *
* operation that will result in purging of:          *
*   [*] system and application log files             *
*   [*] past authentication records                  *
*   [*] audit records                                *
*   [*] expired guest accounts                       *
*   [*] past auto and manual backups                 *
*   [*] stored reports etc...                        *
*                                                    *
******************************************************
Are you sure you want to continue? [y|n]: y
INFO - Starting system cleanup
INFO - Purging diagnostic dumps
INFO - Detected empty core directory
INFO - Performing system cleanup tasks
INFO - Purging platform logs
INFO - Purging application logs
INFO - Performing database cleanup tasks
INFO - Completed system cleanup
```

gen-recovery-key

Use the **gen-recovery-key** command to generate the recovery key for the system.

Example

The following example generates the recovery key for the system:

```
[appadmin]# system gen-recovery-key
Recovery key='04U2FsdGVkX18To8NDWayziQ17LzKA17DW5y+AZvGj41c='
```

gen-support-key

Use the **gen-support-key** command to generate the support key for the system.

Syntax

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

Example

The following example generates the support key for the system:

```
[appadmin]#  system gen-support-key
system gen-support-key
Support key='01U2FsdGVkX1+/WS9jZKQajERyzXhM8mF6zAKrzxrHvaM='
```

install-license

Use the **install-license** command to replace the current license key with a new one.

Syntax

```
system install-license <license-key>
```

The following table describes the required and optional parameters for the **install-license** command:

Table 356: *Install-License Command Parameters*

Flag/Parameter	Description
<license-key>	Specifies the newly issued license key. This field is mandatory.

Example

The following example replaces the current license key with a new one:

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

morph-vm

Use the **morph-vm** command to convert an evaluation virtual machine (VM) to a production VM. With this command, licenses are still required to be installed after the morph operation is completed. Use the following steps to convert an evaluation VM to a production VM:

1. Determine the type of the appliance to which you want to morph your evaluation VM.
2. Procure license for the target VM appliance.
3. Shut down the VM.
4. Determine the required capacity of an additional hard disk and attach to the target VM appliance.
5. Adjust the CPU and Memory settings for the evaluation VM to match the target VM appliance.
6. Boot the VM.
7. Execute the **morph-vm** command. The configuration data from the evaluation VM will be migrated to the new disk attached. The node will reboot as a VM of the selected appliance model.
8. Login to the UI and enter the permanent license obtained. Now, the evaluation VM is morphed into a production VM.

Syntax

```
system morph-vm <vm-version: CP-VA-500 | CP-VA-5K | CP-VA-25K>
```

The following table describes the required and optional parameters for the **morph-vm** command:

Table 357: *Morph-VM Commands*

Flag/Parameter	Description
<vm-version>	This is the updated ClearPass version. The following three options are available: • CP-VA-500 • CP-VA-5K • CP-VA-25K This field is mandatory.

Example

The following example converts an evaluation virtual machine (VM) to a production VM for CP-25K version:

```
[appadmin]# system morph-vm CP-25K
```

refresh-license

Use the **refresh-license** command to refresh the license count information .

Syntax

```
system refresh-license
```

Example

The following example refreshes the license count information:

```
[appadmin]# system refresh-license

INFO: Refreshing license count information

INFO: Successfully refreshed license count information
```

restart

Use the **restart** command to restart the system.

Syntax

```
system restart
```

Example

The following example restarts the system with a confirmation:

```
[appadmin]#  system restart
system restart
******************************************************

* WARNING: This command will shut down all applications *

* and reboot the system                                 *
******************************************************
Are you sure you want to continue? [y|Y]: y
```

shutdown

Use the **shutdown** command to shut down the system.

Syntax

```
system shutdown
```

Example

The following example shuts down the system with a confirmation:

```
[appadmin]#  system shutdown
******************************************************
* WARNING: This command will shut down all applications *

* and power off the system                              *
******************************************************
Are you sure you want to continue? [y|Y]: y
```

sso-reset

Use the **sso-reset** command to reset the Single Sign-On (SSO) configuration.

Syntax

```
system sso-reset
```

start-rasession

Use the **start-rasession** command to start a RemoteAssist (RA) session.

Syntax

```
system start-rasession [duration_hours | duration_mins | contact_id | cppm_server_ip]
```

The following table describes the required and optional parameters for the **start-rasession** command:

Table 358: *Start RemoteAssist Session Command Parameters*

Flag/Parameter	Description
duration_hours	Specify session duration in hours. You can specify values between 0 to 12.
duration_mins	Specify session duration in minutes. You can specify values between 0 to 59.
contact_id	The username ID part of the Dell TAC or Engineering contact. For example "bjones".
cppm_server_ip	The W-ClearPass Policy Manager server IP address.

status-rasession

Use the **status-rasession** command to view the status of a RemoteAssist session.

Syntax

```
system status-rasession <session_id>
```

Example

The following example displays the status of a RemoteAssist session:

```
[appadmin]# system status-rasession 3001
```

terminate-rasession

Use the **terminate-rasession** command to terminate a running RemoteAssist session.

Syntax

```
system terminate-rasession <session_id>
```

Example

The following example terminates a running RemoteAssist session:

```
[appadmin]# system terminate-rasession 3001
```

update

The **update** command provides options to manage system patch updates.

Syntax

```
system update [-i [-f] <user@hostname:/<filename> | http://hostname/<filename>>]
system update [-f]
system update [-l]
```

The following table describes the required and optional parameters for the **update** command:

Table 359: *Update Commands*

Flag/Parameter	Description
-i user@hostname:/<filename> | http://hostname/<filename>	Installs the specified patch on the system. This field is optional.
-f	Re-installs the patch in the event of a problem with the initial installation attempt. This field is optional.
-l	Lists the patches installed on the system. This field is optional.

This command supports Secure Copy (SCP), HTTP, and local uploads.

Example

The following example provides options to manage system patch updates:

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

upgrade

The **upgrade** command upgrades the system. This command provides command syntax to upgrade from a Linux server, upgrading from a Web server, and upgrading by performing an offline upgrade.

Syntax

- **Upgrade from a Linux server:**

  `system upgrade user@hostname:/<filepath> [-w] [-l] [-L]`

  See Example 1: Upgrading from a Linux server.
- **Upgrade from a Web server:**
- `system upgrade http://hostname/<filepath> [-w] [-l] [-L]`

  See Example 2: Upgrading from a Web server.
- **Upgrade by performing an offline upgrade:**

  `system upgrade <filepath> [-w] [-l] [-L]`

  See Example 3: Performing an offline upgrade.

Table 360: *Upgrade Commands*

Flag/Parameter	Description
-w	Restores last (one) week of access tracker records after the upgrade.
-l	Restores all access tracker records from this version.
-L	Does not backup or restore access tracker records from this version.
<filepath>	Enter the filepath using the syntax provided in the two examples below. This field is mandatory.

NOTE

This command supports Secure Copy (SCP), HTTP, and local uploads.

NOTE

If none of these **Upgrade** command options are provided, access tracker records are backed up, but they are not restored by default.

Example 1: Upgrading from a Linux server

To upgrade the Policy Manager image from a Linux server:

1. Upload the upgrade image to a Linux server.
2. Use the following syntax to upload the upgrade image:

   ```
   system upgrade user@hostname:/<filepath> [-w] [-l] [-L]
   ```

   For example:

   ```
   [appadmin]# system upgrade admin@sun.us.dellnetworks.com:/tmp/PolicyManager-x86-64-upgrade-71.tgz
   ```

Example 2: Upgrading from a Web server

To upgrade the Policy Manager image from a Web server:

1. Upload the upgrade image to a Web server.
2. Use the following syntax to upload the upgrade image:

   ```
   system upgrade http://hostname/<filepath> [-w] [-l] [-L]
   ```

   For example:

   ```
   [appadmin]# system upgrade http://sun.us.dellnetworks.com/downloads/PolicyManager-x86-64-upgrade-71.tgz
   ```

Example 3: Performing an offline upgrade

To perform an offline upgrade:

1. Log in to the Dell Support Center and select the **Download Software** tab.
2. Navigate to the **ClearPass** > **Policy Manager** > **Current Release** > **Upgrade** folder.
3. In the **Description Remarks** section, click the link for the appropriate upgrade. The upgrade file is uploaded to your local system.
4. Navigate to the ClearPass Policy Manager **Software Updates** page at **Administration** > **Agents and Software Updates** > **Software Updates**.
5. In the **Firmware & Patch Updates** section of the **Software Updates** page, click the **Import Updates** button.

   The **Import from File** dialog appears.
6. Browse to the location of the upgrade file on your system, then click **Import**.

   The selected upgrade file is uploaded to the Dell Networking W-ClearPass Policy Manager.
7. Log in to the Policy Manager command line interface (CLI) with the following user name: *appadmin*.
8. Initiate the upgrade process by entering the following command:

   ```
   system upgrade <filepath> [-w] [-l] [-L]
   ```

   For example:

   ```
   [appadmin]# system upgrade CPPM-upgradeimage.bin
   ```
9. After the upgrade process is complete, restart the machine by issuing the following command in the CLI:

   ```
   system restart
   ```

The Policy Manager restarts and boots up to the most recent version of Dell Networking W-ClearPass Policy Manager.

Miscellaneous Commands

The Policy Manager command line interface includes the following **`miscellaneous`** commands:

ad auth

Use the **`ad auth`** command to authenticate the user against Active Directory.

Syntax

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

The following table describes the required and optional parameters for the **`ad auth`** command:

Table 361: *Ad Auth Command Parameters*

Flag/Parameter	Description
<username>	Specifies the username of the authenticating user. This is a mandatory field.

Example

The following example authenticates the user against Active Directory:

```
[appadmin]#  ad auth --username=mike
```

ad netjoin

Use the **`ad netjoin`** command to join host to the domain.

Syntax

```
ad netjoin <domain-controller.domain-name> [domain NETBIOS name]
```

The following table describes the required and optional parameters for the **ad netjoin** command:

Table 362: *Ad Netjoin Command Parameters*

Flag/Parameter	Description
<domain-controller. domain-name>	Specifies the host to be joined to the domain. This field is mandatory.
[domain NETBIOS name]	Specifies the domain name. This field is optional.

Example

The following example joins host to the domain:

```
[appadmin]#  ad netjoin atlas.us.dellnetworks.com
```

ad netleave

Use the **ad netleave** to remove host from the domain.

Syntax

```
ad netleave
```

Example

The following example removes host from the domain:

```
[appadmin]#  ad netleave
```

ad testjoin

Use the **ad testjoin** to test if the **netjoin** command succeeded. This command also test if Policy Manager is a member of the AD domain.

Syntax

```
ad testjoin
```

Example

The following example tests if the **netjoin** command is succeeded:

```
[appadmin]#  ad testjoin
```

alias

Use the **alias** command to create or remove aliases.

Syntax

```
alias <name>=<command>
```

The following table describes the required and optional parameters for the **alias** command:

Table 363: *Alias Commands*

Flag/Parameter	Description
<name>=<command>	Sets <name> as the alias for <command>.
<name>=	Removes the association.

Example 1

```
[appadmin]# alias sh=show
```

Example 2

```
[appadmin]# alias sh=
```

backup

Use the **backup** command to create backup of Policy Manager configuration data. If no arguments are entered, the system auto-generates a filename and backs up the configuration to this file.

Syntax

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

The following table describes the required and optional parameters for the **backup** command:

Table 364: *Backup Command Parameters*

Flag/Parameter	Description
-f <filename>	Specifies the backup target. If not specified, Policy Manager auto-generates a filename. This field is optional.
-L	Do not backup the log database configuration. This field is optional.
-P	Do not backup password fields from the configuration database. This field is optional.

Example

```
[appadmin]#  backup -f PolicyManager-data.tar.gz
Continue? [y|Y]:  y
```

dump certchain

Use the **dump certchain** command to dump certificate chain of any SSL secured server.

Syntax

```
dump certchain <hostname:port-number>
```

The following table describes the required and optional parameters for the **dump certchain** command:

Table 365: *Dump Certchain Command Parameters*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1

The following example dumps certificate chain of a SSL secured server:

```
[appadmin]#  dump certchain ldap.acme.com:636
dump certchain
```

dump logs

Use the **dump logs** command to dump Policy Manager application log files.

Syntax

```
dump logs -f <output-file-name> [-s yyyy-mm-dd] [-e yyyy-mm-dd] [-n <days>] [-t <log-type>] [-h]
```

The following table describes the required and optional parameters for the **dump logs** command:

Table 366: *Dump Logs Command Parameters*

Flag/Parameter	Description
-f <output-file-name>	Specifies target for concatenated logs.
-s yyyy-mm-dd	Specifies the start date range. The default value is today. This field is optional.
-e yyyy-mm-dd	Specifies the end date range. The default value is today. This field is optional.
-n <days>	Specifies the duration in days (from today). This field is optional.
-t <log-type>	Specifies the type of log to collect. This field is optional.
-h	Specifies the print help for available log types.

Example 1

The following example dumps Policy Manager application log files:

```
[appadmin]#  dump logs –f tips-system-logs.tgz -s 2007-10-06 –e 2007-10-17 –t SystemLogs
```

Example 2

The following example prints help for available log types:

```
[appadmin]#  dump logs -h
```

dump servercert

Use the **dump servercert** command to dump server certificate of SSL secured server.

Syntax

```
dump servercert <hostname:port-number>
```

The following table describes the required and optional parameters for the **dump servercert** command:

Table 367: *Dump Servercert Command Parameters*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example

The following example dumps server certificate of SSL secured server:

```
[appadmin]#  dump servercert ldap.acme.com:636
```

exit

Use the **exit** command to exit shell.

Syntax

```
exit
```

Example

The following example exits the shell:

```
[appadmin]#  exit
```

help

Use the **help** command to display the list of supported commands:

Syntax

```
help <command>
```

Example

The following example displays the list of supported commands:

```
[appadmin]#  help
help
 alias                  Create aliases
 backup                 Backup Policy Manager data
 cluster                Policy Manager cluster related commands
 configure              Configure the system parameters
 dump                   Dump Policy Manager information
 exit                   Exit the shell
 help                   Display the list of supported commands
 netjoin                Join host to the domain
 netleave               Remove host from the domain
 network                Network troubleshooting commands
 quit                   Exit the shell
 restore                Restore Policy Manager database
 service                Control Policy Manager services
 show                   Show configuration details
 system                 System commands
```

krb auth

User the **krb auth** command to perform a kerberos authentication against a kerberos server (such as Microsoft AD).

Syntax

```
krb auth <user@domain>
```

The following table describes the required and optional parameters for the **krb auth** command:

Table 368: *Kerberos Authentication Command Parameters*

Flag/Parameter	Description
<user@domain>	Specifies the username and domain.

Example

The following example performs a kerberos authentication against a kerberos server:

```
[appadmin]#  krb auth mike@corp-ad.acme.com
```

krb list

Use the **`krb list`** command to list the cached kerberos tickets.

Syntax

```
krb list
```

Example

The following example lists the cached kerberos tickets:

```
[appadmin]#  krb list
```

ldapsearch

Use the Linux **`ldapsearch`** command to find objects in an LDAP directory. Note that only the Policy Manager specific command line arguments are listed. For other command line arguments, refer to ldapsearch man pages on the Internet.

Syntax

```
ldapsearch -B <user@hostname>
```

The following table describes the required and optional parameters for the **`ldapsearch`** command:

Table 369: *LDAP Search Command Parameters*

Flag/Parameter	Description
<user@hostname>	Specifies the username and the full qualified domain name of the host. The -B command finds the bind DN of the LDAP directory.

Example

The following example finds objects in an LDAP directory:

```
[appadmin]#  ldapsearch -B admin@corp-ad.acme.com
```

quit

Use the **`quit`** command to exit shell.

Syntax

```
quit
```

Example

The following command quits the shell:

```
[appadmin]# quit
```

restore

Use the **restore** command to restore Policy Manager configuration data from the backup file.

Syntax

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

The following table describes the required and optional parameters for the **restore** command:

Table 370: *Restore Command Parameters*

Flag/Parameter	Description
user@hostname:/<backup-filename>	Specify filepath of restore source.
-c	Restores configuration database (default).
-C	Does not restore configuration database.
-l	If it exists in the backup, restores log database. This field is optional.
-i	Ignores version mismatch errors and proceeds. This field is optional.
-p	Forces restore from a backup file that does not have password fields present. This field is optional.
-s	Restores cluster server/node entries from the backup. Node entries are disabled on restore. This field is optional.

Example

The following example restores Policy Manager configuration data from the backup file:

```
[appadmin]# restore user@hostname:/tmp/tips-backup.tgz -l -i -c -s
```

system start-rasession

The **system start-rasession** command allows administrators to configure and start a Remote Assistance session through the Dell Networking W-ClearPass Policy Manager CLI. Configuring a Remote Assistance session through a CLI can be used if the Dell Networking W-ClearPass Policy Manager UI at the customer site is inaccessible.

Syntax

```
system start-rasession <duration_hours> <duration_mins> <contact> <server_ip>
```

The following table describes the required and optional parameters for the **system start-rasession** command:

Table 371: *Start Remote Session Command Parameters*

Flag/Parameter	Description
<duration_hours>	Defines the duration in hours of the Remote Assistance Session.
<duration_mins>	Defines the duration in minutes of the Remote Assistance Session.
<contact>	Specifies the name of the TAC engineer.
<server_ip>	Specifies the IP address of a Dell Networking W-ClearPass Policy Manager in the cluster.

system terminate-rasession

The **`system terminate-rasession`** allows administrators to terminate the session on the Dell Networking W-ClearPass Policy Manager where the Remote Assistance session is running.

Syntax

```
system terminate-rasession <sessionid>
```

The following table describes the required and optional parameters for the **`system terminate-rasession`** command:

Table 372: *Terminate Remote Session Command Parameters*

Flag/Parameter	Description
<sessionid>	Provides the sessionid that can be used to terminate-session.

system status-rasession

The **`system status-rasession`** command allows administrators to acquire the status on the Dell Networking W-ClearPass Policy Manager in the cluster where the remote session is running.

Syntax

```
system status-rasession <sessionid>
```

The following table describes the required and optional parameters for the **`system status-rasession`** command:

Table 373: *Terminate Remote Session Command Parameters*

Flag/Parameter	Description
<sessionid>	Specifies the id returned when **`system status-rasession`** command is executed.

The Policy Manager administration User Interface allows you to create different types of objects:

- Service rules
- Role mapping policies
- Internal user policies
- Enforcement policies
- Enforcement profiles
- Post-audit rules
- Proxy attribute pruning rules
- Filters for Access Tracker and activity reports
- Attributes editing for policy simulation

When editing all these elements, you are presented with a tabular interface with the same column headers:

- **Type** - Type is the namespace from which these attributes are defined. This is a drop-down list that contains namespaces defined in the system for the current editing context.
- **Name** - Name is the name of the attribute. This is a drop-down list with the names of the attributes present in the namespace.
- **Operator** - Operator is a list of operators appropriate for the data type of the attribute. The drop-down list shows the operators appropriate for data type on the left (that is, the attribute).
- **Value** - The value is the value of the attribute. Again, depending on the data type of the attribute, the value field can be a free-form one-line edit box, a free-form multi-line edit box, a drop-down list containing pre-defined values (enumerated types), or a time or date widget.

In some editing interfaces (for example, enforcement profile and policy simulation attribute editing interfaces) the operator does not change; it is always the EQUALS operator.

Providing a uniform tabular interface to edit all these elements enables you to use the same steps while configuring these elements. Also, providing a context-sensitive editing experience (for names, operators and values) takes the guess-work out of configuring these elements.

The following sections describe namespaces, variables, and operators:

- Namespaces on page 601
- Variables on page 611
- Operators on page 612

Namespaces

Multiple namespaces are displayed in the rules editing interfaces, depending upon what you are editing. For example, multiple namespaces are displayed when you are editing posture policies you work with the posture namespace; when you are editing service rules you work with, among other namespaces, the RADIUS namespace, but not the posture namespace.

For detailed information about the available namespaces, see the following topics:

- Application Namespace on page 602
- Audit Namespaces on page 603

Application Namespace

The Application namespace has one name attribute. This attribute is an enumerated type currently containing the following string values:

- Guest
- Insight
- PolicyManager
- Onboard
- ClearPass

The Application:ClearPass namespace has the following string values available for the **Name** field:

- AssertionConsumerUrl
- Configuration-Profile-ID
- Device-Compromised
- Device-ICCID
- Device-IMEI
- Device-MAC
- Device-MDM-Managed
- Device-NAME
- Device-OS
- Device-PRODUCT
- Device-SERIAL
- Device-UDID
- Device-VERSION
- IDDP-COOKIE-TIMEOUT-MINS
- IDPURL
- MDM-Data-Roaming
- MDM-Voice-Roaming
- Onboard-Max-Devices

- Page-Name
- Provisioning-Settings-ID
- SAMLRequest
- SAMLResponse
- Session-Timeout
- User-Email-Address

Audit Namespaces

The dictionaries in the audit namespace come pre-packaged with the product. The Audit namespace has the notation *Vendor*:Audit, where *Vendor* is the name of the company that has defined attributes in the dictionary.

Examples of dictionaries in the audit namespace are AvendaSystems:Audit or Qualys:Audit.

The Audit namespace appears when editing post-audit rules. See Audit Servers for more information.

The Avenda Systems:Audit namespace appears when editing post-audit rules for NESSUS and NMAP audit servers.

The following figure displays the Audit Namespace attributes:

Table 374: *Audit Namespace Attributes*

Attribute Name	Values
Audit-Status	• AUDIT_ERROR • AUDIT_INPROGRESS • AUDIT_SUCCESS
Device-Type	Type of device returned by an NMAP port scan.
Output-Msgs	The output message returned by Nessus plugin after a vulnerability scan.
Network-Apps	String representation of the open network ports (http, telnet, etc.).
Mac-Vendor	Vendor associated with MAC address of the host.
OS-Info	OS information string returned by NMAP.
Open-Ports	The port numbers of open applications on the host.

Authentication Namespaces

The authentication namespace can be used in role mapping policies to define roles based on the type of authentication method used or the status of the authentication.

Authentication Namespace Editing Context

The following table describes the **Authentication Namespace Attributes** parameters:

Table 375: *Authentication Namespace Attributes*

Attribute Name	Values
InnerMethod	• CHAP • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • EAP-TLS • MSCHAP • PAP **NOTE:** The **EAP-MD5** authentication type is not supported if you use the Dell Networking W-ClearPass Policy Manager in the FIPS mode.
OuterMethod	• CHAP • EAP-FAST • EAP-MD5 • EAP-PEAP • EAP-TLS • EAP-TTLS • MSCHAP • PAP **NOTE:** The **EAP-MD5** authentication type is not supported if you use the Dell Networking W-ClearPass Policy Manager in the FIPS mode.
Phase1PAC	• **None** - No PAC was used to establish the outer tunnel in the EAP-FAST authentication method • **Tunnel** - A tunnel PAC was used to establish the outer tunnel in the EAP-FAST authentication method • **Machine** - A machine PAC was used to establish the outer tunnel in the EAP-FAST authentication method; machine PAC is used for machine authentication (See EAP-FAST in Adding and Modifying Authentication Methods on page 145).
Phase2PAC	• **None** - No PAC was used instead of an inner method handshake in the EAP-FAST authentication method • **UserAuthPAC** - A user authentication PAC was used instead of the user authentication inner method handshake in the EAP-FAST authentication method • **PosturePAC** - A posture PAC was used instead of the posture credential handshake in the EAP-FAST authentication method
Posture	• **Capable** - The client is capable of providing posture credentials • **Collected** - Posture credentials were collected from the client • **Not-Capable** - The client is not capable of providing posture credentials • **Unknown** - It is not known whether the client is capable of providing credentials
Status	• **None** - No authentication took place • **User** - The user was authenticated • **Machine** - The machine was authenticated • **Failed** - Authentication failed

Table 375: *Authentication Namespace Attributes (Continued)*

Attribute Name	Values
	• **AuthSource-Unreachable** - The authentication source was unreachable
MacAuth	• **NotApplicable** - Not a MAC Auth request • **Known Client** - Client MAC address was found in an authentication source • **Unknown Client** - Client MAC address was not found in an authentication source
Username	The username as received from the client (after the strip user name rules are applied).
Full-Username	The username as received from the client (before the strip user name rules are applied).
Source	The name of the authentication source used to authenticate the user.

Authorization Namespaces

Policy Manager supports multiple types of authorization sources. Authorization sources from which values of attributes can be retrieved to create role mapping rules have their own separate namespaces (prefixed with Authorization).

Authorization editing context

Role mapping policies

AD Instance Namespace

For each instance of an Active Directory authentication source, there is an AD instance namespace that appears in the rules editing interface. The AD instance namespace consists of all the attributes that were defined when the authentication source was created. These attribute names are pre-populated. For Policy Manager to fetch the values of attributes from Active Directory, you need to define filters for that authentication source (see Adding and Modifying Authentication Sources on page 169 for more information).

Authorization

The authorization namespace has one attribute: sources. The values are pre-populated with the authorization sources defined in Policy Manager. Use this to check for the authorization source(s) from which attributes were extracted for the authenticating entity.

LDAP Instance Namespace

For each instance of an LDAP authentication source, there is an LDAP instance namespace that appears in the rules editing interface. The LDAP instance namespace consists of all the attributes that were defined when the authentication source was created. These attribute names are pre-populated. For Policy Manager to fetch the values of attributes from an LDAP-compliant directory, you need to define filters for that authentication source (see Adding and Modifying Authentication Sources on page 169).

RSAToken Instance Namespace

For each instance of an RSA Token Server authentication source, there is an RSA Token Server instance namespace that appears in the rules editing interface. The RSA Token Server instance namespace consists of

attributes names defined when you created an instance of this authentication source. The attribute names are pre-populated for administrative convenience.

Sources

This is the list of the authorization sources from which attributes were fetched for role mapping. Authorization namespaces appear in Role mapping policies.

SQL Instance Namespace

For each instance of an SQL authentication source, there is an SQL instance namespace that appears in the rules editing interface. The SQL instance namespace consists of attributes names defined when you created an instance of this authentication source. The attribute names are pre-populated for administrative convenience. For Policy Manager to fetch the values of attributes from a SQL-compliant database, you need to define filters for that authentication source.

Certificate Namespaces

The certificate namespace can be used in role mapping policies to define roles based on attributes in the client certificate presented by the end host. Client certificates are presented in mutually authenticated 802.1X EAP methods (EAP-TLS, PEAP/TLS, EAP-FAST/TLS).

Certificate Namespace Editing Context

Role mapping policies

Table 376: *Certificate Namespace Attributes*

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

Table 376: *Certificate Namespace Attributes (Continued)*

Attribute Name	Values
• Issuer-O • Issuer-OU • Issuer-SN • Issuer-ST • Issuer-UID	
• Subject-AltName-DirName • Subject-AltName-DNS • Subject-AltName-EmailAddress • Subject-AltName-IPAddress • Subject-AltName-msUPN • Subject-AltName-RegisterdID • Subject-AltName-URI	Attributes associated with the subject (user or machine, in this case) alternate name. Not all of these fields are populated in a certificate.

Connection Namespaces

The connection namespace can be used in role mapping policies to define roles based on where the protocol request originated from and where it terminated.

Connection Namespace Editing Contexts

- Role mapping policies
- Service rules

The following table describes the **Connection Namespace Pre-defined Attributes** parameters:

Table 377: *Connection Namespace Pre-defined Attributes*

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

Table 377: *Connection Namespace Pre-defined Attributes (Continued)*

Attribute	Description
Client-Mac-Address	MAC address of the client.
• Client-Mac-Address-Colon • Client-Mac-Address-Dot • Client-Mac-Address-Hyphen • Client-Mac-Address-Nodelim	Client MAC address in different formats.
Client-IP-Address	IP address of the client (if known).

Date Namespaces

The date namespace has three pre-defined attributes:

- Day-of-Week
- Date-of-Year
- Time-of-Day

For Day-of-Week, the supported operators are BELONG_TO and NOT_BELONGS_TO, and the value field shows a multi-select list box with days from Monday through Sunday.

The Time-of-Day attribute shows a time icon in the value field.

The Date-of-Year attribute shows a date, month and year icon in the value field.

The operators supported for Date-of-Year and Time-of-Day attributes are the similar to the ones supported for the integer data type.

Date Namespace Editing Contexts

- Enforcement policies
- Filter rules for Access Tracker and Activity Reports
- Role mapping policies
- Service rules

Device Namespaces

The Device namespace has four pre-defined attributes:

- Location
- OS-Version
- Device-Type
- Device-Vendor

Custom attributes also appear in the attribute list if they are defined as custom tags for the device.

These attributes can be used only if you have pre-populated the values for these attributes when a network device is configured.

Endpoint Namespaces

Use these attributes to look for attributes of authenticating endpoints, which are present in the Policy Manager endpoints list. The Endpoint namespace has the following attributes:

- Disabled By
- Disabled Reason
- Enabled By
- Enabled Reason
- Info URL

Guest User Namespaces

The GuestUser namespace has the attributes associated with the guest user (resident in the Policy Manager guest user database) who authenticated in this session. This namespace is only applicable if a guest user is authenticated. The GuestUser namespace has six pre-defined attributes:

- Company-Name
- Designation
- Email
- Location
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the guest user.

These attributes can be used only if you have pre-populated the values for these attributes when a guest user is configured in Policy Manager.

Host Namespaces

The Host namespace has the following predefined attributes:

- Name*
- OSType*
- FQDN*
- UserAgent**
- CheckType**
- UniqueID
- AgentType*
- InstalledSHAs*

* Only populated when request is originated by a Microsoft NAP-compatible agent.

** Only present if Policy Manager acts as a Web authentication portal.

Local User Namespaces

The LocalUser namespace has the attributes associated with the local user (resident in the Policy Manager local user database) who authenticated in this session. This namespace is only applicable if a local user is authenticated.

The LocalUser namespace has four pre-defined attributes:

- Designation

- Email
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the local user.

These attributes can be used only if you have pre-populated the values for these attributes when a local user is configured in Policy Manager.

Posture Namespaces

The dictionaries in the posture namespace are pre-packaged with the product. The administration interface provides a way to add dictionaries into the system (see Posture Dictionary on page 540) Posture namespace has the notation *Vendor:*Application, where *Vendor* is the name of the Company that has defined attributes in the dictionary, and Application is the name of the application for which the attributes have been defined. The same vendor typically has different dictionaries for different applications.

Some examples of dictionaries in the posture namespace are:

- ClearPass:LinuxSHV
- Microsoft:SystemSHV
- Microsoft:WindowsSHV
- Trend:AV

Posture Namespace Editing Context

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

RADIUS Namespaces

Dictionaries in the RADIUS namespace come pre-packaged with the product. The administration interface does provide a way to add dictionaries into the system (See RADIUS Dictionary on page 538 for more information). RADIUS namespace has the notation RADIUS:Vendor, where Vendor is the name of the Company that has defined attributes in the dictionary. Sometimes, the same vendor has multiple dictionaries, in which case the "Vendor" portion has the name suffixed by the name of device or some other unique string.

IETF is a special vendor for the dictionary that holds the attributes defined in the RFC 2865 and other associated RFCs. Policy Manager comes pre-packaged with a number of vendor dictionaries.

Some examples of dictionaries in the RADIUS namespace are:

- RADIUS:Aruba
- RADIUS:IETF
- RADIUS:Juniper
- RADIUS:Microsoft

RADIUS Namespace Editing Contexts

- Filter rules for Access Tracker and Activity Reports
- Policy simulation attributes
- Post-proxy attribute pruning rules

- RADIUS Enforcement profiles: All RADIUS namespace attributes that can be sent back to a RADIUS client (the ones marked with the OUT or INOUT qualifier)
- Role mapping policies
- Service rules: All RADIUS namespace attributes that can appear in a request (the ones marked with the IN or INOUT qualifier)

Tacacs Namespaces

The Tacacs namespace has the attributes associated with attributes available in a TACACS+ request. Available attributes are:

- AuthSource
- AvendaAVPair
- UserName

Tips Namespaces

The pre-defined attributes for the Tips namespace are *Role* and *Posture*. Values are assigned to these attributes at run-time after Policy Manager evaluates role mapping and posture related policies.

Role

The value for the Role attribute is a set of roles assigned by either the role mapping policy or the post-audit policy. The value of the Role attribute can also be a dynamically fetched "Enable as role" attribute from the authorization source. The posture value is computed after Policy Manager evaluates internal posture policies, and gets posture status from posture servers or audit servers.

Posture

The value for the Posture attribute is one of the following:

- CHECKUP
- HEALTHY
- INFECTED
- QUARANTINE
- TRANSITION
- UNKNOWN

Tips Namespace Editing Context

Enforcement policies

Variables

Variables are populated with the connection-specific values. Variable names (prefixed with % and enclosed in curly braces; for example, %{Username}") can be used in filters, role mapping, enforcement rules, and enforcement profiles. Policy Manager does in-place substitution of the value of the variable during runtime rule evaluation.

The following built-in variables are supported in Policy Manager:

Table 378: *Policy Manager Variables*

Variable	Description
%{*attribute-name*}	*attribute-name* is the alias name for an attribute that you have configured to be retrieved from an authentication source. See Adding and Modifying Authentication Sources on page 169.
%{RADIUS:IETF:MAC-Address-Colon}	MAC address of client in aa:bb:cc:dd:ee:ff format
%{RADIUS:IETF:MAC-Address-Hyphen}	MAC address of client in aa-bb-cc-dd-ee-ff format
%{RADIUS:IETF:MAC-Address-Dot}	MAC address of client in aabb.ccdd.eeff format
%{RADIUS:IETF:MAC-Address-NoDelim}	MAC address of client in aabbccddeeff format

You can also use any other dictionary-based attributes (or namespace attributes) as variables in role mapping rules, enforcement rules, enforcement profiles, and LDAP or SQL filters. For example, you can use %{RADIUS:IETF:Calling-Station-ID}or %{RADIUS:Airespace:Airespace-Wlan-Id} in rules or filters.

Operators

The rules editing interface in Policy Manager supports a rich set of operators. The type of operators presented are based on the data type of the attribute for which the operator is being used. Where the data type of the attribute is not known, the attribute is treated as a string type.

The following table lists the operators presented for common attribute data types:

Table 379: *Attribute Operators*

Attribute Type	Operators
String	• BELONGS_TO • NOT_BELONGS_TO • BEGINS_WITH • NOT_BEGINS_WITH • CONTAINS • NOT_CONTAINS • ENDS_WITH • NOT_ENDS_WITH • EQUALS • NOT_EQUALS • EQUALS_IGNORE_CASE • NOT_EQUALS_IGNORE_CASE • EXISTS • NOT_EXISTS • MATCHES_REGEX • NOT_MATCHES_REGEX
Integer	• BELONGS_TO • NOT_BELONGS_TO • EQUALS • NOT_EQUALS • EXISTS • NOT_EXISTS • GREATER_THAN • GREATER_THAN_OR_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS
Time or Date	• EQUALS NOT_EQUALS • GREATER_THAN • GREATER_THAN_OR_EQUALS

Table 379: *Attribute Operators (Continued)*

Attribute Type	Operators
	• LESS_THAN • LESS_THAN_OR_EQUALS • IN_RANGE
Day	• BELONGS_TO • NOT_BELONGS_TO
List (Example: Role)	• EQUALS • NOT_EQUALS • MATCHES_ALL • NOT_MATCHES_ALL • MATCHES_ANY • NOT_MATCHES_ANY • MATCHES_EXACT • NOT_MATCHES_EXACT
Group (Example: Calling-Station-Id, NAS-IP-Address)	• BELONGS_TO_GROUP • NOT_BELONGS_TO_GROUP and all string data types

The following table describes all operator types:

Table 380: *Operator Types*

Operator	Description
BEGINS_WITH	For string data type, true if the run-time value of the attribute begins with the configured value. Example: `RADIUS:IETF:NAS-Identifier BEGINS_WITH "SJ-"`
BELONGS_TO	For string data type, true if the run-time value of the attribute matches a set of configured string values. Example: `RADIUS:IETF:Service-Type BELONGS_TO Login-User,Framed-User,Authenticate-Only` For integer data type, true if the run-time value of the attribute matches a set of configured integer values. Example: `RADIUS:IETF:NAS-Port BELONGS_TO 1,2,3` For day data type, true if run-time value of the attribute matches a set of configured days of the week. Example: `Date:Day-of-Week BELONGS_TO MONDAY,TUESDAY,WEDNESDAY` When Policy Manager is aware of the values that can be assigned to BELONGS_TO operator, it populates the value field with those values in a multi-select list box; you can select the appropriate values from the presented list. Otherwise, you must enter a comma separated list of values.
BELONGS_TO_GROUP	For group data types, true if the run-time value of the attribute belongs to the configured group (either a static host list or a network device group, depending on the attribute). Example: `RADIUS:IETF:Calling-Station-Id BELONGS_TO_GROUP Printers`.
CONTAINS	For string data type, true if the run-time value of the attribute is a substring of the configured value. Example: `RADIUS:IETF:NAS-Identifier CONTAINS "VPN"`
ENDS_WITH	For string data type, true if the run-time value of the attribute ends with the configured value. Example: `RADIUS:IETF:NAS-Identifier ENDS_WITH "DEVICE"`
EQUALS	True if the run-time value of the attribute matches the configured value. For string data type, this is a case-sensitive comparison. Example: `RADIUS:IETF:NAS-Identifier EQUALS "SJ-VPN-DEVICE"`
EQUALS_IGNORE_CASE	For string data type, true if the run-time value of the attribute matches the configured value, regardless of whether the string is upper case or lower case. Example: `RADIUS:IETF:NAS-Identifier EQUALS_IGNORE_CASE "sj-vpn-device"`
EXISTS	For string data type, true if the run-time value of the attribute exists. This is a unary operator. Example: `RADIUS:IETF:NAS-Identifier EXISTS`

Operator	Description
GREATER_THAN	For integer, time and date data types, true if the run-time value of the attribute is greater than the configured value. Example: `RADIUS:IETF:NAS-Port GREATER_THAN 10`
GREATER_THAN_OR_EQUALS	For integer, time and date data types, true if the run-time value of the attribute is greater than or equal to the configured value. Example: `RADIUS:IETF:NAS-Port GREATER_THAN_OR_EQUALS 10`
IN_RANGE	For time and date data types, true if the run-time value of the attribute is less than or equal to the first configured value and less than equal to the second configured value. Example: `Date:Date-of-Year IN_RANGE 2007-06-06,2007-06-12`
LESS_THAN	For integer, time and date data types, true if the run-time value of the attribute is less than the configured value. Example: `RADIUS:IETF:NAS-Port LESS_THAN 10`
LESS_THAN_OR_EQUALS	For integer, time and date data types, true if the run-time value of the attribute is less than or equal to the configured value. Example: `RADIUS:IETF:NAS-Port LESS_THAN_OR_EQUALS 10`
MATCHES_ALL	For list data types, true if all of the run-time values in the list are found in the configured values. Example: `Tips:Role MATCHES_ALL HR,ENG,FINANCE`. In this example, if the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to true.
MATCHES_ANY	For list data types, true if any of the run-time values in the list match one of the configured values. Example: `Tips:Role MATCHES_ANY HR,ENG,FINANCE`
MATCHES_EXACT	For list data types, true if all of the run-time values of the attribute match all of the configured values. Example: `Tips:Role MATCHES_ALL HR,ENG,FINANCE`. In this example, if the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to false, because there are some values in the configured values that are not present in the run-time values.
MATCHES_REGEX	For string data type, true if the run-time value of the attribute matches the regular expression in the configured value. Example: `RADIUS:IETF:NAS-Identifier MATCHES_REGEX sj-device[1-9]-dev*`

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

Error Codes

The following table shows the CPPM error codes:

Table 381: *CPPM Error Codes*

Code	Description	Type
0	Success	Success
101	Failed to perform service classification	Internal Error
102	Failed to perform policy evaluation	Internal Error
103	Failed to perform posture notification	Internal Error
104	Failed to query authstatus	Internal Error
105	Internal error in performing authentication	Internal Error
106	Internal error in RADIUS server	Internal Error
201	User not found	Authentication failure
202	Password mismatch	Authentication failure
203	Failed to contact AuthSource	Authentication failure
204	Failed to classify request to service	Authentication failure
205	AuthSource not configured for service	Authentication failure
206	Access denied by policy	Authentication failure
207	Failed to get client macAddress to perform webauth	Authentication failure
208	No response from home server	Authentication failure
209	No password in request	Authentication failure
210	Unknown CA in client certificate	Authentication failure

Table 381: *CPPM Error Codes (Continued)*

Code	Description	Type
211	Client certificate not valid	Authentication failure
212	Client certificate has expired	Authentication failure
213	Certificate comparison failed	Authentication failure
214	No certificate in authentication source	Authentication failure
215	TLS session error	Authentication failure
216	User authentication failed	Authentication failure
217	Search failed due to insufficient permissions	Authentication failure
218	Authentication source timed out	Authentication failure
219	Bad search filter	Authentication failure
220	Search failed	Authentication failure
221	Authentication source error	Authentication failure
222	Password change error	Authentication failure
223	Username not available in request	Authentication failure
224	CallingStationID not available in request	Authentication failure
225	User account disabled	Authentication failure
226	User account expired or not active yet	Authentication failure
227	User account needs approval	Authentication failure
228	User account has exceeded bandwidth limit	Authentication failure
229	User account has exceeded session duration limit	Authentication failure
230	User account has exceeded session count limit	Authentication failure
5001	Internal Error	Command and Control
5002	Invalid MAC Address	Command and Control
5003	Invalid request received	Command and Control
5004	Insufficient parameters received	Command and Control
5005	Query - No MAC address record found	Command and Control

Table 381: *CPPM Error Codes (Continued)*

Code	Description	Type
5006	Query - No supported actions	Command and Control
5007	Query - Cannot fetch MAC address details	Command and Control
5008	Request - MAC address not online	Command and Control
5009	Request - No MAC address record found	Command and Control
6001	Unsupported TACACS parameter in request	TACACS Protocol
6002	Invalid sequence number	TACACS Protocol
6003	Sequence number overflow	TACACS Protocol
6101	Not enough inputs to perform authentication	TACACS Authentication
6102	Authentication privilege level mismatch	TACACS Authentication
6103	No enforcement profiles matched to perform authentication	TACACS Authentication
6201	Authorization failed as session is not authenticated	TACACS Authorization
6202	Authorization privilege level mismatch	TACACS Authorization
6203	Command not allowed	TACACS Authorization
6204	No enforcement profiles matched to perform command authorization	TACACS Authorization
6301	New password entered does not match	TACACS Change Password
6302	Empty password	TACACS Change Password
6303	Change password allowed only for local users	TACACS Change Password
6304	Internal error in performing change password	TACACS Change Password
9001	Wrong shared secret	RADIUS Protocol
9002	Request timed out	RADIUS Protocol
9003	Phase2 PAC failure	RADIUS Protocol
9004	Client rejected after PAC provisioning	RADIUS Protocol
9005	Client does not support posture request	RADIUS Protocol
9006	Received error TLV from client	RADIUS Protocol
9007	Received failure TLV from client	RADIUS Protocol

Table 381: *CPPM Error Codes (Continued)*

Code	Description	Type
9008	Phase2 PAC not found	RADIUS Protocol
9009	Unknown Phase2 PAC	RADIUS Protocol
9010	Invalid Phase2 PAC	RADIUS Protocol
9011	PAC verification failed	RADIUS Protocol
9012	PAC binding failed	RADIUS Protocol
9013	Session resumption failed	RADIUS Protocol
9014	Cached session data error	RADIUS Protocol
9015	Client does not support configured EAP methods	RADIUS Protocol
9016	Client did not send Cryptobinding TLV	RADIUS Protocol
9017	Failed to contact OCSP Server	RADIUS Protocol
9018	RADIUS protocol error	RADIUS Protocol
9019	Client sent conflicting identities	RADIUS Protocol

SNMP Trap Details

Dell Networking W-ClearPass Policy Manager leverages native SNMP support from the UC Davis 'net-SNMP' MIB package to send trap notifications for the following events.

In these trap OIDs, the value of X varies from 1 through N, depending on the number of process states that are being checked. Details about specific OIDs associated with the processes are listed in this section.

For more information, see:

- SNMP Daemon Trap Events on page 620
- CPPM Processes Stop and Start Events on page 621
- Network Interface up and Down Events on page 621
- Disk Utilization Threshold Exceed Events on page 621
- CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds on page 621
- SNMP Daemon Traps on page 621
- Process Status Traps on page 621
- Network Interface Status Traps on page 629
- Disk Space Threshold Traps on page 629
- CPU Load Average Traps on page 629

SNMP Daemon Trap Events

OIDs:

.1.3.6.1.6.3.1.1.5.1 ==> Cold Start

.1.3.6.1.6.3.1.1.5.2 ==> Warm Start

Network Interface up and Down Events

OIDs:

.1.3.6.1.6.3.1.1.5.3 ==> Link Down

.1.3.6.1.6.3.1.1.5.4 ==> Link Up

CPPM Processes Stop and Start Events

OIDs:

.1.3.6.1.4.1.2021.8.1.2.X ==> Process Name

.1.3.6.1.4.1.2021.2.1.101.X ==> Process Status Message

Disk Utilization Threshold Exceed Events

OIDs:

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag for disk partition

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition

CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds

OIDs

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag for disk partition

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition

SNMP Daemon Traps

This section contains OIDs for various trap events that are sent from CPPM.

.1.3.6.1.6.3.1.1.5.1 ==> Coldstart trap indicating the reinitialization of 'netsnmp' daemon and its configuration file may have been altered.

.1.3.6.1.6.3.1.1.5.2 ==> Warmstart trap indicating the reinitialization of 'netsnmp' daemon and its configuration file is not altered.

Figure 528: *SNMP daemon traps example*

Process Status Traps

RADIUS server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.5

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.5: cpass-radius-server

.1.3.6.1.4.1.2021.8.1.101.5: Radius server [cpass-radius-server] is stopped

RADIUS server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.5

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.5: cpass-radius-server

.1.3.6.1.4.1.2021.8.1.101.5: Radius server [cpass-radius-server] is running

Admin Server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.1

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.1: cpass-admin-server

.1.3.6.1.4.1.2021.8.1.101.1: Admin server [cpass-admin-server] is stopped

Admin Server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.1

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.1: cpass-admin-server

.1.3.6.1.4.1.2021.8.1.101.1: Admin server [cpass-admin-server] is running

System Auxiliary server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.2

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.2: cpass-system-auxiliary-server

.1.3.6.1.4.1.2021.8.1.101.2: System auxiliary service [cpass-system-auxiliary-server] is stopped

System Auxiliary server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.2

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.2: cpass-system-auxiliary-server

.1.3.6.1.4.1.2021.8.1.101.2: System auxiliary service [cpass-system-auxiliary-server] is running

Policy server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.3

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.3: cpass-policy-server

.1.3.6.1.4.1.2021.8.1.101.3: Policy server [cpass-policy-server] is stopped

Policy server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.3

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.3: cpass-policy-server

.1.3.6.1.4.1.2021.8.1.101.3: Policy server [cpass-policy-server] is running

Async DB write service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.6

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.6: cpass-dbwrite-server

.1.3.6.1.4.1.2021.8.1.101.6: Async DB write service [cpass-dbwrite-server] is stopped

Async DB write service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.6

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.6: cpass-dbwrite-server

.1.3.6.1.4.1.2021.8.1.101.6: Async DB write service [cpass-dbwrite-server] is running

DB replication service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.7

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.7: cpass-repl-server

.1.3.6.1.4.1.2021.8.1.101.7: DB replication service [cpass-repl-server] is stopped

DB replication service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.7

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.7: cpass-repl-server

.1.3.6.1.4.1.2021.8.1.101.7: DB replication service [cpass-repl-server] is running

DB Change Notification server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.8

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.8: cpass-dbcn-server

.1.3.6.1.4.1.2021.8.1.101.8: DB change notification server [cpass-dbcn-server] is stopped

DB Change Notification server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.8

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.8: cpass-dbcn-server

.1.3.6.1.4.1.2021.8.1.101.8: DB change notification server [cpass-dbcn-server] is running

Async netd service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.9

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.9: cpass-async-netd

.1.3.6.1.4.1.2021.8.1.101.9: Async netd service [cpass-async-netd] is stopped

Async netd service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.9

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.9: cpass-async-netd

.1.3.6.1.4.1.2021.8.1.101.9: Async netd service [cpass-async-netd] is running

Multi-master Cache service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.10

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.10: cpass-multi-master-cache-server

.1.3.6.1.4.1.2021.8.1.101.10: Multi-master cache [cpass-multi-master-cache-server] is stopped

Multi-master Cache service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.10

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.10: cpass-multi-master-cache-server

.1.3.6.1.4.1.2021.8.1.101.10: Multi-master cache [cpass-multi-master-cache-server] is running

AirGroup Notification service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.11

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.11: airgroup-notify

.1.3.6.1.4.1.2021.8.1.101.11: AirGroup notification service [airgroup-notify] is stopped

AirGroup Notification service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.11

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.11: airgroup-notify

.1.3.6.1.4.1.2021.8.1.101.11: AirGroup notification service [airgroup-notify] is running

Micros Fidelio FIAS service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.12

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.12: fias_server

.1.3.6.1.4.1.2021.8.1.101.12: Micros Fidelio FIAS [fias_server] is stopped

Micros Fidelio FIAS service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.12

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.12: fias_server

.1.3.6.1.4.1.2021.8.1.101.12: Micros Fidelio FIAS [fias_server] is running

TACACS server stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.4

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.4: cpass-tacacs-server

.1.3.6.1.4.1.2021.8.1.101.4: TACACS server [cpass-tacacs-server] is stopped

TACACS server start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.4

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.4: cpass-tacacs-server

.1.3.6.1.4.1.2021.8.1.101.4: TACACS server [cpass-tacacs-server] is running

Virtual IP service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.13

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.13: cpass-vip-service

.1.3.6.1.4.1.2021.8.1.101.13: ClearPass Virtual IP service [cpass-vip-service] is stopped

Virtual IP service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0:

.1.3.6.1.2.1.88.2.1.3.0:

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.13

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.13: cpass-vip-service

.1.3.6.1.4.1.2021.8.1.101.13: ClearPass Virtual IP service [cpass-vip-service] is running

Stats Collection service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.15

.1.3.6.1.2.1.88.2.1.5.0: 3

.1.3.6.1.4.1.2021.8.1.2.15: cpass-statsd-server

.1.3.6.1.4.1.2021.8.1.101.15: Stats collection service [cpass-statsd-server] is stopped

Stats Collection service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.15

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.15: cpass-statsd-server

.1.3.6.1.4.1.2021.8.1.101.15: Stats collection service [cpass-statsd-server] is running

Stats Aggregation service stop SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.2

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.14

.1.3.6.1.2.1.88.2.1.5.0: 1

.1.3.6.1.4.1.2021.8.1.2.14: cpass-carbon-server

.1.3.6.1.4.1.2021.8.1.101.14: Stats aggregation service [cpass-carbon-server] is stopped

stats Aggregation service start SNMP trap

snmpTrapOID: .1.3.6.1.2.1.88.2.0.3

.1.3.6.1.2.1.88.2.1.1.0: extTable

.1.3.6.1.2.1.88.2.1.2.0

.1.3.6.1.2.1.88.2.1.3.0

.1.3.6.1.2.1.88.2.1.4.0: .1.3.6.1.4.1.2021.8.1.100.14

.1.3.6.1.2.1.88.2.1.5.0: 0

.1.3.6.1.4.1.2021.8.1.2.14: cpass-carbon-server

.1.3.6.1.4.1.2021.8.1.101.14: Stats aggregation service [cpass-carbon-server] is running.

Network Interface Status Traps

.1.3.6.1.6.3.1.1.5.3 ==> Indicates the linkdown trap with the 'ifAdminStatus' and 'ifOperStatus' values set to 2.

.1.3.6.1.6.3.1.1.5.4 ==> Indicates the linkup trap with the 'ifAdminStatus' and 'ifOperStatus' values set to 1.

In each case, the 'ifIndex' value is set to 2 for management interface and 3 for the data port interface.

Figure 529: *Network interface status traps example*

25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3 1.3.6.1.2.1.2.2.1.1.3 = 3 1.3.6.1.2.1.2.2.1.7.3 = 2 1.3.6.1.2.1.2.2.1.8.3 = 2
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4 1.3.6.1.2.1.2.2.1.1.2 = 2 1.3.6.1.2.1.2.2.1.7.2 = 1 1.3.6.1.2.1.2.2.1.8.2 = 1

Disk Space Threshold Traps

.1.3.6.1.4.1.2021.9.1.100.1 ==> Error flag indicating the disk or partition is under the minimum required space configured for it. Value of 1 indicates the system has reached the threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.9.1.2.1 ==> Name of the partition which has met the above condition.

Figure 530: *Disk Space Threshold Traps Example*

25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.2.1.1.3.0 = 44 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.2 1.3.6.1.2.1.88.2.1.1.0 = dskTable 1.3.6.1.2.1.88.2.1.2.0 = 1.3.6.1.2.1.88.2.1.3.0 = 1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.9.1.100.1 1.3.6.1.2.1.88.2.1.5.0 = 1 1.3.6.1.4.1.2021.9.1.2.1 = / 1.3.6.1.4.1.2021.9.1.101.1 = /: less than 99% free (= 13%)
25-Mar-13 01:57 PM	10.162.111.30	public	1.3.6.1.2.1.1.3.0 = 43 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3 1.3.6.1.2.1.88.2.1.1.0 = memory 1.3.6.1.2.1.88.2.1.2.0 = 1.3.6.1.2.1.88.2.1.3.0 = 1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.4.100.0 1.3.6.1.2.1.88.2.1.5.0 = 0 1.3.6.1.4.1.2021.4.2.0 = swap 1.3.6.1.4.1.2021.4.101.0 =

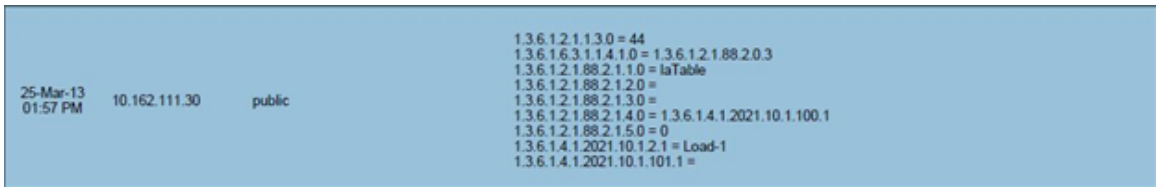
CPU Load Average Traps

OIDs

.1.3.6.1.4.1.2021.10.1.100.1 ==> Error flag on the CPU load-1 average. Value of 1 indicates the load-1 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.1 ==> Name of CPU load-1 average

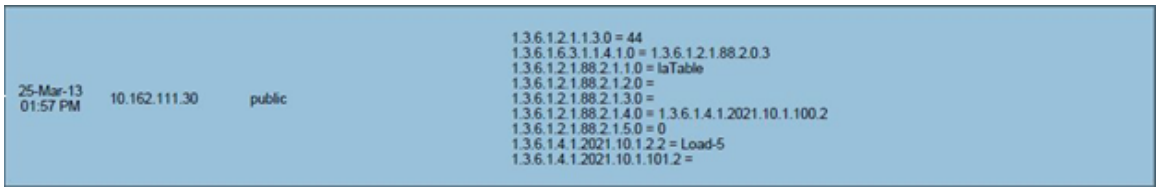
Figure 531: *CPU load-1 average example*



.1.3.6.1.4.1.2021.10.1.100.2 ==> Error flag on the CPU load-5 average. Value of 1 indicates the load-5 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.2 ==> Name of CPU load-5 average

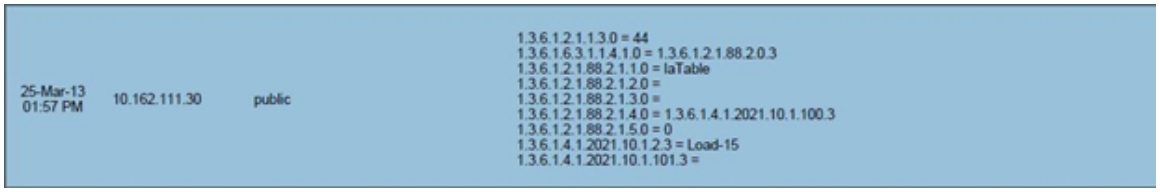
Figure 532: *CPU load-5 average example*



.1.3.6.1.4.1.2021.10.1.100.3 ==> Error flag on the CPU load-15 average. Value of 1 indicates the load-15 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.3 ==> Name of CPU load-15 average.

Figure 533: *CPU load-15 average example*



Important System Events

This topic describes the important System Events logged by ClearPass. These messages are available for consumption on the administrative interface, and in the form of a syslog stream. The events below are in the following format

<Source>, <Level>, <Category>, <Message>

Elements listed below within angular brackets (<content>) are variable, and are substituted by ClearPass as applicable (such as an IP address).

Refer to the Service Names on page 634 section for the list of available service names.

Admin UI Events

Critical Events

"Admin UI", "ERROR" "Email Failed", "Sending email failed"

"Admin UI", "ERROR" "SMS Failed", "Sending SMS failed"

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

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

Info Events

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

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

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

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

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

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

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

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

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

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

Admin Server Events

Info Events

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

Async Service Events

Info Events

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

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

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

ClearPass/Domain Controller Events

Critical Events

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

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

Info Events

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

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

ClearPass System Configuration Events

Critical Events

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

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

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

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

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

Info Events

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

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

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

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

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

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

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

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

ClearPass Update Events

Critical Events

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

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

Info Events

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

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

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

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

Cluster Events

Critical Events

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

Info Events

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

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

Command Line Events

Info Events

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

DB Replication Services Events

Info Events

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

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

"DB change notification server", "INFO", "Performed action start on DB change notification server"

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

Licensing Events

Critical Events

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

Info Events

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

Policy Server Events

Info Events

"Policy Server", "INFO", "Performed action start on Policy server"

"Policy Server", "INFO", "Performed action stop on Policy server"

RADIUS/TACACS+ Server Events

Critical Events

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

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

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

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

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

Info Events

"RADIUS", "INFO", "Performed action start on Radius server"

"RADIUS", "INFO", "Performed action restart on Radius server

"TACACS server", "INFO", "Performed action start on TACACS server"

"TACACS server", "INFO", "Performed action stop on TACACS server"

SNMP Events

Critical Events

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

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

Info Events

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

Support Shell Events

Info Events

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

System Auxiliary Service Events

Info Events

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

System Monitor Events

Critical Events

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

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

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

Info Events

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

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

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

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

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

Service Names

- AirGroup notification service
- Async DB write service
- Async network services
- DB change notification server
- DB replication service
- Micros Fidelio FIAS

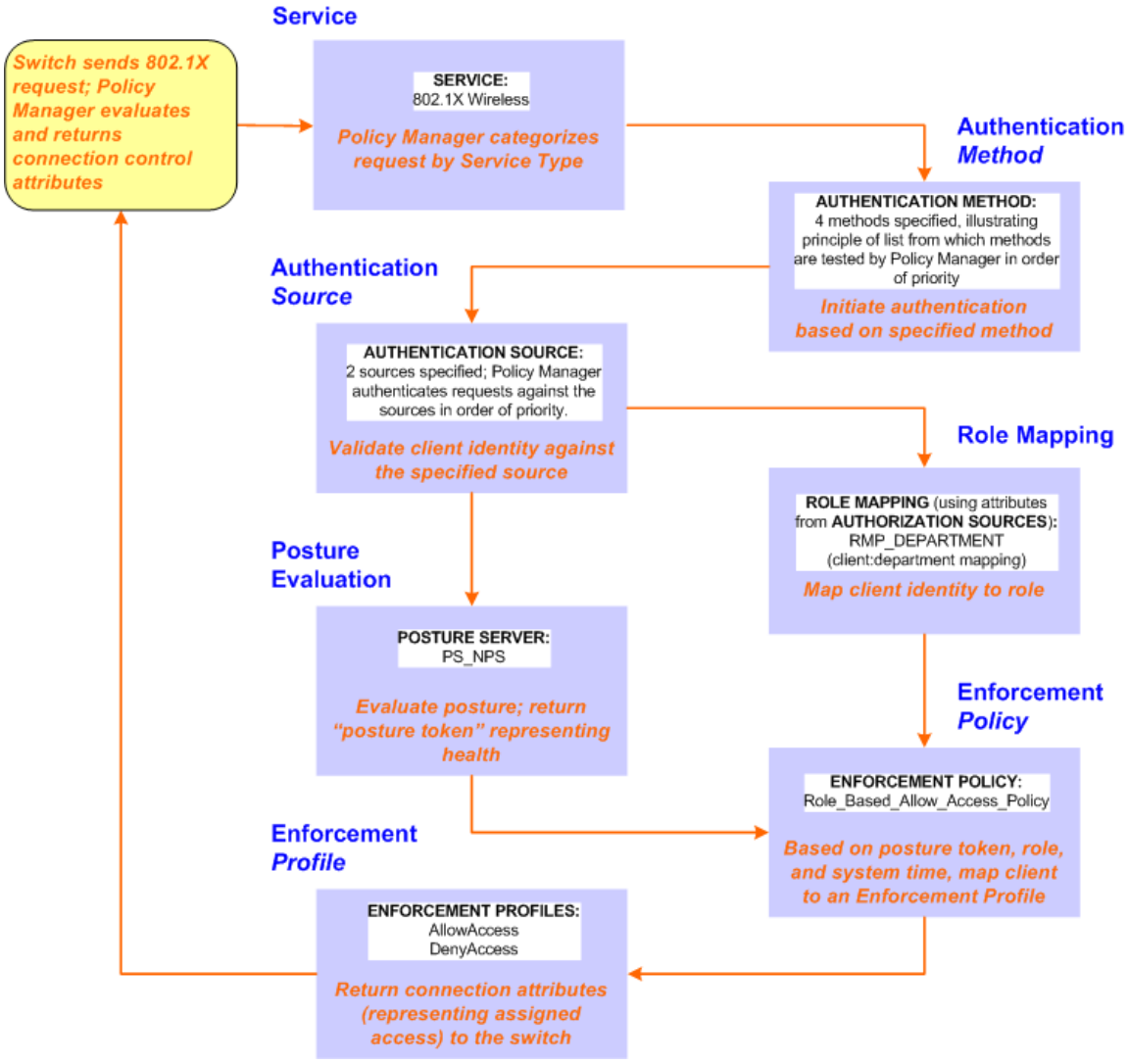
- Multi-master cache
- Policy server
- RADIUS server
- System auxiliary services
- System monitor service
- TACACS server
- Virtual IP service
- [YOURSERVERNAME] Domain service

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

802.1X Wireless Use Case

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

Figure 534: *Flow of Control, Basic 802.1X Configuration Use Case*



Policy Manager ships with fourteen preconfigured services. In this use case, you select a service that supports 802.1X wireless requests. Follow the steps below to configure this basic 802.1X service that uses **[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.

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. 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.

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)**.

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.

Configuring a Service

1. Navigate to **Configuration > Services.**
2. Click the Add icon to add a service. The **Configuration > Services > Add** window opens.
3. If it is not already selected, click the **Service** tab and define basic service information.
   a. Enter a name for the service in the **Name** field.
   b. Click the **Type** drop-down list and select **802.1X Wireless**.
   c. (Optional) click the Monitor Mode checkbox to allow handshakes to occur (for monitoring purposes), but without enforcement.
   d. Click **Next** to display the **Authentication** tab.
4. Configure authentication.
   a. In the **Authentication Methods** field, select **[EAP Fast]**.
   b. In the Authentication Sources field, click the Select to Add drop-down list and select the following sources.
      - [Local User Repository] [Local SQL DB]
      - [Guest User Repository] [Local SQL DB]
      - [Guest Device Repository] [Local SQL DB]
      - [Endpoints Repository] [Local SQL DB]
      - [Onboard Devices Repository] [Local SQL DB]
      - [Admin User Repository] [Local SQL DB]
      - [Active Directory]
   c. (Optional) Select **Strip Username Rules** to pre-process the user name (to remove prefixes and suffixes) before sending it to the authentication source.

Creating a New Role Mapping Policy

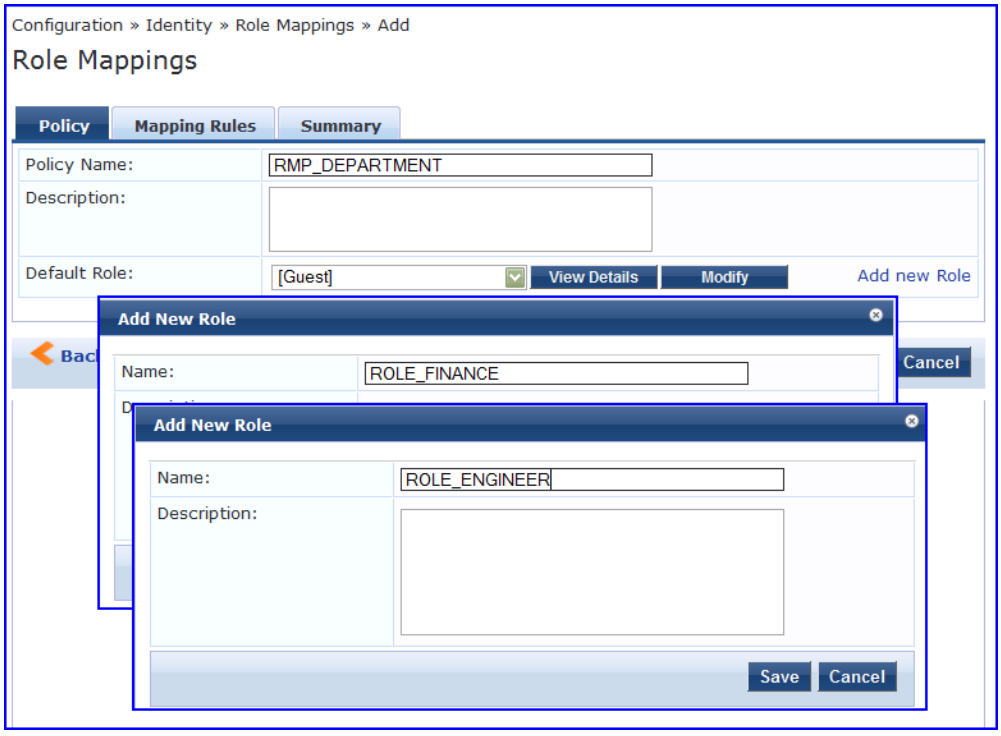
To create a new Role Mapping policy:

1. Click the **Roles** tab.
2. Click **Add new Role Mapping Policy**. The **Role Mappings** page opens.

Figure 535: *Role Mapping Navigation and Settings*

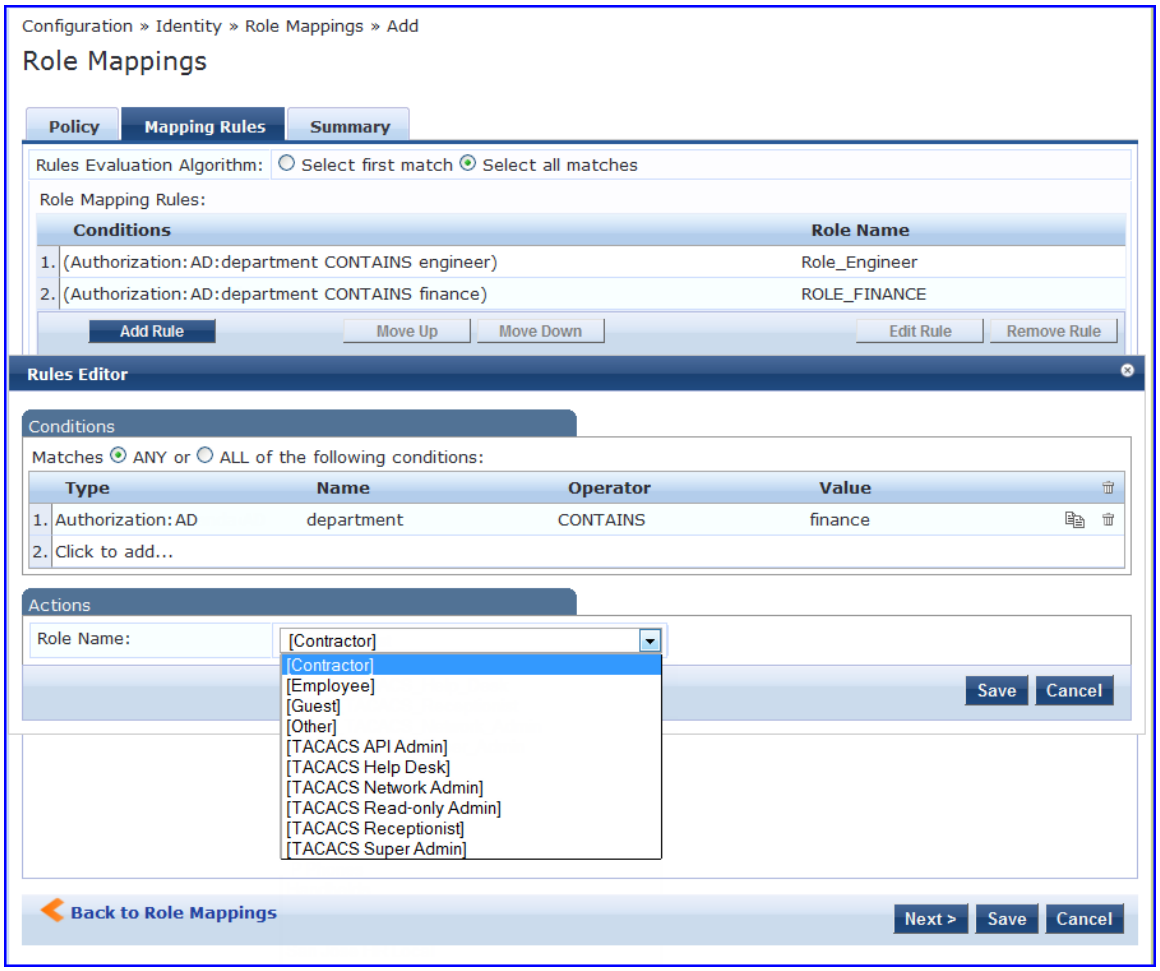
3. Add a new role, navigate to the **Policy** tab. Enter the **Policy Name**, For example, ROLE_ENGINEER and click **Save**. Repeat the same step for ROLE_FINANCE. The following figure displays the **Policy** tab:

Figure 536: *Policy Tab*



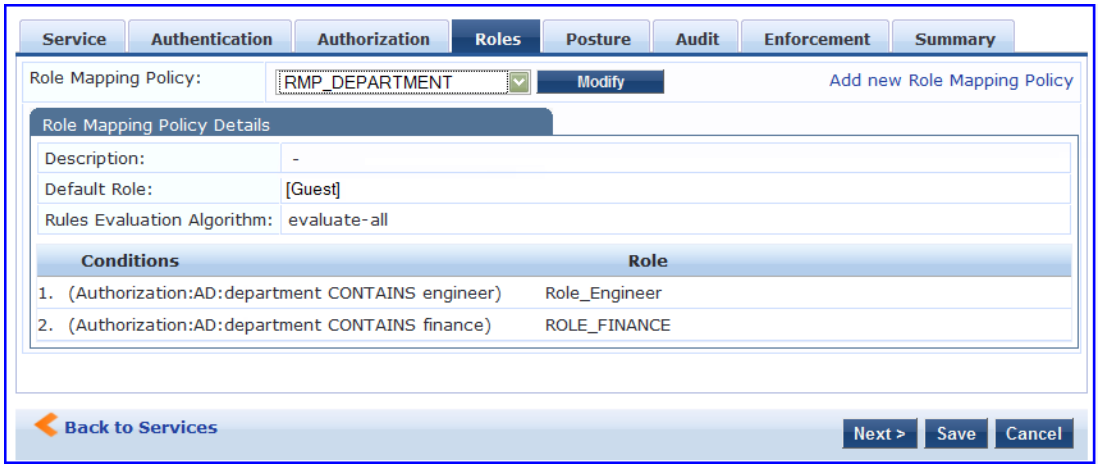
4. Click the **Next** button in the **Rules Editor**.
5. Create rules to map client identity to a role. From the **Mapping Rules** tab, select the **Rules Evaluation Algorithm** radio button. The following figure displays the **Mapping Rules** tab:

Figure 537: *Mapping Rules Tab*



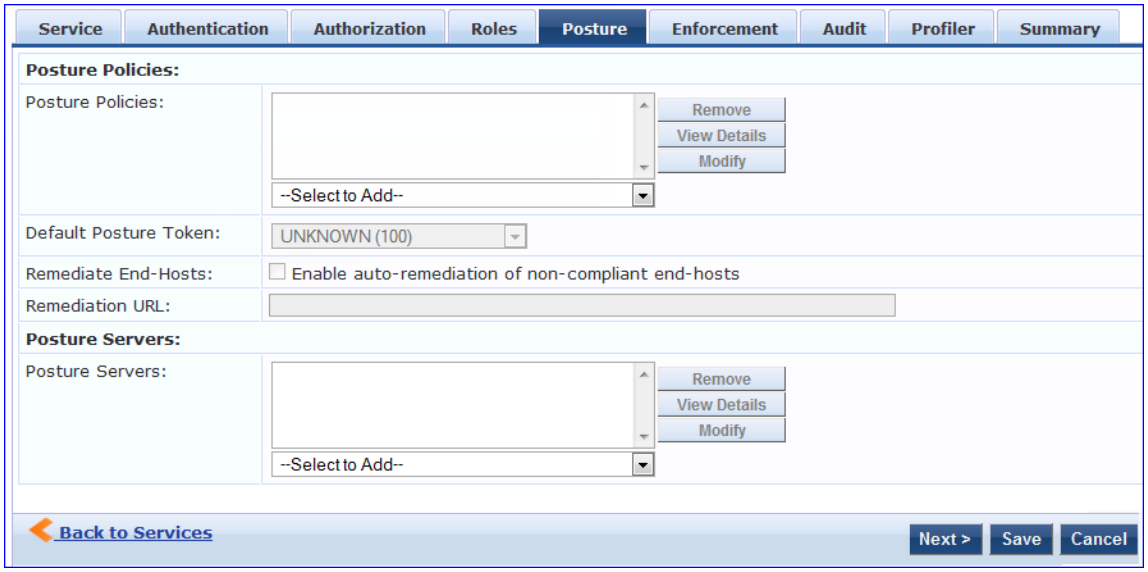
6. Select the **Select all matches** radio button.
7. Match the conditions with the role name. Click the **Add Rule** button. The **Rules Editor** pop-up opens. Upon completion of each rule, click the **Save** button in the **Rules Editor**.
8. Click the **Save** button.
9. Add the new role mapping policy to the service from the **Roles** tab. The following figure displays the **Roles** tab:

Figure 538: *Roles Tab*



10. Select **Role Mapping Policy**, for example, RMP_DEPARTMENT. Click **Next**.
11. Add an **Micrsoft NPS** external posture serverto the 802.1X service. Click the **Posture** tab. The following figure displays the **Posture** tab:

Figure 539: *Posture Tab*

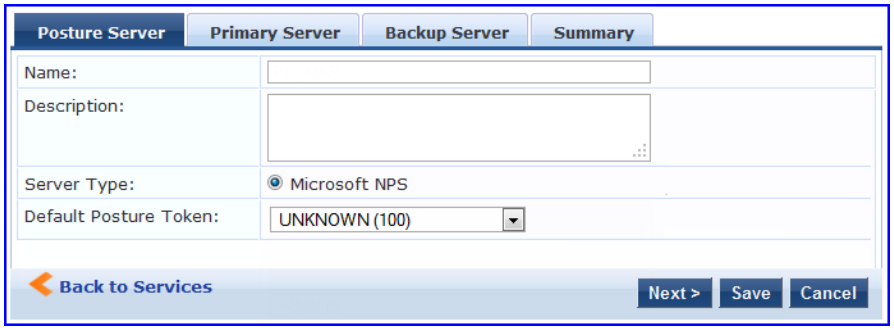


12. Click **Add new Posture Server** to add a new posture server.
13. Configure the following posture settings examples:

- **Name** (freeform): **PS_NPS**
- **Server Type** radio button: **Microsoft NPS**
- **Default Posture Token** (selector): **UNKOWN**

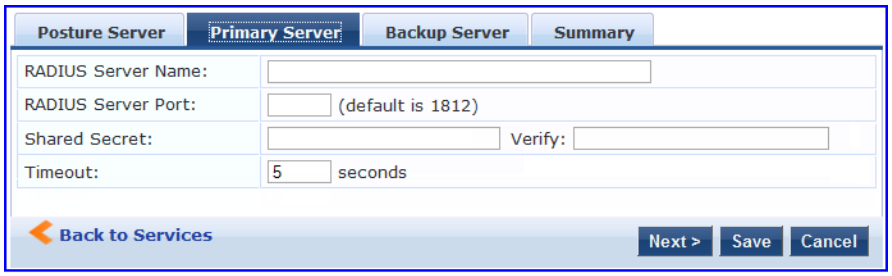
The following figure displays the **Posture Server** tab:

Figure 540: *Posture Server Tab*



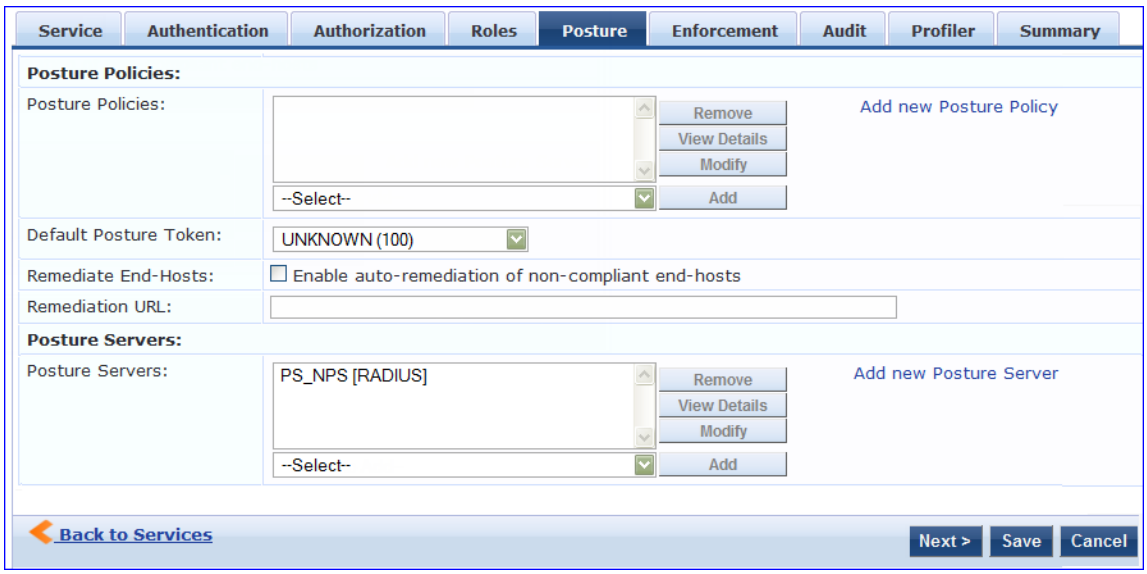
14. Click **Next**.
15. Configure connection settings in the **Primary/ Backup Server** tabs by entering the connection information for the RADIUS posture server. The following figure displays the **Primary Server** tab:

Figure 541: *Primary Server Tab*



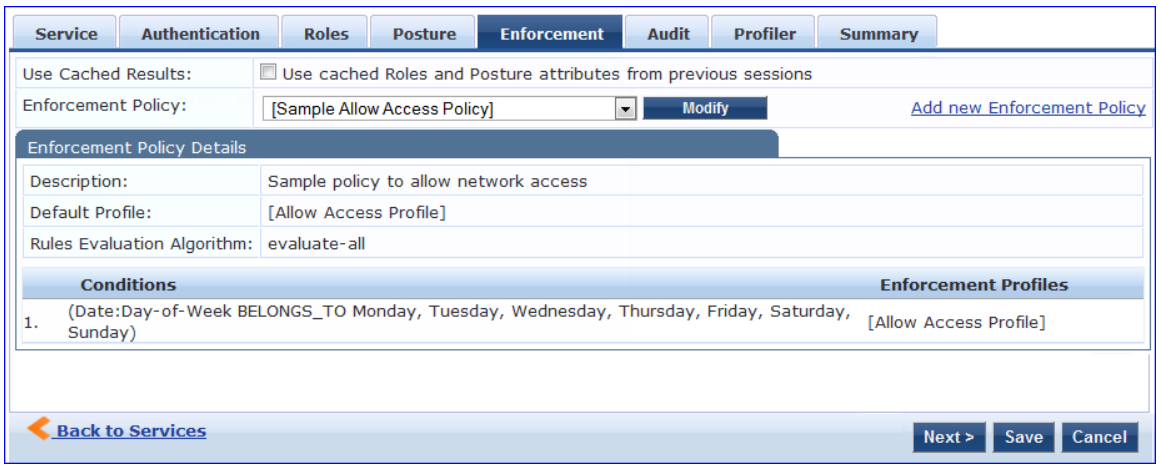
16. Click **Next** from primary server to backup server. Click **Save**.
17. Add the new posture server to the service. From the **Posture** tab, enter the **Posture Servers**, for example, **PS_NPS**, then click the **Add** button. The following figure displays the **Posture** tab:

Figure 542: *Posture Tab*



18. Click the **Next** button. Assign an enforcement policy.
19. 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. The following figure displays the **Enforcement** tab:

Table 382: *Enforcement Policy Navigation and Settings*

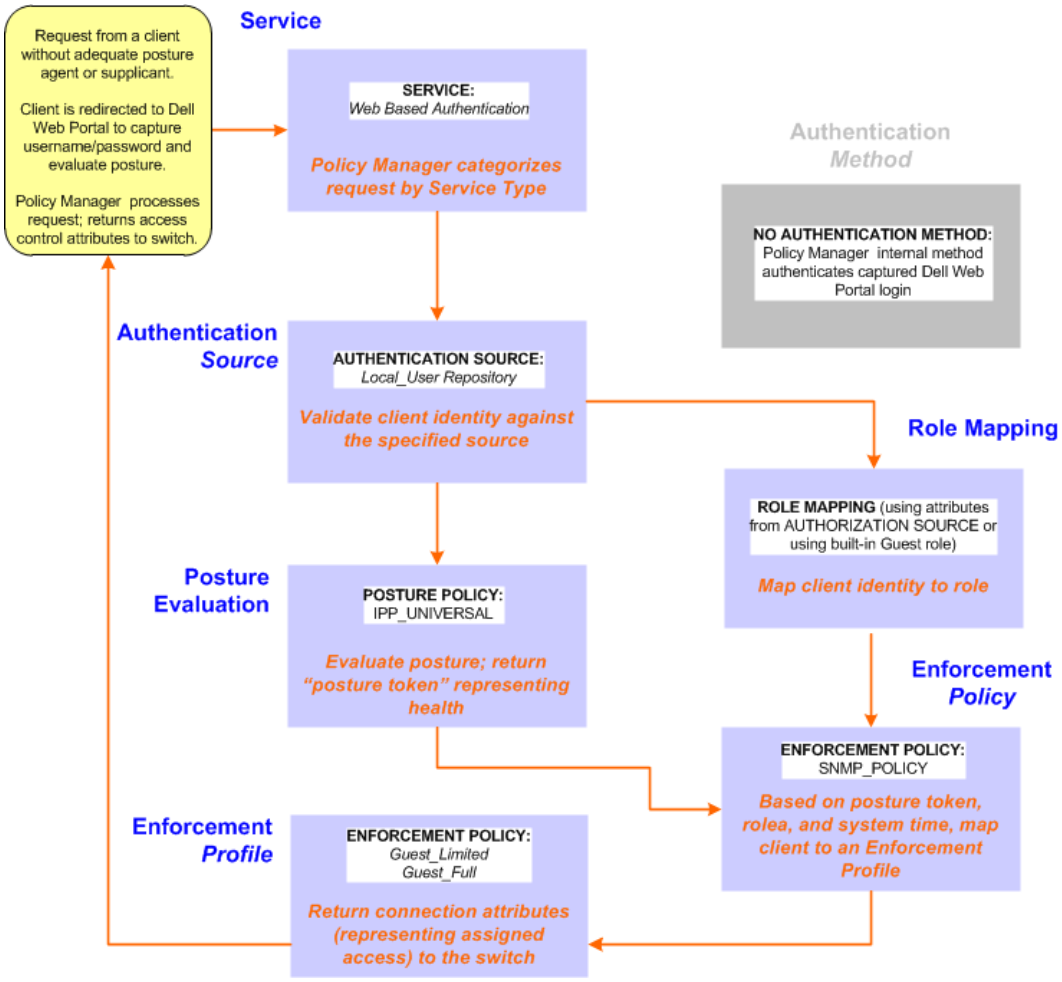


20. **From the Enforcement** tab, select the **Enforcement Policy**, for example, **Role_Based_Allow_Access_Policy.** For instructions about how to build such an enforcement policy, refer to "Configuring Enforcement Policies " on page 1.
21. Save the service.

Web Based Authentication Use Case

This Service supports known Guests with inadequate 802.1X supplicants or posture agents. The following figure illustrates the overall flow of control for this Policy Manager Service.

Figure 543: *Flow-of-Control of Web-Based Authentication for Guests*



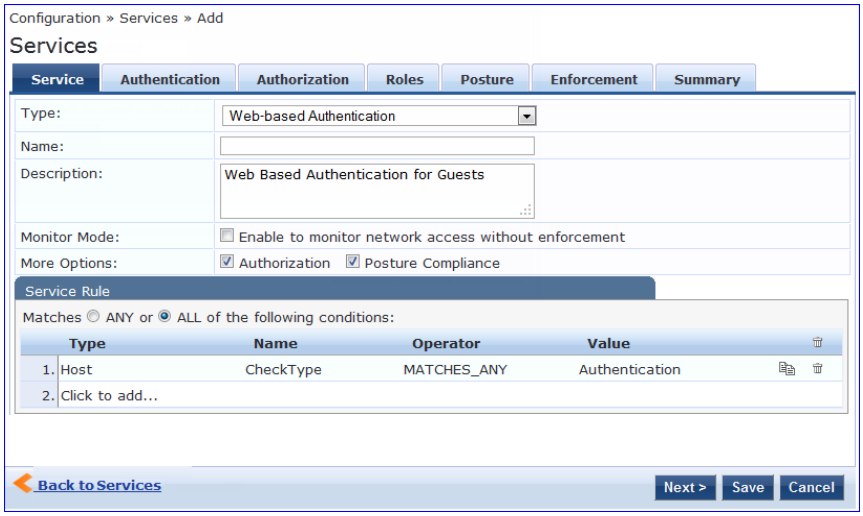
Configuring a Service

Perform the following steps to configure Policy Manager for WebAuth-based Guest access.

1. Prepare the switch to pre-process WebAuth requests for the Policy Manager *Dell WebAuth* service.

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

Table 383: *Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): Dell Web-Based Authentication > • **Name/Description** (freeform) > • Upon completion, click **Next**.	

3. Set up the Authentication.
   a. Method: The Policy Manager WebAuth service authenticates WebAuth clients internally.
   b. Source: Administrators typically configure Guest Users in the local Policy Manager database.
4. Configure a Posture Policy.

For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options. This use case demonstrates the Posture Policy.

As of the current version, Policy Manager ships with five pre-configured posture plugins that evaluate the health of the client and return a corresponding posture token.

To add the internal posture policy *IPP_UNIVERSAL_XP*, which (as you will configure it in this Use Case, checks any Windows® XP clients to verify the most current Service Pack).

Table 384: *Local Policy Manager Database Navigation and Settings*

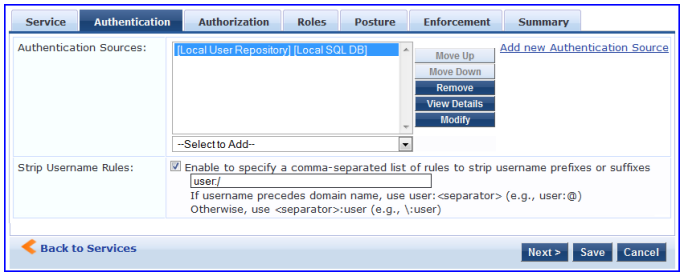
Navigation	Settings
Select the local Policy Manager database: • **Authentication** (tab) > • **Sources** (**Select** drop-down list): **[Local User Repository]** > • **Add** > • **Strip Username Rules** (check box) > • Enter an example of preceding or following separators (if any), with the phrase “user”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

Table 385: *Posture Policy Navigation and Settings*

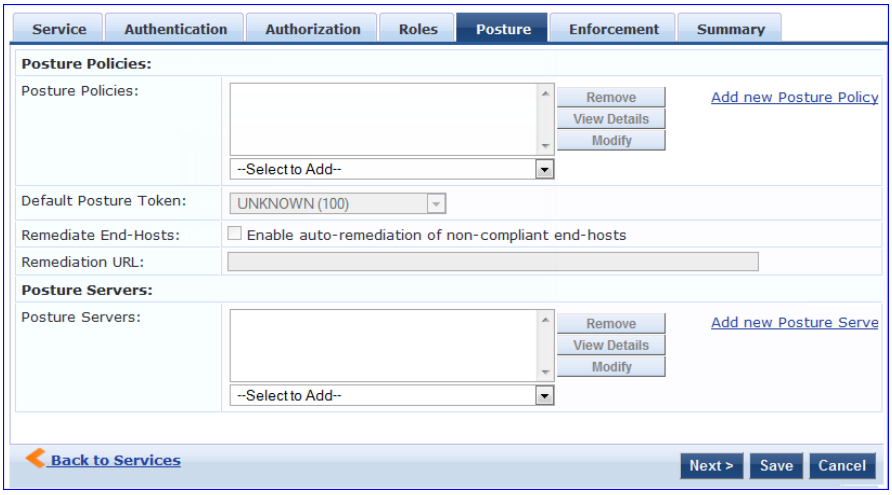
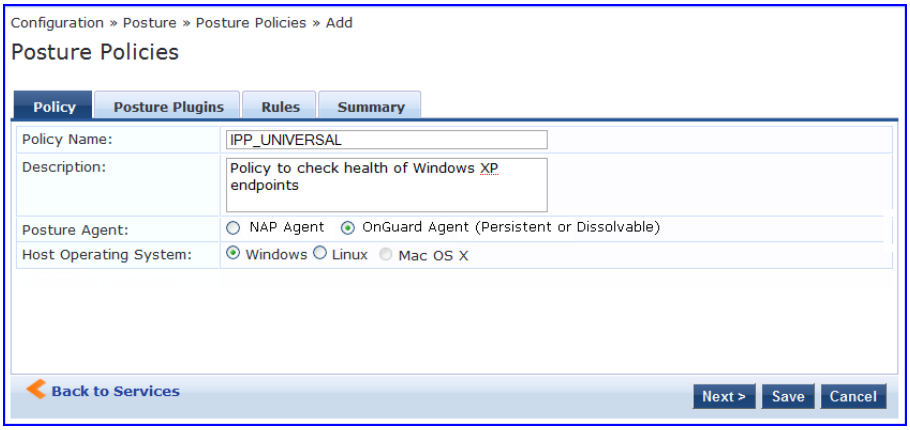
Navigation	Setting
Create a Posture Policy: • **Posture** (tab) > • Enable **Validation Check** (check box) > • **Add new Internal Policy** (link) >	
Name the Posture Policy and specify a general class of operating system: • **Policy** (tab) > • **Policy Name** (freeform): *IPP_UNIVERSAL* > • **Host Operating System** (radio buttons): **Windows** > • When finished working in the **Policy** tab, click **Next** to open the Posture Plugins tab	

Table 385: *Posture Policy Navigation and Settings (Continued)*

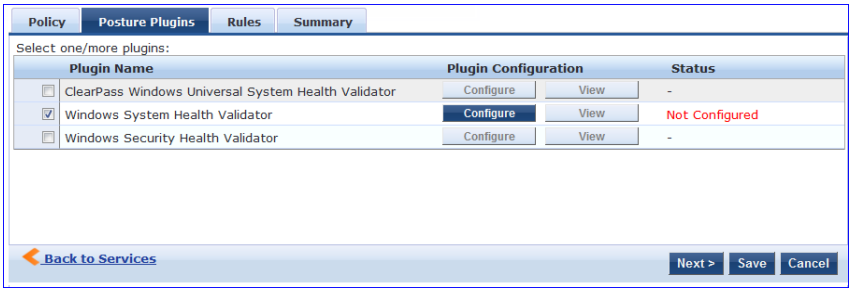
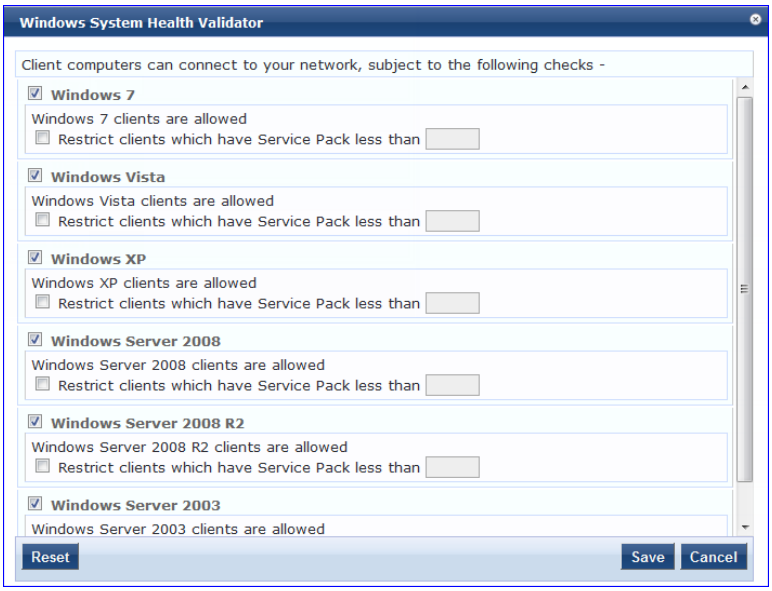
Navigation	Setting
Select a Validator: • **Posture Plugins** (tab) > • Enable **Windows Health System Validator** >• **Configure** (button) >	
Configure the Validator: • **Windows System Health Validator** (popup) >• **Enable all Windows operating systems** (check box) >• Enable Service Pack levels for Windows 7, Windows Vista®, Windows XP Windows Server® 2008, Windows Server 2008 R2, and Windows Server 2003 (check boxes) >• **Save** (button) >	

Table 385: *Posture Policy Navigation and Settings (Continued)*

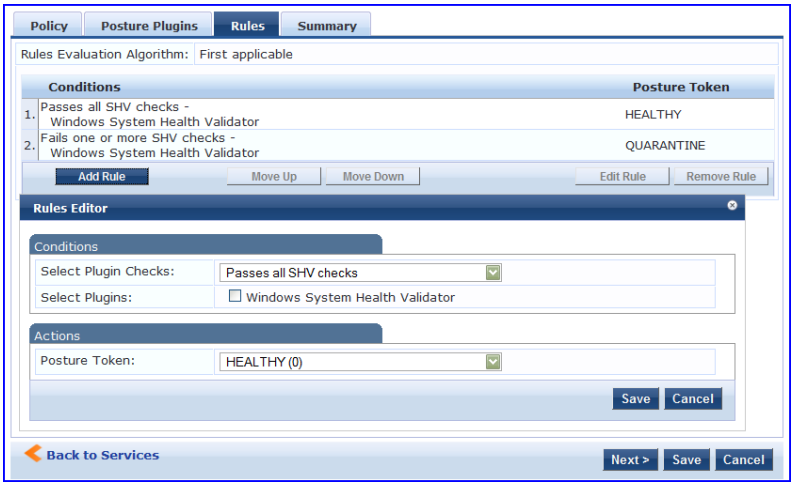
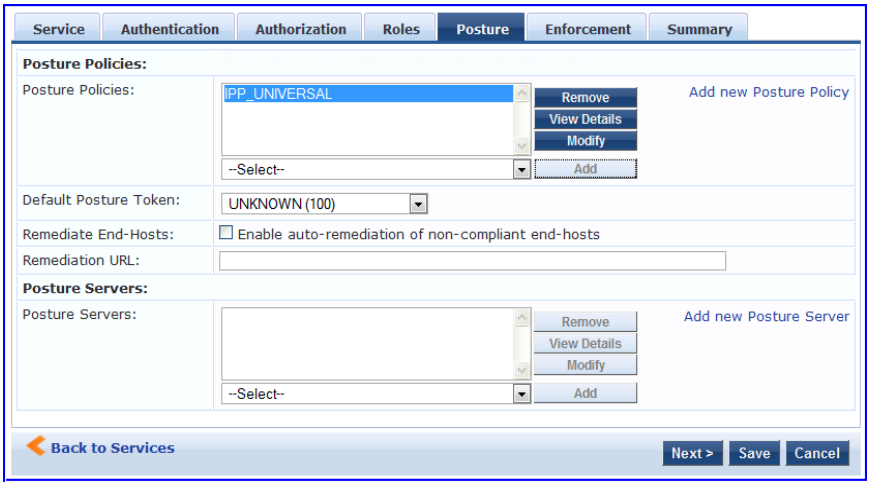
Navigation	Setting
• When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)	
Set rules to correlate validation results with posture tokens: • **Rules** (tab) > • **Add Rule** (button opens popup) > • **Rules Editor** (popup) > • **Conditions/ Actions:** match Conditions (Select Plugin/ Select Plugin checks) to Actions (Posture Token)> • In the **Rules Editor,** upon completion of each rule, click the **Save** button > • When finished working in the **Rules** tab, click the **Next** button.	

Table 385: *Posture Policy Navigation and Settings (Continued)*

Navigation	Setting
Add the new Posture Policy to the Service: Back in **Posture** (tab) > **Internal Policies** (selector): **IPP_UNIVERSAL_XP**, then click the **Add** button	

The following fields deserve special mention:

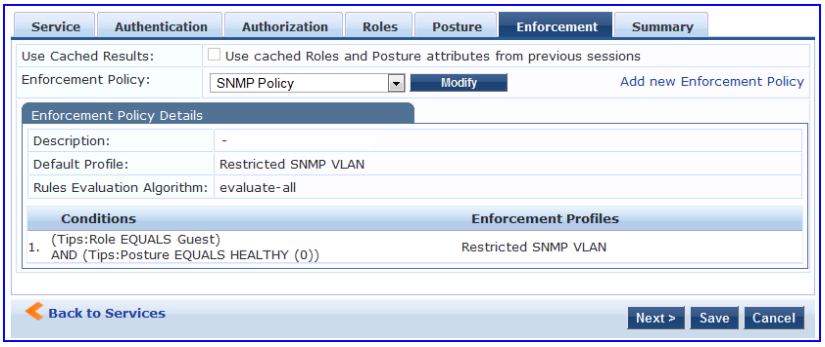
- **Default Posture Token.** Value of the posture token to use if health status is not available.
- **Remediate End-Hosts.** When a client does not pass posture evaluation, redirect to the indicated server for remediation.
- **Remediation URL.** URL of remediation server.

5. Create an Enforcement Policy.

   Because this Use Case assumes the *Guest* role, and the *Dell Web Portal* agent has returned a posture token, it does not require configuration of Role Mapping or Posture Evaluation.

The SNMP_POLICY selected in this step provides full guest access to a Role of [Guest] with a Posture of Healthy, and limited guest access.

Table 386: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Add a new Enforcement Policy: • **Enforcement** (tab) > • Enforcement Policy (selector): **SNMP_POLICY** • Upon completion, click **Save**.	

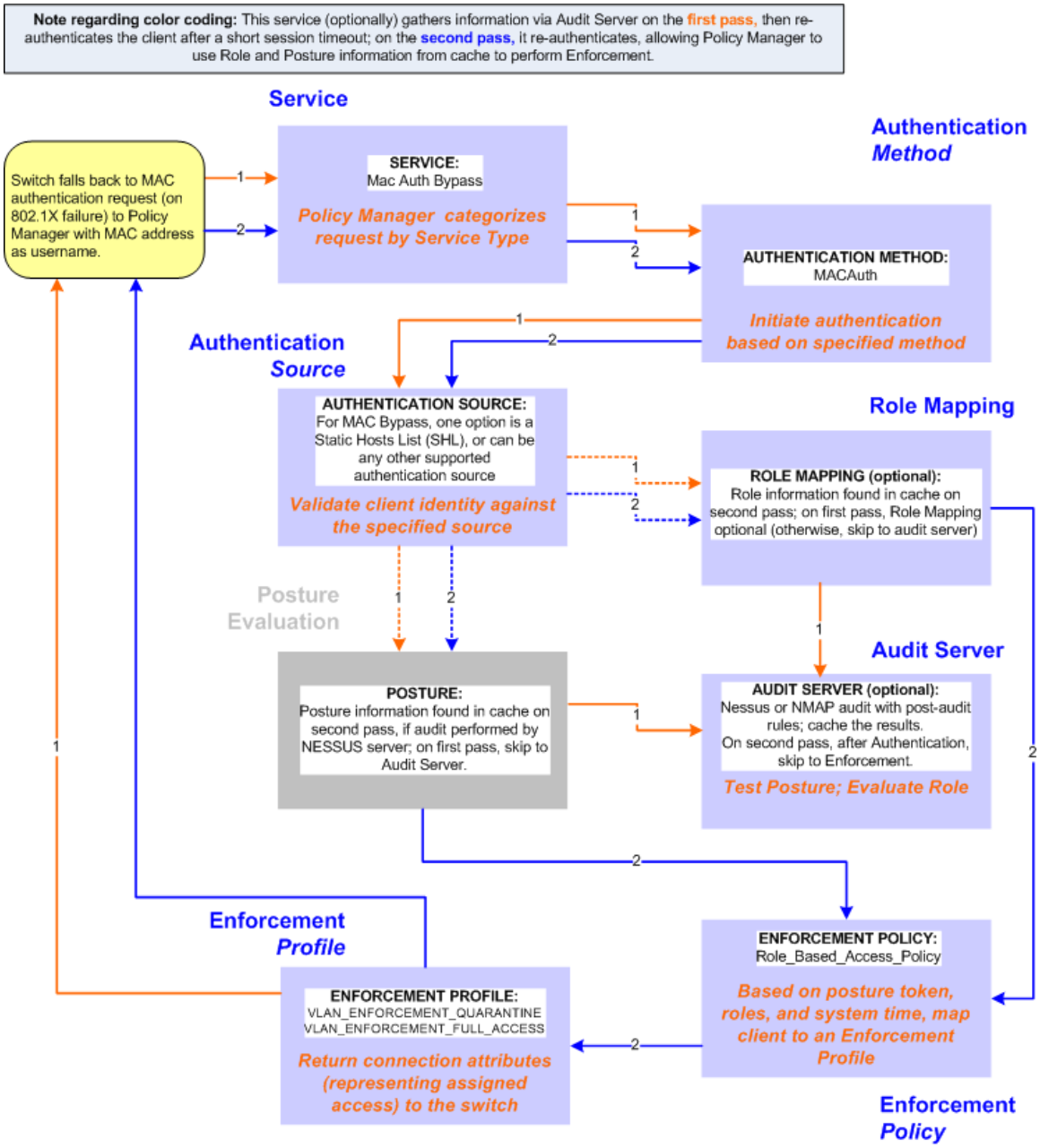
6. Save the Service.

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

MAC Authentication Use Case

This Service supports *Network Devices,* such as printers or handhelds. The following image illustrates the overall flow of control for this Policy Manager Service. In this service, an audit is initiated on receiving the first MAC Authentication request. A subsequent MAC Authentication request (forcefully triggered after the audit, or triggered after a short session timeout) uses the cached results from the audit to determine posture and role(s) for the device.

Figure 544: *Flow-of-Control of MAC Authentication for Network Devices*

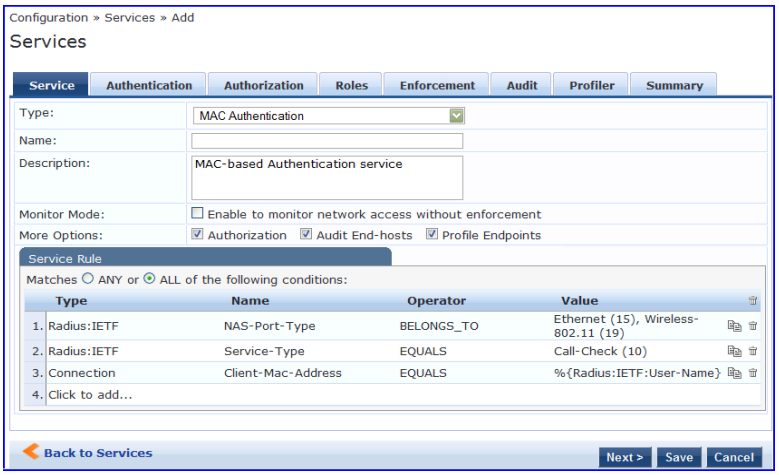


Configuring the Service

Follow these steps to configure Policy Manager for MAC-based Network Device access.

1. Create a MAC Authentication Service.

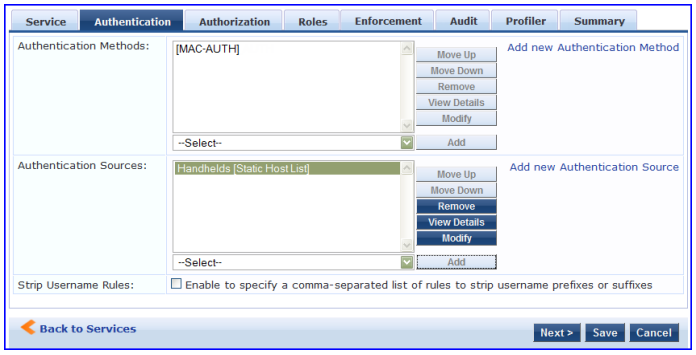
Table 387: *MAC Authentication Service Navigation and Settings*

Navigation	Settings
Create a new Service: • **Services** > • **Add Service** (link) >	
Name the Service and select a pre-configured Service Type: • **Service** (tab) > • **Type** (selector): **MAC Authentication** > • **Name/Description** (freeform) > • Upon completion, click **Next** to configure Authentication	

2. Set up Authentication.

   You can select any type of authentication/authorization source for a MAC Authentication service. Only a Static Host list of type MAC Address List or MAC Address Regular Expression shows up in the list of authentication sources (of type Static Host List). Refer to Adding and Modifying Static Host Lists on page 223 for more information. You can also select any other supported type of authentication source.

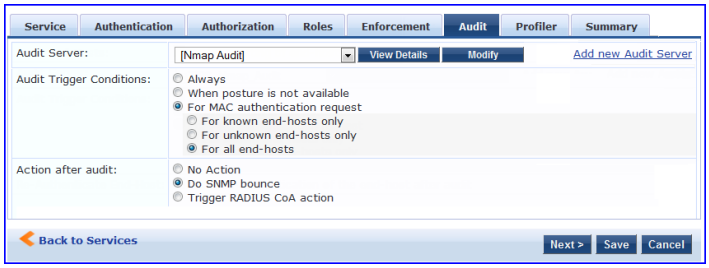
Table 388: *Authentication Method Navigation and Settings*

Navigation	Settings
Select an Authentication Method and two authentication sources - one of type Static Host List and the other of type Generic LDAP server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (This method is automatically selected for this type of service): **[MAC AUTH]** > • **Add** > • **Sources** (**Select** drop-down list): **Handhelds [Static Host List]** and Policy Manager Clients White List [Generic LDAP] > • **Add** > • Upon completion, **Next** (to Audit)	

3. Configure an Audit Server.

This step is optional if no Role Mapping Policy is provided, or if you want to establish health or roles using an audit. An audit server determines health by performing a detailed system and health vulnerability analysis (NESSUS). You can also configure the audit server (NMAP or NESSUS) with post-audit rules that enable Policy Manager to determine client identity.

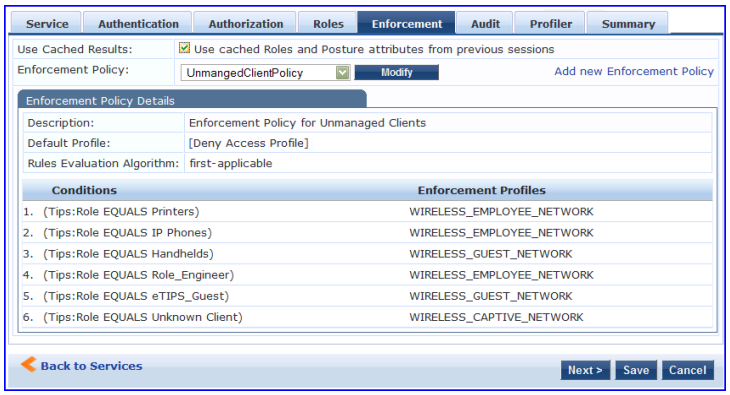
Table 389: *Audit Server Navigation and Settings*

Navigation	Settings
Configure the Audit Server: • **Audit** (tab) > • **Audit End Hosts** (enable) > • **Audit Server** (selector): **NMAP** • **Trigger Conditions** (radio button): **For MAC authentication requests** • **Reauthenticate client** (check box): **Enable**	

Upon completion of the audit, Policy Manager caches Role (NMAP and NESSUS) and Posture (NESSUS), then resets the connection (or the switch reauthenticates after a short session timeout), triggering a new request, which follows the same path until it reaches Role Mapping/Posture/Audit; this appends cached information for this client to the request for passing to Enforcement. Select an Enforcement Policy.

4. Select the Enforcement Policy *Sample_Allow_Access_Policy*:

Table 390: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: • **Enforcement** (tab) > • **Use Cached Results** (check box): Select **Use cached Roles and Posture attributes from previous sessions** > • **Enforcement Policy** (selector): UnmanagedClientPolicy • When you are finished with your work in this tab, click **Save**.	

Unlike the 802.1X Service, which uses the same Enforcement Policy (but uses an explicit Role Mapping Policy to assess Role), in this use case Policy Manager applies post-audit rules against attributes captured by the Audit Server to infer Role(s).

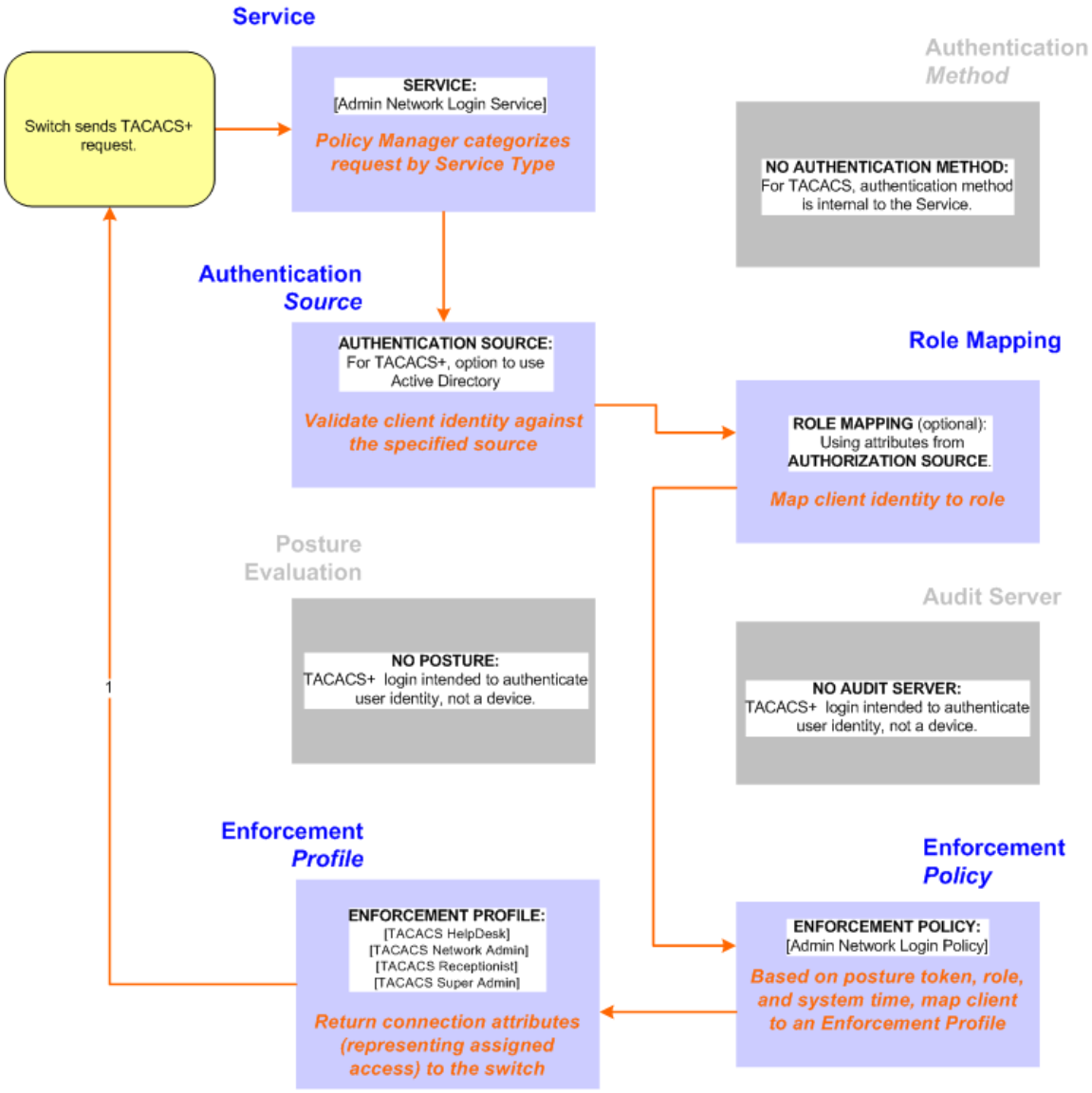
5. Save the Service.

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

TACACS+ Use Case

This Service supports Administrator connections to Network Access Devices via TACACS+. The following image illustrates the overall flow of control for this Policy Manager Service.

Figure 545: *Administrator connections to Network Access Devices via TACACS+*



Configuring the Service

Perform the following steps to configure Policy Manager for TACACS+-based access:

1. Navigate to **Configuration > Services.**
2. Click the Add icon to add a service. The **Configuration > Services > Add** window opens.
3. If it is not already selected, click the **Service** tab and define basic service information.
   a. Enter a name for the service in the **Name** field.
   b. Click the **Type** drop-down list and select the preconfigured service type that matches your Policy Manager Admin Network Login Service.
   c. Click **Next** to display the **Authentication** tab.

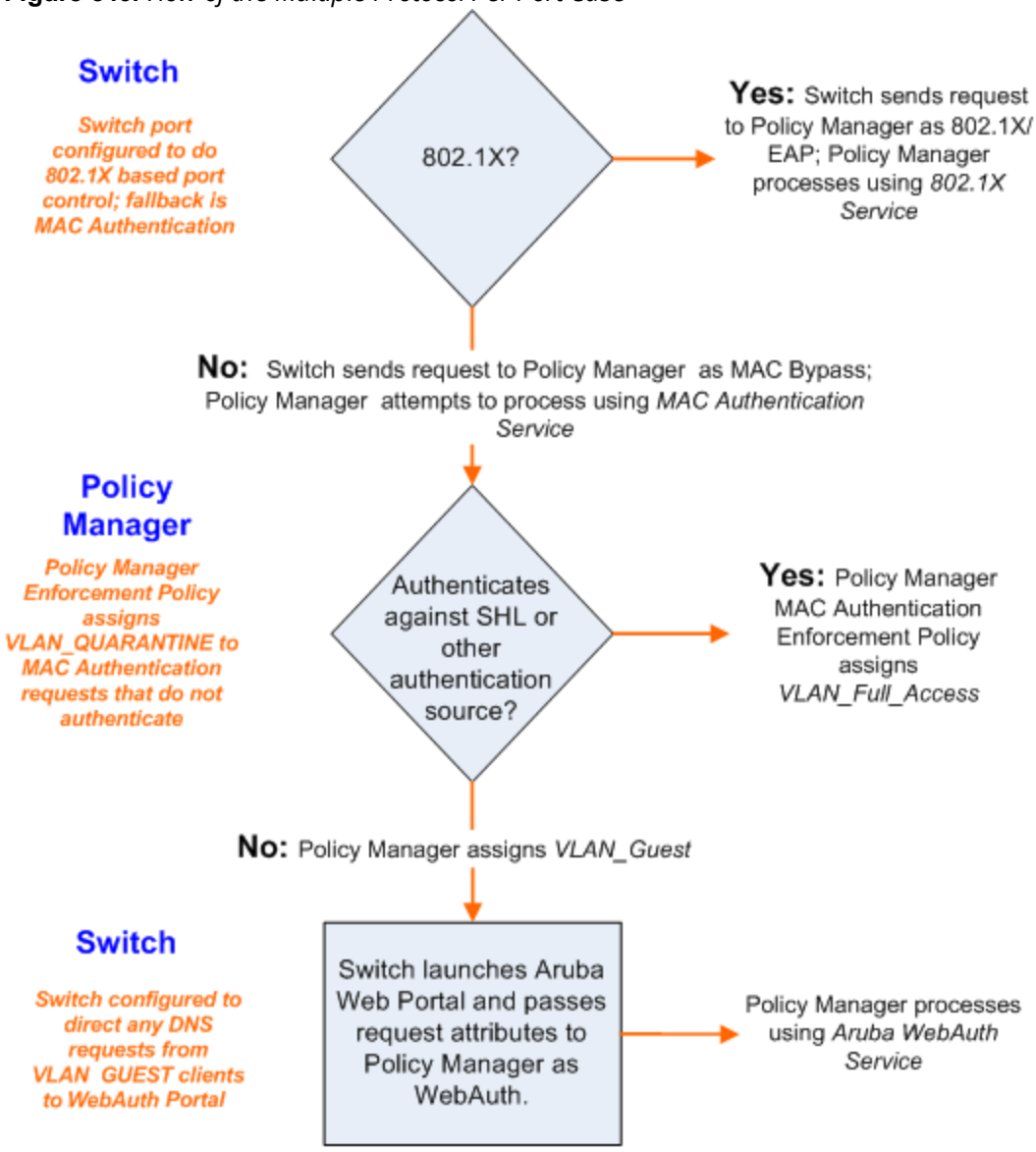
4. Define the Authentication settings for the service. Authentication methods can be left to their default values, as the Policy Manager TACACS+ service authenticates TACACS+ requests internally.
   a. In the **Authentication Sources** section, click the **Select to Add** drop-down list.
   b. Select **AD (Active Directory)**. For this use case example, Network Access Device authentication data will be stored in the Active Directory.
5. Click the **Enforcement** tab and select an Enforcement Policy.
   a. Click the Enforcement Policy drop-down list and select the Enforcement Policy **[Admin Network Login Policy]** that distinguishes the two allowed roles (**Net Admin Limited** and **Device SuperAdmin)**.
6. Click **Save.** The Service now appears at the bottom of the **Services** list.

Single Port Use Case

This Service supports all three types of connections on a single port.

The following figure illustrates both the overall flow of control for this hybrid service, in which complementary switch and Policy Manager configurations allow all three types of connections on a single port:

Figure 546: *Flow of the Multiple Protocol Per Port Case*



You can configure the OnGuard Dissolvable Agent flow in different modes to perform health scan on endpoints. This section provides information on configuring OnGuard Dissolvable Agent in the following modes and the end-to-end flow:

- **Native agents only** - Native Dissolvable Agent communicates with ClearPass Guest to send information about endpoints such as status, health status, remediation messages and so on. This communication is independent of the operating systems and browsers.
- **Native agents with Java fallback** - The configuration for the **Native agents with Java fallback** mode is similar to the **Native agents only** mode. The posture assessment is performed based on the user's preference.
- **Java Only** - The communication is dependent on the browsers and the Java Runtime Environment (JRE) versions installed. For the supported Java versions and browsers, see Supported Browsers and Java Versions.

Native Agents Only Mode

A Native Dissolvable Agent communicates with ClearPass Guest portal to send information about endpoints such as status, health status, remediation messages, and so on. This communication is independent of the operating systems and browsers.

Native Dissolvable Agent supports the following browsers and operating systems:

Table 391: *Supported Operating Systems and Browsers*

OS	Browsers
Windows	• Internet Explorer • FireFox • Google Chrome
Mac OS X	• Safari • FireFox • Google Chrome
Linux	• FireFox

Dell Networking W-ClearPass Policy Manager hosts the Native Dissolvable Agent binary files with OnGuard Persistent Agent installers. You can use the links to download the binaries in the **OnGuard Settings** (**Administration** > **Agents and Software Updates** > **OnGuard Settings**) page for Windows (.exe) and Mac OS X (.DMG).

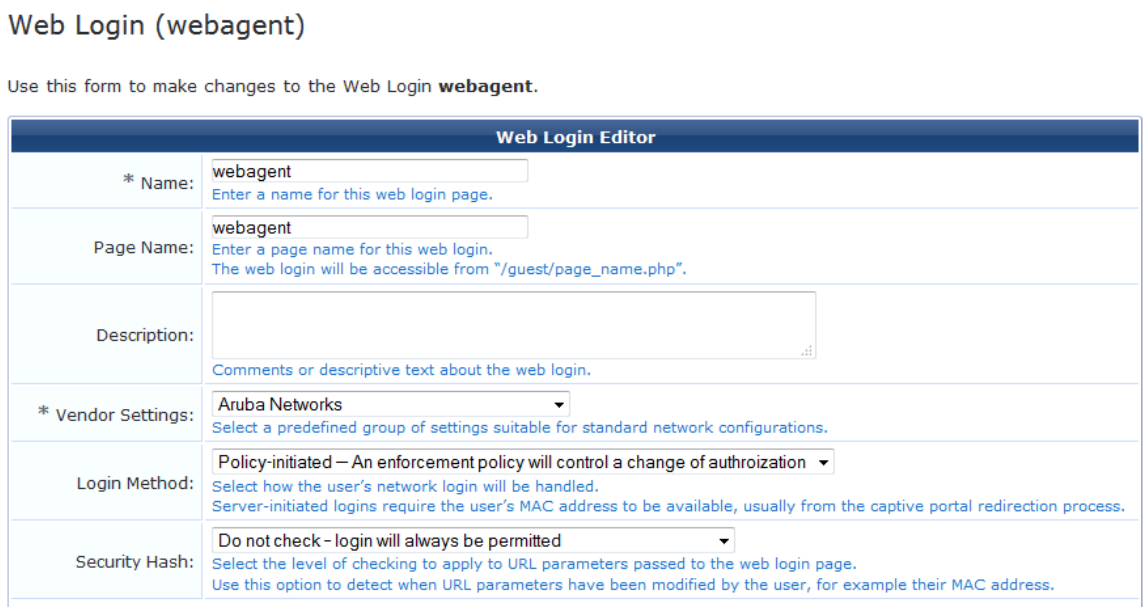
Configuring Workflow in Native Agents Only Mode

In ClearPass Guest, the web login page is enhanced to avoid an additional web authentication service and simplifies the configuration on dissolvable agent flow with policy-initiated login method.

Use the following steps to configure the OnGuard Dissolvable Agent in **Native agents only** mode:

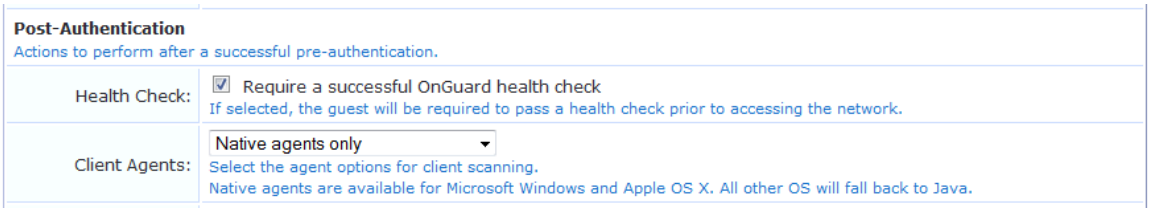
1. Select the **Policy-initiated - An enforcement policy will control a change of authorization** option from the drop-down list in the **Login Method** field. The following figure displays the policy-initiated login method in the **Web Login Editor** page:

Figure 547: *Policy-initiated Login Method*



2. Select the **Require a successful OnGuard health check** option in the **Health Check** field. If you select this field, the guest needs to pass a health check before accessing the network. Select the **Native agents only** mode in the **Client Agents** field:

Figure 548: *Native Agents Only Mode*



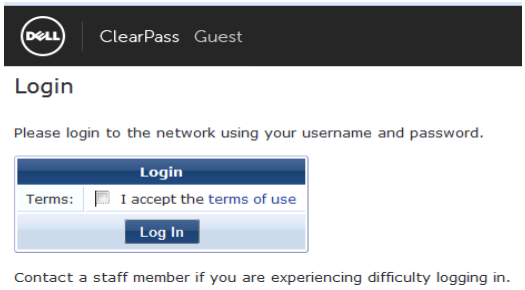
End-to-end flow in Native Agents Only Mode

The following steps describe the end-to-end flow of the OnGuard Dissolvable Agent running on the **Native agents only** mode:

1. You are redirected to the ClearPass Guest portal where you can download the native agent installer. Run the Native Agent Installer after accepting the terms and conditions for collecting end point posture assessment scan checks and performing remediation actions.

The following figure shows an example of the Native Dissolvable Agent **Login** page:

Figure 549: *Native Dissolvable Agent - Login Page*

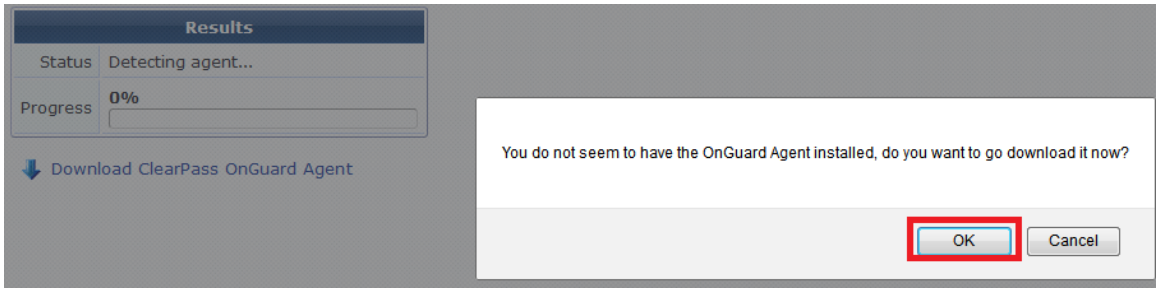


NOTE

The **Terms** specified in the **Login** page is optional. You can configure this optionally by selecting the **Require a Terms and Conditions confirmation** check box in the **Terms** field in ClearPass Guest Login Form.

2. The figure similar to the following OnGuard Agent download prompt appears when you login for the first time to the Native Dissolvable Agent:

Figure 550: *Native Dissolvable Agent Installer Prompt*

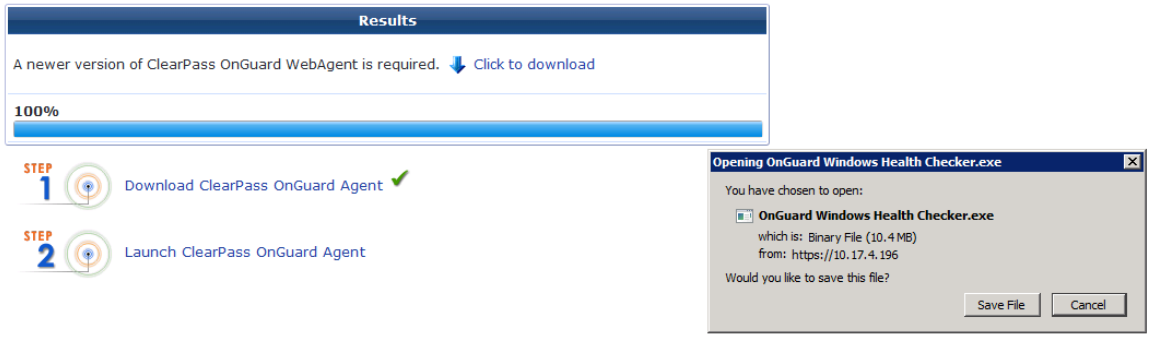


NOTE

The download options are available only when you login for the first time. Alternatively, you can download the OnGuard agent by clicking the **Download ClearPass OnGuard Agent** link.

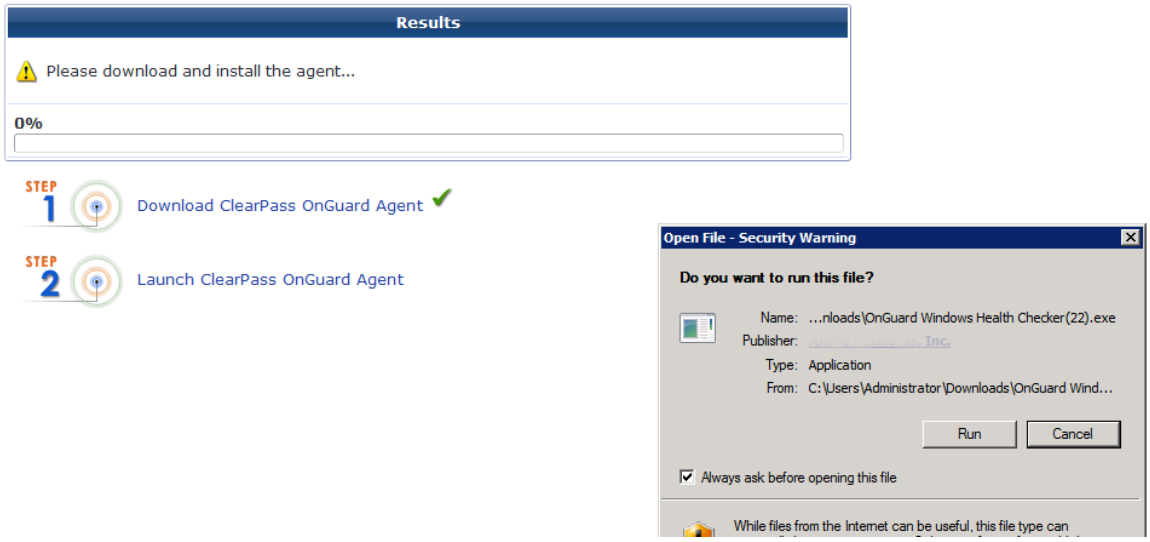
3. Click **OK** to download the OnGuard Agent. The figure shows an example of the **OnGuard Windows Health Checker** binary download window:

Figure 551: *Native Dissolvable Agent Binary Downloader*



4. Click **Save File** to download the OnGuard agent. Click **Run** to install the OnGuard agent.

Figure 552: *Native Dissolvable Agent Installation*



NOTE

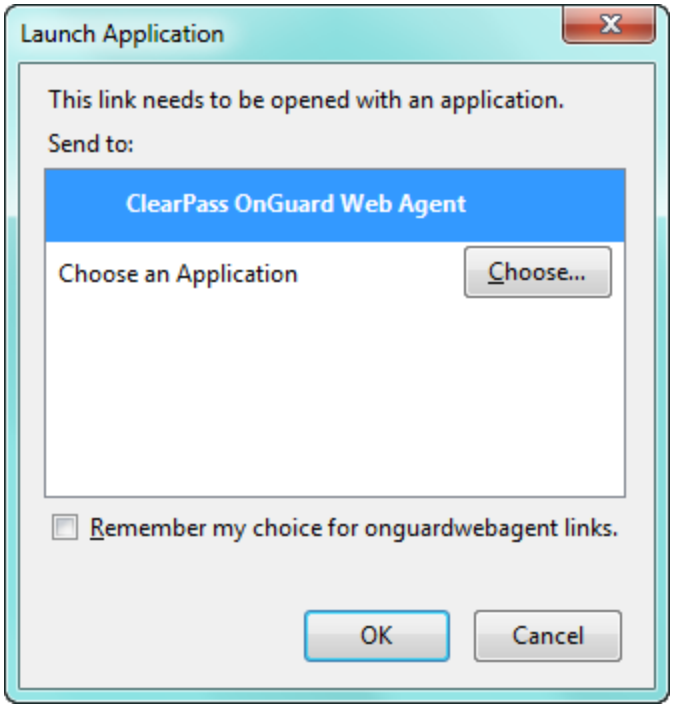
If you are running Windows OS, Internet Explorer provides options to **Run** or **Save**. FireFox and Chrome browsers provide option to save the .exe files.

NOTE

If you are running Mac OS X, FireFox provides options to open the binary with **DiskImageMounter** or **Save** the .DMG files. Safari and Google Chrome browsers provide the option to **Save** only.

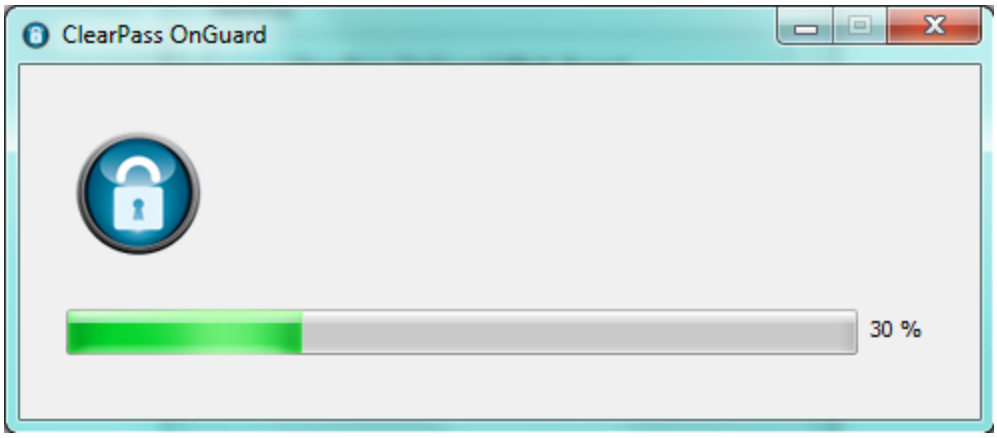
5. Select the **ClearPass OnGuard Web Agent** application in the **Launch Application** page. Select **Remember my choice for onguardwebagent links** to register and perform auto-launch of native OnGuard agent on successive log-ins. Click **OK**.

Figure 553: *Native Dissolvable Agent Application Launcher*



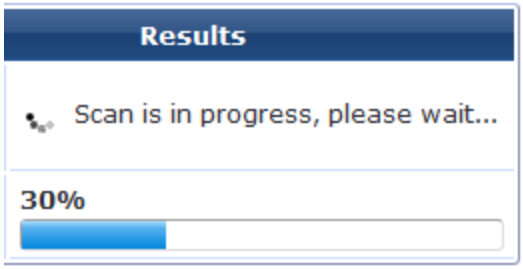
6. The following progress screen appears and shows the progress:

Figure 554: *Native Dissolvable Agent Installation Progress*



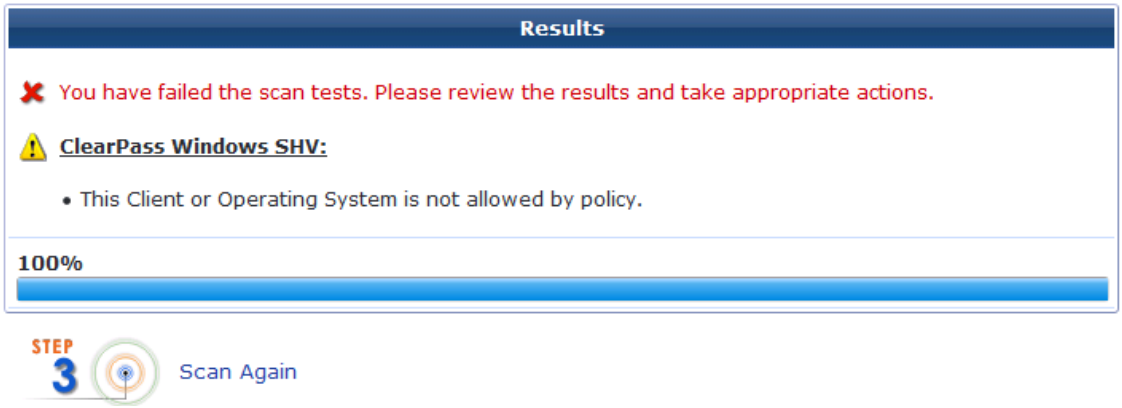
7. After the successful installation, the health check scanning is initiated. The following figure shows an example of the progress indicator:

Figure 555: *Health Check Progress*



8. After the health check scanning is completed, the figure similar to the following example appears with the health check results if the client is unhealthy:

Figure 556: *Health Check Results*



9. Take the appropriate actions to fix the issues listed in remediation and agent enforcement messages and click **Scan Again**. Repeat this step till the client becomes healthy. Once the client is healthy, you can access the destination URL.
10. You can track the events with the end-to-end flow in the **Access Tracker** page. The following figure shows an example of the **Access Tracker** page with the native dissolvable agent flow:

Figure 557: *Access Tracker Page*

10.	RADIUS	suribabu	1X-Wireless	ACCEPT	2014/07/10 16:07:12
10.	WEBAUTH	7cd1c373c4e4	Health-only	ACCEPT	2014/07/10 16:07:03
10.	RADIUS	suribabu	1X-Wireless	ACCEPT	2014/07/10 16:06:30

The Auto-launch feature works in the **Native agents only** and **Java Only** modes without user intervention to click pop ups and options that are described in the complete end-to-end flow above except configuring **Terms** in the ClearPass Guest **Login** page.

Auto-Login

The Native dissolvable agent supports **Auto-Login** method which eliminates the **Require a Terms and Conditions confirmation** check box in the **Guest Web Login** page by avoiding the web page and submitting automatically.

Troubleshooting

In Windows, Native Dissolvable Agent flow logs are available at **%appdata%Aruba Networks/ ClearPassOnguard Temp/Logs**. In MAC OS X, the Native dissolvable agent flow logs are available at **~/Library/Logs/ClearPassOnGuardTemp/logs**.

Native Agents with Java Fallback Mode

The configuration steps for **Native agents with or Java fallback** work flow is similar to the **Native agents only** mode. The posture assessment is performed based on your selection.

Configuring Native Agents with Java Fallback Mode

Use the following steps to configure the OnGuard Dissolvable Agent in **Native agents with Java fallback** mode:

1. Select the **Policy-initiated - An enforcement policy will control a change of authorization** option from the drop-down list in the **Login Method** field. The following figure shows an example configuration of the Policy-initiated **Login** method:

Figure 558: *Policy-initiated Login Method*

Web Login (webagent)

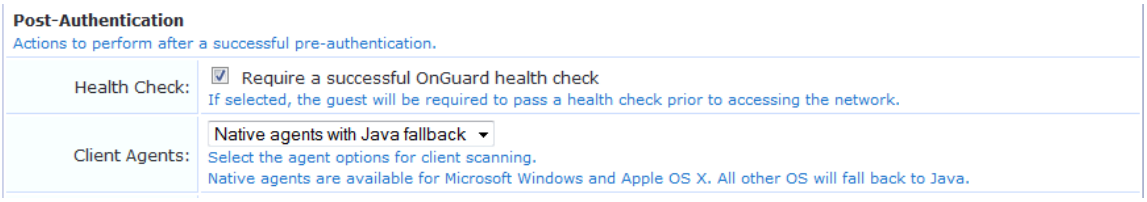
Use this form to make changes to the Web Login **webagent**.

Web Login Editor

* Name:	webagent Enter a name for this web login page.
Page Name:	webagent Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
Login Method:	Policy-initiated — An enforcement policy will control a change of authroization Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Security Hash:	Do not check - login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

2. Select the **Require a successful OnGuard health check** option in the **Health Check** field. If you select this field, the guest needs to pass a health check before accessing the network. Select the **Native agents with Java fallback** mode in the **Client Agents** field:

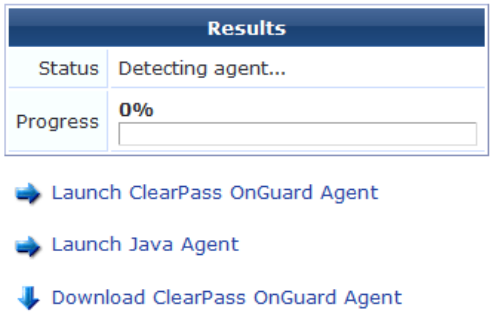
Figure 559: *Native Agents with Java Fallback Mode*



End-to-end flow in Native Agents with Java Fallback Mode

The posture assessment is performed based on your selection. If you select Java, the Java applet is downloaded and posture assessment is performed. The native agent link is provided in **Java launcher** to avoid the JRE files loaded into the system. The following figure shows an example of the **Native agents with Java fallback** options:

Figure 560: *Native Dissolvable Agents with Java Fallback*



Configuring Web Agent Flow - Java Only Mode

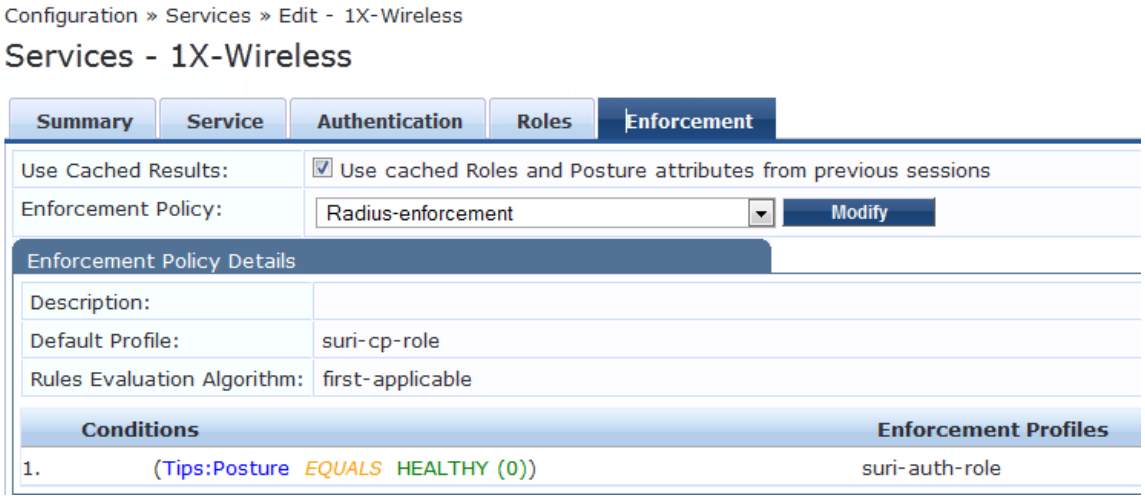
You can configure a new web agent flow in two different locations (Dell Networking W-ClearPass Policy Manager and ClearPass Guest) to perform health scan on endpoints.

Configuring Web Agent Flow in Dell Networking W-ClearPass Policy Manager

Use the following steps to configure a new web agent flow in Dell Networking W-ClearPass Policy Manager:

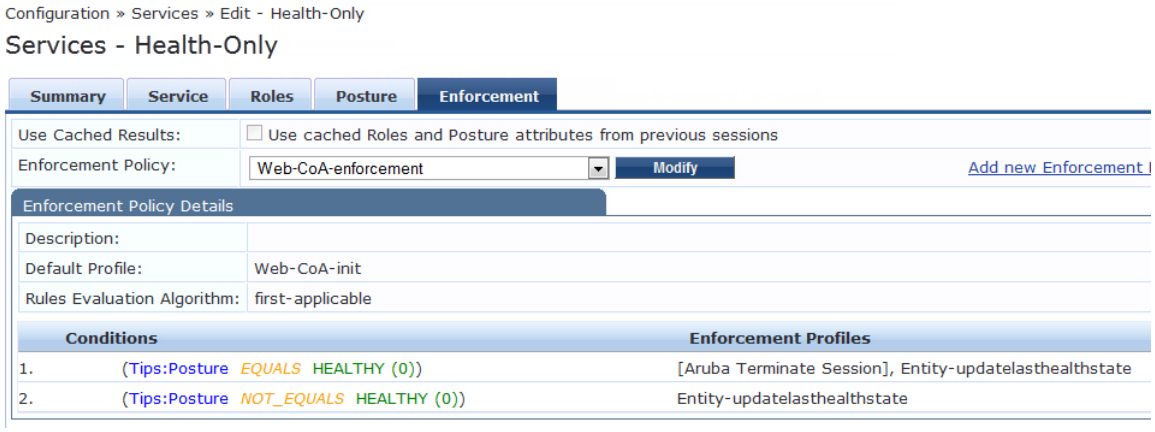
1. Create a 802.1X service to perform RADIUS authentication and enforce restricted or full access based on end point posture assessments. The following figure shows an example of the **Web Agent Flow - 802.1X Service** page:

Figure 561: *Web Agent Flow - 802.1X Service*



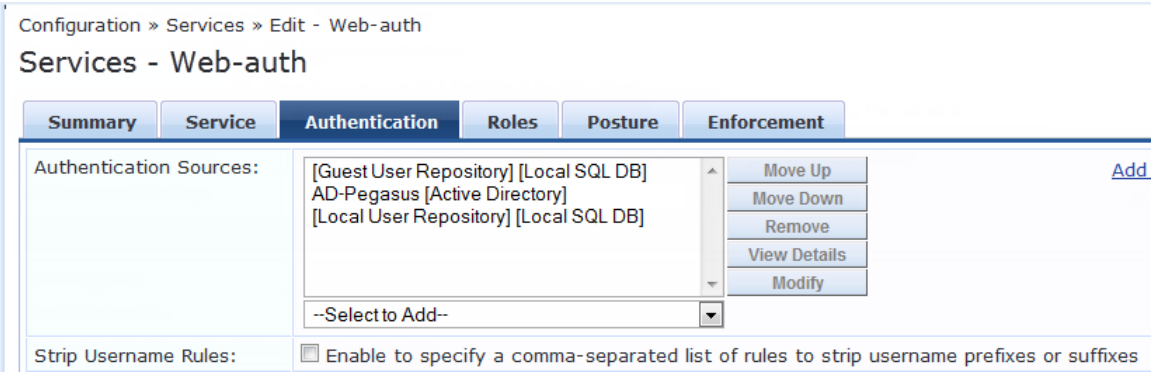
2. Create a service named **Web-based Health Check Only** on the Dell Networking W-ClearPass Policy Manager server. The following figure shows an example of the **Web Agent Flow - Health Only** page:

Figure 562: *Web Agent Flow - Health Only*



3. Create a simple Web Auth service to authenticate users against ClearPass Guest user database to accept or perform App authentication request after completing a sandwich flow. The following figure shows an example of the **Web Agent Flow - Services Web Auth** page:

Figure 563: *Web Agent Flow - Services Web Auth*

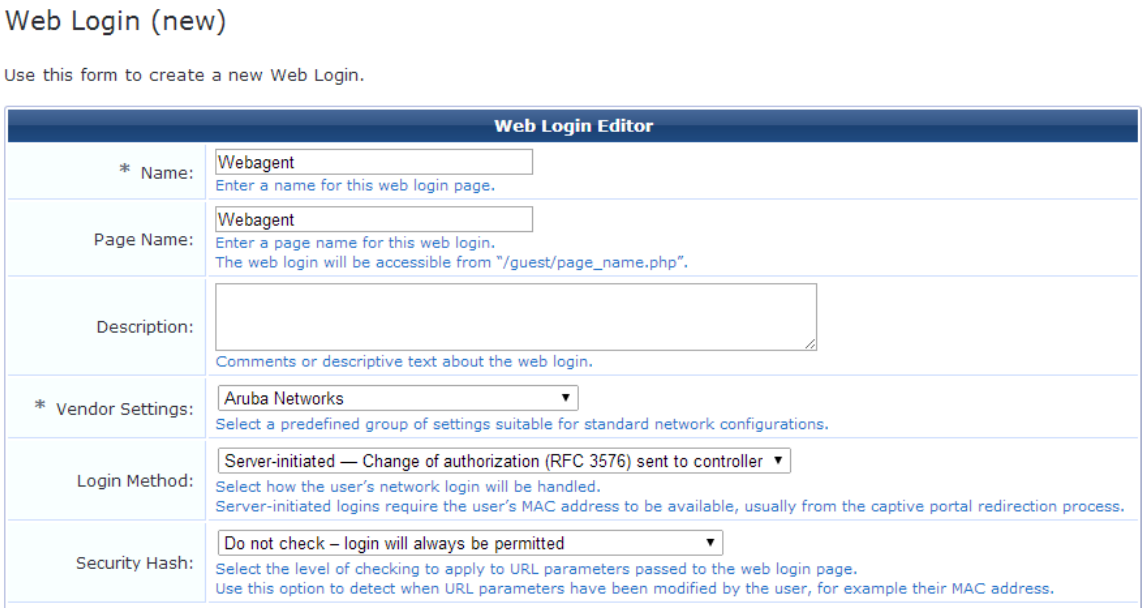


Configuring Web Agent Flow in ClearPass Guest

Use the following steps to create a web agent flow in ClearPass Guest:

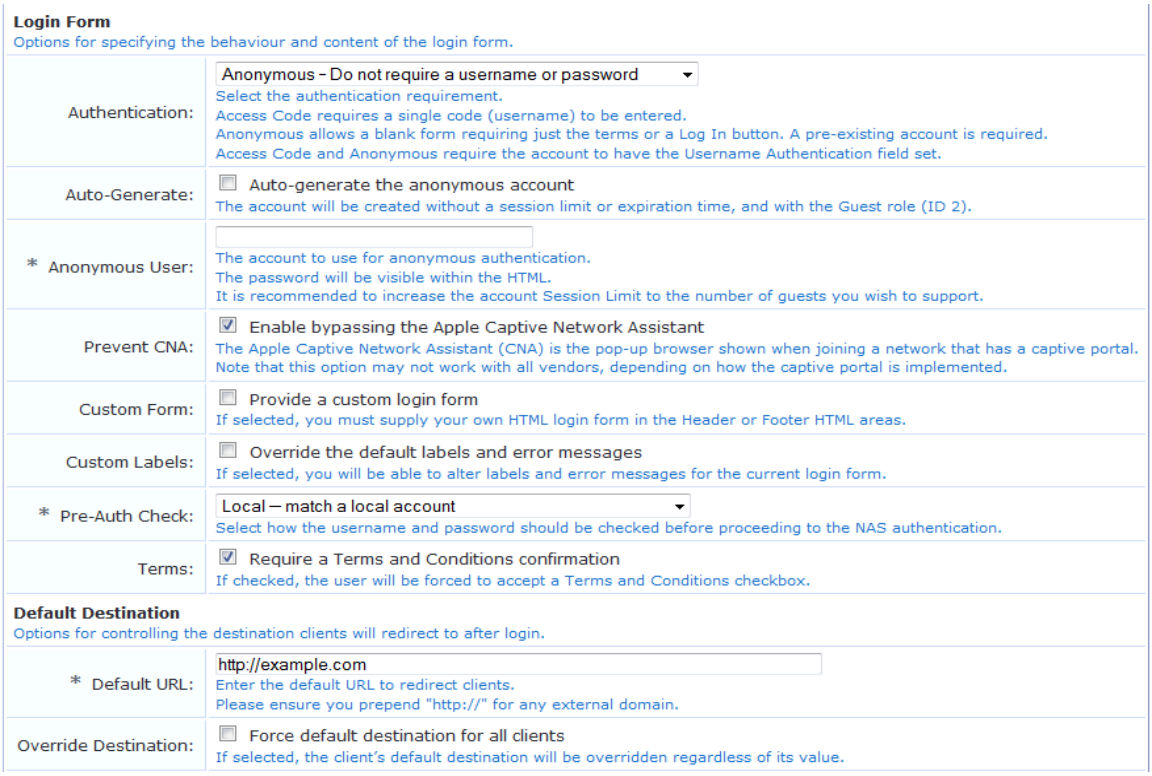
1. Click **Create a new web login page** on the right corner of the ClearPass Guest UI. The following figure shows an example of the **Web Login Editor** page:

Figure 564: *Web Login Editor*



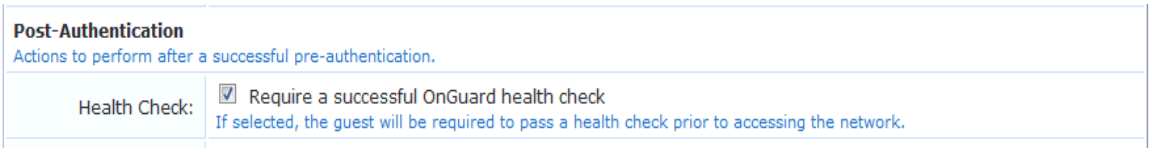
2. Select the **Anonymous - Do not require a username or password** option from the drop-down.
3. Check the **Enable bypassing the Apple Captive Network Assistant** option in the **Prevent CNA** field.
4. Select the **Local - match a local account** option in the **Pre-Auth Check** field.
5. Check the **Require Terms and Conditions confirmation** option in the **Terms** field.
6. Specify the destination URL to which the client must be redirected after health checks in the **Default destination** field.

Figure 565: *Web Login - Login Form*

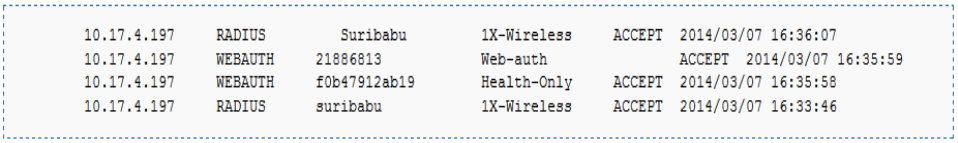


7. Select the **Local - match a local account** option in the **Post Authentication** field. The following figure shows an example of the **Web Login - Post-Authentication** page:

Figure 566: *Web Login - Post-Authentication*



The following figure shows an example of the final web agent flow:



For more information, refer to ClearPass Guest Online Help.

Native Dissolvable Agent - Supported Browsers

This section provides information on supported browsers for the Native Dissolvable Agent. The versions given in the following table are tested and are up to date at the time of this release:

Table 392: *Supported Browsers and Java Versions*

Operating System	Browser	Test Results	Known Issues	Tested Versions
Windows 7 64-bit	Chrome	Passed	#24518 #24986	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Chrome 38.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Firefox 33.X
	IE	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and IE-9.X
Windows 7 32-bit	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Chrome 38.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Firefox 33.X
	IE 10.X 32-bit	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and IE-10.X
Windows 8 64-bit	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Chrome 38.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Firefox 33.X
	IE 10.X 32-bit	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and IE 10.X
Windows 8 32-bit	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Chrome 39.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Firefox 34.X
	IE 10.X	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and IE 10.X
Windows 8.1 64-bit	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Chrome 39.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Firefox 34.X
	IE 32-bit	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and IE-11.x
Windows 2008 64-bit	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Chrome 38.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Firefox 33.X

Table 392: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
	IE 8.X 32-bit	Passed	#24766	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and IE-9.x
Windows XP SP3	Chrome	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Chrome 34.X
	Firefox	Not supported	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Firefox 30.X
	IE 8.X 32-bit	Not supported	#24768	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and IE-8.X
Windows 2003 32-bit	Chrome	Not supported	#24898	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Chrome 35.X
	Firefox	Not supported	#24898	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Firefox 30.X
	IE	Not supported	#24898	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and IE-8.X
Windows Vista	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Chrome 39.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Firefox 34.X
	IE 7.X 32-bit	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and IE 7.X
MAC 10.9	Safari	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Safari 7.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Firefox 33.X
	Chrome	Passed	#24518 #24986	Dell Networking W-ClearPass Policy Manager 6.5.0.69430 and Chrome-38.X
MAC 10.8	Safari	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69277 and Safari-6.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69277 and Firefox-33.X
	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.69277 and Chrome-38.X
MAC 10.7.5	Safari	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Safari 6.X
	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Firefox 34.X

Table 392: *Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
	Chrome	Passed	#24986	Dell Networking W-ClearPass Policy Manager 6.5.0.70143 and Chrome 39.X
Ubuntu 12.04 32-bit LTS	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Firefox-34.X
	Chromium	Failed	#27264	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Chromium 39.X
Ubuntu 12.04 64-bit LTS	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Firefox-34.X
	Chromium	Failed	#27264	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Chromium 39.X
Ubuntu 14.04 32-bit LTS	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Firefox-34.X
	Chromium	Failed	#27264	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Chromium 39.X
Ubuntu 14.04 64-bit LTS	Firefox	Passed	None	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Firefox-34.X
	Chromium	Failed	#27264	Dell Networking W-ClearPass Policy Manager 6.5.0.69931 and Chromium 39.X

For more information on known issues, refer to *Dell Networking W-ClearPass Policy Manager 6.5 Release Notes*.