ClearPass Policy Manager

a Hewlett Packard Enterprise company

User Guide

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code.

Contents

Chapter 1
About ClearPass Policy Manager

This chapter provides an overview of the ClearPass 6.6 Policy Manager Access Management System.

This chapter includes the following information:

- About the ClearPass Access Management System
- Using the Policy Manager Dashboard
- Accessing Configuration Information
- Importing and Exporting Information

About the ClearPass Access Management System

This section contains the following information:

- About This Guide
- ClearPass Access Management System Overview
- Key Features
- Advanced Policy Management
- ClearPass Specifications

About This Guide

Welcome to the ClearPass Policy Manager 6.6 *User Guide*.

The *ClearPass Policy Manager 6.6 User Guide* provides a general overview of ClearPass Policy Manager features, as well as detailed descriptions of the configuration settings used to manage and monitor your Policy Manager deployment.

Intended Audience

The intended audience for the *ClearPass Policy Manager* 6.6 *User Guide* includes customers, partners, and field Sales Engineers.

Please note that this document is not a training guide, and it is assumed that the reader has at minimum foundational training in ClearPass Essentials and, if possible, Aruba Certified Professional (ACCP) certification.

The user of this guide should have a working knowledge of the following:

- AAA technologies (RADIUS, TACACS, 802.1X, MAC address authentication, and Web authentication)
- Layer-2 and Layer-3 networking
- User Identity stores, such as Active Directory

NOTE

Providing information about network device configurations and capabilities is outside the scope of this guide. For information on these topics, refer to the documentation provided by the vendor of your network equipment.

Getting Started

If you are new to ClearPass Policy Manager, refer to the following sections:

- For a general description of ClearPass Policy Manager features, refer to the following topics in this section, ClearPass Access Management System Overview and Key Features.
- For a description of how to use the Dashboard, see Using the Policy Manager Dashboard on page 25.

- For a list of common configuration tasks and pointers to information about how to perform each task, refer to Accessing Configuration Information on page 28.
- If you are planning a new ClearPass Policy Manager deployment, refer to the *ClearPass Deployment Guide*. The *ClearPass Deployment Guide* is organized in a way that presents the recommended sequence in which ClearPass deployment should take place, and makes the major deployment tasks easy to implement.

ClearPass Access Management System Overview

The ClearPass Policy Manager™ Access Management System provides a window into your network and covers all your access security requirements from a single platform. You get complete views of mobile devices and users and have total control over what they can access.

With ClearPass, IT can centrally manage network policies, automatically configure devices and distribute security certificates, admit guest users, assess device health, and even share information with third-party solutions—through a single pane of glass, on any network and without changing the current infrastructure.

Role-Based and Device-Based Access

The ClearPass Policy Manager platform provides role-based and device-based network access control for employees, contractors, and guests across any wired, wireless, and VPN infrastructure.

ClearPass works with any multivendor network and can be extended to business and IT systems that are already in place.

Self-Service Capabilities

ClearPass delivers a wide range of unique self-service capabilities. Users can securely onboard their own devices for enterprise use or register AirPlay, AirPrint, Digital Living Network Alliance (DLNA), and Universal Plug and Play (UPnP) devices that are enabled for sharing, sponsor guest Wi-Fi access, and even set up sharing for Apple TV and Google Chromecast.

Leveraging Contextual Data

The power of ClearPass comes from integrating ultra-scalable AAA (authentication, authorization, and accounting) with policy management, guest network access, device onboarding, and device health checks with a complete understanding of context.

From this single ClearPass policy and AAA platform, contextual data is leveraged across the network to ensure that users and devices are granted the appropriate access privileges.

ClearPass leverages a user's role, device, location, application use, and time of day to execute custom security policies, accelerate device deployments, and streamline network operations across wired networks, wireless networks, and VPNs.

Third-Party Security and IT Systems

ClearPass can be extended to third-party security and IT systems using REST-based APIs to automate work flows that previously required manual IT intervention. ClearPass integrates with mobile device management to leverage device inventory and posture information, which enables well-informed policy decisions.

Key Features

ClearPass's key features are as follows:

- Bring Your Own Device (BYOD) Certificate Authority for secure self service onboarding
- Auto Sign-On and single sign-on (SSO) support via Security Assertion Markup Language (SAML) v2.0
- Social network and Cloud application SSO via OAuth2, Facebook, Twitter, LinkdIn, Office365, Google Apps, and so on

- Enterprise reporting, monitoring, and alerting
- Role-based network access enforcement for multivendor Wi-Fi, wired, and VPN networks
- High performance, scalability, High Availability, and load balancing
- A Web-based user interface that simplifies policy configuration and troubleshooting
- Network Access Control (NAC), Network Access Protection (NAP) posture and health checks, and Mobile Device Management (MDM) integration for mobile device posture checks
- Advanced reporting of all user authentications and failures
- HTTP/RESTful APIs for integration with third-party systems, Internet security, and MDM
- Device profiling and self-service onboarding
- Guest access with extensive branding and customization and sponsor-based approvals
- IPv6 administration support

Advanced Policy Management

ClearPass advanced policy management support includes:

- **Employee access**

  ClearPass offers user and device authentication based on 802.1X, non-802.1X, and Web Portal access methods. To strengthen security in any environment, you can concurrently use multiple authentication protocols, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public.

  For fine-grained control, you can use attributes from multiple identity stores, such as Microsoft Active Directory, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database, token servers, and internal databases across domains within a single policy.

  Additionally, you can add posture assessments and remediation to existing policies at any time.
- **Device profiling**

  ClearPass provides a profiling service that discovers and classifies all endpoints, regardless of device type. You can obtain a variety of contextual data(such as MAC OUIs, DHCP fingerprinting, and other identity-centric device data) and use this data within policies.

  Stored profiling data identifies device profile changes and dynamically modifies authorization privileges. For example, if a printer appears as a Windows laptop, ClearPass Policy Manager can automatically deny access.
- **Access for unmanaged endpoints**

  Unmanaged non-802.1X devices (such as printers, IP phones, and IP cameras) can be identified as *known* or *unknown* upon connecting to the network. The identity of these devices is based on the presence of their MAC address in an external or internal database.
- **Secure configuration of personal devices**

  ClearPass Onboard fully automates the provisioning of any Windows, Mac OS X, iOS, Android, Chromebook, and Ubuntu devices via a built-in captive portal. Valid users are redirected to a template-based interface to configure required SSIDs and 802.1X settings, and download unique device credentials.

  Additional capabilities include the ability for IT to revoke and delete credentials for lost or stolen devices, and the ability to configure mobile email settings for Exchange ActiveSync and VPN clients on some device types.
- **Customizable visitor management**

  ClearPass Guest simplifies work flow processes so that receptionists, employees, and other non-IT staff can create temporary guest accounts for secure Wi-Fi and wired network access. Self-registration allows guests to create their credentials.
- **Device health checks**

ClearPass OnGuard, as well as separate OnGuard persistent or dissolvable agents, performs advanced endpoint posture assessments. Traditional NAC (Network Admission Control) health-check capabilities ensure compliance and network safeguards before devices connect.

You can use information about endpoint integrity (such as status of anti-virus, anti-spyware, firewall, and peer-to-peer applications) to enhance authorization policies. Automatic remediation services are also available for non-compliant devices.

ClearPass Specifications

ClearPass Policy Manager

- Comprehensive identity-based policy engine
- Posture agents for Windows, Macintosh OS X, and Linux operating systems
- Built-in AAA services: RADIUS, TACACS+, and Kerberos
- Web, 802.1X, and non-802.1X authentication and authorization
- Reporting, analytics, and troubleshooting tools
- External captive portal redirect to multivendor equipment
- Interactive policy simulation and monitor mode utilities
- Deployment templates for any network type, identity store, and endpoint

Framework and Protocol Support

- RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
- Wireless and wired 802.1X and VPN
- Microsoft Network Access Protection (NAP) and Network Access Control (NAC)
- Windows machine authentication
- MAC address authentication (non-802.1X devices)
- Audit based on port and vulnerability scans

Supported Identity Stores

- Microsoft Active Directory
- Kerberos
- Any LDAP-compliant directory
- Any ODBC-compliant SQL server
- Token servers
- Built-in SQL store
- Built-in static-hosts list

Using the Policy Manager Dashboard

The Policy Manager Dashboard organizes and presents the key information about the status and performance of the current ClearPass server or cluster, as well as a set of Quick Links to the most commonly used functions, such as configuring policies, viewing the Access Tracker, and so on.

The Dashboard information is illustrated in interactive bar chart, graph, and table formats.

To customize the Dashboard layout to display the information you most want to see (as described in Table 1), drag and drop from the list of the Widget elements on the left pane to one of the available Dashboard slots in the right pane.

Table 1: *Dashboard Widget Summary*

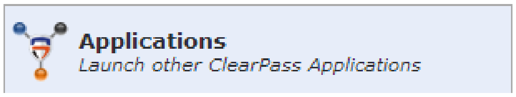
Alerts *Latest Alerts*	To view the table with latest system level events, drag and drop the **Alerts** widget to the Dashboard. - Clicking on a row drills down to the **Event Viewer**.
All Requests *Trend all Policy Manager requests*	To view the graph that displays all requests processed by Policy Manager over the past week, drag and drop the **All Requests** widget. - 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.
 **Applications** *Launch other ClearPass Applications*	To view the links to the Aruba Insight, Guest, and Onboard applications that are integrated with Policy Manager, drag and drop the **Applications** widget to the Dashboard.
Authentication Status *Trend Successful and Failed authentications*	To view a graph of the failed and successful requests over the past week, drag and drop the **Authentication Status** to the Dashboard. - 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 that shows the failed and successful requests for the day specified.
Cluster Status *Monitor the status of the entire cluster*	To view the status of all nodes in a cluster, drag and drop the **Cluster Status** widget to the Dashboard. The following fields are shown for each node: - **Status**: Shows the overall health status of the cluster. Green indicates healthy status. Red indicates connectivity problems or high CPU or high 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. - **Zone**: The configured cluster zone. - **Server Role**: Indicates whether the cluster node is a publisher or subscriber.

Table 1: *Dashboard Widget Summary (Continued)*

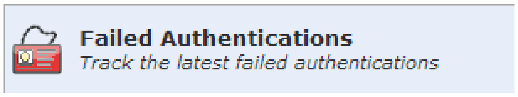
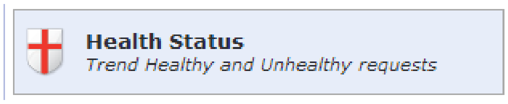
	- **Last Replication**: Date of the last replication. - **Status**: Indicates the status of the cluster node.
Device Category *Device Categories*	To view the chart that shows the graph of all profiled devices categorized into the following categories: - Access Points - Computer - Conflict Indicates a conflict occurred in the categorization of the device. - Datacenter Appliance - Game Console - Monitoring Devices - Network Boot Agents - Physical Security - Printer - Router - Server - Smart Device - Switch - Unknown Indicates devices that are not included in the Profiler database. - VOIP phone
Device Family *Device Family*	To view the device family of a particular device category: 1. Drag and drop the **Device Category** widget to the Dashboard. 2. From the drop-down, select the device category. The device family is displayed. For example, selecting **Computer** would show that the device family is *Windows*.
Endpoint Profiler Summary *Endpoint profiling details*	To view a display that shows the number of smart devices, computers, and unmanaged devices, as well as the total number of devices defined by the Endpoint Profiler for this ClearPass server, drag and drop the **Endpoint Profiler Summary** widget to the Dashboard.
 **Failed Authentications** *Track the latest failed authentications*	- To view the table with the latest failed authentications, drag and drop the **Failed Authentications** widget to the Dashboard. - 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.
 **Health Status** *Trend Healthy and Unhealthy requests*	To view the graph of the healthy and unhealthy requests over the past week, drag and drop the **Health Status** widget. - *Healthy requests* are the requests to which the health state was deemed to be healthy based on the posture data sent from the client.

Table 1: *Dashboard Widget Summary (Continued)*

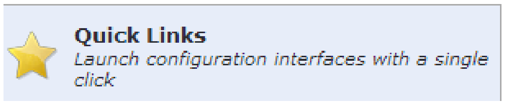
	• *Unhealthy requests* are the requests to which the health state was deemed to be *quarantined* (posture data received but health status is not compliant) or *unknown* (no posture data received). This includes RADIUS and WebAuth requests. The default data filters **Health Requests** and **Unhealthy Requests** are used to plot this graph. • Clicking on each circle on the line graph drills down to the **Access Tracker** page that shows the healthy and unhealthy requests for the last week.
 Latest Authentications *Latest Authentications*	To view the table with the latest authentications, drag and drop the **Latest Authentications** widget to the Dashboard. • Clicking on a row in the table drills down to the **Access Tracker** page that shows requests sorted by timestamp with the latest request displayed on the top.
 MDM Discovery Summary *Mobile Device Management discovery details*	To view the charts that show the endpoints discovered, drag and drop the **MDM Discovery Summary** widget to the Dashboard. • 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. The results 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 **Endpoints** page.
 OnGuard Clients Summary *OnGuard Clients details*	To view a display that shows the number of Linux, Mac, and Windows OnGuard clients, as well as the total number of OnGuard clients for this ClearPass server, drag and drop the **OnGuard Clients Summary** to the Dashboard.
 **Quick Links** *Launch configuration interfaces with a single click*	To view the links to the following configuration tasks, drag and drop the **Quick Links** widget to the Dashboard: • **Start Configuring Policies** • **Manage Services** • **Access Tracker** • **Analysis and Trending** • **Network Devices** • **Server Manager** • **ClearPass Guest** • **ClearPass Onboard**
 Request Processing Time *Trend total request processing time*	To view the trend of total request processing time, drag and drop the **Request Processing Time** widget to the Dashboard.

Table 1: *Dashboard Widget Summary (Continued)*

Service Categorization *Monitor Service Categorization of authentications*	To view the bar chart with each bar representing a categorized Policy Manager service request, drag and drop the **Service Categorization** widget to the Dashboard. ● Clicking on a bar drills down to the **Access Tracker** that shows the requests that were categorized into a specific service.
Successful Authentications *Track the latest successful authentications*	To view a table with the latest successful authentications, drag and drop the **Successful Authentications** widget to the Dashboard. ● Clicking on a row in the table drills down to the **Access Tracker** page that shows successful requests sorted by timestamp, with the latest request displayed on the top.
System CPU Utilization *CPU usage for last 30 mins*	To view the CPU usage for the last 30 minutes, drag and drop the **System CPU Utilization** widget to the Dashboard. ● The widget displays the CPU utilization time in minutes and percentage for System, User, and IO Wait time, indicated by color. ● CPU utilization is presented in five-minute increments.
System Summary *Snapshot of system usage*	To view the Percentage Used statistics for the following components, drag and drop the **System Summary** widget to Dashboard: ● Main Memory ● Swap Memory ● Disk ● Swap Disk

Accessing Configuration Information

This section contains the following information:

- Introduction
- Start Here
- Services
- Authentication and Authorization
- Identity
- Posture
- Enforcement
- Network
- Policy Simulation
- Profile Settings

Introduction

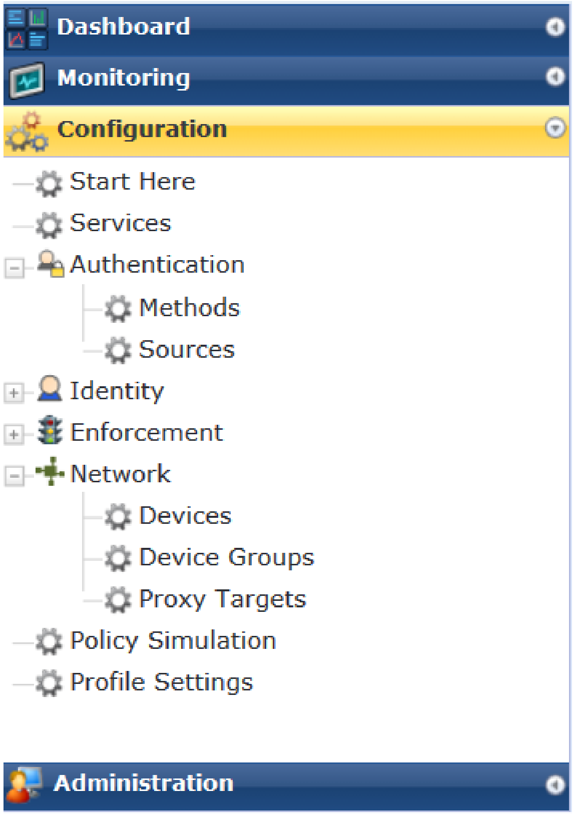
This section provides pointers to information on how to configure the primary configuration tasks in ClearPass Policy Manager.

You can access all these configuration tasks via the **ClearPass Configuration** menu.

To access the **ClearPass Configuration** menu, select **Configuration**.

The **ClearPass Configuration** menu appears (see Figure 1):

Figure 1: *ClearPass Policy Manager Configuration Menu*



Start Here

The ClearPass Policy Manager **Start Here** page provides the ability to create templates for services that will allows you to define baseline policies and require specific data when you create services.

For more information, see Start Here: About Policy Manager Service Templates on page 34.

Services

The **Services** page provides options to add, modify, and remove a service. For more information, refer to the following sections:

- Services Architecture and Flow on page 33
- Start Here: About Policy Manager Service Templates on page 34
- Configuring Policy Manager Services on page 70

This page also shows the current list and order of services that ClearPass Policy Manager keeps track of during authentication and authorization.

Authentication and Authorization

The **Authentication** page provides options to configure the following components:

- Adding and Configuring Authentication Methods on page 165
- Adding and Configuring Authentication Sources on page 190
- Configuring Authentication Methods for an Existing Service on page 163

Identity

The **Identity** page provides options on the settings required to configure ClearPass Policy Manager Identity settings. For more information, refer to the following sections:

- Configuring Single Sign-On on page 233
- Managing Local Users on page 236
- Adding and Modifying Endpoints on page 242
- Managing Static Host Lists on page 252

Posture

The **Posture** page provides options to configure posture policies and audit servers. For more information, refer to the following sections:

- Posture Architecture and Flow on page 263
- Creating a New Posture Policy on page 267
- Configuring Audit Servers on page 338

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 section:

- Configuring Enforcement Policies on page 355
- Configuring Enforcement Profiles on page 357

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. The NAD in this context is usually a mobility controller or a switch.

For more information, refer to the following sections :

- Adding a Network Device on page 448
- Adding and Modifying Device Groups on page 459
- Adding and Modifying Proxy Targets on page 458
- Configuring the Ingress Event Sources on page 704

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 Configuring Policy Simulation on page 409.

Profile Settings

The **Profile Settings** page provides options to configure the following elements:

- Subnet Scans: See Configuring Subnet Scans on page 441 and Initiating a Network Discovery Scan on page 141.
- SNMP Configuration: See SNMP Credentials Configuration on page 135.
- SSH Configuration: See SSH Credentials Configuration on page 137.
- WMI Configuration: See WMI Credentials Configuration.

Importing and Exporting Information

This section contains the following information:

- Importing Information Into ClearPass
- Exporting Information From ClearPass

The option to import or export is available from many ClearPass components, such as services, authentication methods, authentication sources, and enforcement policies.

Importing Information Into ClearPass

Most pages in Policy Manager allow you to import configuration and administration-related information.

This information is stored as an XML file, which can be password protected. For information about the tags and attributes in the XML file, refer to Appendix B, "Using the ClearPass Configuration API" in the *ClearPass Deployment Guide*.

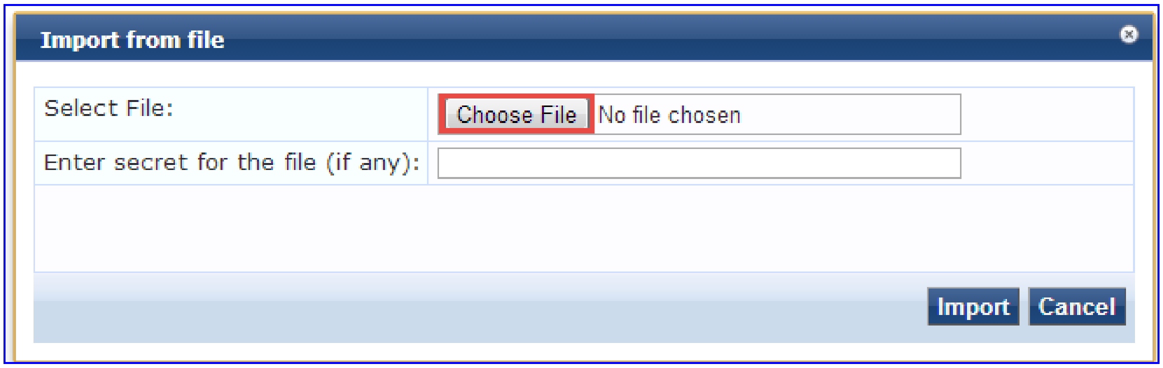
In the top-right corner of the configuration pages, the **Add**, **Import**, and **Export All** options are displayed:

To import information into ClearPass:

1. Click the **Import** link.

   The **Import from file** dialog box opens.

Figure 2: *Import From File Page*



2. Click **Choose File**.
3. Browse to the file you want to import.
   - You must select an XML file in the correct format.

- See Appendix B, "Using the ClearPass Configuration API" in the *ClearPass Deployment Guide* for more information about the format and contents of XML files.
- If you have exported files from different locations within Policy Manager, ensure that you are selecting the correct file.

4. If the file is password protected, enter the password in the **Enter secret for the file (if any)** field.
5. Click **Import**.

Exporting Information From ClearPass

Most pages in Policy Manager allow you to export configuration and administration-related information.

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

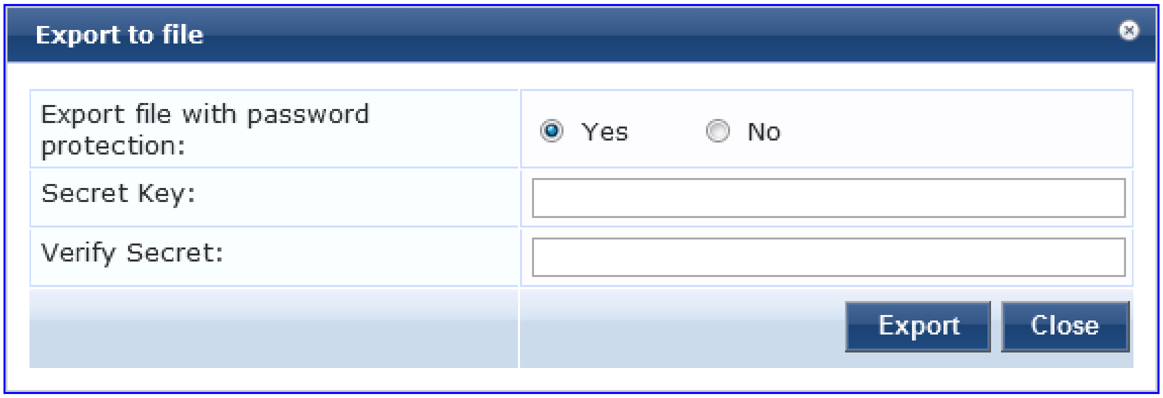
The configuration and administration information is exported as an XML file; you can set this file to be password protected (see Table 2 for details).

To export information from ClearPass:

1. Click the **Export All** link at the top-right corner of the configuration page.

   The **Export to File** dialog opens.

Figure 3: *Export to File Dialog*



Export to file

Export file with password protection: ● Yes ○ No

Secret Key:

Verify Secret:

2. Specify the export parameters based on Table 2.
3. Click **Export**.
4. Enter the XML file name in the **Save As** dialog box.
5. Click **Save**.

Table 2 describes the **Export to file** parameters:

Table 2: *Export to File Dialog Parameters*

Parameter	Action/Description
Export file with password protection	1. To export the file with password protection, choose **Yes**.
Secret Key/ Verify Secret	2. Enter the secret key. Then reenter the secret key.

Chapter 2
Services

This chapter describes the following topics:

The Policy Manager policy model groups policy components that serve a specific type of request into the **Services** page.

Services Architecture and Flow

Service Classification

Policy Manager services are classified as follows:

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

Service Flow Control

The flow control for requests follows this sequence:

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

Approaches to Creating a New Service

There are two approaches to creating a new service in ClearPass:

Bottom-Up

1. Create all the policy components first as needed:
   - Authentication method
   - Authentication source
   - Role-mapping policy
   - Posture policy
   - Audit servers
   - Enforcement profiles
   - Enforcement policy
2. Create the service using the **Service** creation wizard.

Top-Down

1. Start with the **Service** creation wizard.

2. Create the associated policy components as and when required, all in the same flow.

   To help you get started, ClearPass provides 17 service types or templates. If these service types do not suit your needs, you can create a new service using custom rules (as described in the next sectionStart Here: About Policy Manager Service Templates).

Start Here: About Policy Manager Service Templates

This section includes the following information:

- Creating Templates for ClearPass Services
- Service Templates Provided
- Service Templates Supported for High Capacity Guest Mode

ClearPass Policy Manager Service templates provide a way to step through the template-creation process so that you can easily create services and configure their specific components, such as role-mapping policies, enforcement policies, associated network devices, and so on.

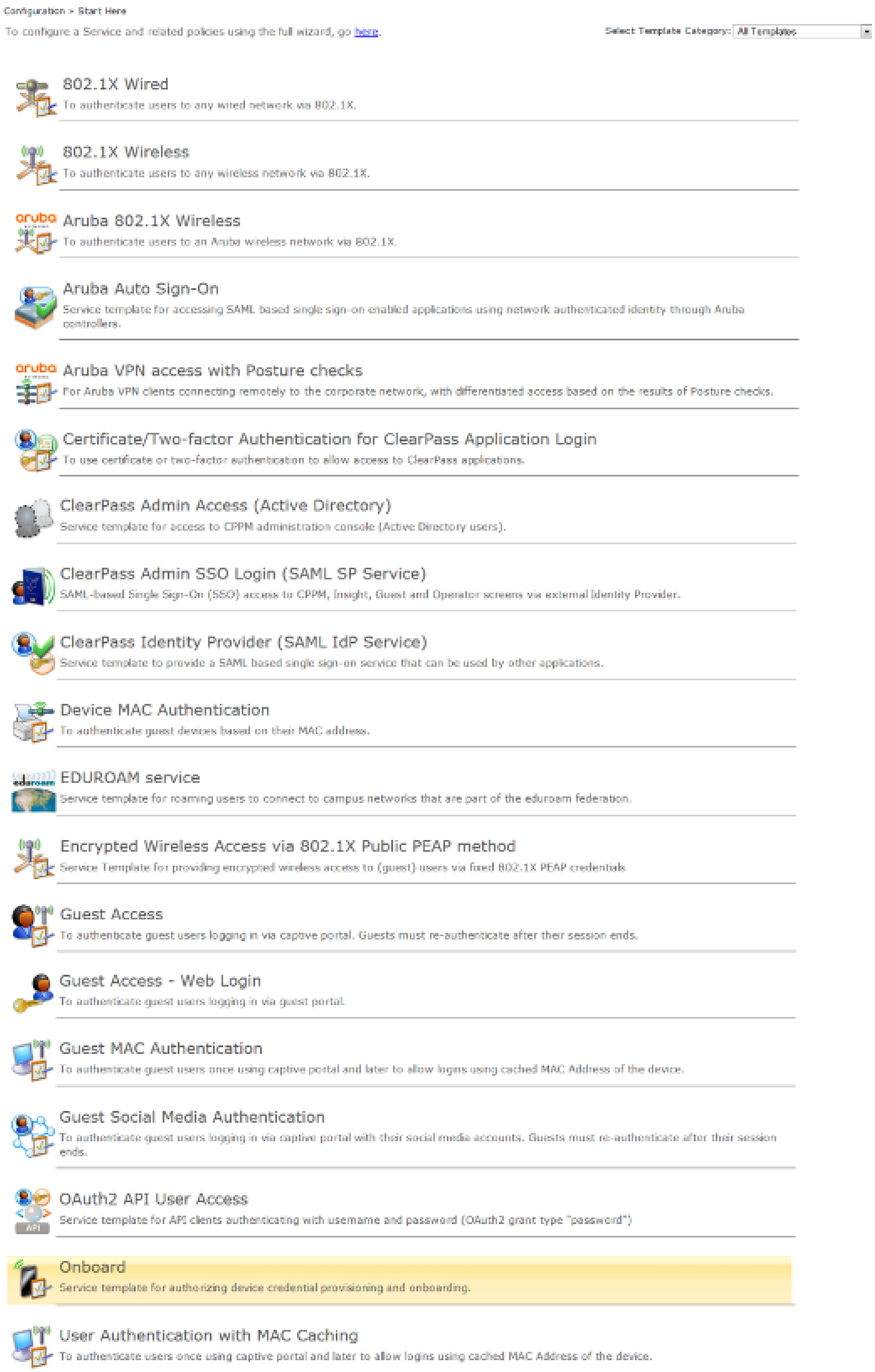
Creating Templates for ClearPass Services

To create templates for services for which you can define baseline policies and require specific data:

1. Navigate to the **Configuration** > **Start Here** page.

   The **Start Here** page opens.

Figure 4: *Start Here Page (Partial View)*



Configuration > Start Here

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

Select Template Category: All Templates

802.1X Wired

To authenticate users to any wired network via 802.1X.

802.1X Wireless

To authenticate users to any wireless network via 802.1X.

Aruba 802.1X Wireless

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

Aruba Auto Sign-On

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

Aruba VPN access with Posture checks

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

Certificate/Two-factor Authentication for ClearPass Application Login

To use certificate or two-factor authentication to allow access to ClearPass applications.

ClearPass Admin Access (Active Directory)

Service template for access to CPPM administration console (Active Directory users).

ClearPass Admin SSO Login (SAML SP Service)

SAML-based Single Sign-On (SSO) access to CPPM, Insight, Guest and Operator screens via external Identity Provider.

ClearPass Identity Provider (SAML IdP Service)

Service template to provide a SAML based single sign-on service that can be used by other applications.

Device MAC Authentication

To authenticate guest devices based on their MAC address.

EDUROAM service

Service template for roaming users to connect to campus networks that are part of the eduroam federation.

Encrypted Wireless Access via 802.1X Public PEAP method

Service Template for providing encrypted wireless access to (guest) users via fixed 802.1X PEAP credentials

Guest Access

To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.

Guest Access - Web Login

To authenticate guest users logging in via guest portal.

Guest MAC Authentication

To authenticate guest users once using captive portal and later to allow logins using cached MAC Address of the device.

Guest Social Media Authentication

To authenticate guest users logging in via captive portal with their social media accounts. Guests must re-authenticate after their session ends.

OAuth2 API User Access

Service template for API clients authenticating with username and password (OAuth2 grant type "password")

Onboard

Service template for authorizing device credential provisioning and onboarding.

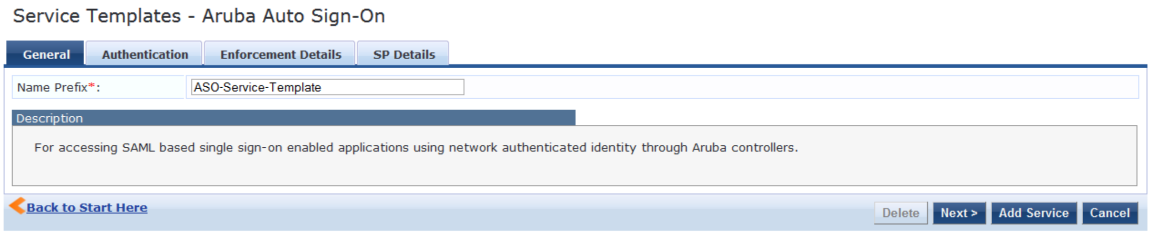
User Authentication with MAC Caching

To authenticate users once using captive portal and later to allow logins using cached MAC Address of the device.

2. Select the desired service template.

   The configuration dialog for the selected service template opens, as shown in the following example figure:

Figure 5: *Auto Sign-On Service Template*



Service Templates - Aruba Auto Sign-On

Name Prefix*: ASO-Service-Template

Description

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

3. Fill in the various fields that are presented in the templates—Policy Manager then creates the configuration elements that are needed for that particular service.

Service Templates Provided

Refer to the following descriptions of the ClearPass service templates for configuration details:

- 802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless Service Template on page 44
- Auto Sign-On Service Template on page 48
- Aruba VPN Access with Posture Checks Service Template on page 49
- Certificate/Two-Factor Authentication for ClearPass Application Login Service Template on page 51
- ClearPass Admin Access Service Template on page 53
- ClearPass Admin SSO Login (SAML SP Service) Service Template on page 54
- ClearPass Identity Provider (SAML IdP Service) Service Template on page 55
- Device MAC Authentication Service Template on page 56
- EDUROAM Service Template on page 58
- Encrypted Wireless Access via 802.1X Public PEAP Method Service Template on page 60
- Guest Access Service Template on page 61
- Guest Access Web Login Service Template on page 63
- Guest Authentication with MAC Caching Service Template on page 64
- Guest Social Media Authentication Service Template on page 66
- OAuth2 API User Access Service Template on page 68
- Onboard Service Template on page 68

Service Templates Supported for High Capacity Guest Mode

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
- Aruba Application Authentication
- Aruba Application Authorization
- TACACS+ Enforcement
- Web-based Authentication
- Web-based Open Network Access

Viewing the List of Services

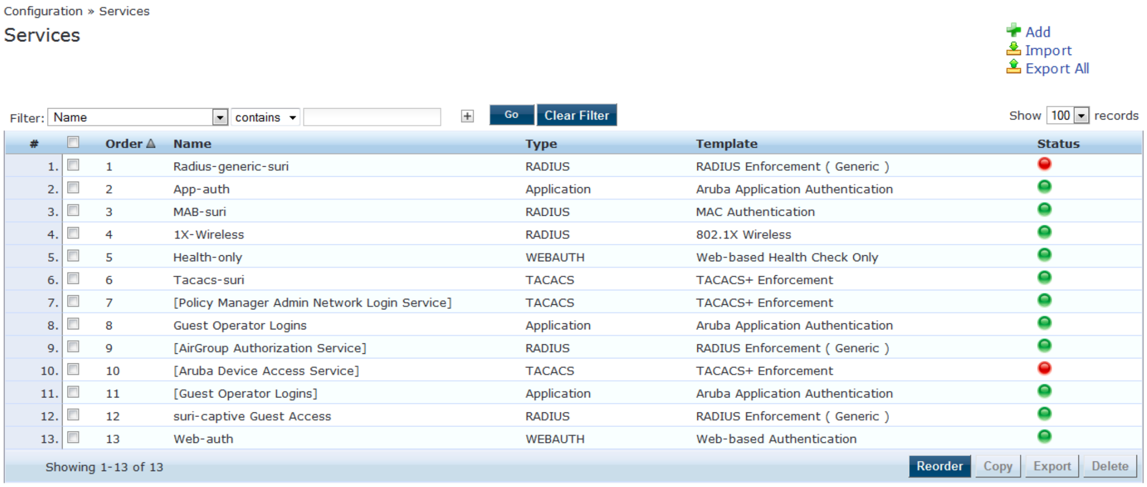
The **Services** page shows the current list and order of services that ClearPass Policy Manager follows during authentication and authorization. You can use the configured default service types or you can add additional services. Services included in square brackets "[ ]" indicate default services.

To view the list of services on the current ClearPass server:

Navigate to **Configuration** > **Services**.

The **Services** page opens:

Figure 6: *Services Page*



Configuration » Services

Services

#	□	Order ▲	Name	Type	Template	Status
1.	□	1	Radius-generic-suri	RADIUS	RADIUS Enforcement (Generic)	🟥
2.	□	2	App-auth	Application	Aruba Application Authentication	🟩
3.	□	3	MAB-suri	RADIUS	MAC Authentication	🟩
4.	□	4	1X-Wireless	RADIUS	802.1X Wireless	🟩
5.	□	5	Health-only	WEBAUTH	Web-based Health Check Only	🟩
6.	□	6	Tacacs-suri	TACACS	TACACS+ Enforcement	🟩
7.	□	7	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	🟩
8.	□	8	Guest Operator Logins	Application	Aruba Application Authentication	🟩
9.	□	9	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	🟩
10.	□	10	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	🟥
11.	□	11	[Guest Operator Logins]	Application	Aruba Application Authentication	🟩
12.	□	12	suri-captive Guest Access	RADIUS	RADIUS Enforcement (Generic)	🟩
13.	□	13	Web-auth	WEBAUTH	Web-based Authentication	🟩

Showing 1-13 of 13

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

Table 3: *Services Page Parameters*

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

For more information, see:

- Adding Services on page 1
- Modifying Services on page 1
- Reordering Services on page 42

Viewing Existing Services

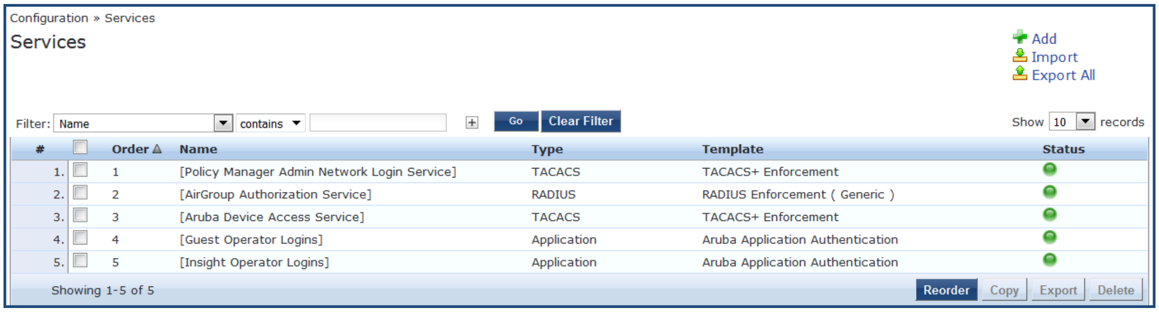
You can view all configured services in a list or drill down to individual services in the **Services** page. You can filter the list of services by phrase or sort the services by order.

To view a list of services:

1. Navigate to **Configuration > Services**.

   The **Services** page opens:

Figure 7: *Services Page*



#	□	Order	Name	Type	Template	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	□	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
3.	□	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●
4.	□	4	[Guest Operator Logins]	Application	Aruba Application Authentication	●
5.	□	5	[Insight Operator Logins]	Application	Aruba Application Authentication	●

Showing 1-5 of 5

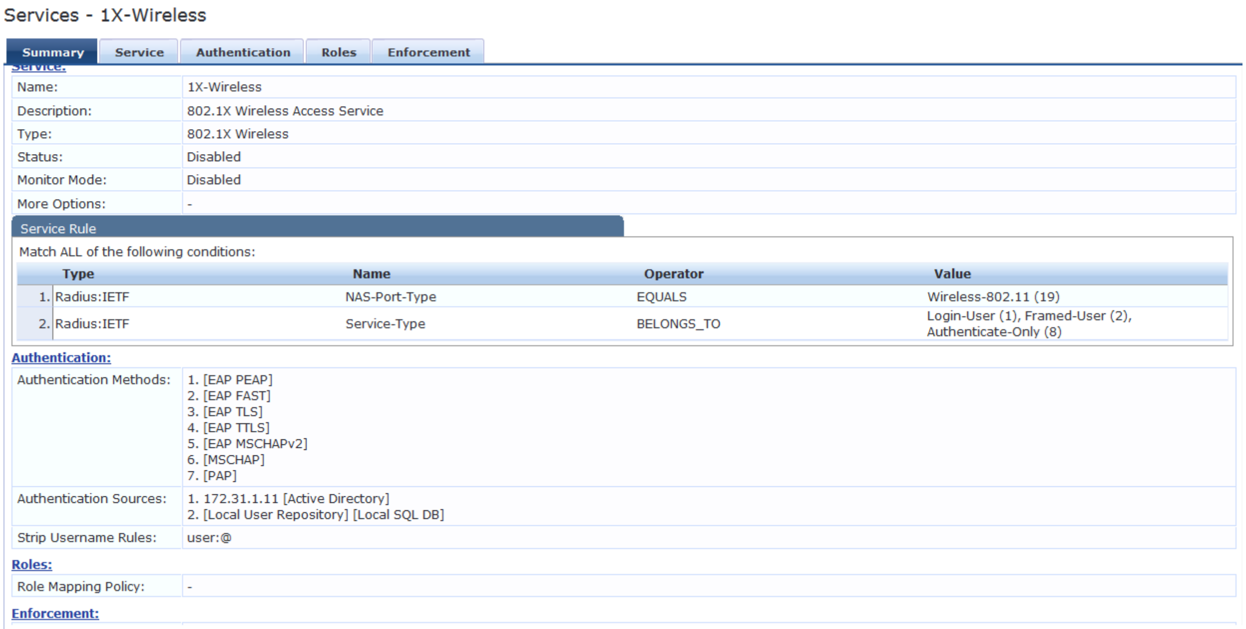
2. To view a service's details, select the service.

   The **Edit Services** page opens to the **Summary** tab. The **Summary** tab provides the detailed information about the selected service configuration.

   For example, to add authentication sources and authentication methods, click the **Authentication** tab.

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

Figure 8: *Details for an Individual Service*



Services - 1X-Wireless

Service:

Name:	1X-Wireless
Description:	802.1X Wireless Access Service
Type:	802.1X Wireless
Status:	Disabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

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

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS] 5. [EAP MSCHAPv2] 6. [MSCHAP] 7. [PAP]
Authentication Sources:	1. 172.31.1.11 [Active Directory] 2. [Local User Repository] [Local SQL DB]
Strip Username Rules:	user:@

Roles:

Role Mapping Policy:	-

Enforcement:

Adding and Removing Services

This section provides the following information:

- Adding a New Service
- Modifying a Service
- Removing a Non-Default Service

You can modify a list of services by creating a new service, copying an existing service, and then modifying or deleting the existing service.

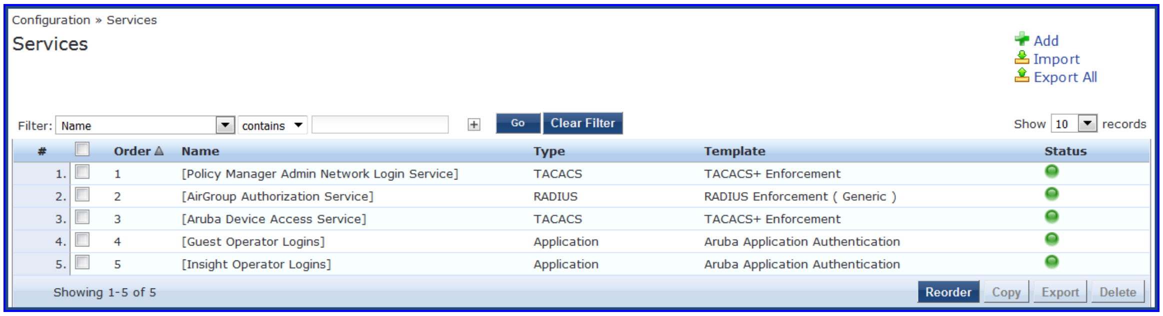
Adding a New Service

To add a new service:

1. Navigate to **Configuration** > **Services**.

   The **Services** page opens.

Figure 9: *Services Page*



Configuration » Services

Services

Filter: Name contains Go Clear Filter Show 10 records

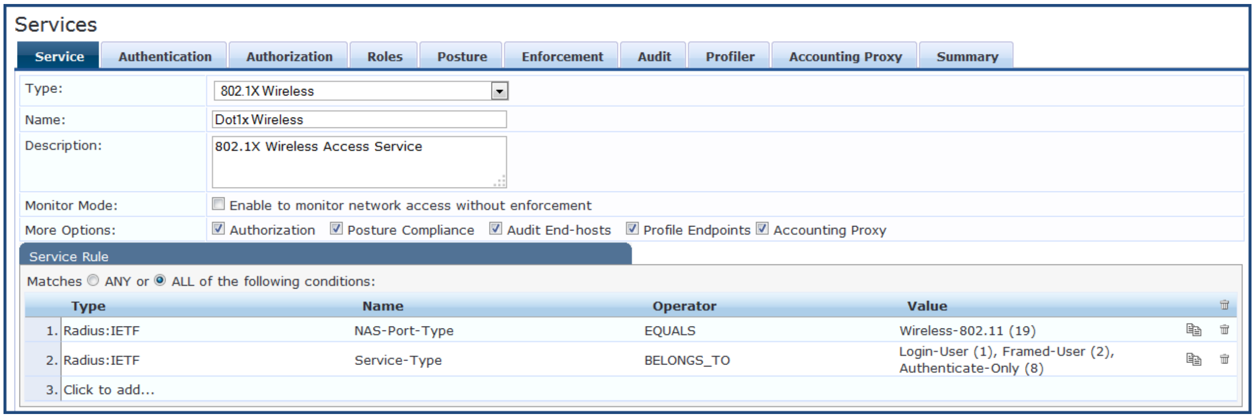
#	□	Order	Name	Type	Template	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	□	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
3.	□	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●
4.	□	4	[Guest Operator Logins]	Application	Aruba Application Authentication	●
5.	□	5	[Insight Operator Logins]	Application	Aruba Application Authentication	●

Showing 1-5 of 5

2. Click **Add**.

   The **Add Services** dialog opens.

Figure 10: *Add Services Page*



Services

Type:	802.1X Wireless
Name:	Dot1x Wireless
Description:	802.1X Wireless Access Service
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☑ Posture Compliance ☑ Audit End-hosts ☑ Profile Endpoints ☑ Accounting Proxy

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

3. Specify the **Add Services** configuration parameters as described in Table 4, then click **Save**.

   Note that the available settings vary, depending upon the service type selected.

Table 4: *Add Services Page Parameters*

Parameter	Action/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:** ClearPass 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 875 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.

Table 4: *Add Services Page Parameters (Continued)*

Parameter	Action/Description
Monitor Mode	Optionally check the **Enable to monitor network access without enforcement** to allow authentication and health validation exchanges to take place between endpoint and Policy Manager, but without enforcement. In **Monitor Mode**, no enforcement profiles (and associated attributes) are sent to the network device. Policy Manager also allows *Policy Simulation* (**Monitoring > Policy Simulation**), where the administrator can test the results of a particular configuration of policy components.
More Options	Select any of the available check boxes to enable the configuration tabs for those options. The available check boxes varies based on the type of service that is selected and may include one or more of the following: ● **Authorization**: Select an authorization source from the drop-down list to add the source or select the **Add new Authentication Source** link to create a new source. ● **Posture Compliance:** Select a Posture Policy from the drop-down list to add the policy or create a new policy by clicking the link. Select the default Posture token. Specify whether to enable auto-remediation of non-compliant end hosts. If this is enabled, then enter the Remediation URL. You can specify the **Posture Server** from the drop-down list or add a new server by clicking the **Add new Posture Server** link. ● **Audit End-hosts:** Select an **Audit Server**, either built-in or customized. Refer to Configuring Audit Servers on page 338 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.

Creating a Service by Copying an Existing Service

NOTE

You can perform a service copy operation only on a Publisher node.

To create a service template by making a copying an existing service:

From the **Services** page, select the check box by a service, then click **Copy**.

Modifying a Service

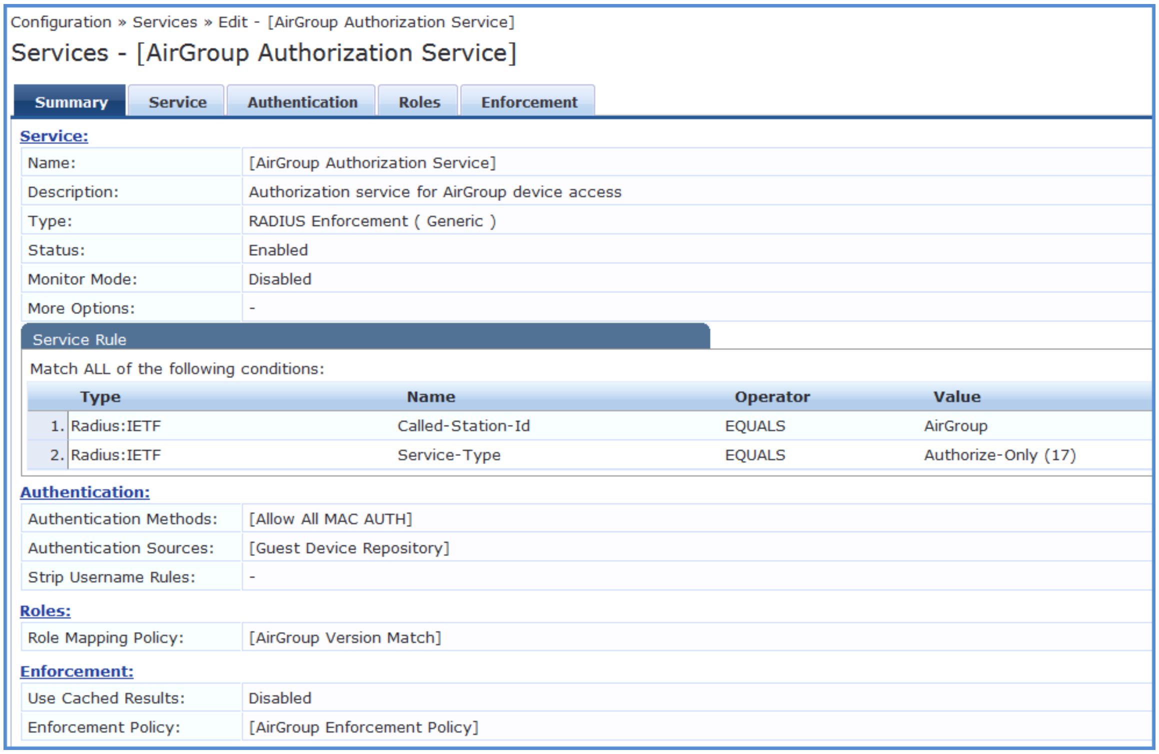
For full access in modifying a service, you must log in to the Publisher node.

To modify an existing service:

1. From the **Services** page, click the check box for the service you want to modify.

   The **Configuration** > **Services** > **Edit** > <*service name*> dialog opens.

Figure 11: *Edit Services Dialog*



Configuration » Services » Edit - [AirGroup Authorization Service]

Services - [AirGroup Authorization Service]

Service:

Name:	[AirGroup Authorization Service]
Description:	Authorization service for AirGroup device access
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	Called-Station-Id	EQUALS	AirGroup
2.	Radius:IETF	Service-Type	EQUALS	Authorize-Only (17)

Authentication:

Authentication Methods:	[Allow All MAC AUTH]
Authentication Sources:	[Guest Device Repository]
Strip Username Rules:	-

Roles:

Role Mapping Policy:	[AirGroup Version Match]

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	[AirGroup Enforcement Policy]

2. Select the **Service** tab to edit the service information.
3. Modify the parameters as needed, then click **Save**.

   You can also disable or enable a service from the **Edit Services** dialog page by clicking **Disable** or **Enable** in the lower right of the page.

Removing a Non-Default Service

To remove a non-default service:

1. From the **Services** page, select the check box for the non-default service you want to remove.
2. Click **Delete**.

Reordering Services

ClearPass 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.

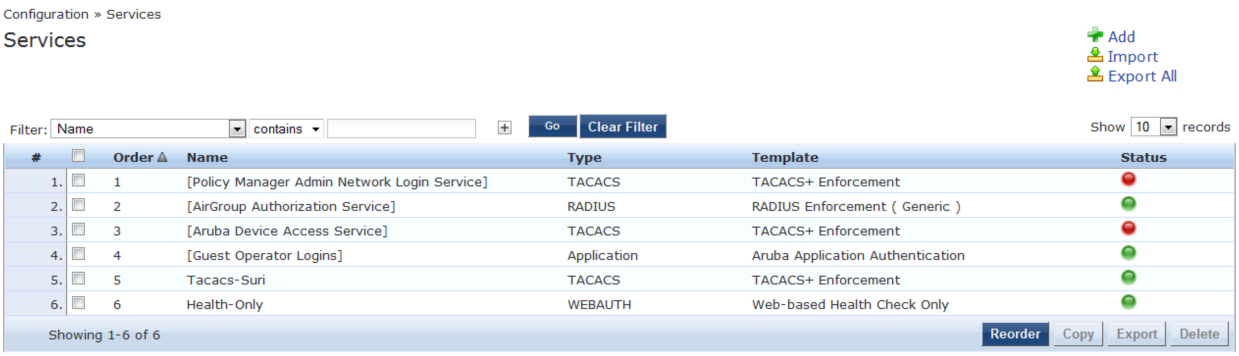
To change the order in which service rules are processed, you can change the order of services.

To change the order of the services:

1. Navigate to the **Configuration > Services** page.

   The **Services** page appears.

Figure 12: *Services Page Reorder Button*



Configuration » Services

Services

#	☐	Order ▲	Name	Type	Template	Status
1.	☐	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	🔴
2.	☐	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	🟢
3.	☐	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	🔴
4.	☐	4	[Guest Operator Logins]	Application	Aruba Application Authentication	🟢
5.	☐	5	Tacacs-Suri	TACACS	TACACS+ Enforcement	🟢
6.	☐	6	Health-Only	WEBAUTH	Web-based Health Check Only	🟢

Showing 1-6 of 6

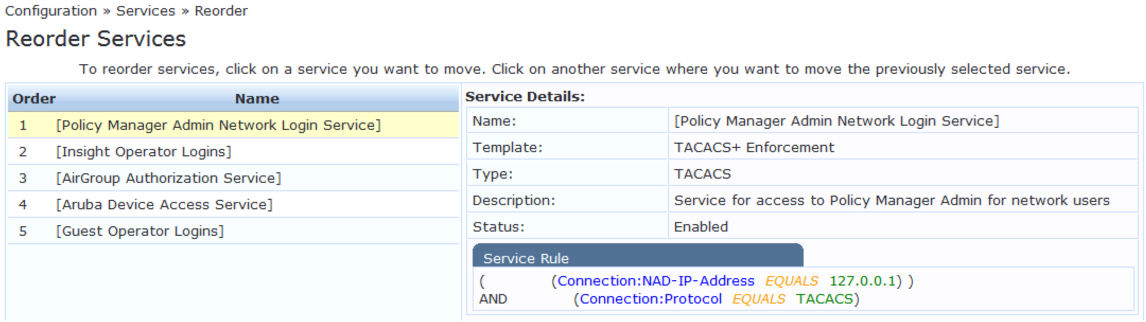
2. Click the **Reorder** button (located on the lower-right portion of the page).

   The Reorder Services page appears.

3. Click the service you want to move to another position in the order (see Figure 13).

   In this example, we will move **Guest Operator Logins** at the 5th position to the 2nd position.

Figure 13: *Selecting the Service to Be Reordered*



Configuration » Services » Reorder

Reorder Services

To reorder services, click on a service you want to move. Click on another service where you want to move the previously selected service.

Order	Name
1	[Policy Manager Admin Network Login Service]
2	[Insight Operator Logins]
3	[AirGroup Authorization Service]
4	[Aruba Device Access Service]
5	[Guest Operator Logins]

Service Details:

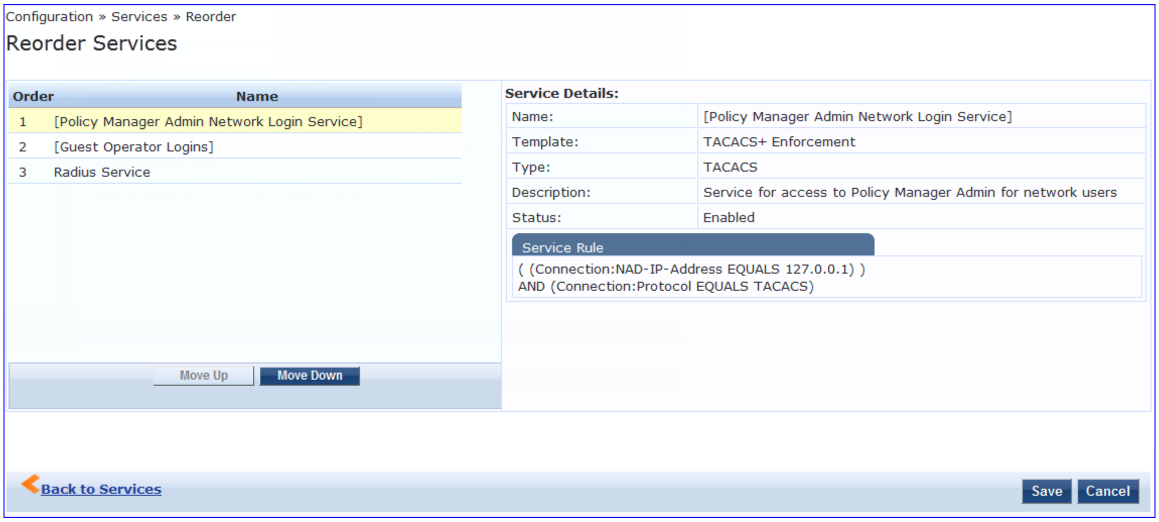
Name:	[Policy Manager Admin Network Login Service]
Template:	TACACS+ Enforcement
Type:	TACACS
Description:	Service for access to Policy Manager Admin for network users
Status:	Enabled

Service Rule

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

4. Select the position where you want to move the service (see Figure 14).

Figure 14: *Selecting the Destination Order Position*



Configuration » Services » Reorder

Reorder Services

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

Service Details:

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

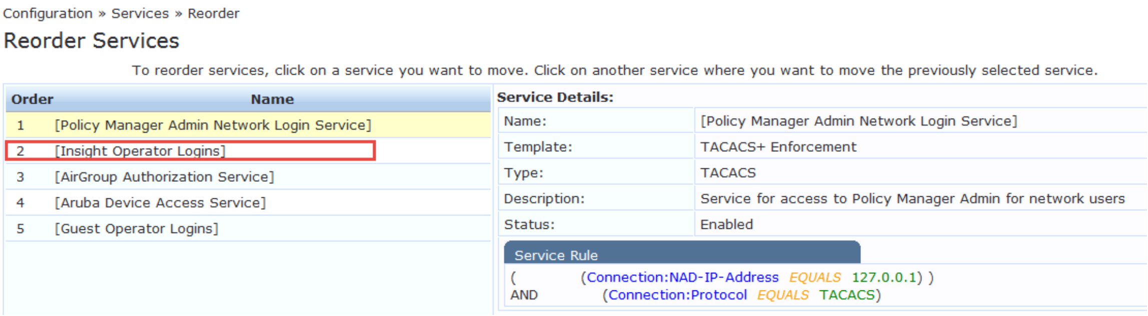
Service Rule

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

5. Click the selected destination position (see Figure 15).

   The service is now moved to its new position in the services order.

Figure 15: *Service Moved to New Order Position*



Configuration » Services » Reorder

Reorder Services

To reorder services, click on a service you want to move. Click on another service where you want to move the previously selected service.

Order	Name
1	[Policy Manager Admin Network Login Service]
2	[Insight Operator Logins]
3	[AirGroup Authorization Service]
4	[Aruba Device Access Service]
5	[Guest Operator Logins]

Service Details:

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

Service Rule

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

6. Click **Save**.

   You return to the Services page, which shows the service in its new order and displays the message:

   Services have been reordered successfully.

Configuring Service Templates

Refer to the following descriptions of the ClearPass Policy Manager Service Templates for configuration details:

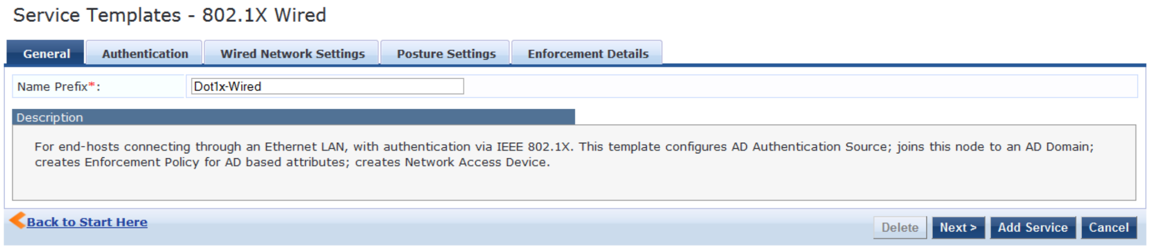
- 802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless Service Template on page 44
- Auto Sign-On Service Template on page 48
- Aruba VPN Access with Posture Checks Service Template on page 49
- Certificate/Two-Factor Authentication for ClearPass Application Login Service Template on page 51
- ClearPass Admin Access Service Template on page 53
- ClearPass Admin SSO Login (SAML SP Service) Service Template on page 54
- ClearPass Identity Provider (SAML IdP Service) Service Template on page 55
- Device MAC Authentication Service Template on page 56
- EDUROAM Service Template on page 58
- Encrypted Wireless Access via 802.1X Public PEAP Method Service Template on page 60
- Guest Access Service Template on page 61
- Guest Access Web Login Service Template on page 63
- Guest Authentication with MAC Caching Service Template on page 64
- Guest Social Media Authentication Service Template on page 66
- OAuth2 API User Access Service Template on page 68
- Onboard Service Template on page 68

802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless Service Template

- The **802.1X Wired** service template is designed for wired end-hosts connecting through an Ethernet LAN using IEEE 802.1X authentication. The **802.1X Wired** service template allows configuration of both identity-based and posture-based policies.
- The **802.1X Wireless** template is for wireless end-hosts connecting through an 802.11 wireless access device or controller using IEEE 802.1X authentication. The **802.1X Wireless** template allows configuring both identity-based and posture-based policies.
- The **Aruba 802.1X Wireless** template is designed for wireless end-hosts connecting through an Aruba 802.11 wireless access device or controller using IEEE 802.1X authentication (service rules customized for Aruba WLAN controllers).

All three service templates are configured using identical parameters.

Figure 16: *Service Templates > 802.1X Wired Service Template*



Service Templates - 802.1X Wired

Name Prefix*: Dot1x-Wired

Description

For end-hosts connecting through an Ethernet LAN, with authentication via IEEE 802.1X. This template configures AD Authentication Source; joins this node to an AD Domain; creates Enforcement Policy for AD based attributes; creates Network Access Device.

Adding a New Service for the Selected 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.

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** drop-down. Selecting a prefix from the drop-down populates the existing configuration for the service.

4. Specify the parameters in the 802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless service templates as described in the following table:

Table 5: *802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless Service Template Parameters*

Parameter	Action/Description
General	
Select Prefix	1. Select a prefix from the existing list of prefixes. This populates the preconfigured information in the **Authentication** and **Enforcement Details** sections. The **Name Prefix** field is not editable.
Name Prefix	2. Enter a prefix that is appended to services using this template. Use this to identify the services that use templates.
Authentication	
Select Authentication Source	1. Select any available authentication source from the list. The information updated in the **Authentication** and **Enforcement Details** tabs will be auto-populated.
Active Directory	2. Enter the name of the Active Directory. This field is mandatory.

Table 5: *802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless Service Template Parameters (Continued)*

Parameter	Action/Description
Name	
Description	3. Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	4. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Port	5. Enter the TCP port where the server is listening for a connection. This field is mandatory.
Identity	6. Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
Password	7. Enter the account password. This field is mandatory.
NetBIOS	8. Enter the server Active Directory domain name. This field is mandatory.
Base DN	9. Enter the DN of the node in your directory tree from which to start searching for records. This field is mandatory.
Enforcement Details	
Attribute Name	The attributes defined in the **Authentication Source** are listed here. 1. 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	2. Enter the active directory attribute value for the selected name in the **Attribute Name** field.
VLAN ID	3. Enter the standard RADIUS-IETF VLAN ID.
Wired Network Settings	
Select Switch	1. Select any switch from the drop-down list.
Device Name	2. Enter the name of the device.
IP Address	3. Enter the IP address of the device.

Table 5: *802.1X Wired, 802.1X Wireless, and Aruba 802.1X Wireless Service Template Parameters (Continued)*

Parameter	Action/Description
Vendor Name	4. Select the manufacturer of the wired controller.
RADIUS Shared Secret	5. Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	6. 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. 7. Change this value only if you defined a custom port on the network device.
Wireless Network Settings	
Wireless Controller Name	1. Enter the name of the wireless controller.
Controller IP Address	2. Enter the IP address of the wireless controller.
Vendor Name	3. Select the manufacturer of the wireless controller.
RADIUS Shared Secret	4. Enter the shared secret that is configured on the controller and Policy Manager to send and receive RADIUS requests.
Enable RADIUS CoA	5. Select to enable RADIUS initiated CoA on the network device.
RADIUS CoA Port	Specifies the default port **3799** if RADIUS CoA is enabled. 6. Change this value only if you defined a custom port on the network device.
Posture Settings	
Enable Posture Checks	7. Select the check box to perform health checks post authentication. This enables the **Host Operating System** and **Quarantine Message** fields.
Host Operating System	8. Select the operating system: **Windows**, **Linux**, or **Mac OS X**.
Quarantine Message	9. Specify the quarantine message that will appear on the client.

Deleting a Service

To delete a service:

1. Select the appropriate service from the **Select Prefix** drop-down.
2. Click **Delete**.

All the configured entries under the **Services**, **Authentication Source, Roles**, **Role Mapping**, **Enforcement Policies** and **Profiles** menu are deleted if these entities were created from the service template.

NOTE

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

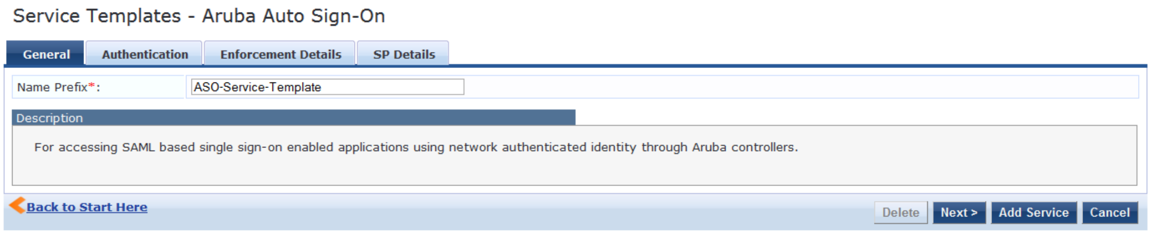
Do not delete entities used in service configurations that are not created using the service template.

Auto Sign-On Service Template

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

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

Figure 17: *Auto Sign-On Service Template*



Service Templates - Aruba Auto Sign-On

Name Prefix*: ASO-Service-Template

Description

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

Specify the **Auto Sign-On** service template parameters as described in the following table:

Table 6: *ClearPass Auto Sign-On Service Template Parameters*

Parameter	Action/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.

Table 6: *ClearPass Auto Sign-On Service Template Parameters (Continued)*

Parameter	Action/Description
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	Configure an optional enforcement policy based on the following attributes: ● Department ● Email ● Name ● Phone ● UserDN ● company ● memberOf ● Title
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	

Aruba VPN Access with Posture Checks Service Template

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

- Configures an Active Directory authentication source
- Joins this node to the Active Directory domain
- Creates an enforcement policy for Active Directory-based attributes
- Creates a Network Access Device (NAD)

NOTE

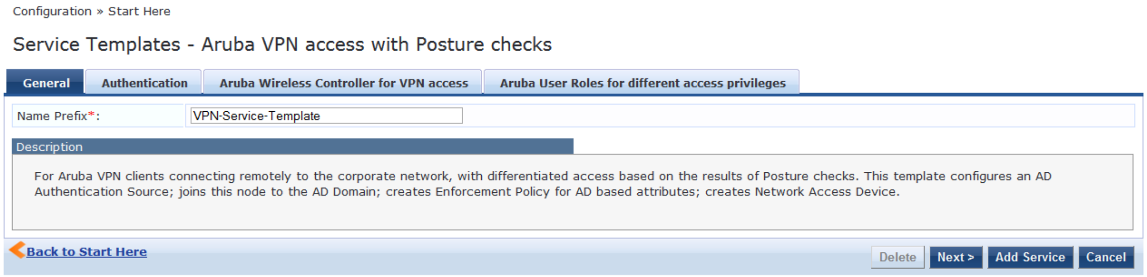
Posture checks are not performed if **High Capacity Guest** mode is enabled in the cluster.

NOTE

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

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

Figure 18: *Aruba VPN Access with Posture Checks Service Template*



Configuration » Start Here

Service Templates - Aruba VPN access with Posture checks

General
Authentication
Aruba Wireless Controller for VPN access
Aruba User Roles for different access privileges

Name Prefix*: VPN-Service-Template

Description

For Aruba VPN clients connecting remotely to the corporate network, with differentiated access based on the results of Posture checks. This template configures an AD Authentication Source; joins this node to the AD Domain; creates Enforcement Policy for AD based attributes; creates Network Access Device.

Specify the **Aruba VPN Access with Posture Checks** service template parameters as described in the following table:

Table 7: *Aruba VPN Access with Posture Checks Service Template Parameters*

Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured information in the **Authentication Aruba Wireless Controller for VPN Settings** and **Aruba 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**, **Aruba Wireless Controller for VPN Settings**, and **Aruba 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 host name or the IP address of the Active Directory server.
Identity	Enter the Distinguished Name (DN) of the administrator account.
NetBIOS	Enter the server Active Directory domain name.
Base DN	Enter the Distinguished Name (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.
Aruba Wireless Controller for VPN Access	

Table 7: *Aruba VPN Access with Posture Checks Service Template Parameters (Continued)*

Parameter	Action/Description
Select Wireless Controller	Select a wireless controller from the drop-down list.
Wireless controller name	Enter the name given to the wireless controller.
Controller IP Address	Enter the wireless controller's IP address.
Vendor Name	Select the manufacturer of the wireless controller.
RADIUS Shared Secret	Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.
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. **NOTE:** Change this value only if you defined a custom port on the network device.
Aruba 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.

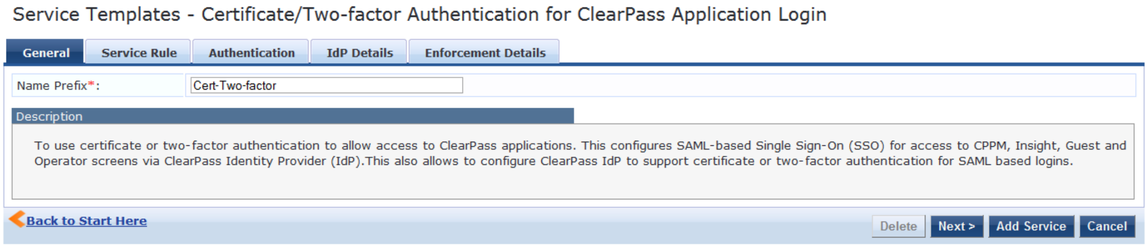
Certificate/Two-Factor Authentication for ClearPass Application Login Service Template

This service template allows administrators and operators to log in to ClearPass using a smart card and TLS (Transport Layer Security) certificates.

To log in using a smart card and TLS certificates, ensure that the services are configured using the **Certificate/Two-Factor Authentication for ClearPass Application Login** service template.

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

Figure 19: *Certificate/Two-Factor Authentication Service Template*



Service Templates - Certificate/Two-factor Authentication for ClearPass Application Login

Name Prefix*: Cert-Two-factor

Description

To use certificate or two-factor authentication to allow access to ClearPass applications. This configures SAML-based Single Sign-On (SSO) for access to CPPM, Insight, Guest and Operator screens via ClearPass Identity Provider (IdP).This also allows to configure ClearPass IdP to support certificate or two-factor authentication for SAML based logins.

Specify the **Certificate/Two-Factor Authentication for ClearPass Application Login** service template parameters as described in the following table:

Table 8: *ClearPass Certificate/Two-Factor Authentication Service Template Parameters*

Parameter	Action/Description
General	
Select Prefix	1. 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	2. Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Service Rule	
Application	3. 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	
Select Authentication Source	4. 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	5. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	6. Enter a description that helps you to identify the characteristics of this template. This field is mandatory.
Server	7. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Port	8. 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	9. Enter the DN of the administrator account. This field is mandatory.
Password	10. Enter the account password. This field is mandatory.
NETBIOS	11. Enter the server Active Directory domain name. This field is mandatory.
Base DN	12. Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
IdP Details	
Page Name	13. Select the **Web Login** pages from the drop-down list. For more information, see the next section, Creating a New Web Login Page.
Enforcement Details	

Table 8: *ClearPass Certificate/Two-Factor Authentication Service Template Parameters (Continued)*

Parameter	Action/Description
Certificate Attribute - Super Admin Condition	14. Select the certificate attribute from the drop-down list. 15. 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	16. Select the certificate attribute from the drop-down list. 17. 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	18. Select the certificate attribute from the drop-down list. 19. Enter the value in the **Help Desk Admin Condition** field that matches the **Certificate Attribute** value to provide the help desk administrator access.

Creating a New Web Login Page

To create a new Web Login page:

1. 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.

2. To log in using a smart card and TLS certificates, navigate to **ClearPass Guest** > **Configuration** > **Pages** > **Web Logins**.

3. In the **Vendor Settings** field, select **Single Sign On -SAML Identity Provider**.

   a. When you select **Optional - Request a client certificate from the user**, but allow none from the **Client Certificate** field, the user needs to provide a certificate, username, and password.

   b. When you select **Required - Require a client certificate from the user** from the **Client Certificate** field, the user needs to provide only certificates for authentication.

      This enables the **Authentication** field with the following options:

      - **Certificate only - No username or password required:** Requires only certificate authentication.
      - **Credentials - Also require a username and password**: Requires the username and password.

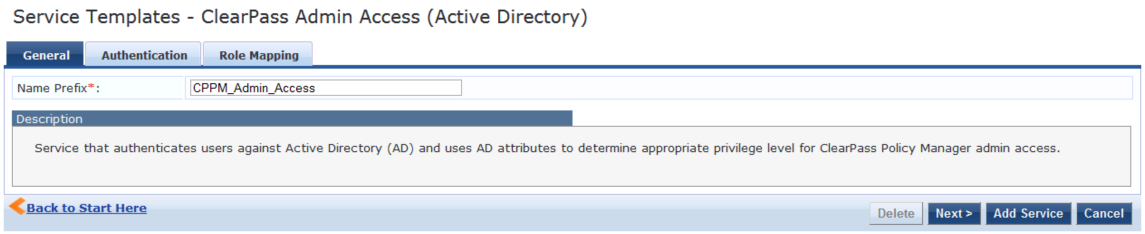
ClearPass Admin Access Service Template

This template is designed for services that authenticate users against Active Directory.

Use Active Directory attributes to determine appropriate privilege levels for ClearPass Policy Manager admin access.

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

Figure 20: *ClearPass Admin Access Service Template*



Service Templates - ClearPass Admin Access (Active Directory)

Name Prefix*: CPPM_Admin_Access

Description

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

Specify the **ClearPass Admin Access** service template parameters as described in the following table:

Table 9: *ClearPass Admin Access Service Template Parameters*

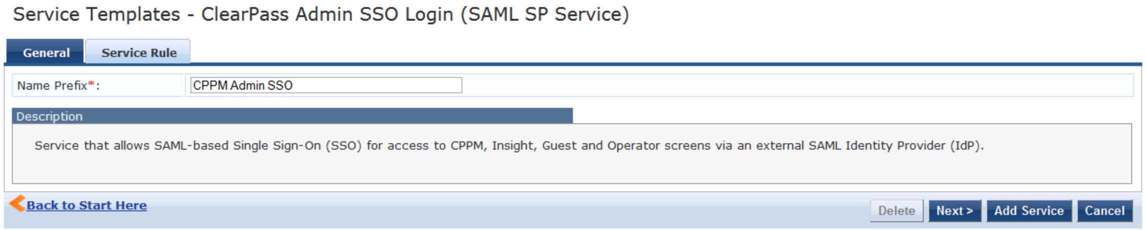
Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured information in the **Authentication** and **Role Mapping** sections. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.
Authentication: Create an Active Directory Authentication Source	
Select Authentication Source	Select an authentication source from the list. The information updated in the **Authentication** and **Role Mapping** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps to identify the characteristics of this template. This field is mandatory.
Server	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
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 the DN of the administrator account. 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) Service Template

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



Service Templates - ClearPass Admin SSO Login (SAML SP Service)

Name Prefix*: CPPM Admin SSO

Description

Service that allows SAML-based Single Sign-On (SSO) for access to CPPM, Insight, Guest and Operator screens via an external SAML Identity Provider (IdP).

Specify the **ClearPass Admin SSO Login** service template parameters as described in the following table:

Table 10: ClearPass *Admin SSO Login Service Template Parameters*

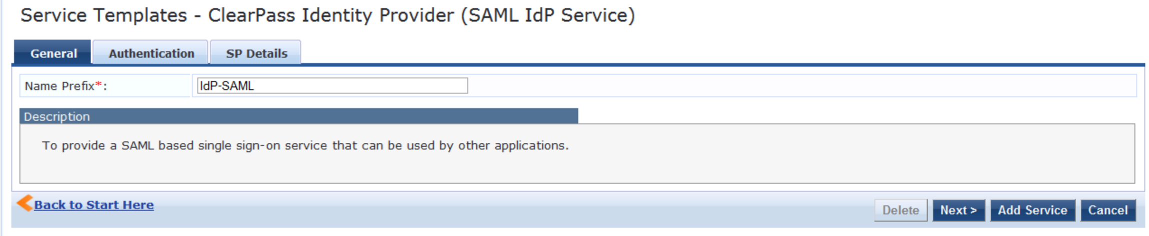
Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured information in the **Service Rule** tab. The **Name Prefix** field is not editable.
Name Prefix	Enter a prefix that you want to append to services using this template. 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) Service Template

This template is designed for services that act as an Identity Provider (IdP). This Identity Provider feature allows the Layer-2 device, RADIUS server, and SAML Identity Provider 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 22: *ClearPass Identity Provider (SAML IdP Service)*



Service Templates - ClearPass Identity Provider (SAML IdP Service)

Name Prefix*: IdP-SAML

Description

To provide a SAML based single sign-on service that can be used by other applications.

Specify the **ClearPass Identity Provider (SAML IdP Service)** service template parameters:

Table 11: *ClearPass Identity Provider (SAML IdP Service) Service Template Parameters*

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

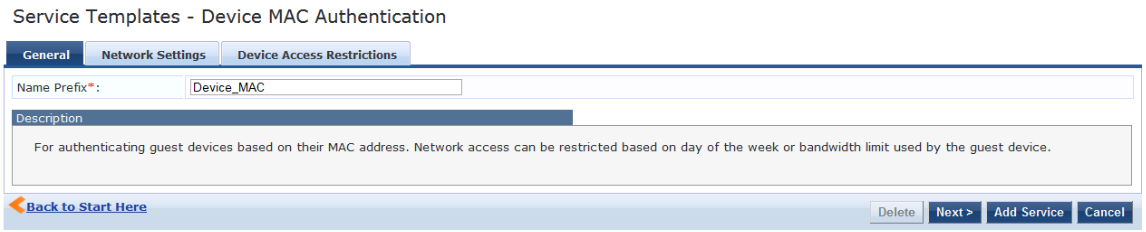
Device MAC Authentication Service Template

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 by the bandwidth limit.

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

Figure 23: *Device MAC Authentication Service Template*



Service Templates - Device MAC Authentication

Name Prefix*: Device_MAC

Description

For authenticating guest devices based on their MAC address. Network access can be restricted based on day of the week or bandwidth limit used by the guest device.

Specify the parameters in the **Device MAC Authentication** service template as described in the following table:

Table 12: *Device MAC Authentication Template Parameters*

Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured 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 preconfigured 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 controllerand in 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.

Table 12: *Device MAC Authentication Template Parameters (Continued)*

Parameter	Action/Description
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 Template

This template is designed for the following scenarios:

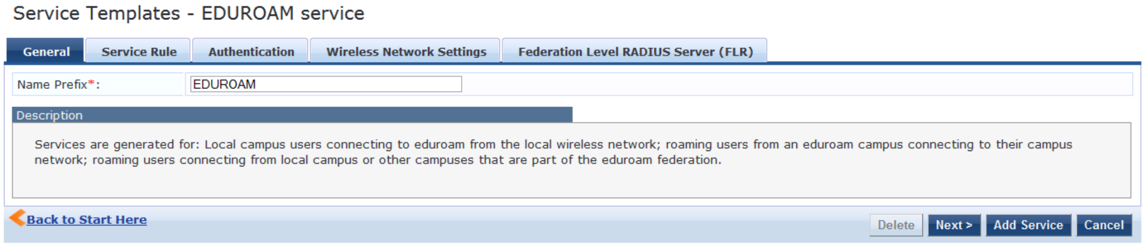
- Local campus users connecting to eduroam from the local wireless network.
- Roaming users from an eduroam campus connecting to their campus network.
- Roaming users connecting from local campus or other campuses that are part of the eduroam federation.

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 24: *EDUROAM Service Template*



Service Templates - EDUROAM service

General
Service Rule
Authentication
Wireless Network Settings
Federation Level RADIUS Server (FLR)

Name Prefix*: EDUROAM

Description

Services are generated for: 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.

Specify the parameters used in the **EDUROAM** service template as described in the following table:

Table 13: *EDUROAM Service Template Parameters*

Parameter	Action/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	

Table 13: *EDUROAM Service Template Parameters (Continued)*

Parameter	Action/Description
Enter domain details	Enter the domain name of the network. For example, @edunet.ucla.com. This field is mandatory.
Select Vendor	Select the vendor of the network device. This field is mandatory.
Authentication	
Select Active Directory	Select an authentication source from the list, the information updated in the **Authentication**, **Wireless**, and **Federation Level Radius Server (FLR)** tabs are auto-populated.
Active Directory Name	Enter the hostname or the IP address of the Active Directory server. This field is mandatory.
Description	Enter a description that helps you identify the characteristics of this template. This field is mandatory.
Server	Enter the host name or the IP address of the Active Directory server. This field is mandatory.
Identity	Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.
NetBIOS	Enter the server Active Directory domain name. This field is mandatory.
Base DN	Enter the Distinguished Name (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 controllerand 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 13: *EDUROAM Service Template Parameters (Continued)*

Parameter	Action/Description
Federation Level RADIUS Server (FLR)	
Host Name	Enter the host name 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 controllerand 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. **NOTE:** Change this value only if you defined a custom port on the network device.
RADIUS Authentication Port	Enter the port number for the RADIUS Authentication Port.
RADIUS Accounting Port	Enter the port number for the RADIUS Accounting Port.

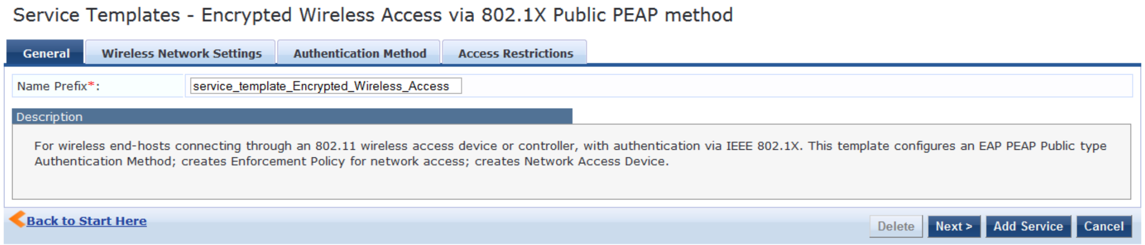
Encrypted Wireless Access via 802.1X Public PEAP Method Service Template

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 an enforcement policy for network access.

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

Figure 25: *Encrypted Wireless Access via 802.1X Public PEAP Method Service Template*



Service Templates - Encrypted Wireless Access via 802.1X Public PEAP method

Name Prefix*: service_template_Encrypted_Wireless_Access

Description

For wireless end-hosts connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. This template configures an EAP PEAP Public type Authentication Method; creates Enforcement Policy for network access; creates Network Access Device.

Specify the parameters used in the **Encrypted Wireless Access via 802.1X Public PEAP method** service template s described in the following table:

Table 14: *Encrypted Wireless Access via 802.1X Public PEAP Method Service Template Parameters*

Parameter	Action/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 controllerand 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. **NOTE:** Change this value only if you defined a custom port on the network device.
Authentication Method	
Public Username	Enter the public username for the EAP PEAP Public type authentication method.
Public Password	Enter the password for the EAP PEAP Public type authentication method.
Access Restrictions	
Days allowed for access	Select the days on which network access is allowed.

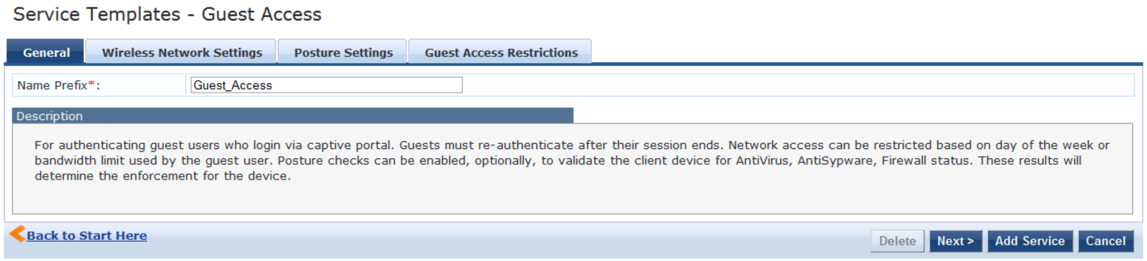
Guest Access Service Template

This template is designed for authenticating guest users who log in using captive portal.

Guests must reauthenticate 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 26: *Guest Access Service Template*



Service Templates - Guest Access

Name Prefix*: Guest_Access

Description

For authenticating guest users who login via captive portal. Guests must re-authenticate after their session ends. Network access can be restricted based on day of the week or bandwidth limit used by the guest user. 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.

Specify the parameters used in the **Guest Access** service template as described in the following table:

Table 15: *Guest Access Service Template Parameters*

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

Table 15: *Guest Access Service Template Parameters (Continued)*

Parameter	Action/Description
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 days of the week that 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 (MB) to which a user is allowed per day. A value of 0 (zero), the default, means no limit is set.

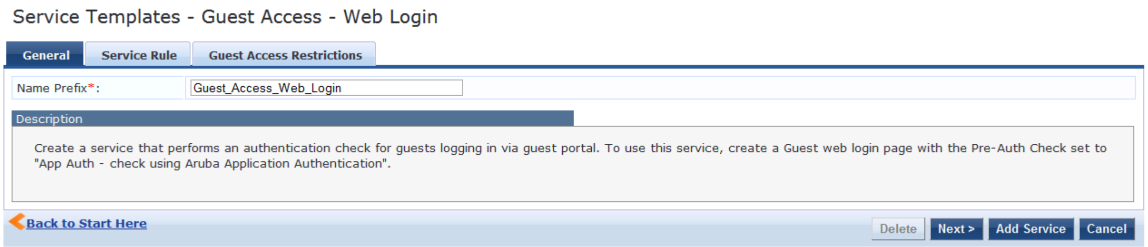
Guest Access Web Login Service Template

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 **Aruba Application Authentication**.

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

Figure 27: *Guest Access Web Login Service Template*



Service Templates - Guest Access - Web Login

Name Prefix*: Guest_Access_Web_Login

Description

Create a service that performs an authentication check for guests logging in via guest portal. To use this service, create a Guest web login page with the Pre-Auth Check set to "App Auth - check using Aruba Application Authentication".

Specify the **Guest Access Web Login** service template parameters as described in the following table:

Table 16: *Guest Web Login Service Template Parameters*

Parameter	Action/Description
General	
Select Prefix	Select any one prefix from the existing list of prefixes. This populates the preconfigured 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.

Table 16: *Guest Web Login Service Template Parameters (Continued)*

Parameter	Action/Description
	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 session for the Guest Web Login page.
Guest Access Restrictions	
Days allowed for access	Select the days of the week that guest users are allowed network access. **NOTE:** All seven days of the week are enabled by default.

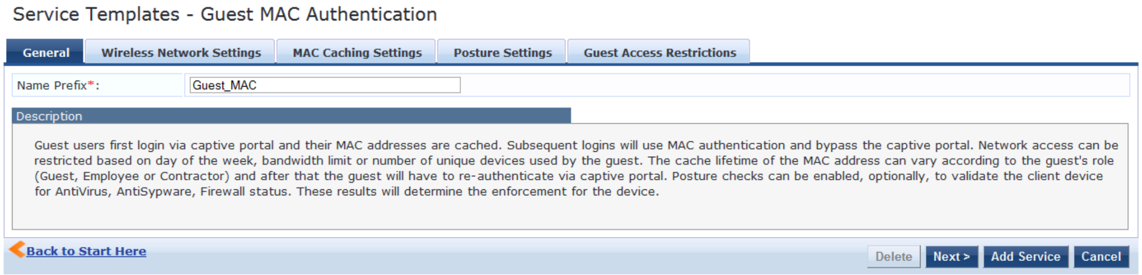
Guest Authentication with MAC Caching Service Template

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 a different lifetime for the cached MAC address.

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

Figure 28: *Guest MAC Authentication Service Template*



Service Templates - Guest MAC Authentication

Name Prefix*: Guest_MAC

Description

Guest users first login via captive portal and their MAC addresses are cached. Subsequent logins 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 guest. The cache lifetime of the MAC address can vary according to the guest's role (Guest, Employee or Contractor) and after that the guest will have to re-authenticate via 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.

Specify the **Guest MAC Authentication** service template parameters as described in the following table:

Table 17: *Guest MAC Authentication Service Template Parameters*

Parameter	Action/Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured 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	

Table 17: *Guest MAC Authentication Service Template Parameters (Continued)*

Parameter	Action/Description
Wireless SSID	Enter the SSID name of your network.
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 this check box to enable RADIUS initiated CoA (Change of Authorization) on the network device.
RADIUS CoA Port	Specifies the default port **3799** if RADIUS CoA is enabled. **NOTE:** Change this value only if you defined a custom port on the network device.
MAC Caching Settings	
Cache Duration for Employee	From the Account Expiry Time drop-down, select the MAC caching duration for employees: - One Day - One Week - One Month - Six Months **NOTE:** When this duration expires, users must reauthenticate via the captive portal. **NOTE:** You must specify the cache duration for at least one role.
Cache Duration for Guest	From the Account Expiry Time drop-down, select the MAC caching duration for guests: - One Day - One Week - One Month - Six Months
Cache Duration for Contractor	From the Account Expiry Time drop-down, select the MAC caching duration for contractors: - One Day - One Week - One Month - Six Months
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(s): Windows, Linux, or Mac OS X.
Quarantine Message	Specify the quarantine message that will appear on the client.

Table 17: *Guest MAC Authentication Service Template Parameters (Continued)*

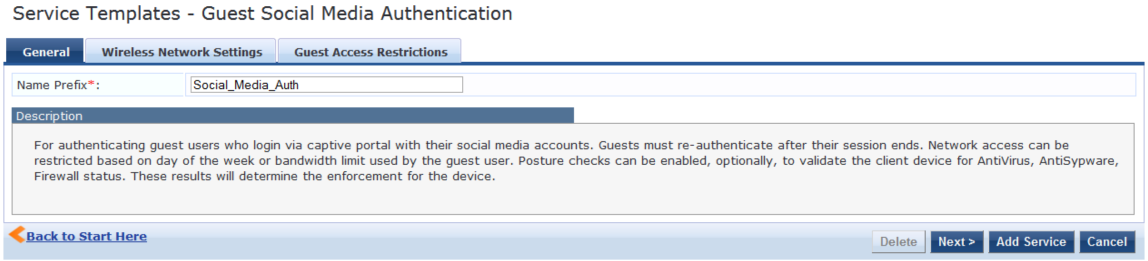
Parameter	Action/Description
Initial Role/VLAN	Enter the initial role of the client before posture checks are performed.
Quarantine Role/VLAN	Enter the role of clients that fail posture checks.
Access Restrictions	
Enforcement Type	Select one of the following enforcement types: - Aruba Role Enforcement - VLAN Enforcement - Filter ID-Based Enforcement **NOTE:** Enforcement Type applies to the **Captive Portal Access**, **Employee Access**, **Guest Access**, and **Contractor Access** fields. At least one of these must be specified.
Captive Portal Access	TBD
Days allowed for access	Select the days of the week that guest users are allowed network access. By default, all seven days of the week are enabled.
Maximum number of devices allowed per user	Enter the maximum number of devices that 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.
Employee Access	TBD
Guest Access	TBD
Contractor Access	TBD

Guest Social Media Authentication Service Template

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

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

Figure 29: *Guest Social Media Authentication Service Template*



Service Templates - Guest Social Media Authentication

Name Prefix*: Social_Media_Auth

Description

For authenticating guest users who login via captive portal with their social media accounts. Guests must re-authenticate after their session ends. Network access can be restricted based on day of the week or bandwidth limit used by the guest user. 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.

Specify the **Guest Social Media Authentication** service template parameters as described in the following table:

Table 18: *Guest Social Media Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes. This populates the preconfigured 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 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 (Change of Authorization) on the network device.
RADIUS CoA Port	Specifies the default port **3799** if RADIUS CoA is enabled. **NOTE:** Change this value only if you defined a custom port on the network device.
Guest Access Restrictions	

Table 18: *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 days of the week that the guest users are allowed network access. By default, all seven days of the week are enabled.
Maximum bandwidth allowed per user	Specify the maximum amount of data in Megabytes a user is allowed per day. A value of **0** (zero) means no limit is set (the default).

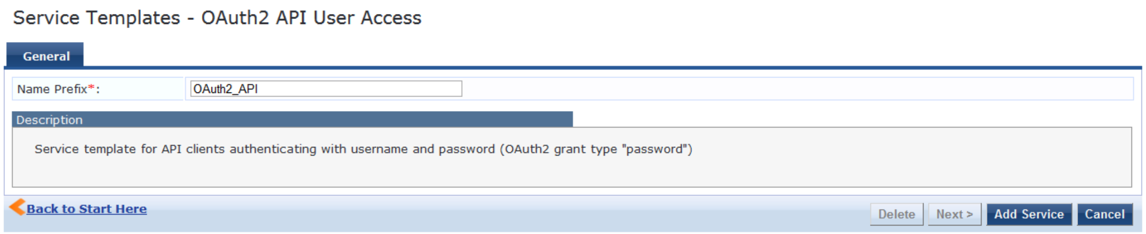
OAuth2 API User Access Service Template

This template is designed for configurations that supports ClearPass Policy Manager authenticating API clients with the 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 30: *OAuth2 API User Access Service Template*



Service Templates - OAuth2 API User Access

Name Prefix*: OAuth2_API

Description

Service template for API clients authenticating with username and password (OAuth2 grant type "password")

Specify the **OAuth2 API User Access** service template parameter as described in the following table:

Table 19: *OAuth2 API User Access Service Template Parameter*

Parameter	Description
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 Service Template

This service creates an Onboard Pre-Authentication service to check the user's credentials before starting the device provisioning process.

This service template also creates an authorization service that checks whether a user's device can be provisioned using Onboard.

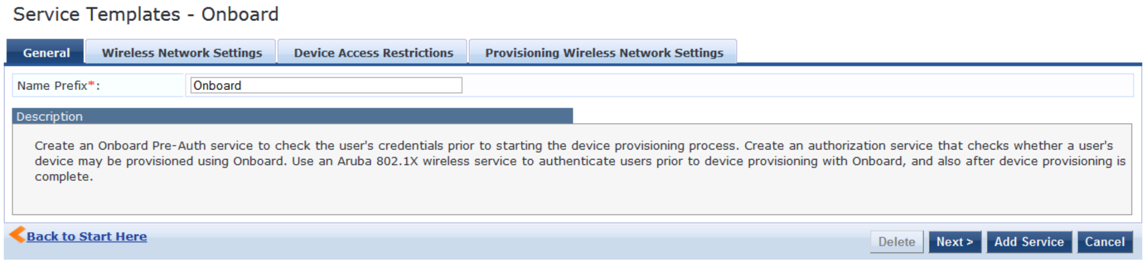
To authenticate users prior to device provisioning with Onboard, as well as after device provisioning is completed, use an **Aruba 802.1X Wireless** service .

NOTE

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

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

Figure 31: *Onboard Pre-Authorization Service Template*


Service Templates - Onboard
General
Wireless Network Settings
Device Access Restrictions
Provisioning Wireless Network Settings
Back to Start Here
Delete
Next >
Add Service
Cancel

Name Prefix*: Onboard

Description

Create an Onboard Pre-Auth service to check the user's credentials prior to starting the device provisioning process. Create an authorization service that checks whether a user's device may be provisioned using Onboard. Use an Aruba 802.1X wireless service to authenticate users prior to device provisioning with Onboard, and also after device provisioning is complete.

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

Table 20: *Onboard Authorization Service Template Parameters*

Parameter	Description
General	
Select Prefix	Select a prefix from the existing list of prefixes or enter the name of a new prefix. This populates the preconfigured 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	
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 (Change of Authorization) on the network device.
RADIUS CoA Port	Specifies the default port **3799** if RADIUS CoA is enabled. **NOTE:** Change this value only if you defined a custom port on the network device.
Device Access Restrictions	
Days allowed for access	Select the days of the week that guest users are allowed network access.

Table 20: *Onboard Authorization Service Template Parameters (Continued)*

Parameter	Description
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.

Configuring Policy Manager Services

You can configure the following types of services in ClearPass Policy Manager:

- Aruba 802.1X Wireless Service on page 71
- 802.1X Wireless—Identity Only Service on page 82
- 802.1X Wired Service on page 70
- 802.1X Wired—Identity Only Service on page 71
- Cisco Web Authentication Proxy Service on page 83
- MAC Authentication Service on page 83
- RADIUS Authorization Service on page 84
- RADIUS Enforcement (Generic) Service on page 85
- RADIUS Proxy Service on page 85
- Aruba Application Authentication Service on page 86
- Aruba Application Authorization Service on page 87
- ClearPass OnConnect Enforcement Service on page 87
- Event-Based Enforcement Service on page 89
- TACACS+ Enforcement Service on page 91
- Web-Based Authentication Service on page 92
- Web-based Health Check Only Service on page 96
- Web-Based Open Network Access Service on page 97

802.1X Wired Service

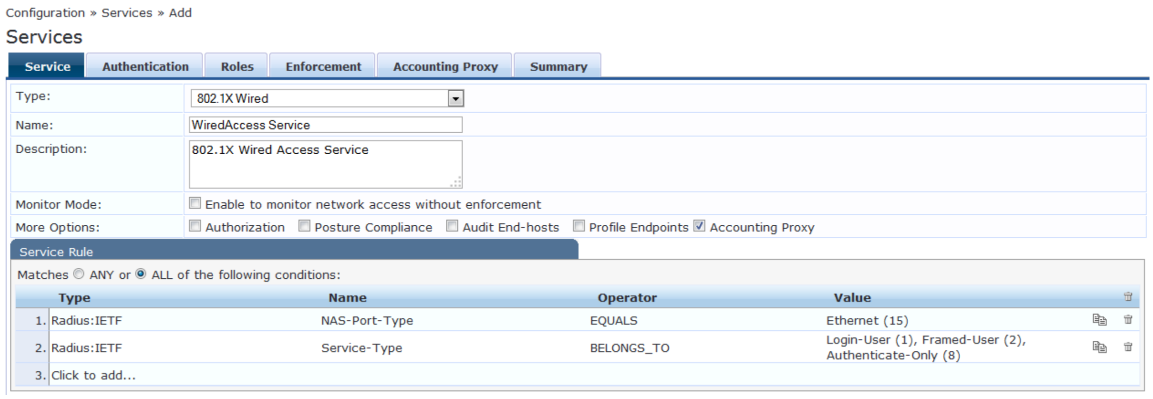
Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X.

Except for the NAS-Port-Type service rule value (which is **Ethernet** for an 802.1X Wired service and **Wireless 802.11** for an 802.1X Wireless service), configuration for the rest of the tabs is similar to the Aruba 802.1X Wireless service.

For more information, see Aruba 802.1X Wireless Service on page 71.

The following figure displays the **Add 802.1X Wired Service** page:

Figure 32: *Add 802.1X Wired Service Dialog*



Configuration » Services » Add

Services

Type: 802.1X Wired

Name: WiredAccess Service

Description: 802.1X Wired Access Service

Monitor Mode: □ Enable to monitor network access without enforcement

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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

802.1X Wired—Identity Only Service

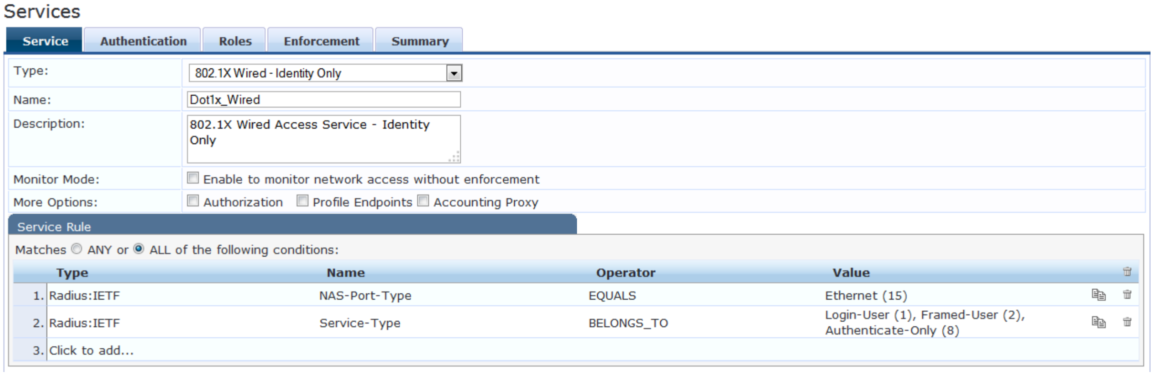
Configure this service for clients connecting through an Ethernet LAN with authentication using IEEE 802.1X.

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 Service on page 70.

The following figure displays the **802.1X Wired—Identity Only Service** dialog:

Figure 33: *802.1X Wired—Identity Only Service*



Services

Type: 802.1X Wired - Identity Only

Name: Dot1x_Wired

Description: 802.1X Wired Access Service - Identity Only

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: □ Authorization □ Profile Endpoints □ Accounting Proxy

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

Aruba 802.1X Wireless Service

This section provides the following information:

- Service Configuration on page 72
- Authentication Configuration on page 74
- Roles Configuration on page 77
- Enforcement Configuration on page 78
- Summary Information on page 82

You can configure the following additional Aruba 802.1X Wireless Service parameters by checking the appropriate **More Options** check box:

- Authorization Configuration on page 75
- Posture Configuration on page 77
- Audit Configuration on page 79
- Profile Endpoints Configuration on page 80

- Accounting Proxy Configuration on page 81

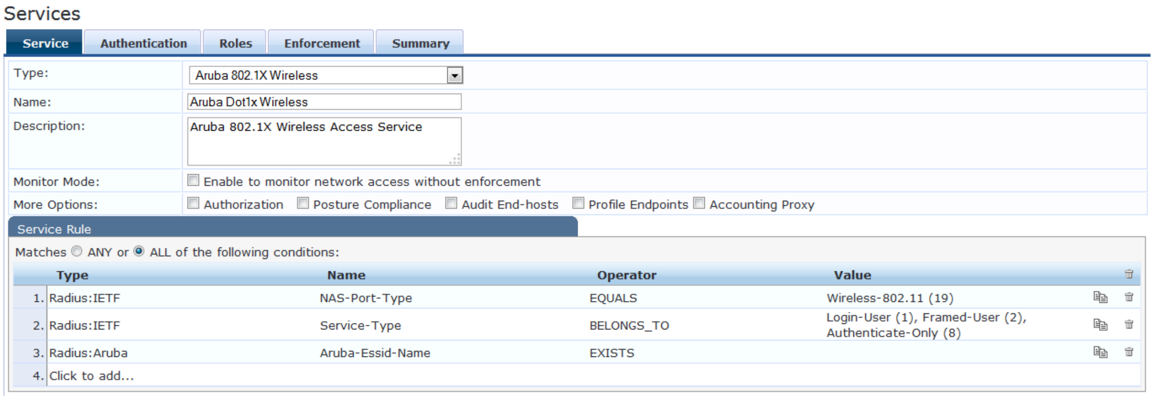
Configure this service for wireless hosts that are connecting through an Aruba 802.1X wireless access device or controller using IEEE 802.1X authentication.

Service rules are customized for a typical Aruba WLAN Controller deployment.

The Aruba 802.1X service includes a rule that specifies that an Aruba ESSID exists.

The following figure displays the **Add Aruba 802.1X Wireless Service** dialog:

Figure 34: *Add Aruba 802.1X Wireless Service Dialog*



Services

Type: Aruba 802.1X Wireless

Name: Aruba Dot1x Wireless

Description: Aruba 802.1X Wireless Access Service

Monitor Mode: □ Enable to monitor network access without enforcement

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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

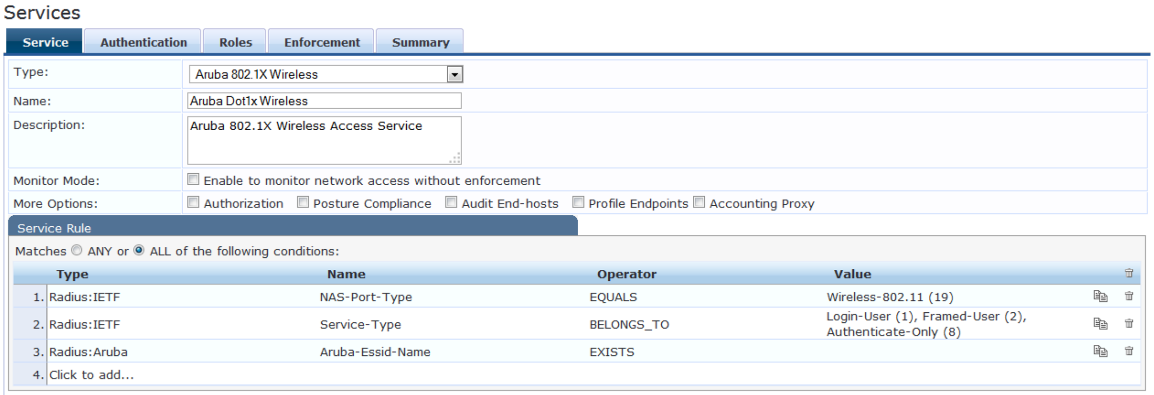
Service Configuration

The **Service** tab provides basic configuration parameters for 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 predefined.

You can click on a service rule to modify any of its options.

Figure 35: *Add Aruba 802.1X Wireless Service > Service Dialog*



Services

Type: Aruba 802.1X Wireless

Name: Aruba Dot1x Wireless

Description: Aruba 802.1X Wireless Access Service

Monitor Mode: □ Enable to monitor network access without enforcement

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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

1. Specify the **Service** tab parameters as described in the following table:

Table 21: *Add Aruba 802.1X Wireless Service > Service Tab Parameters*

Parameter	Action/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 monitor network access activity without enforcement.
More Options	Check these boxes to access the additional configuration tabs: ● Authorization ● Posture Compliance ● Audit End-hosts ● Profile Endpoints ● Accounting Proxy
Service Rule	
Type	Select the service rule type.
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. The value 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 predefined.

2. Click a service rule to modify its options.

NOTE

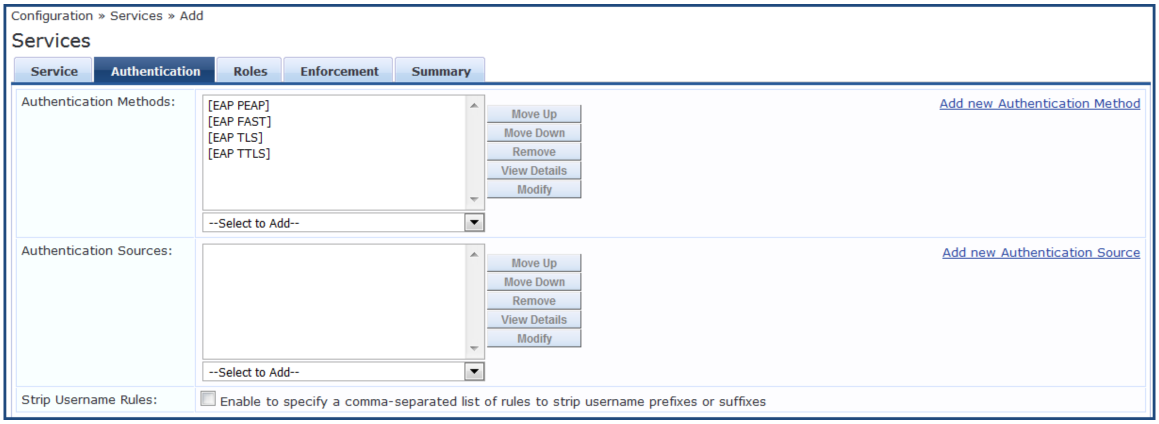
If you want to administer the same set of policies for wired and wireless access, you can combine the service rule to define one single service. The other option is to keep two services for wired and wireless access, but reuse the policy components (authentication methods, authentication source, authorization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

Authentication Configuration

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

The following figure displays the **Authentication** dialog:

Figure 36: *Add Aruba 802.1X Wireless Service > Authentication Dialog*



Configuration » Services » Add

Services

Authentication Methods: [EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS]

--Select to Add--

Authentication Sources:

--Select to Add--

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

1. Specify the **Authentication** tab parameters as described in the following table:

Table 22: *Add Aruba 802.1X Wireless Service > Authentication Parameters*

Parameter	Action/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 • EAP MSCHAPV2 The **EAP-MD5** authentication type is not supported if you use ClearPass Policy Manager in **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 Configuring Authentication Methods on page 165 • Adding and Configuring Authentication Sources on page 190.
Authentication Sources	Specify the authentication sources using the **Select to Add** field. This can be one or more instances of the following list of authentication sources: • avenda313 [Active Directory] • Admin User Repository • Blacklist User Repository • Endpoints Repository • Guest Device Repository • Guest User Repository • Insight Repository • Local User Repository • Onboard Devices Repository • Social Login Repository • Time Source **NOTE:** When you attempt to specify more than 23 Services authentication sources, the following error message is displayed: **No. of Authentication Sources cannot exceed 23**.
Strip Username Rules	Select the check box to preprocess the user name (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.

Authorization Configuration

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 **More Options** > **Authorization** check box.

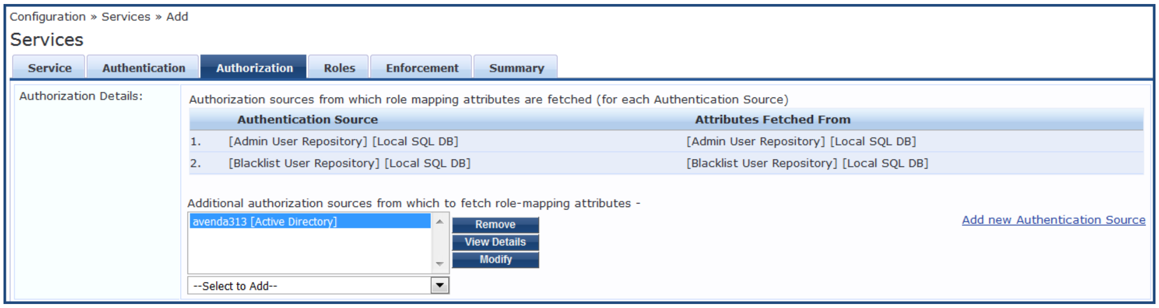
ClearPass fetches role-mapping attributes from the authorization sources associated with the service, regardless of which authentication source was used to authenticate the user.

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** dialog:

Figure 37: *Add Aruba 802.1X Wireless Service > Authorization Dialog*



Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

	Authentication Source	Attributes Fetched From
1.	[Admin User Repository] [Local SQL DB]	[Admin User Repository] [Local SQL DB]
2.	[Blacklist User Repository] [Local SQL DB]	[Blacklist User Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

avenda313 [Active Directory]

--Select to Add--

2. Specify the **Authorization** parameters as described in the following table:

Table 23: *Add Aruba 802.1X Wireless Service > Authorization Parameters*

Parameter	Action/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	Specify the authorization sources using the **Select to Add** field. This can be one or more instances of the following list of authorization sources: ● Admin User Repository ● avenda313 [Active Directory] ● Blacklist User Repository ● Endpoints Repository ● Guest Device Repository ● Guest User Repository ● Insight Repository ● Local User Repository ● Onboard Devices Repository ● Social Login Repository ● Time Source **NOTE:** When you attempt to specify more than 23 Services authorization sources, the following error message is displayed: **No. of Authorization Sources cannot exceed 23**.

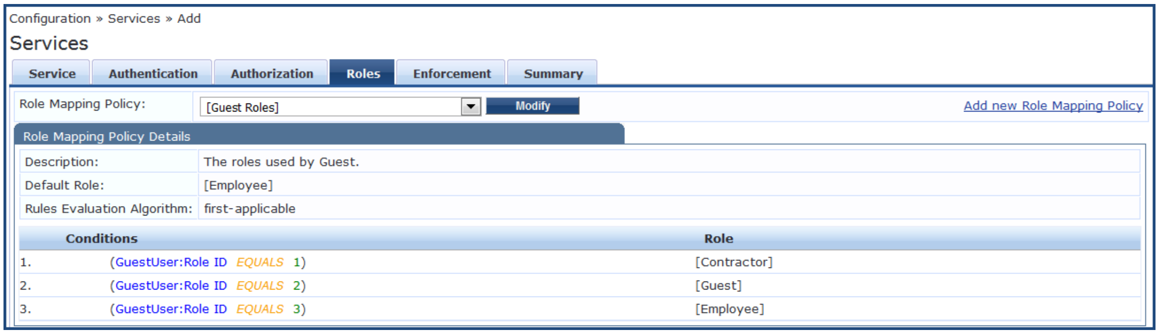
For more information on configuring authorization sources, see Adding and Configuring Authentication Methods on page 165.

Roles Configuration

Use the **Roles** tab to associate a role-mapping policy with this service.

The following figure displays the **Aruba 802.1X Wireless Service** > **Roles** dialog:

Figure 38: *Add Aruba 802.1X Wireless Service > Roles Dialog*


Configuration » Services » Add
Services
Service
Authentication
Authorization
Roles
Enforcement
Summary
Modify
Add new Role Mapping Policy
Role Mapping Policy Details

Role Mapping Policy: [Guest Roles]

Description:	The roles used by Guest.
Default Role:	[Employee]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(GuestUser:Role ID EQUALS 1)	[Contractor]
2.	(GuestUser:Role ID EQUALS 2)	[Guest]
3.	(GuestUser:Role ID EQUALS 3)	[Employee]

1. Specify the **Roles** parameters as described in the following table:

Table 24: *Add Aruba 802.1X Wireless Service > Roles Tab Parameters*

Parameter	Action/Description
Role Mapping Policy	Select a role mapping policy from the drop-down list. Policy Manager ships a number of preconfigured roles. **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	Provide additional information about the selected role-mapping policy.
Default Role	Specify the role to which Policy Manager defaults when the role-mapping policy does not produce a match.
Rules Evaluation Algorithm	Shows the first matched rule.

For information on configuring role-mapping policies, see Configuring a Role and Role-Mapping Policy on page 255.

Posture Configuration

The **Posture** tab is not enabled by default. To enable posture checking for this service:

1. Select the **More Options** > **Posture Compliance** check box.

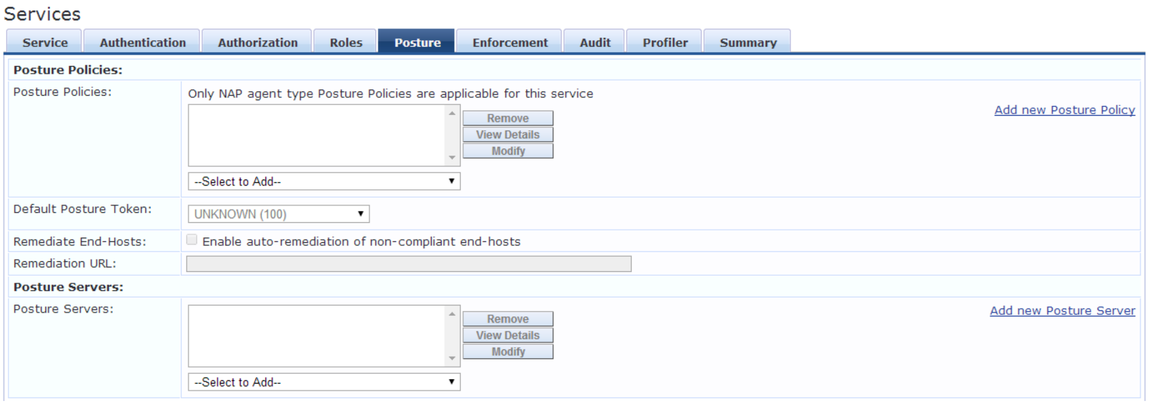
   You can enable the posture checking for this kind of service, if you deploy any of the following:

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

The **Posture** tab cannot be enabled when **High Capacity Guest** mode is enabled in the ClearPass cluster.

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

Figure 39: *Add Aruba 802.1X Wireless Service > Posture Dialog*



Posture Policies:

Posture Policies: Only NAP agent type Posture Policies are applicable for this service

--Select to Add--

Default Posture Token: UNKNOWN (100)

Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts

Remediation URL:

Posture Servers:

Posture Servers: --Select to Add--

2. Specify the Wireless Service **Posture** parameters as described in Table 25:

Table 25: *Add Aruba 802.1X Wireless Service > Posture Parameters*

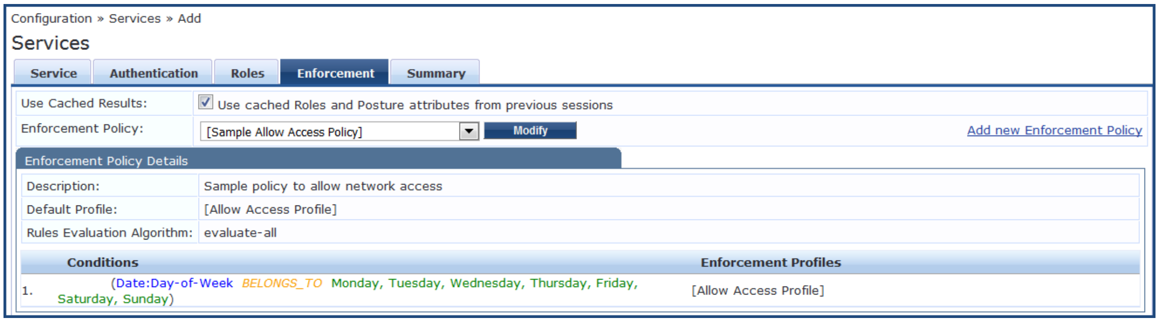
Parameter	Action/Description
Posture Policies	
Posture Policies	Select the posture policy from the **Select to Add** drop-down list. If you do not have any preconfigured posture policies, click **Add New Posture Policy** to create a new posture policy. **NOTE:** Only NAP agent-type posture policies are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

For more information on configuring posture polices, see Configuring Posture Policy Agents and Hosts on page 269.

Enforcement Configuration

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

Figure 40: *Aruba 802.1X Wireless Service > Enforcement Dialog*


Configuration » Services » Add
Services
Service
Authentication
Roles
Enforcement
Summary
Modify
Add new Enforcement Policy
Enforcement Policy Details

Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: [Sample Allow Access Policy]

Description: Sample policy to allow network access

Default Profile: [Allow Access Profile]

Rules Evaluation Algorithm: evaluate-all

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

1. Specify the **Enforcement** parameters as described in the following table:

Table 26: *Aruba 802.1X Wireless Service > Enforcement Parameters*

Parameter	Action/Description
Use Cached Results	Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	Select the preconfigured enforcement policy from the drop-down list. This is mandatory. If you do not have any preconfigured 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 ClearPass Policy Manager.
Rules Evaluation Algorithm	Shows the first matched rule.

For more information, see Configuring Enforcement Policies on page 355.

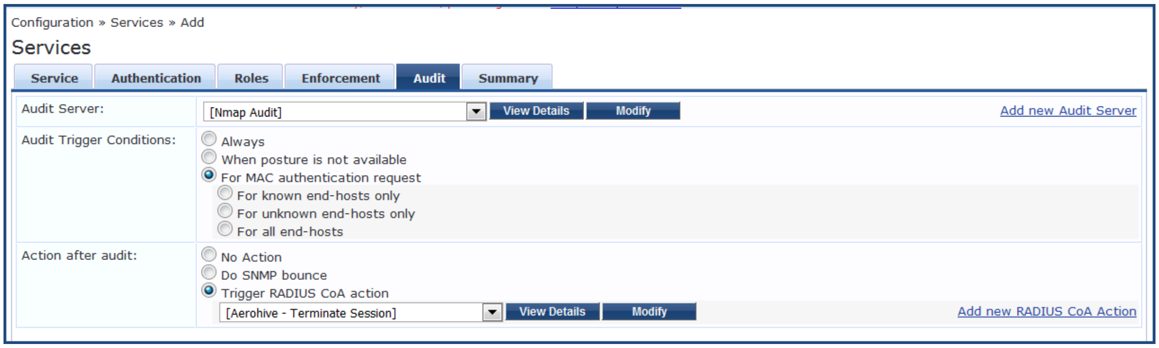
Audit Configuration

Use the **Audit** tab to enable the Audit checking for this service.

1. To enable the **Audit** tab, select the **Audit End-hosts** check box from the **More Options** field on the **Service** tab.

   The **Audit** dialog opens.

Figure 41: *Add Aruba 8021X Wireless Service > Audit Dialog*



Audit Server: [Nmap Audit]

Audit Trigger Conditions:
○ Always
○ When posture is not available
● For MAC authentication request
○ For known end-hosts only
○ For unknown end-hosts only
○ For all end-hosts

Action after audit:
○ No Action
○ Do SNMP bounce
● Trigger RADIUS CoA action
[Aerohive - Terminate Session]

2. Specify the **Audit End-Hosts** parameters as described in the following table:

Table 27: *Add Aruba 802.1X Wireless Service > Audit End-Hosts Parameters*

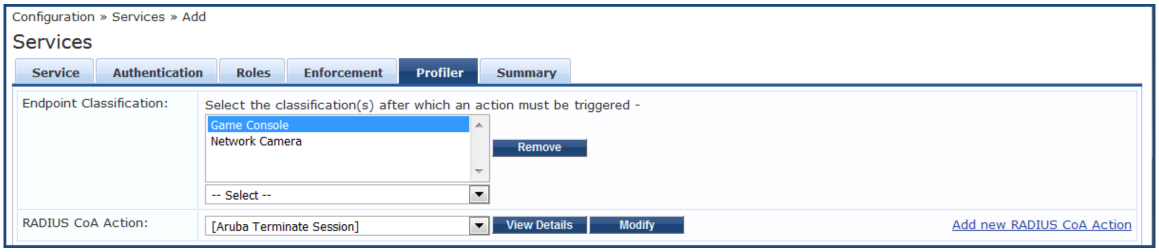
Parameter	Action/Description
Audit Server	Select the audit server from the following options: - **Nessus Server**: Interfaces with Policy Manager primarily to perform vulnerability scanning. - **Nmap Audit**: Performs specific Nmap audit functions. ■ To view the **Policy Manager Entity Details** dialog with the summary of audit server details, click the **View Details** button. ■ To view the **Summary** tab with audit server details, click the **Modify** button.
Audit Trigger Conditions	Select an audit trigger condition: - **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, Policy Manager presents the following three additional settings: ■ **For known end-hosts only:** 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:** Select this option when the 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	Specify 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 reapplies 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 reauthentication (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 ClearPass. - **Trigger RADIUS CoA action**: This option sends a RADIUS CoA command from ClearPass to the network device.

Profile Endpoints Configuration

The **Profiler** tab is not displayed by default. To access this tab, select the **More Options** > **Profile Endpoints** check box.

The **Add Profile Endpoints** dialog opens:

Figure 42: *Add Aruba 802.1X Wireless Service > Profile Endpoints Dialog*



Configuration » Services » Add

Services

Endpoint Classification: Select the classification(s) after which an action must be triggered -

Game Console
Network Camera

RADIUS CoA Action: [Aruba Terminate Session]

1. Specify the **Profile Endpoints** parameters as described in the following table:

Table 28: *Add Aruba 802.1X Wireless Service > Profile Endpoints Parameters*

Parameter	Action/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. ● To view the **Policy Manager Entity Details** page with the summary of enforcement profile details, click the **View Details** button. ● To view the **Summary** tab with profile details, click the **Modify** button. ● To create a new RADIUS CoA action, click the **Add New RADIUS CoA Action** link.

Accounting Proxy Configuration

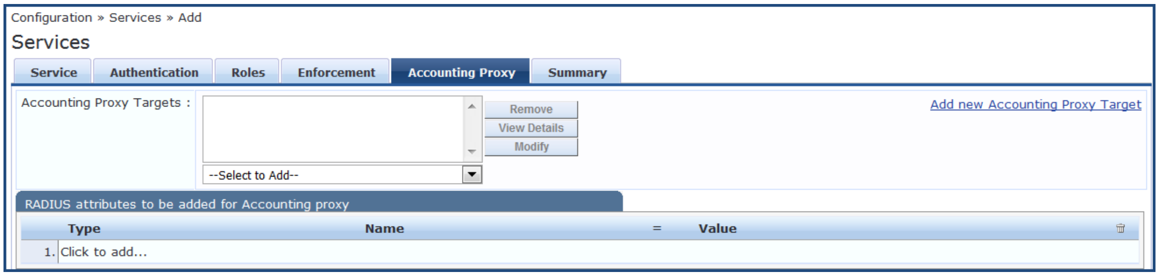
Use the **Accounting Proxy** tab to broadcast the RADIUS accounting packets to all the proxy targets.

You can configure the proxy targets to which RADIUS server should be forwarded and the attributes to be added in the accounting. This enables the external security solutions to use the RADIUS account event to detect when a user connects and disconnects to the server.

1. To enable the **Accounting Proxy** tab, select the **More Options** > **Accounting Proxy** check box.

   The following figure displays the **Add Accounting Proxy** dialog:

Figure 43: *Add 802.1X Wireless > Accounting Proxy Dialog*



Configuration » Services » Add

Services

Accounting Proxy Targets :

RADIUS attributes to be added for Accounting proxy

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

2. Specify the **Accounting Proxy** parameters as described in the following table:

Table 29: *Add Aruba 802.1X Wireless Service > Accounting Proxy Tab Parameters*

Parameter	Action/Description
Accounting Proxy Targets	Specify the proxy targets to which the RADIUS server should be forwarded and the 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	
Type	Select the RADIUS attribute type from the drop-down list: ● Radius:IETF ● Radius:Cisco ● Radius:Hewlett-Packard-Enterprise ● Radius:Alcatel-Lucent-Enterprise ● Radius:Microsof ● Radius:Avenda ● Radius:Aruba
Name	Select the name of the RADIUS attribute from the drop-down list.
Value	Select the value from the **Value** drop-down list. The values displayed here depend on the RADIUS attribute **Type** selected.

Summary Information

The **Summary** page presents the summary of parameters defined when you created a new service.

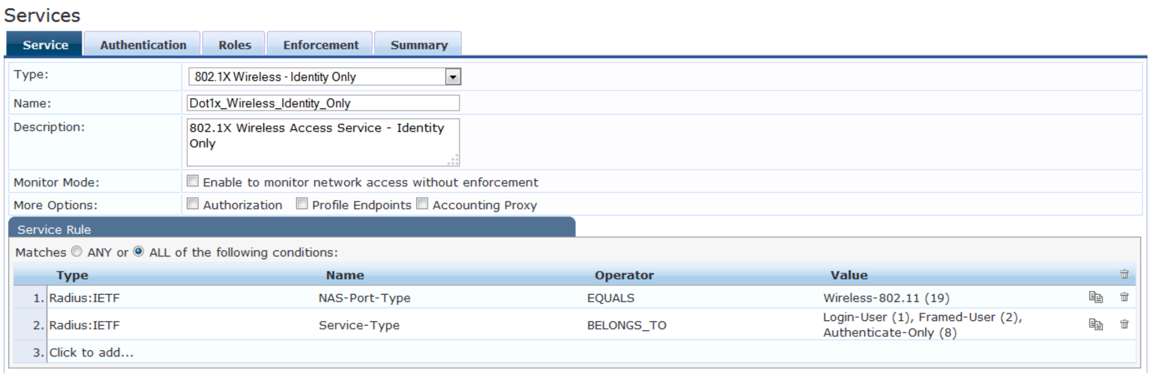
802.1X Wireless—Identity Only Service

Configuration for this type of service is the same as the **Aruba 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 Service on page 1.

The following figure displays the **Configuration** > **Services** > **Add 802.1X Wireless—Identity Only Service** dialog:

Figure 44: *802.1X Wireless—Identity Only Service Dialog*



Type:	802.1X Wireless - Identity Only
Name:	Dot1x_Wireless_Identity_Only
Description:	802.1X Wireless Access Service - Identity Only
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

Cisco Web Authentication Proxy Service

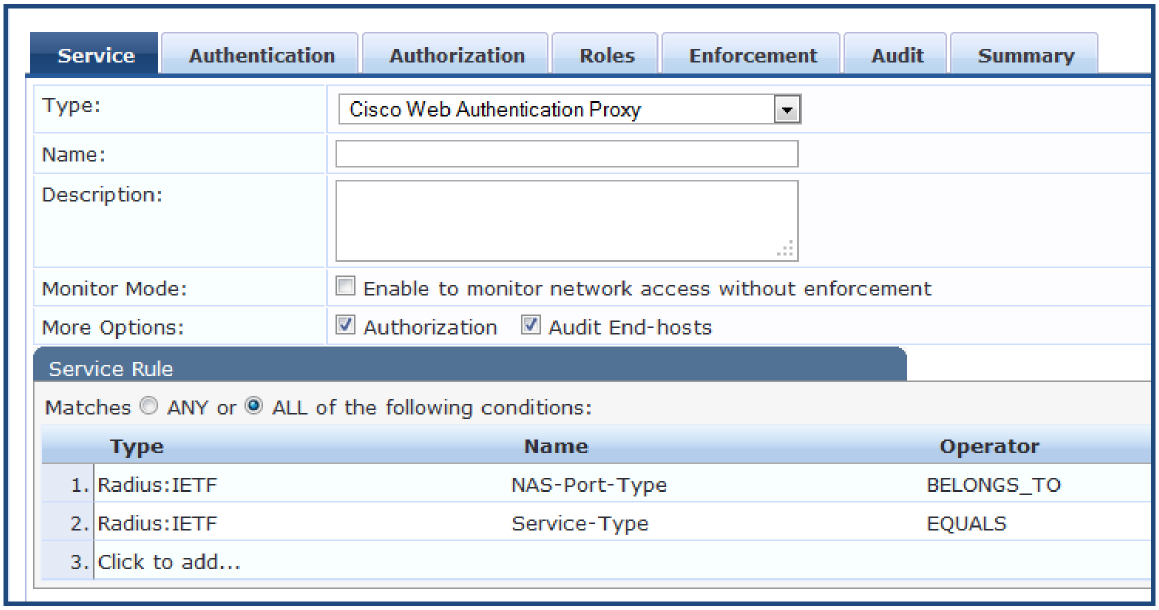
This service is a web-based authentication service for guests or agent-less hosts.

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 45: *Cisco Web Authentication Proxy Service*



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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

Configuring the **Cisco Web Authentication Proxy** service is similar to configuring the **Aruba 802.1X Wireless** service except that the Posture Compliance and Profile Endpoints options are not available. For more information on configuration, see Aruba 802.1X Wireless Service on page 71.

MAC Authentication Service

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

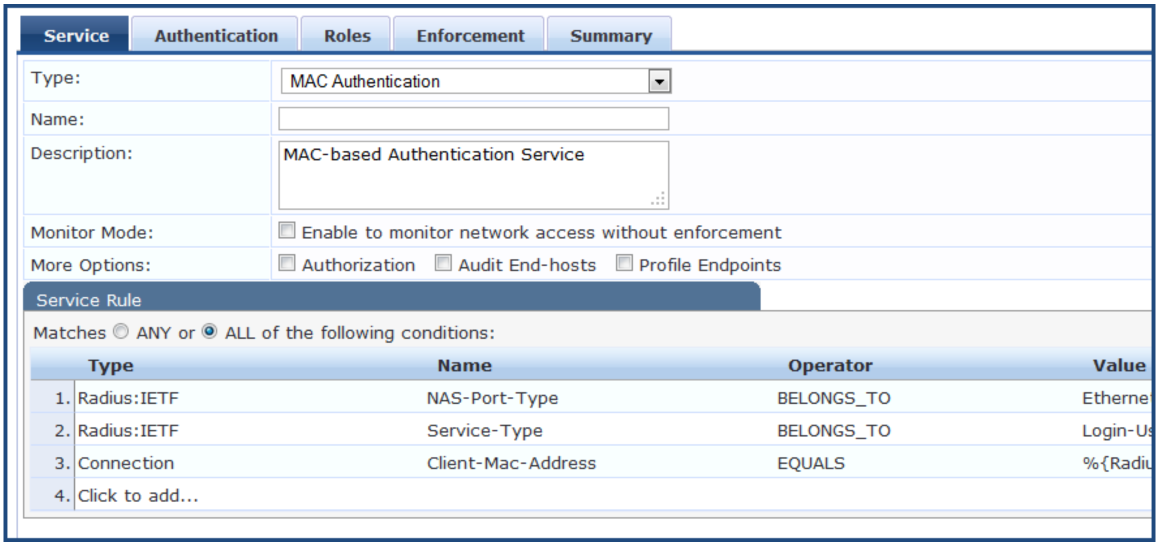
The network access device sends a MAC authentication request to Policy Manager. Policy Manager can look up the client in a white list or a black list, authenticate, and authorize the client against an external authentication or authorization source, and optionally perform an audit on the client.

NOTE

You cannot configure posture for this type of service.

The following figure displays the **MAC Authentication** service configuration dialog.

Figure 46: *MAC Authentication Service Configuration Dialog*



Type: MAC Authentication

Name:

Description: MAC-based Authentication Service

Monitor Mode: □ Enable to monitor network access without enforcement

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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

The **Posture** tab is not available for the MAC-based authentication service.

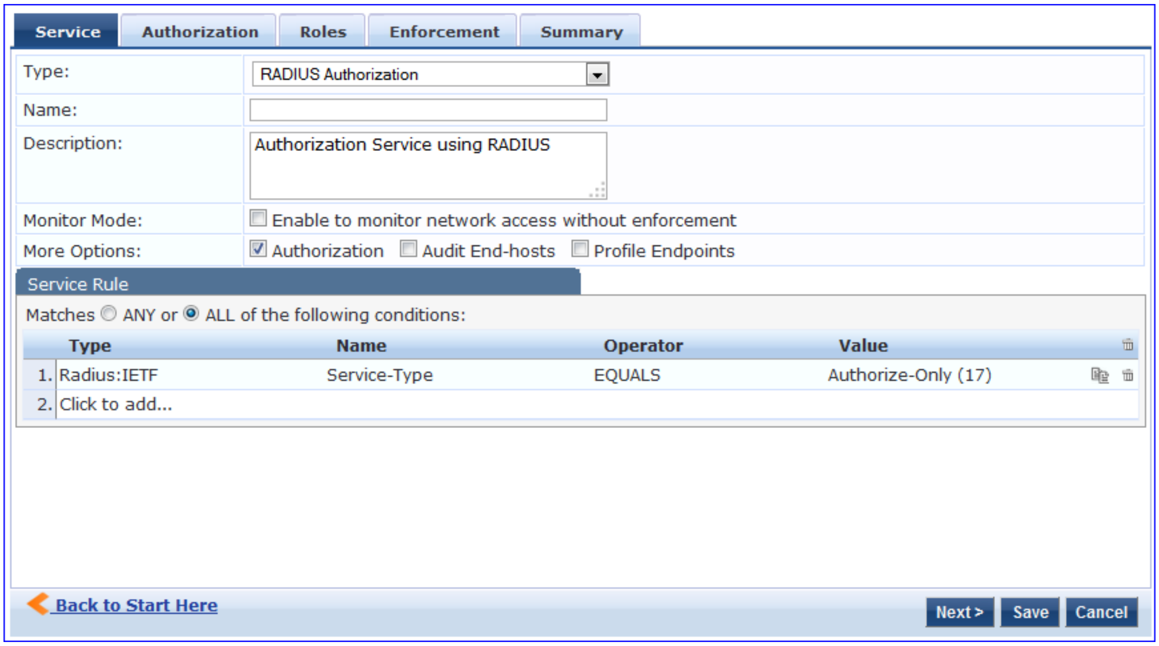
Configuration for the rest of the tabs is similar to the **Aruba 802.1X Wireless** service configuration. For details on this service's configuration, see Aruba 802.1X Wireless Service on page 71.

RADIUS Authorization Service

Configure the **RADIUS Authorization** service type for services that perform authorization using RADIUS.

When you select this service, the **Authorization** tab is enabled. The following figure displays the **RADIUS Authorization** service configuration dialog:

Figure 47: *RADIUS Authorization Service Configuration Dialog*



Type: RADIUS Authorization

Name:

Description: Authorization Service using RADIUS

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: ☑ Authorization □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

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) Service on page 85 for more information.

RADIUS Enforcement (Generic) Service

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

NOTE

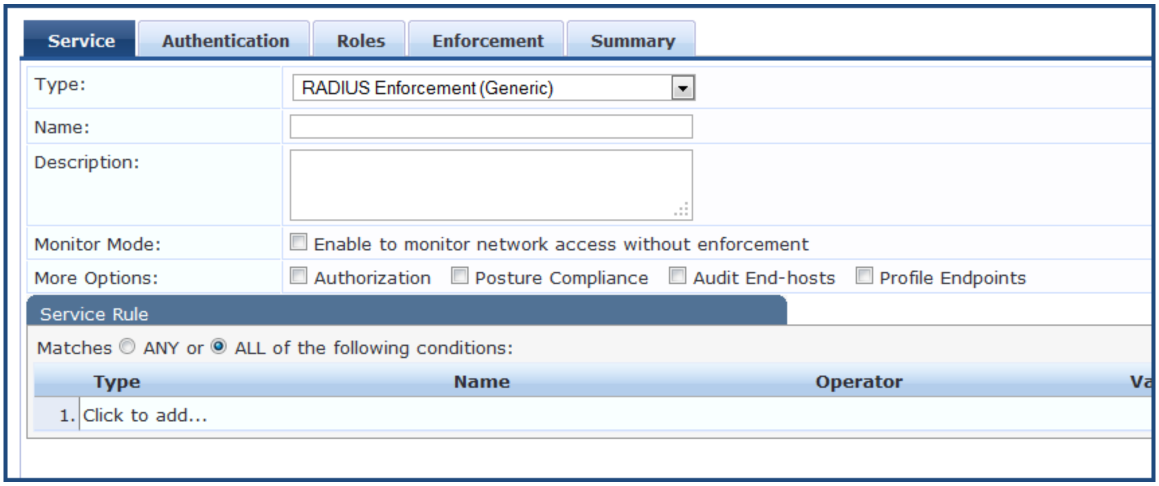
The **AirGroup Authorization Service** service is the only **RADIUS Enforcement (Generic)** service that is available by default.

In addition to the default configuration tabs (**Service**, **Authentication**, **Roles**, and **Enforcement**), from **More Options** you can also enable the **Authorization**, **Posture Compliance**, **Audit End Hosts**, and **Profile Endpoints** tabs.

There are no default rules associated with this service type. You can add Rules to handle any type of standard or vendor-specific RADIUS attributes (that is, any attribute that is loaded through the prepackaged vendor-specific or standard RADIUS dictionaries, or through other dictionaries imported into Policy Manager).

The following figure displays the **RADIUS Enforcement (Generic)** service configuration dialog:

Figure 48: *RADIUS Enforcement (Generic) Service Configuration Dialog*



Type:	RADIUS Enforcement (Generic)
Name:	
Description:	
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

Configuring a service for RADIUS requests is similar to configuring the **Aruba 802.1X Wireless** service. For details, see Aruba 802.1X Wireless Service on page 71.

RADIUS Proxy Service

Configure the **RADIUS Proxy** service for any kind of RADIUS request that needs to be proxied to another RADIUS server (that is, a proxy target).

There are no default rules associated with this service type. You can add rules to handle any type of standard or vendor-specific RADIUS attributes. Typically, proxying is based on the realm or the domain of the user who is 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.

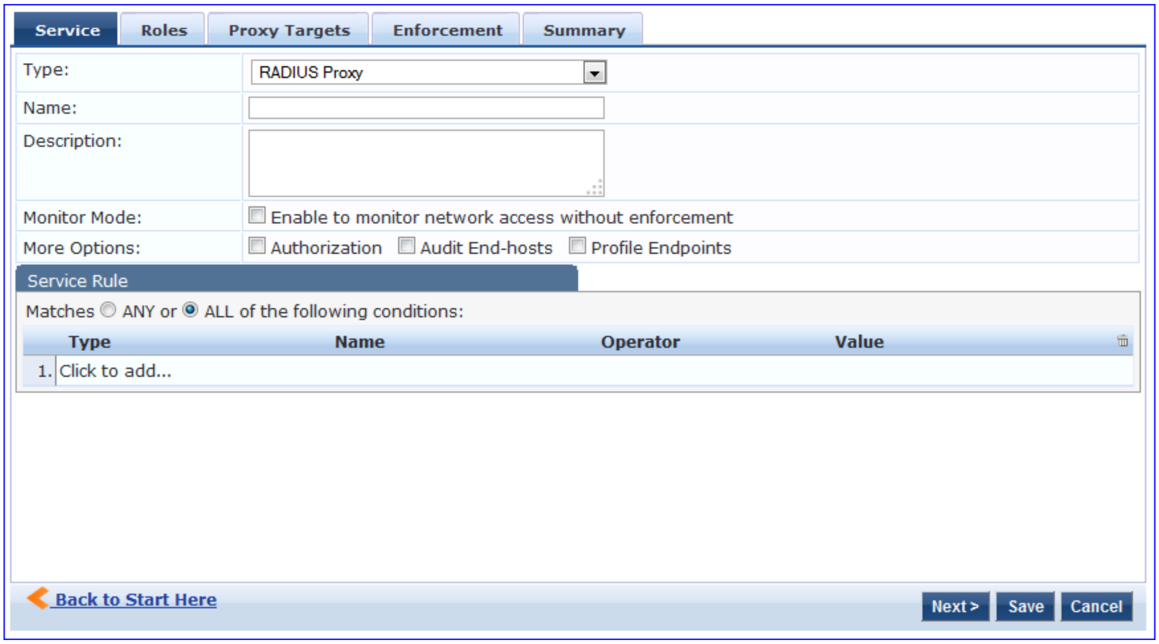
However, you need to configure proxy targets (the servers to which requests are proxied). Requests can be dispatched to the proxy targets randomly, and are load balanced.

However, in **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 configuration dialog:

Figure 49: *RADIUS Proxy Service Configuration Dialog*



Type: RADIUS Proxy

Name:

Description:

Monitor Mode: □ Enable to monitor network access without enforcement

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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

For configuration details, see RADIUS Enforcement (Generic) Service on page 85.

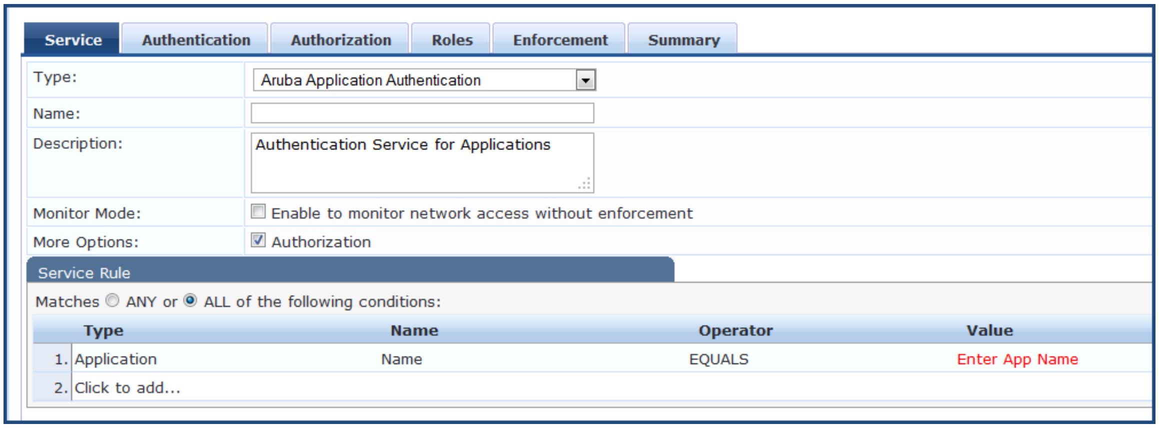
Aruba Application Authentication Service

This type of service provides authentication and authorization to users of ClearPass Guest and ClearPass Insight.

You can send Generic Application Enforcement Profile on page 388 to these or other generic applications for authenticating and authorizing the users.

The following figure displays the **Aruba Application Authentication** service configuration dialog:

Figure 50: *Aruba Application Authentication Configuration Dialog*



Type: Aruba Application Authentication

Name:

Description: Authentication Service for Applications

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: ☑ Authorization

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

Configuring the **Aruba Application Authentication** service is similar to configuring the **Aruba 802.1X Wireless** service except that the *Posture Compliance*, *Audit End-hosts*, and *Profile Endpoints* options are not available.

For configuration details, see Aruba 802.1X Wireless Service on page 71.

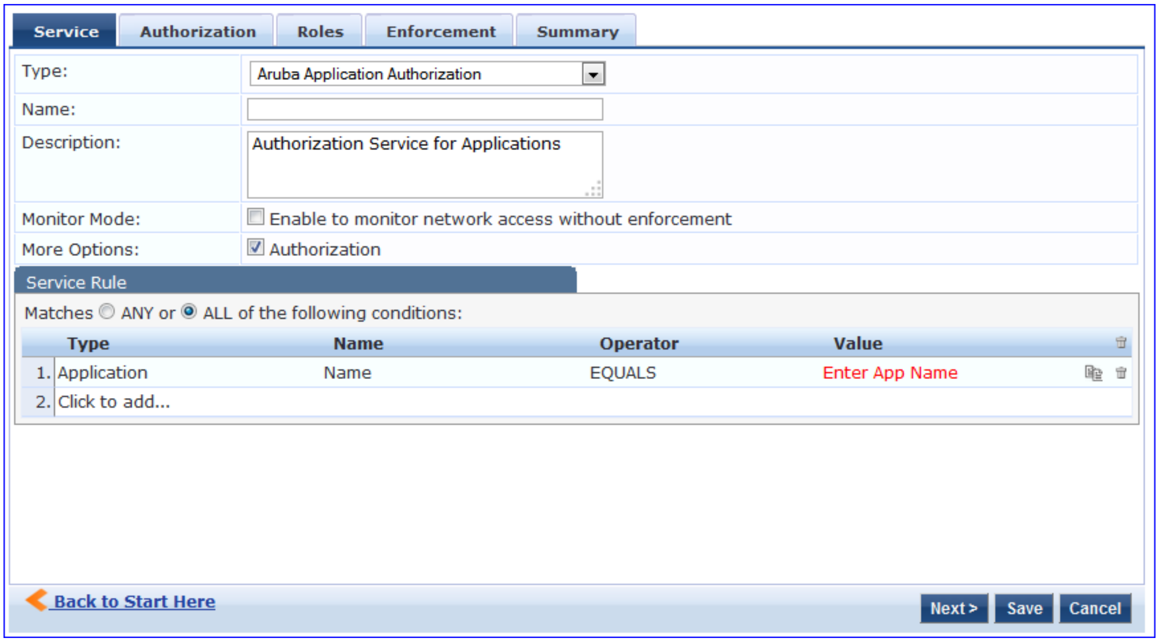
Aruba Application Authorization Service

This type of service provides authorization for users of Aruba applications: ClearPass Guest and ClearPass Insight.

You can send Generic Application Enforcement Profile on page 388 to these or other generic applications for authorizing the users.

The following figure displays the **Aruba Application Authorization** service configuration dialog:

Figure 51: *Aruba Application Authorization Configuration Dialog*



Type:	Aruba Application Authorization
Name:	
Description:	Authorization Service for Applications
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	☑ Authorization

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

Configuring the Aruba Application Authorization service is similar to configuring the Aruba 802.1X Wireless service except that the *Posture Compliance*, *Audit End-hosts*, and *Profile Endpoints* options are not available.

For configuration details, see Aruba 802.1X Wireless Service on page 71.

ClearPass OnConnect Enforcement Service

This section provides the following information:

- Adding a ClearPass OnConnect Enforcement Service
- Associating the ClearPass OnConnect Service with an Enforcement Policy

ClearPass OnConnect Enforcement is an enforcement model that allows you to use non-802.1X methods for device scans, VLAN placement, and so on. ClearPass OnConnect Enforcement allows enforcement in non-802.1X environments without the need for an agent, such as OnGuard, on the endpoint.

For related information, see:

- Enabling ClearPass OnConnect Enforcement on a Network Device on page 454
- OnConnect Setting on page 483

When ClearPass OnConnect Enforcement is enabled, ClearPass performs the following actions:

- Detects when a new endpoint connects to the network.
- Scans the endpoint to identify the logged-in user and other device-specific information.
- Triggers a Web-based authentication (WebAuth) for the device.
- Performs SNMP-based enforcement to change the network access profile for the device.

Adding a ClearPass OnConnect Enforcement Service

To add an OnConnect Enforcement service:

1. Navigate to **Configuration** > **Services**.

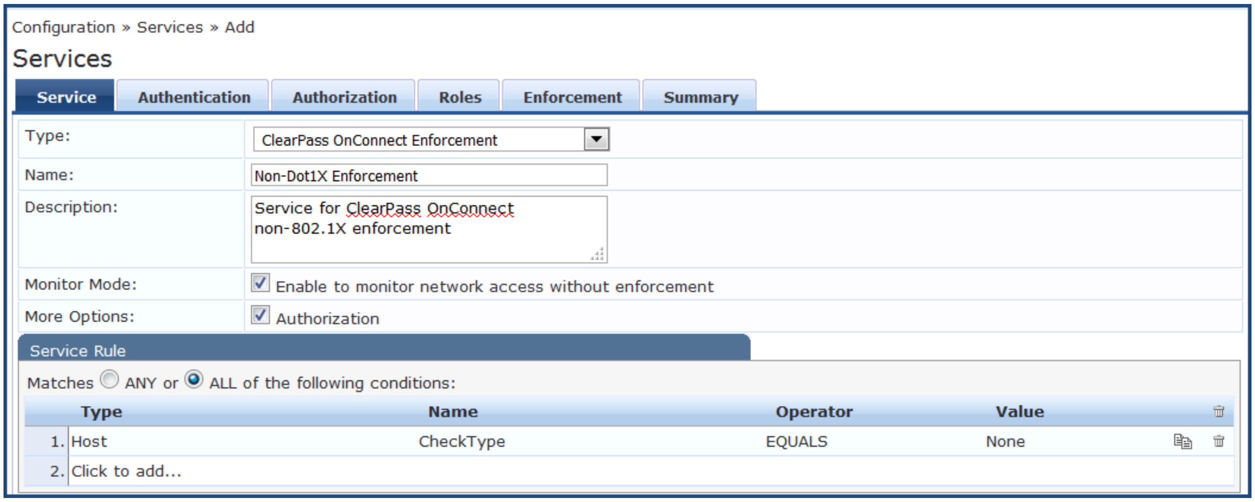
   The **Services** page opens.

2. To add the service, click **Add**.

   The **Add Services** dialog opens.

3. From the **Type** drop-down list, select **ClearPass OnConnect Enforcement** (see Figure 52).

Figure 52: *Specifying ClearPass OnConnect Enforcement*



Type:	ClearPass OnConnect Enforcement
Name:	Non-Dot1X Enforcement
Description:	Service for ClearPass OnConnect non-802.1X enforcement
Monitor Mode:	☑ Enable to monitor network access without enforcement
More Options:	☑ Authorization

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

4. Enter the name or label of the OnConnect Enforcement service.

5. Enter the values for any other parameters, including service rules, required for this service.

   For a description of all the parameters in the **Service** page, see Adding Services on page 1.

Associating the ClearPass OnConnect Service with an Enforcement Policy

After you create the ClearPass OnConnect Enforcement service, you must associate the service with an enforcement policy.

WMI (Windows Management Instrumentation) configuration is used to retrieve the Loggedin User information.

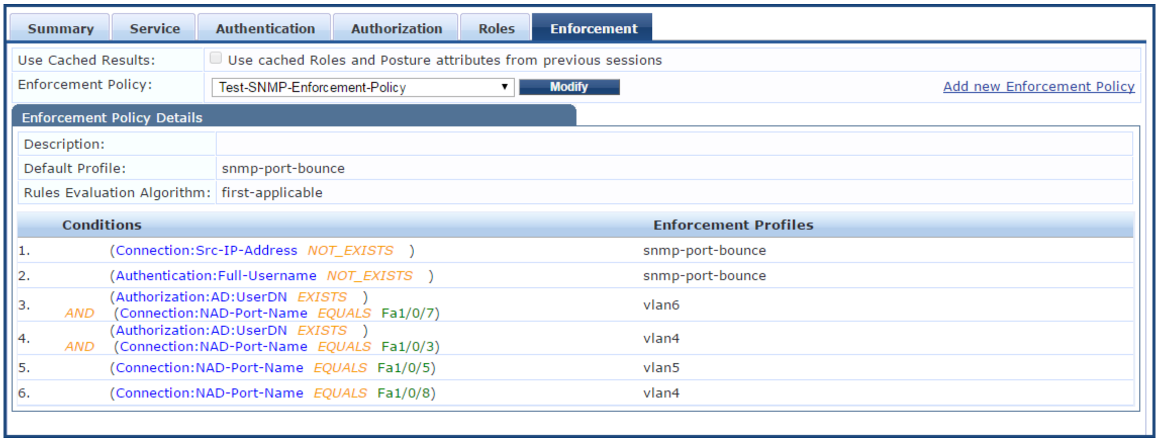
Whenever a domain-joined Windows client connects to an OnConnect-enabled port with the domain user logged in, Authorization attributes for this user are fetched from authorization sources to determine the role of the user; this information is then used in configuring Policy Enforcement. For details on configuring WMI credentials, see WMI Credentials Configuration on page 139.

To associate a ClearPass OnConnect Enforcement service with an enforcement policy:

1. When finished with the parameter settings on the **Add Services** > **Service** page, click **Next**.

   The **Services** > **Enforcement** page appears.

Figure 53: *Selecting the ClearPass OnConnect Enforcement Policy*



Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Test-SNMP-Enforcement-Policy

Enforcement Policy Details

Description:	
Default Profile:	snmp-port-bounce
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Connection:Src-IP-Address NOT_EXISTS)	snmp-port-bounce
2.	(Authentication:Full-Username NOT_EXISTS)	snmp-port-bounce
3.	(Authorization:AD:UserDN EXISTS) AND (Connection:NAD-Port-Name EQUALS Fa1/0/7)	vlan6
4.	(Authorization:AD:UserDN EXISTS) AND (Connection:NAD-Port-Name EQUALS Fa1/0/3)	vlan4
5.	(Connection:NAD-Port-Name EQUALS Fa1/0/5)	vlan5
6.	(Connection:NAD-Port-Name EQUALS Fa1/0/8)	vlan4

From the **Services** > **Add** > **Enforcement** page, you can either select an existing enforcement policy or create a new one.

2. From the **Enforcement Policy** drop-down list, select the appropriate OnConnect Enforcement policy.
   a. If you have not configured an OnConnect-type Enforcement policy, click **Add New Enforcement Policy** to create a new enforcement policy.
3. Specify the values for the remaining parameters as described in Table 30, then click **Save**.

Table 30: *Service Enforcement Page Parameters*

Parameter	Description
Use Cached Results	1. Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	2. From the drop-down list, select the preconfigured enforcement policy. This is a mandatory step.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

Event-Based Enforcement Service

The **Event-Based Enforcement** service manages enforcement actions in response to threat-event processing.

When there is a suspicious user, this user could represent a common DOS attack or some other threat. When a threat is detected, ClearPass performs enforcement operations as configured; for example, executing a change of authorization (COA) to disconnect a suspicious user from the network.

To add an event-based enforcement service:

1. Navigate to **Configuration** > **Services**.

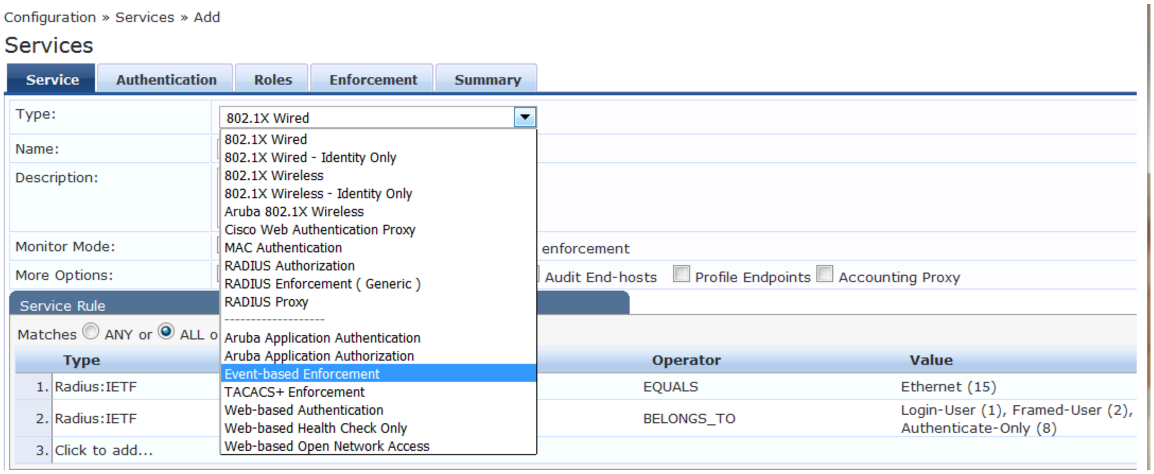
The **Services** page appears. The **Services** page provides options to add, modify, and remove a service.

2. To add the service, click **Add**.

   The **Add Services** dialog appears.

3. From the **Type** drop-down list, select **Event-based Enforcement** (see Figure 54).

Figure 54: *Specifying Event -Based Enforcement*



Configuration » Services » Add

Services

Service | Authentication | Roles | Enforcement | Summary

Type: 802.1X Wired

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

Name:

Description:

Monitor Mode: enforcement

More Options: Audit End-hosts □ Profile Endpoints □ Accounting Proxy

Service Rule

Matches ○ ANY or ● ALL o

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

4. Enter the name or label of the event-based enforcement service.

5. Enter the values for any other parameters, including service rules, required for this service.

   For a description of all the parameters in the **Service** page, see Adding Services on page 1.

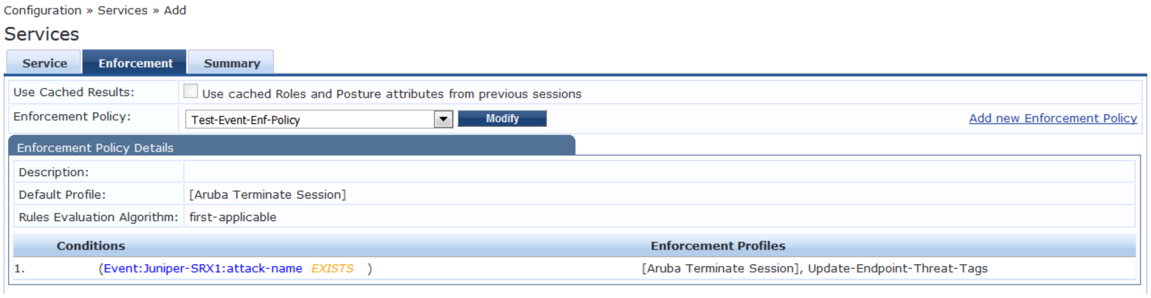
Associating the Service with an Enforcement Policy

After you create the event-based enforcement service, you must associate the service with an enforcement policy. You can do this from the **Services** > **Add > Enforcement** page.

1. When finished with the parameter settings on the **Add Services** > **Service** page, click **Next**.

   The **Services** > **Enforcement** page appears.

Figure 55: *Selecting the Ingress Events Enforcement Policy*



Configuration » Services » Add

Services

Service | Enforcement | Summary

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Test-Event-Enf-Policy [Modify] Add new Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Aruba Terminate Session]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Event:Juniper-SRX1:attack-name EXISTS)	[Aruba Terminate Session], Update-Endpoint-Threat-Tags

From the **Services** > **Add > Enforcement** page, you can either select an existing enforcement policy or create a new one.

2. From the **Enforcement Policy** drop-down list, select the appropriate Event Enforcement policy.

3. If you have not configured Event-type Enforcement policies, click **Add New Enforcement Policy** to create a new enforcement policy.

4. Specify the values for the remaining parameters as described in Table 31, then click **Save**.

Table 31: *Service Enforcement Page Parameters*

Parameter	Description
Use Cached Results	1. Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	2. From the drop-down list, select the preconfigured enforcement policy. This is mandatory.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

TACACS+ Enforcement Service

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
- 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.

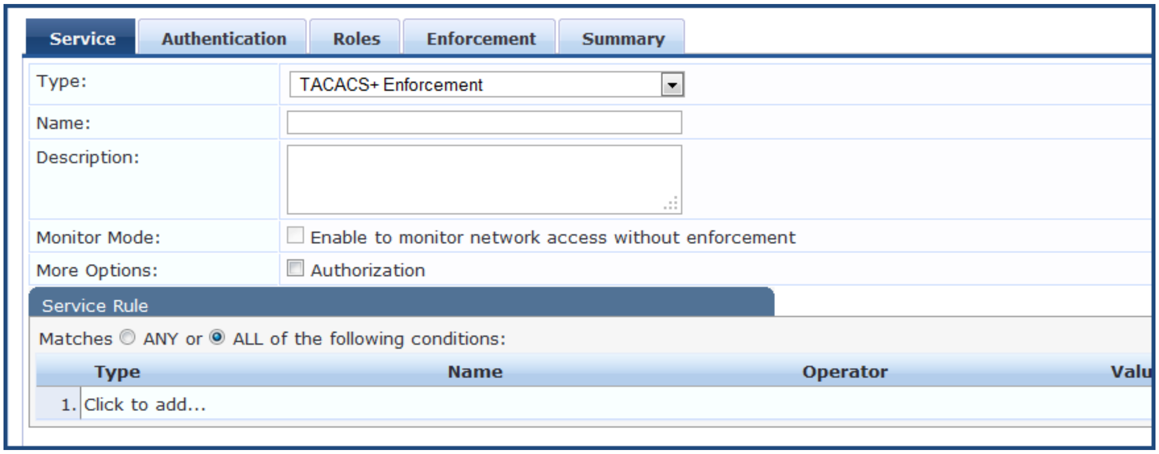
To enable this tab, select the **Authorization** check box from **More Options** on the **Service** tab.

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 Profile on page 403 for more information.

The following figure displays the **TACACS+ Enforcement** service:

Figure 56: *TACACS+ Enforcement Service*



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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

Configuring the **TACACS+ Enforcement** service is similar to configuring the **Aruba 802.1X Wireless** service except that the **Posture Compliance**, **Audit End-hosts**, and **Profile Endpoints** options are not available.

Web-Based Authentication Service

This section provides the following information:

- About the Web-Based Authentication Service
- Selecting a Web-Based Authentication Service by the OS Name
- Service Rule > Host Attributes

About the Web-Based Authentication Service

Configure a web-based authentication service for guests or agentless hosts that connect through the ClearPass Portal. The user is redirected to the ClearPass 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 the user name and password, and also optionally collects health information on the following operating systems (see the Attribute Name **OSType** in Table 32 for details):

- Linux
- Mac OS X
- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2003
- Windows Server 2003 R2

An internal service rule—Connection:Protocol EQUALS WebAuth—categorizes requests into this type of service. You can add additional rules if needed.

In addition, you can select a Web-based Authentication service based on the operating system (OS) name. You can specify or exclude specific OS versions (for details, see the next section, Selecting a Web-Based Authentication Service by the OS Name).

For service configuration details, see Adding and Removing Services on page 39.

To configure a web-based authentication service:

1. Navigate to **Configuration** > **Services**.

   The **Services** page opens.

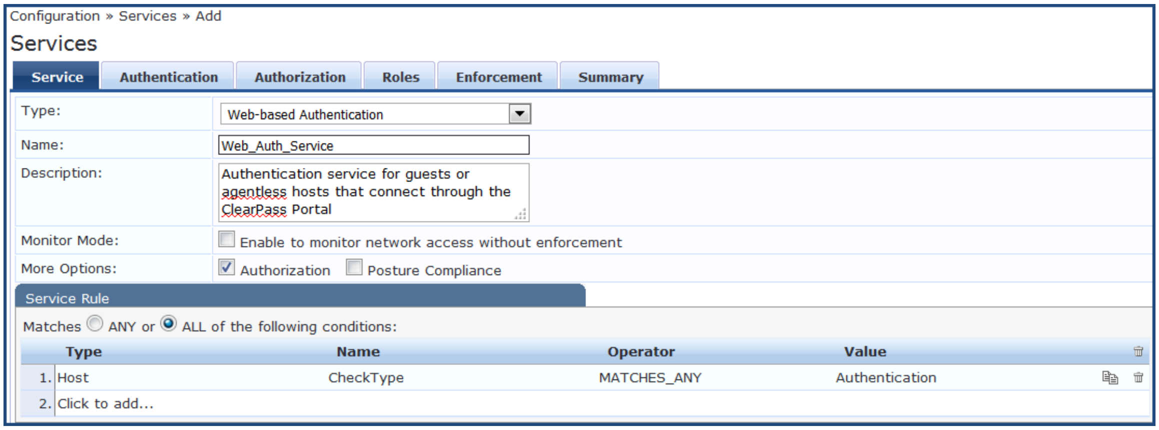
2. Select the **Add** link.

   The **Add Services** page opens.

3. From the Type drop-down list, select **Web-Based Authentication**.

   The following service configuration dialog opens:

Figure 57: *Web-Based Authentication Service Configuration Dialog*



Type: Web-based Authentication

Name: Web_Auth_Service

Description: Authentication service for guests or agentless hosts that connect through the ClearPass Portal

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: ☑ Authorization □ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

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

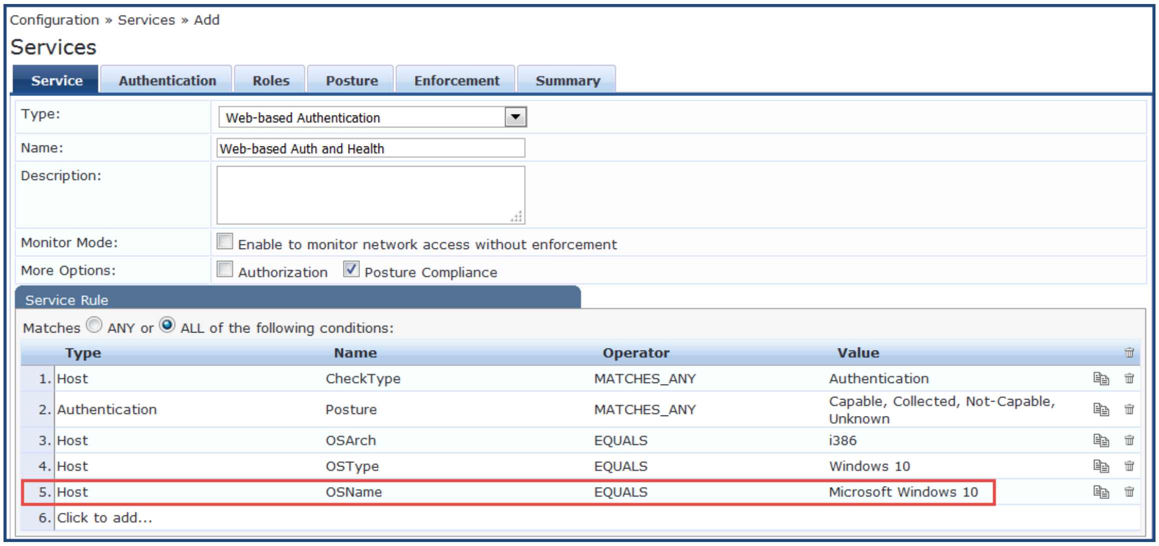
Selecting a Web-Based Authentication Service by the OS Name

The **Service Rule** > **Host:OSName** attribute allows you to select a Web-based Authentication service based on the OS name. You can specify or exclude specific OS versions.

To select a web-based authentication service by the OS name and version:

1. From the **Service** tab > **Service Rule** area, select **Click to add**.

Figure 58: *Host OS Name Specified in the Web-Based Authentication Service*



Type: Web-based Authentication

Name: Web-based Auth and Health

Description:

Monitor Mode: □ Enable to monitor network access without enforcement

More Options: □ Authorization ☑ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ANY	Authentication
2.	Authentication	Posture	MATCHES_ANY	Capable, Collected, Not-Capable, Unknown
3.	Host	OSArch	EQUALS	i386
4.	Host	OSType	EQUALS	Windows 10
5.	Host	OSName	EQUALS	Microsoft Windows 10
6.	Click to add...			

2. Specify the **Host OS Architecture** attribute as follows:
   - Type=**Host**
   - Name=**OSArch**
   - Operator=**EQUALS**
   - Value=**i386** or **x86_64**
3. Specify the **Host OS Type** attribute as follows:
   - Type=**Host**
   - Name=**OSType**
   - Operator=**EQUALS**
   - Value=**Windows 10**
4. Specify the **Host OS Name** attribute as follows:
   - Type=**Host**
   - Name=**OSName**
   - Operator=**EQUALS**
   - Value=**Microsoft Windows 10**

Example Showing How to Differentiate Between Windows 8 and Windows 8.1

- Type=**Host**
- Name=**OSName**
- Operator=**CONTAINS**
- Value=**Microsoft Windows 8.1**

Service Rule > Host Attributes

The following table describes the list of other attributes that can be used to create services based on the client's information.

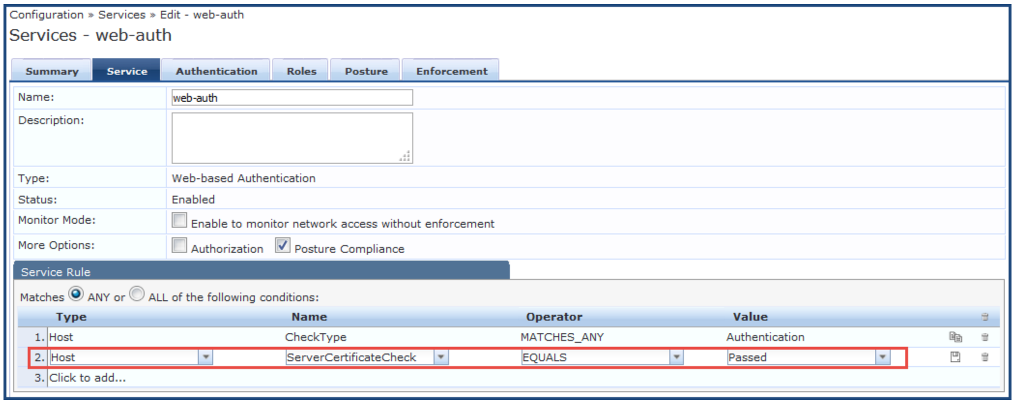
Table 32: *Service Rule > Host Attributes*

Attribute Type	Attribute Name	Description
Host	AgentType	Specifies the type of OnGuard Agent. This attribute provides a way to define a separate service for each OnGuard Agent Type. The supported values are: ● **OnGuardAgent**: OnGuard Agent ● **OnGuardAgentService**: OnGuard Agent running as a service ● **NativeWebAgent**: Native Dissolvable Agent ● **JavaWebAgent**: Java Dissolvable Agent
	Agent Version	OnGuard Agent version. This attribute can be used to create a service based on the OnGuard Agent version.
	CheckType	Specifies the type of check OnGuard Agent is performing based on the **Mode** setting in the OnGuard Settings page (for details, see OnGuard

Table 32: *Service Rule > Host Attributes (Continued)*

Attribute Type	Attribute Name	Description
		Settings on page 679). For **Authenticate with health checks**, the value of this attribute is **Authentication, Health**. The supported values are: - **Authentication**: OnGuard Agent is performing authentication; that is, the request contains credentials. - **Health**: OnGuard Agent is performing health checks; that is, the request contains Posture information. - **None**
	FQDN	Indicates the Fully Qualified Domain Name of the client.
	HealthCheckLevel	Indicates the level of health checks performed by OnGuard Agent; that is, whether the user is logged in at the time of health check or not. This attribute can be used to see the health check level when OnGuard Agent is running as **Service** or **BothServiceAndUser**. - **System**: The user is *not* logged in when health checks are being run. - **User**: The user is logged in when health checks are being run.
	InterfaceType	Specifies the type of **Network Interface**. This attribute can be used to define different services based on Network Interface type. The supported values are: - **Wired** - **Wireless** - **VPN**
	Name	This is the host name of the client (without the domain name).
	OSArch	Specifies whether the client is running a 32-bit or 64-bit OS. The supported values are: - **i386**: 32-bit OS - **x86_64**: 64-bit OS
	OSName	Indicates the full Operating System name. This attribute can be used to create services for a specific OS. For example, you can use this attribute to differentiate between Windows 8 and Windows 8.1
	OSType	Specifies the Operating System type. The

Table 32: *Service Rule > Host Attributes (Continued)*

Attribute Type	Attribute Name	Description
		supported values are: - **Linux** - **Mac OS X** - **Windows XP** - **Windows 7** - **Windows 8** - **Window 10** - **Windows Server 2003** - **Windows Server 2003 R2** - **Windows Server 2008** - **Windows Server 2008 R2**
	ServerCertificateCheck	This attribute's value shows the status of the ClearPass Server Certificate Check performed by OnGuard agent while sending a WebAuth request to the ClearPass server.This attribute can also be used in a Service Classification. The value of this attribute can be one of the following: - **Passed**: OnGuard Agent successfully verified the ClearPass Server Certificate. - **Failed**: OnGuard Agent failed to verify the ClearPass Server Certificate.
	 Configuration » Services » Edit - web-auth Services - web-auth Summary | Service | Authentication | Roles | Posture | Enforcement Name: web-auth Description: Type: Web-based Authentication Status: Enabled Monitor Mode: □ Enable to monitor network access without enforcement More Options: □ Authorization ☑ Posture Compliance Service Rule Matches ● ANY or ○ ALL of the following conditions: Type | Name | Operator | Value 1. Host | CheckType | MATCHES_ANY | Authentication 2. Host | ServerCertificateCheck | EQUALS | Passed 3. Click to add...	
	UserAgent	The value of this attribute contains both **Agent Type** and **Agent Version**. For example, OnGuard 6.6.5.89660.

Web-based Health Check Only Service

This type of service is the same as the **Web-based Authentication** service except that there is no authentication performed; only health check are performed.

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.

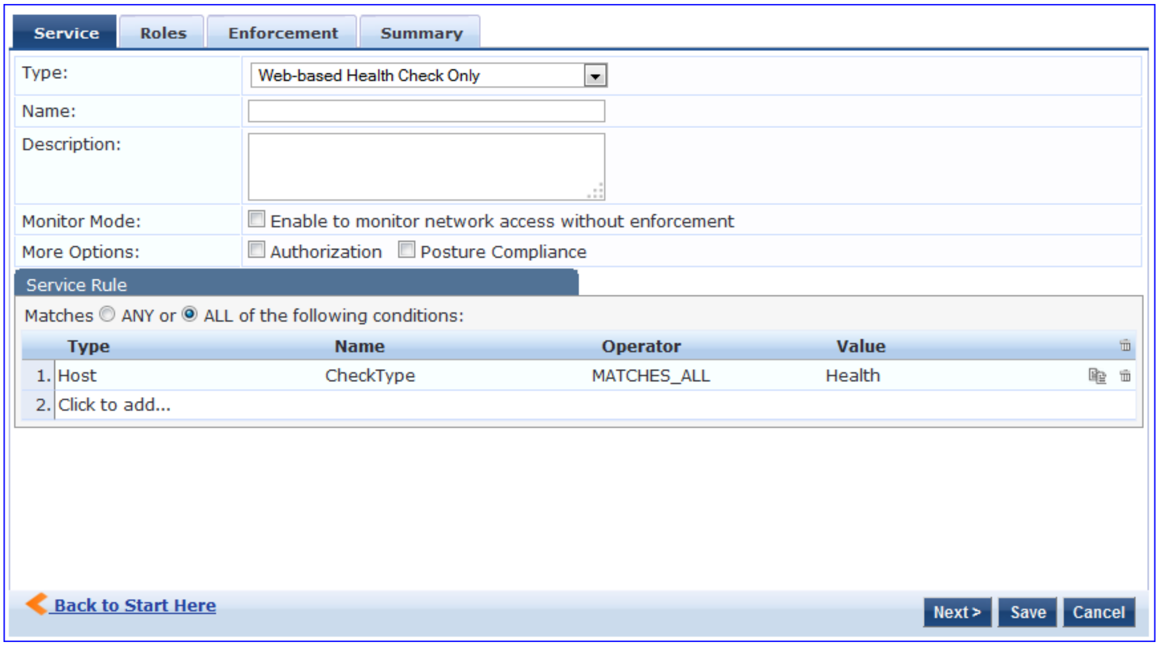
For more information, see Web-Based Authentication Service on page 92.

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 configuration dialog:

Figure 59: *Web-Based Health Check Only Service Configuration Dialog*



Type:	Web-based Health Check Only
Name:	
Description:	
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

For configuration details, see Aruba 802.1X Wireless Service on page 71.

Web-Based Open Network Access Service

Configuration for this service is the same as **Web-based Authentication** service, except that a health check is not performed on the endpoints.

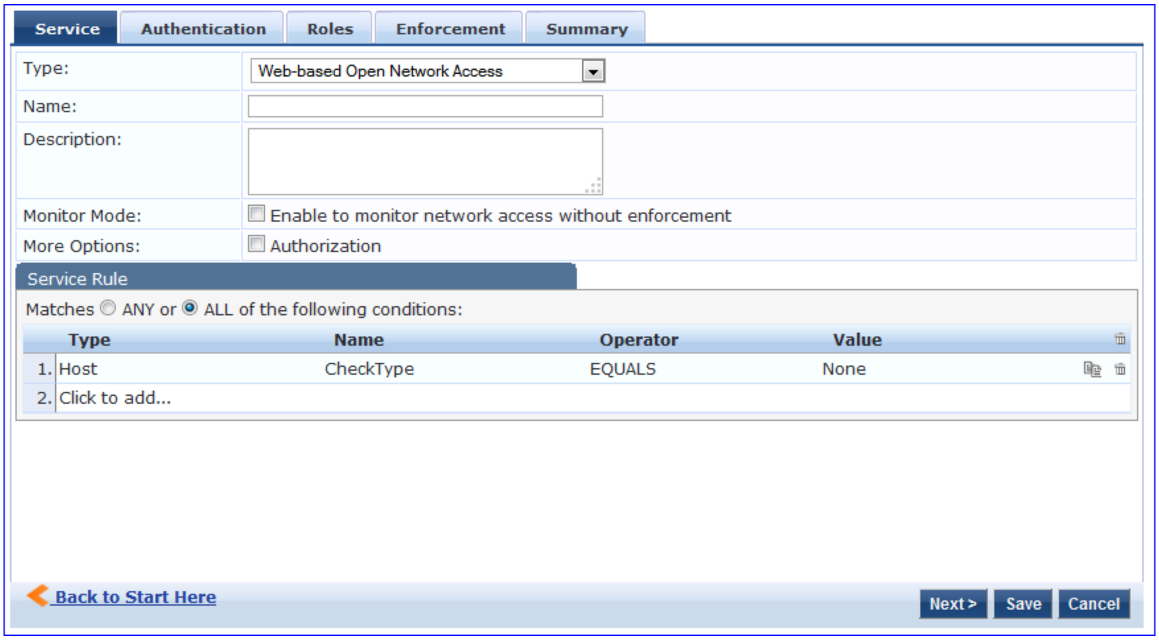
A Terms of Service page (as configured on the ClearPass Guest Portal page) is presented to the user.

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 Service on page 92.

The following figure displays the **Web-based Open Network** service page configuration dialog:

Figure 60: *Web-based Open Network Access Service Configuration Dialog*



Type:	Web-based Open Network Access
Name:	
Description:	
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

For configuration details, see Aruba 802.1X Wireless Service on page 71.

Chapter 3
Monitoring

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

- Network Discovery
  - Profiler and Discovery: Network Discovery on page 134
- Live Monitoring
  - Live Monitoring: Access Tracker on page 99
  - Live Monitoring: Accounting on page 111
  - Live Monitoring: Analysis and Trending on page 127
  - Live Monitoring: OnGuard Activity on page 121
  - Live Monitoring: System Monitor on page 128
- Audit Viewer
  - Audit Viewer on page 148
- Event Viewer
  - Event Viewer on page 150
- Data Filters
  - Data Filters on page 153
- Blacklisted Users
  - Restoring Blacklisted Users to the Network on page 158

Live Monitoring: Access Tracker

This section provides the following information:

- About the Access Tracker
- Customizing the Access Tracker
- Viewing Access Tracker Session Details

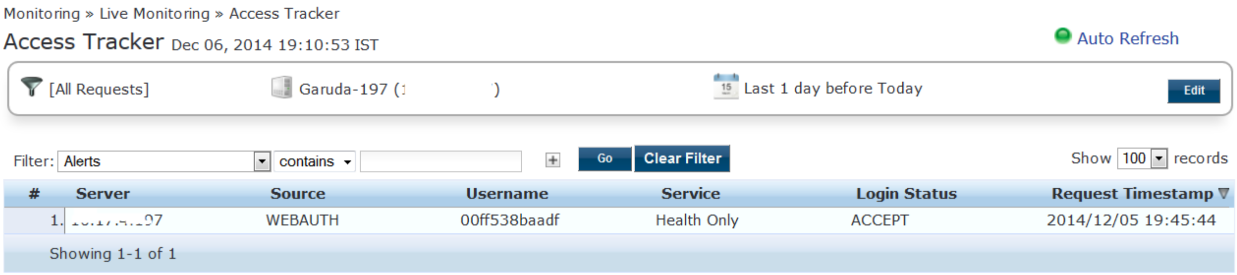
About the Access Tracker

The **Access Tracker** provides a real-time display of per-session access activity on the selected server or domain.

1. To view this page, navigate to **Monitoring > Live Monitoring > Access Tracker**.

   The **Access Tracker** page opens.

Figure 61: *Access Tracker Page*



Monitoring » Live Monitoring » Access Tracker

Access Tracker Dec 06, 2014 19:10:53 IST

[All Requests] Garuda-197 (1) Last 1 day before Today

Filter: Alerts contains

Show 100 records

#	Server	Source	Username	Service	Login Status	Request Timestamp ▽
1.	[illegible]97	WEBAUTH	00ff538baadf	Health Only	ACCEPT	2014/12/05 19:45:44

Showing 1-1 of 1

Table 33 describes the information in the **Access Tracker** page:

Table 33: *Access Tracker Page Columns*

Column	Description
Server	Displays the IP address of the server.
Source	Displays the authentication source for the session. For example, TACACS or web authentication (WEBAUTH).
Username	Displays the username or MAC address of the host.
Service	Displays the name of the service.
Login Status	Displays the status of the request, such as **Accept**, **Reject**, or **Timeout**.
Enforcement Profiles	Displays the names of the enforcement profiles associated with the Service.
Request Timestamp	Displays the date and time when the status was last updated.

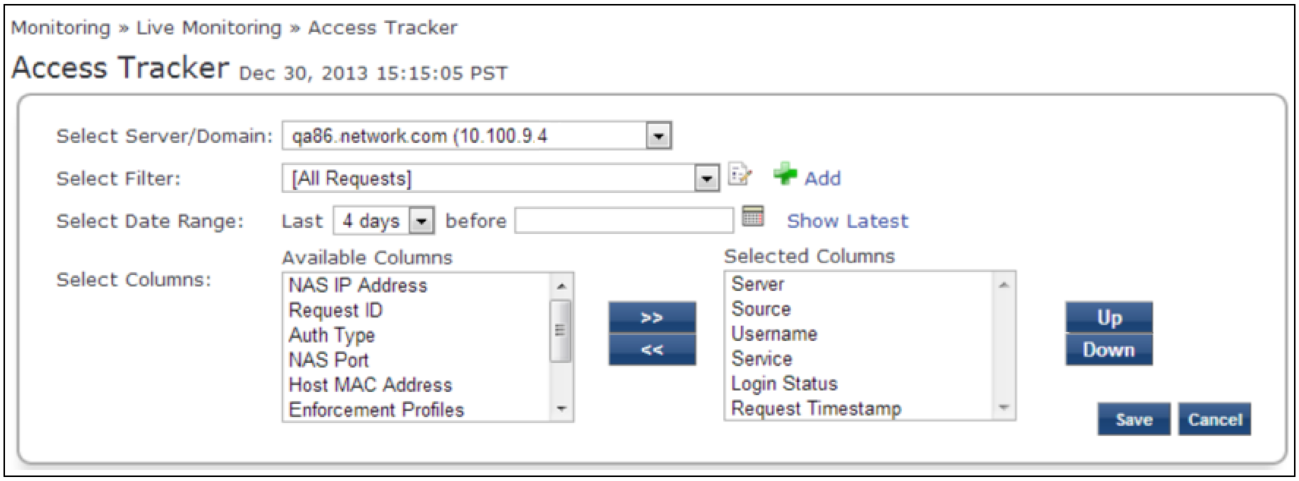
Customizing the Access Tracker

To customize the **Access Tracker** parameters:

1. From the **Access Tracker** page, click the **Edit** button (in the upper-right corner of the page).

   The **Edit Access Tracker** page opens.

Figure 62: *Edit Access Tracker Page*



Monitoring » Live Monitoring » Access Tracker

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

Select Server/Domain: qa86.network.com (10.100.9.4

Select Filter: [All Requests]

Select Date Range: Last 4 days before

Select Columns:

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

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

2. Modify the **Edit Access Tracker** page parameters as described in the following table, then click **Save**:

Table 34: *Edit Access Tracker Page Parameters*

Parameter	Action/Description
Select Server/ Domain	Displays information for the selected server or domain on the **Access Tracker** page. To display transactions from all nodes in the Policy Manager cluster, select all the servers.
Select Filter	Select a filter category to filter the displayed data. For a description of available filters, see Data Filters on page 153.
Modify Filter	To modify the current data filter, click the 📝 icon. For more information, see Data Filters on page 153.
Add Filter	To add a data filter, click the ➕ Add icon. The **Data Filters** page opens. For more information, see Data Filters on page 153.
Select Date Range	To select the start of the range of dates for which the **Access Tracker** table displays data, click the **Last** drop-down list. Available options are one to six days, or one week.
Select Date	To select a date, click the 📅 icon.
Show Latest	To set the date in the **before** field to the current date, click **Show Latest**.
Select Columns	This section displays the following two fields: ● **Available Columns**: Displays the data column available to be displayed 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, then click the **Up** or **Down** buttons.

Viewing Access Tracker Session Details

This section provides the following information:

- RADIUS Session
- WebAuth Session
- TACACS+ Session

RADIUS Session

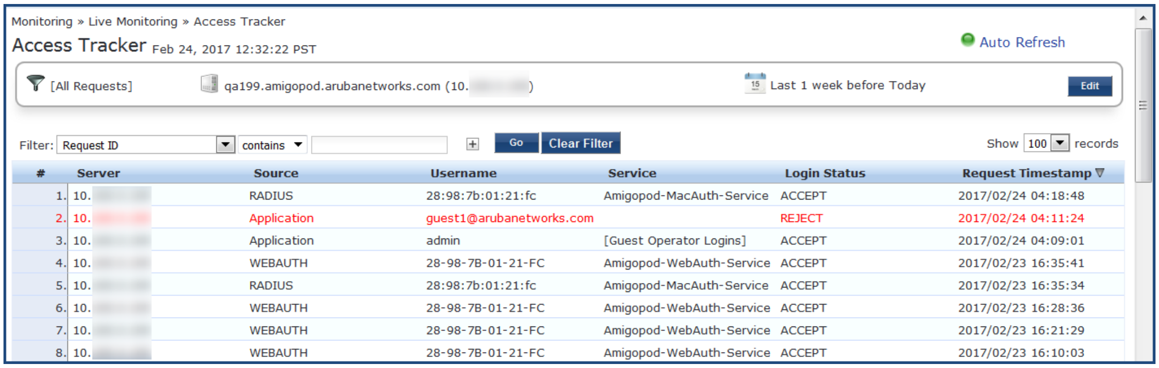
This section provides the following information:

- RADIUS > Summary Tab
- RADIUS > Input Tab
- RADIUS > Output Tab
- RADIUS > Accounting Tab

To view details about a selected RADIUS session:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.

Figure 63: *Access Tracker Page*



Monitoring » Live Monitoring » Access Tracker

Access Tracker Feb 24, 2017 12:32:22 PST

[All Requests] qa199.amigopod.arubanetworks.com (10.[redacted]) Last 1 week before Today

Filter: Request ID contains

Show 100 records

#	Server	Source	Username	Service	Login Status	Request Timestamp ▽
1.	10.[redacted]	RADIUS	28:98:7b:01:21:fc	Amigopod-MacAuth-Service	ACCEPT	2017/02/24 04:18:48
2.	10.[redacted]	Application	guest1@arubanetworks.com		REJECT	2017/02/24 04:11:24
3.	10.[redacted]	Application	admin	[Guest Operator Logins]	ACCEPT	2017/02/24 04:09:01
4.	10.[redacted]	WEBAUTH	28-98-7B-01-21-FC	Amigopod-WebAuth-Service	ACCEPT	2017/02/23 16:35:41
5.	10.[redacted]	RADIUS	28:98:7b:01:21:fc	Amigopod-MacAuth-Service	ACCEPT	2017/02/23 16:35:34
6.	10.[redacted]	WEBAUTH	28-98-7B-01-21-FC	Amigopod-WebAuth-Service	ACCEPT	2017/02/23 16:28:36
7.	10.[redacted]	WEBAUTH	28-98-7B-01-21-FC	Amigopod-WebAuth-Service	ACCEPT	2017/02/23 16:21:29
8.	10.[redacted]	WEBAUTH	28-98-7B-01-21-FC	Amigopod-WebAuth-Service	ACCEPT	2017/02/23 16:10:03

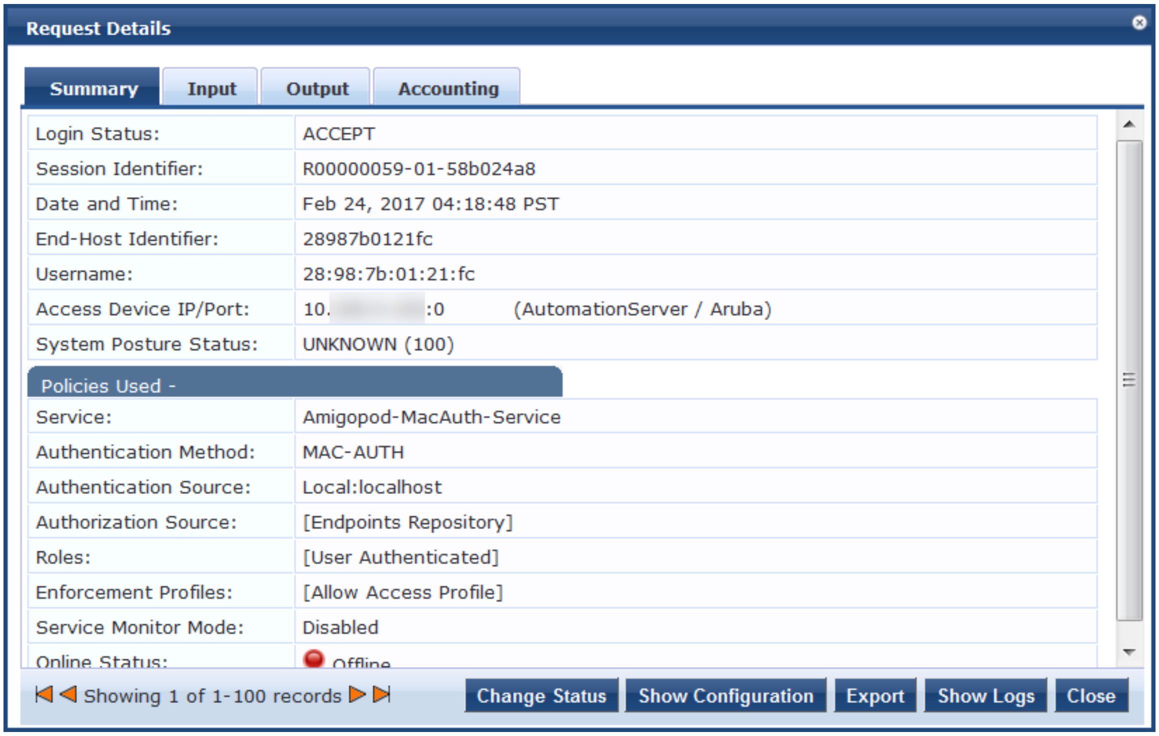
2. Click a **RADIUS** session in the **Access Tracker** table.

   The Session Details for the selected RADIUS transaction are displayed. The information in this page varies, depending upon the session selected.

RADIUS > Summary Tab

The **Summary** page shows the basic high-level information of the transaction.

Figure 64: *Access Tracker > RADIUS Request Details > Summary Page*



Request Details

Login Status:	ACCEPT
Session Identifier:	R00000059-01-58b024a8
Date and Time:	Feb 24, 2017 04:18:48 PST
End-Host Identifier:	28987b0121fc
Username:	28:98:7b:01:21:fc
Access Device IP/Port:	10.[redacted]:0 (AutomationServer / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Amigopod-MacAuth-Service
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Endpoints Repository]
Roles:	[User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	● Offline

Showing 1 of 1-100 records

RADIUS > Input Tab

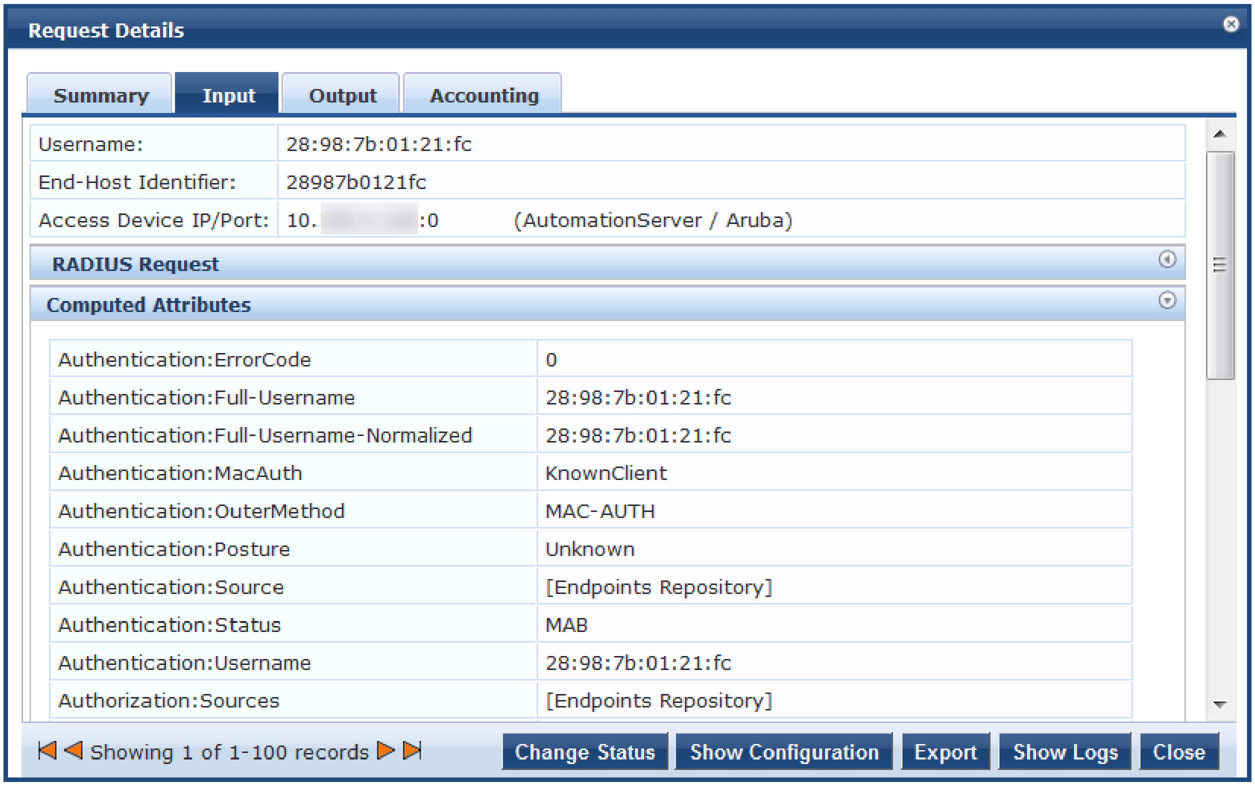
The **Input** tab shows protocol-specific attributes that Policy Manager received in a transaction request, including authentication and posture details (if available).

The **Input** tab also shows computed attributes that Policy Manager derived from the request attributes. All of these attributes can be used in role -mapping rules.

1. To view the **Input** tab, click RADIUS session in the **Access Tracker** page, then select the **Input** tab.

   The **Request Details** > **Input** page opens.

Figure 65: *Access Tracker > RADIUS Request Details > Input Page*



Username:	28:98:7b:01:21:fc
End-Host Identifier:	28987b0121fc
Access Device IP/Port:	10.[redacted]:0 (AutomationServer / Aruba)

Authentication:ErrorCode	0
Authentication:Full-Username	28:98:7b:01:21:fc
Authentication:Full-Username-Normalized	28:98:7b:01:21:fc
Authentication:MacAuth	KnownClient
Authentication:OuterMethod	MAC-AUTH
Authentication:Posture	Unknown
Authentication:Source	[Endpoints Repository]
Authentication:Status	MAB
Authentication:Username	28:98:7b:01:21:fc
Authorization:Sources	[Endpoints Repository]

RADIUS > Output Tab

The **RADIUS Request Details** > **Output** tab shows the attributes that were sent to the network device (switch or controller) and the posture-capable endpoint (for example, MAC devices).

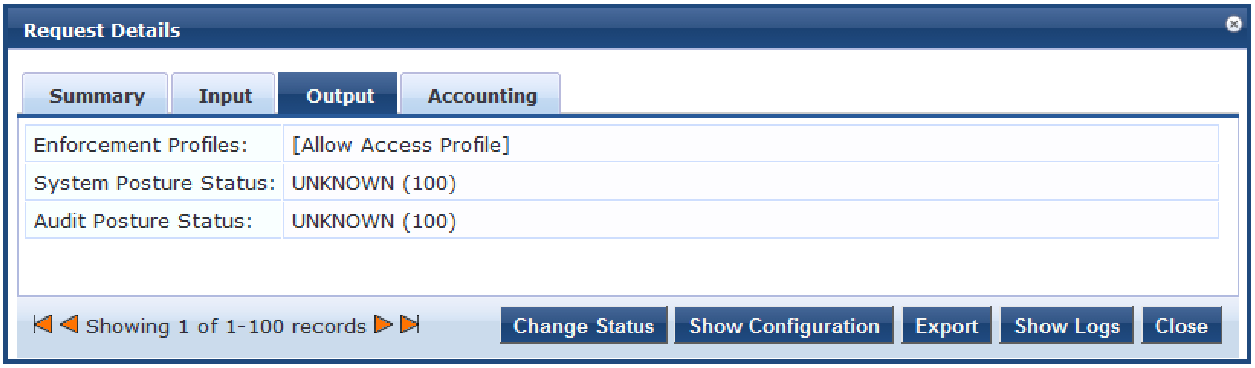
You can view the posture response and posture evaluation with accurate results. For example, you can view details such as missing registry keys and the reasons for a failed registry key check.

To view the **Request Details** > **Output** page:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.
2. Click any RADIUS session in the **Access Tracker** page.
3. Select the **Output** tab.

   The **RADIUS Request Details** > **Output** page opens:

Figure 66: *Access Tracker > RADIUS Request Details > Output Page*



Enforcement Profiles:	[Allow Access Profile]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

NOTE

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

RADIUS > Accounting Tab

The **RADIUS Request Details** > **Accounting** tab shows the account session details, as well as the following information:

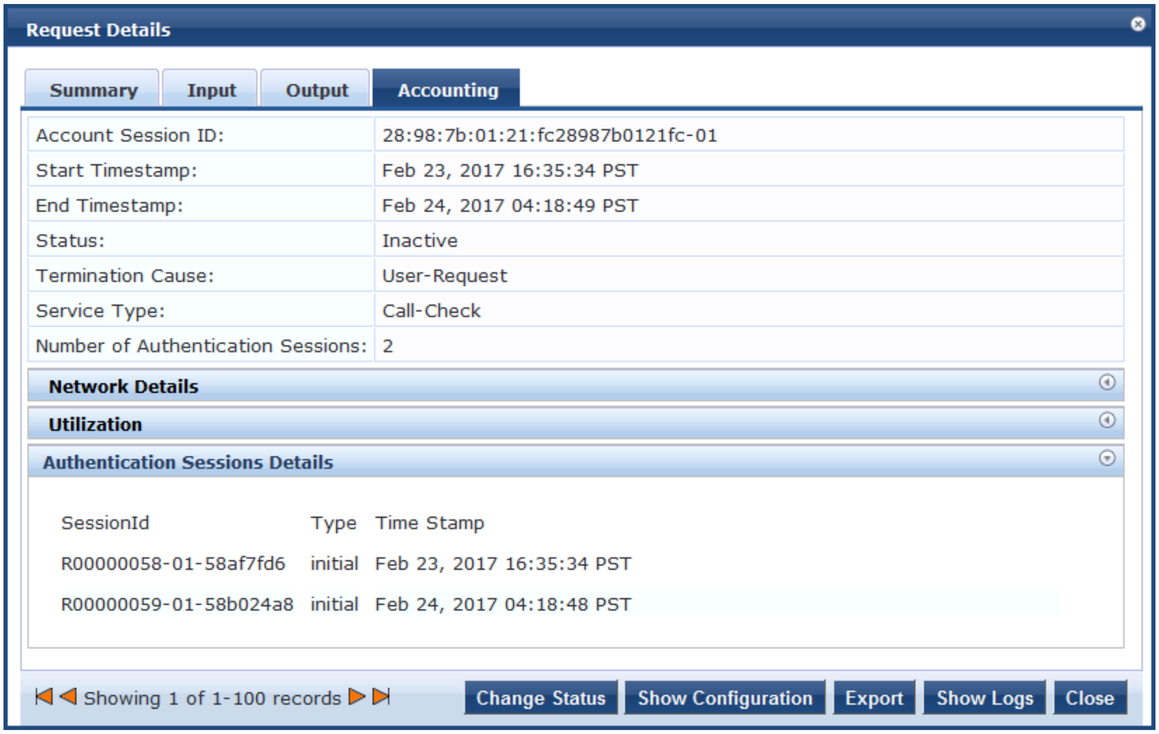
- Network Details
- Utilization information
- Authentication Session Details

To view the **RADIUS Request Details** > **Accounting** page:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.
2. Click any RADIUS session in the **Access Tracker** page.
3. Select the **Accounting** tab.

   The **Request Details** > **Accounting** page opens:

Figure 67: *Access Tracker > RADIUS Request Details > Accounting Tab*



Account Session ID:	28:98:7b:01:21:fc28987b0121fc-01
Start Timestamp:	Feb 23, 2017 16:35:34 PST
End Timestamp:	Feb 24, 2017 04:18:49 PST
Status:	Inactive
Termination Cause:	User-Request
Service Type:	Call-Check
Number of Authentication Sessions:	2

SessionId	Type	Time Stamp
R00000058-01-58af7fd6	initial	Feb 23, 2017 16:35:34 PST
R00000059-01-58b024a8	initial	Feb 24, 2017 04:18:48 PST

Showing 1 of 1-100 records

WebAuth Session

WebAuth (Web Authentication) is a single sign-on (SSO) authentication system for web pages and web applications. The first time a user attempts to access a web page protected by WebAuth, they are sent to a central login server and prompted to authenticate. Users are typically asked for a username and password, although other authentication methods are possible.

Once the user has logged in, the weblogin server sends their encrypted identity back to the original web page they were trying to access. Their identity is also stored in a cookie set by the weblogin server and they will not need to authenticate again until their credentials expire, even if they visit multiple protected web sites.

To view details about a selected WebAuth session:

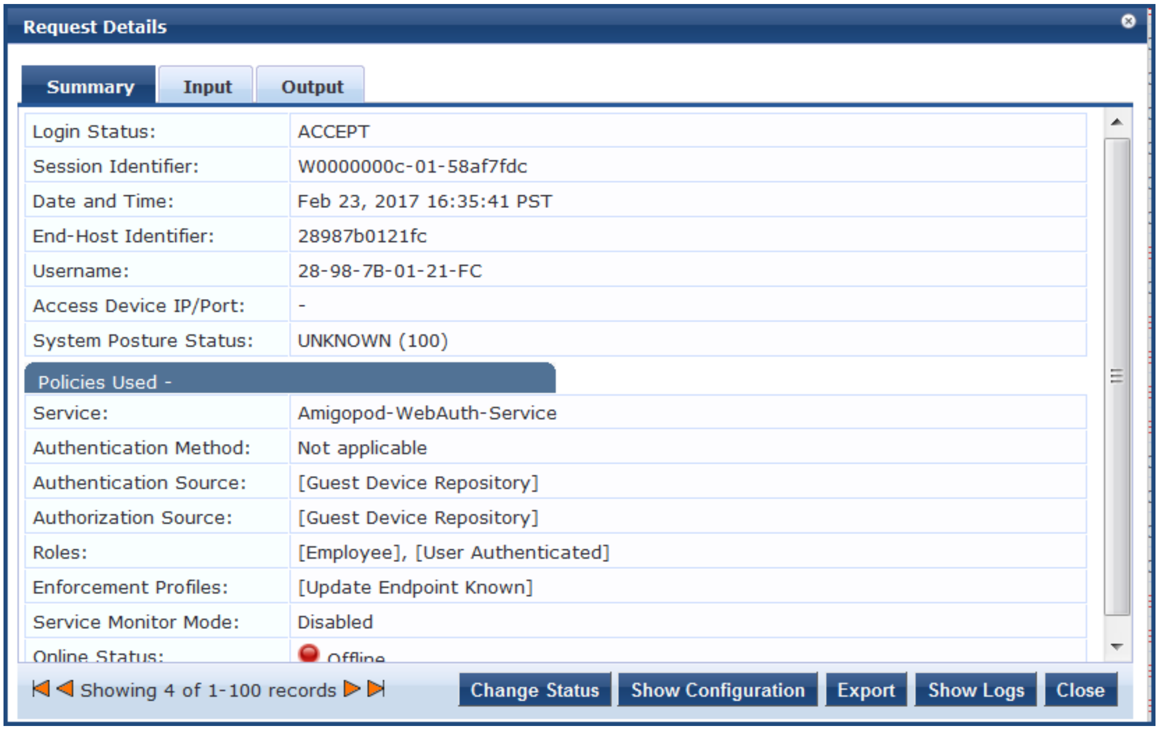
1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.

   The **Access Tracker** page opens.
2. Click a **WebAuth** session in the **Access Tracker** table.

WebAuth > Summary Tab

The **Request Details** page for the selected WebAuth (Web Authentication) transaction opens to the **Summary** page. The information in this page varies, depending upon the type of session selected.

Figure 68: *Access Tracker > WebAuth Request Details > Summary Page*



Login Status:	ACCEPT
Session Identifier:	W0000000c-01-58af7fdc
Date and Time:	Feb 23, 2017 16:35:41 PST
End-Host Identifier:	28987b0121fc
Username:	28-98-7B-01-21-FC
Access Device IP/Port:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Amigopod-WebAuth-Service
Authentication Method:	Not applicable
Authentication Source:	[Guest Device Repository]
Authorization Source:	[Guest Device Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	[Update Endpoint Known]
Service Monitor Mode:	Disabled
Online Status:	● Offline

The **WebAuth Request Details** > **Summary** page displays the basic WebAuth session information (login status, date and time, end-host identifier, and so on), as well as providing a section that summarizes the service being applied and details about the policies and profiles in use.

WebAuth Input Tab

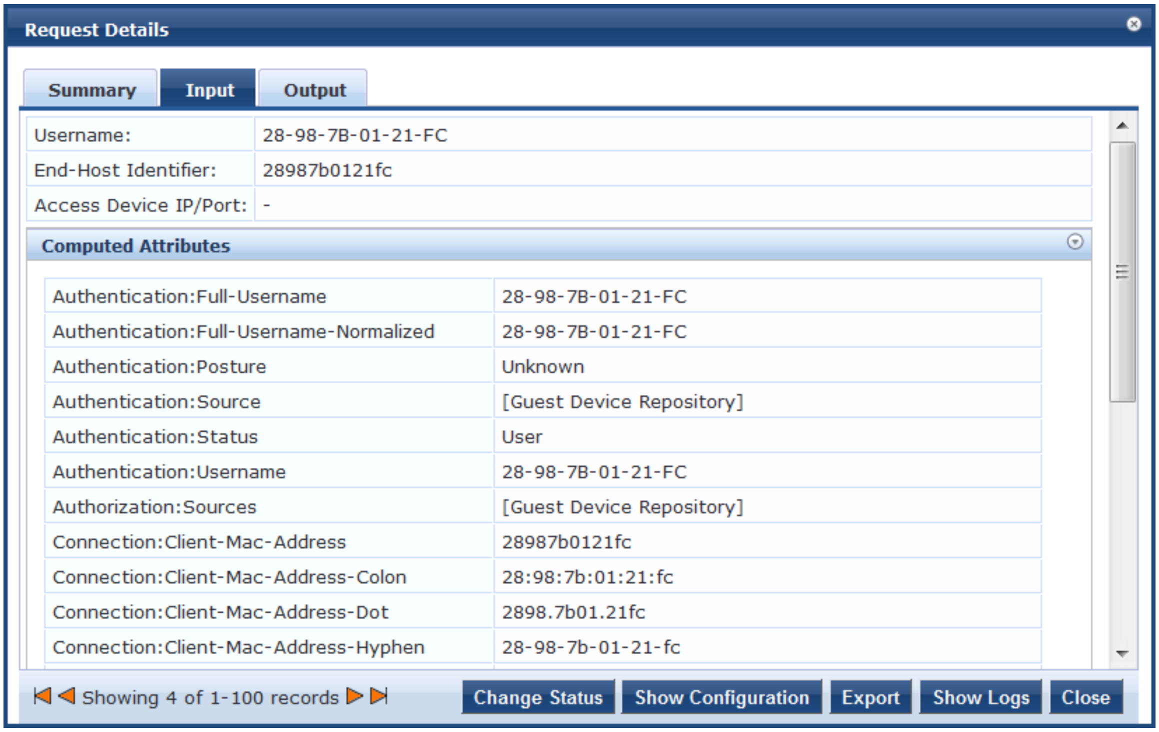
The **Input** tab shows protocol-specific attributes that Policy Manager received in a transaction request, including authentication and posture details (if available).

The **Input** tab also shows computed attributes that Policy Manager derived from the request attributes. All of these attributes can be used in role -mapping rules.

1. To view the **Input** tab, click a WebAuth session in the **Access Tracker** page, then select the **Input** tab.

   The **WebAuth Request Details** > **Input** page opens.

Figure 69: *Access Tracker > WebAuth Request Details > Input Page*



Username:	28-98-7B-01-21-FC
End-Host Identifier:	28987b0121fc
Access Device IP/Port:	-

Computed Attributes

Authentication:Full-Username	28-98-7B-01-21-FC
Authentication:Full-Username-Normalized	28-98-7B-01-21-FC
Authentication:Posture	Unknown
Authentication:Source	[Guest Device Repository]
Authentication:Status	User
Authentication:Username	28-98-7B-01-21-FC
Authorization:Sources	[Guest Device Repository]
Connection:Client-Mac-Address	28987b0121fc
Connection:Client-Mac-Address-Colon	28:98:7b:01:21:fc
Connection:Client-Mac-Address-Dot	2898.7b01.21fc
Connection:Client-Mac-Address-Hyphen	28-98-7b-01-21-fc

WebAuth > Output Tab

The **WebAuth Request Details** > **Output** tab shows the attributes that were sent to the network device (switch or controller) and the posture-capable endpoint (for example, MAC devices).

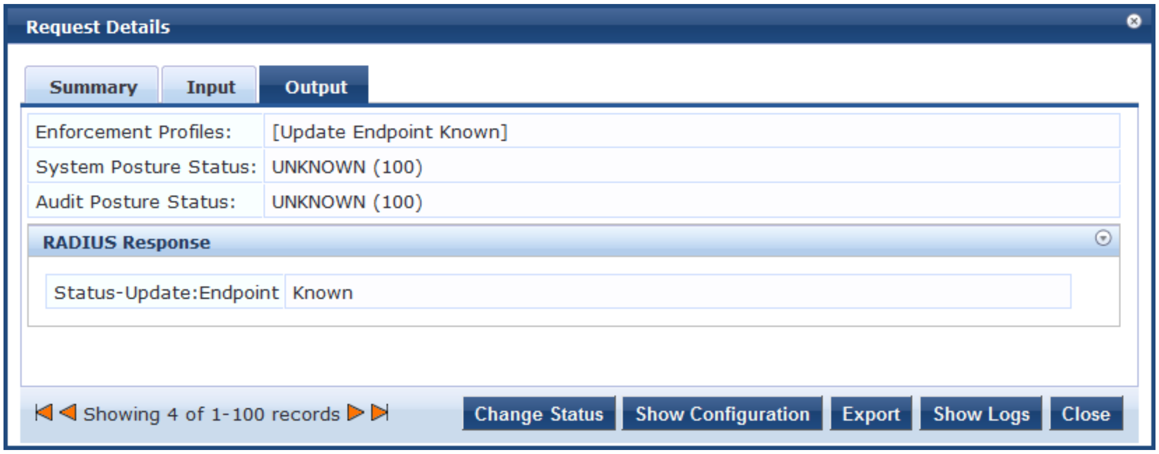
You can view the posture response and posture evaluation with accurate results. For example, you can view details such as missing registry keys and the reasons for a failed registry key check. The Output page also provides the RADIUS response summary.

To view the **WebAuth Request Details** > **Output** page:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.
2. Click any WebAuth session in the **Access Tracker** page.
3. Select the **Output** tab.

   The **WebAuth Request Details** > **Output** page opens:

Figure 70: *Access Tracker > WebAuth Request Details > Output Page*



Enforcement Profiles:	[Update Endpoint Known]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Status-Update:Endpoint	Known

TACACS+ Session

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service.

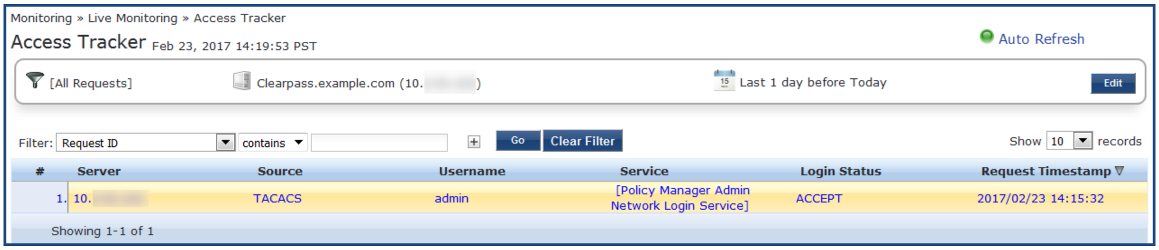
TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

To view details about a selected TACACS+ session:

1. Navigate to the **Monitoring > Live Monitoring > Access Tracker** page.

   The **Access Tracker** page opens.

Figure 71: *Access Tracker Page with TACACS+ Session*



Monitoring » Live Monitoring » Access Tracker
Access Tracker Feb 23, 2017 14:19:53 PST
Auto Refresh
[All Requests]
Clearpass.example.com (10.[redacted])
Last 1 day before Today
Edit
Filter: Request ID
contains
Go
Clear Filter
Show 10 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.[redacted]	TACACS	admin	[Policy Manager Admin Network Login Service]	ACCEPT	2017/02/23 14:15:32

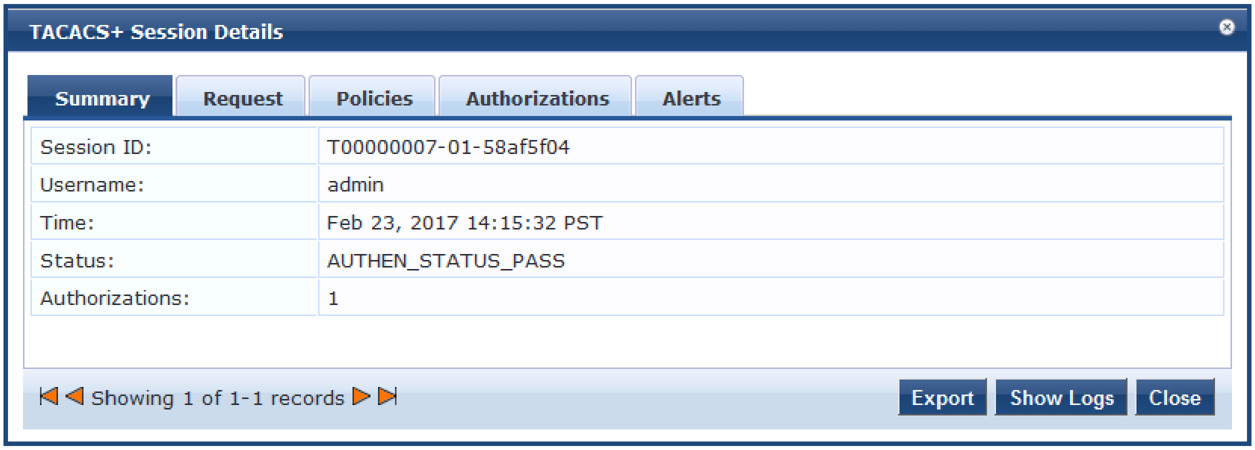
Showing 1-1 of 1

2. Click a **TACACS+** session in the **Access Tracker** table.

TACACS+ > Summary Tab

The Session Details for the selected TACACS+ transaction opens to the **Summary** page.

Figure 72: *Access Tracker > TACACS Session Details > Summary Page*



Session ID:	T00000007-01-58af5f04
Username:	admin
Time:	Feb 23, 2017 14:15:32 PST
Status:	AUTHEN_STATUS_PASS
Authorizations:	1

Table 35 describes the parameters in the TACACS+ Session Details Summary page.

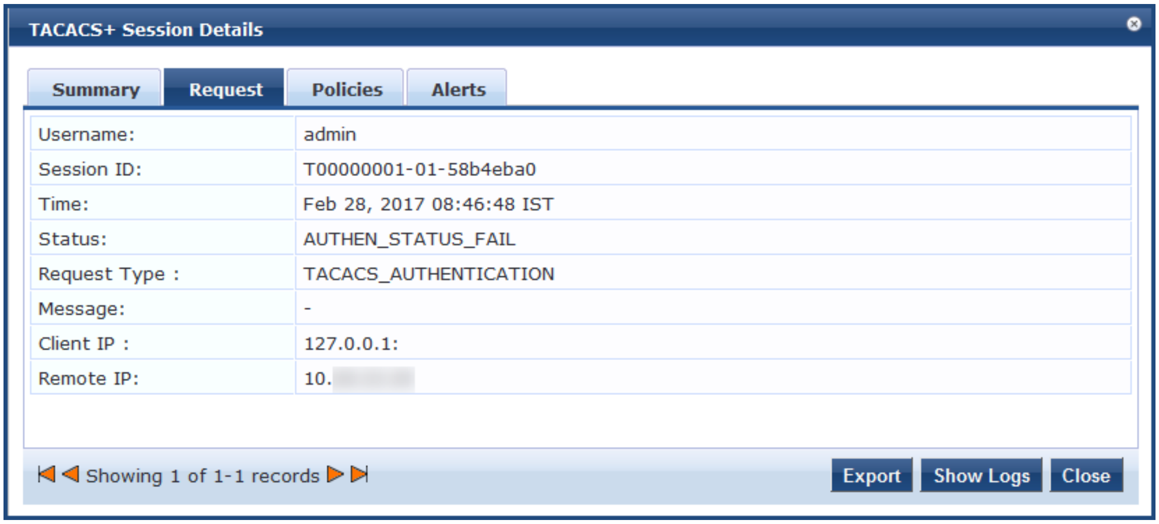
Table 35: *TACACS Session Details > Summary Page Parameters*

Field	Action/Description
Session ID	Displays the automatically-generated session ID for the selected TACACS+ session.
Username	Indicates the name of the admin user.
Time	Indicates the time that the TACACAS+ session was initiated.
Status	Indicates the authentication status of the selected TACACS+ session.
Authorizations	Indicates the number of authentication authorizations that have taken place for this session.
Export	To export the TACACS+ summary information, click **Export**. For details, see Importing and Exporting Information on page 31.
Show Logs	When you click **Show Logs**, the **Request log details for session:** <*session_number*> are displayed.

TACACS+ > Request Tab

The **TACACS+ Request** page provides the essential information regarding the TACACS+ authentication request.

Figure 73: *Access Tracker > TACACS Session Details > Request Page*



Username:	admin
Session ID:	T00000001-01-58b4eba0
Time:	Feb 28, 2017 08:46:48 IST
Status:	AUTHEN_STATUS_FAIL
Request Type :	TACACS_AUTHENTICATION
Message:	-
Client IP :	127.0.0.1:
Remote IP:	10.[redacted]

Table 36 describes the parameters in the **TACACS+ Session Details Request** page.

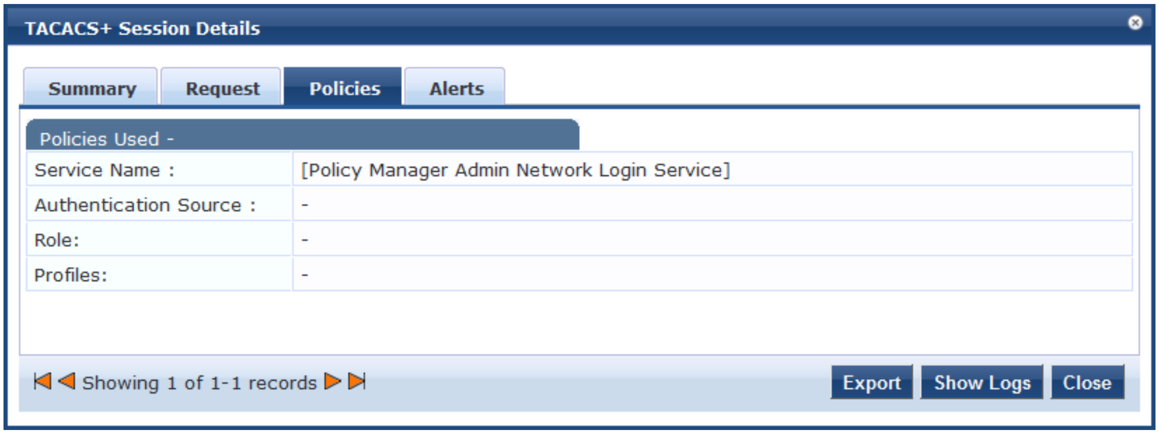
Table 36: *TACACS Session Details > Request Page Parameters*

Field	Action/Description
Username	Indicates the name of the admin user.
Session ID	Displays the automatically-generated session ID for the selected TACACS+ session.
Time	Indicates the time that the TACACS+ session was initiated.
Status	Indicates the authorization status of the selected TACACS+ session. The possible values are: ● AUTHEN_STATUS_PASS ● AUTHEN_STATUS_FAIL ● AUTHEN_STATUS_GETDATA ● AUTHEN_STATUS_GETUSER ● AUTHEN_STATUS_GETPASS ● AUTHEN_STATUS_RESTART ● AUTHEN_STATUS_ERROR ● AUTHEN_STATUS_FOLLOW
Request Type	Indicates the type of authentication request. There are three supported request types: ● TACACS Authentication ● TACACS Authorization ● TACACS Accounting
Message	This is a message to be displayed to the user.
Client IP	This is the IP address of the device (for example, the ArubaOS switch)the remote IP device is attempting to log into.
Remote IP	This is the source IP address of the user device (for example, a laptop) attempting to log into the client device.

TACACS+ > Policies Tab

The **TACACS+ > Policies** page provides the details regarding the Policy Manager role mapping policies used, authentication sources, and enforcement policies used (if available).

Figure 74: *Access Tracker > TACACS Session Details > Policies Page*



Service Name :	[Policy Manager Admin Network Login Service]
Authentication Source :	-
Role:	-
Profiles:	-

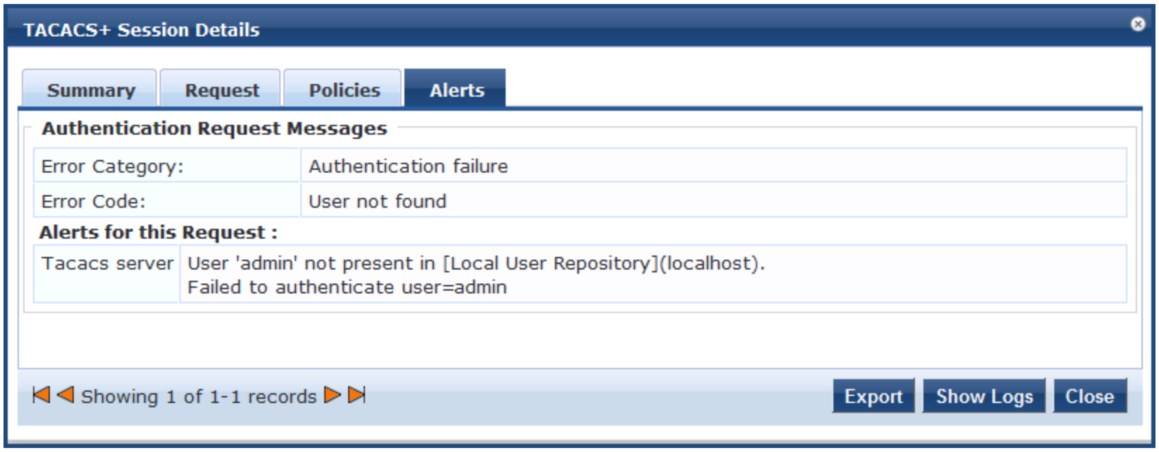
Table 37: *TACACS Session Details > Policies Used Page Parameters*

Field	Action/Description
Service Name	Indicates the name of the ClearPass service through which the user is authenticated.
Authentication Source	Specifies the authentication source used bythe client. For more information, see Adding and Configuring Authentication Sources on page 190.
Role	Indicates the Policy Manager role assigned to the client. For more information, see Adding and Modifying Roles on page 257.
Profiles	Indicates the Enforcement Profile configured for this service. For more information, see Configuring Enforcement Profiles on page 357.

TACACS+ > Alerts Tab

The **TACACS+ > Alerts** page shows information about a session that has an error.

Figure 75: *Access Tracker > TACACS+ Session Details > Alerts Page*



Authentication Request Messages

Error Category:	Authentication failure
Error Code:	User not found

Alerts for this Request :

Tacacs server	User 'admin' not present in [Local User Repository](localhost). Failed to authenticate user=admin

Showing 1 of 1-1 records

Table 38: *TACACS Session Details > AlertsPage Parameters*

Field	Action/Description
Authentication Request Messages	
Error Category	Indicates the error category.
Error Code	Dispays the error code.
Alerts for This Request	
Alert source	Indicates the source for this alert; in this case, the TACACS+ server.
Alert message	Displays the alert message.

Live Monitoring: Accounting

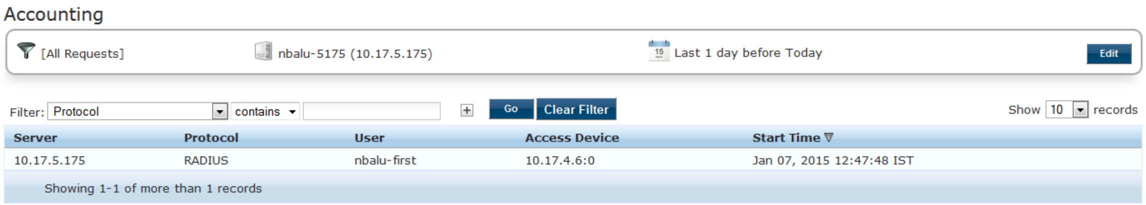
This section provides the following information:

- Modifying the Accounting Page Parameters
- RADIUS Accounting Details > Summary Tab
- RADIUS Accounting Record Details > Auth Sessions Tab
- RADIUS Accounting Record Details > Utilization Tab
- RADIUS Accounting Record Details > Details Tab
- TACACS+ Accounting Record Details > Request Tab
- TACACS+ Accounting Record Details > Auth Sessions Tab
- TACACS+ Accounting Record Details > Details Tab

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 76: *Live Monitoring > Accounting Page*



Accounting

[All Requests]   nbalu-5175 (10.17.5.175)   Last 1 day before Today   Edit

Filter: Protocol   contains   Go   Clear Filter   Show 10 records

Server	Protocol	User	Access Device	Start Time
10.17.5.175	RADIUS	nbalu-first	10.17.4.6:0	Jan 07, 2015 12:47:48 IST

Showing 1-1 of more than 1 records

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

Table 39: *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 the Accounting page to drill down and display the corresponding **Accounting Record Details** page for the selected session. For details, see RADIUS Accounting Details > Summary Tab on page 112 and TACACS+ Accounting Record Details > Auth Sessions Tab on page 119.

Modifying the Accounting Page Parameters

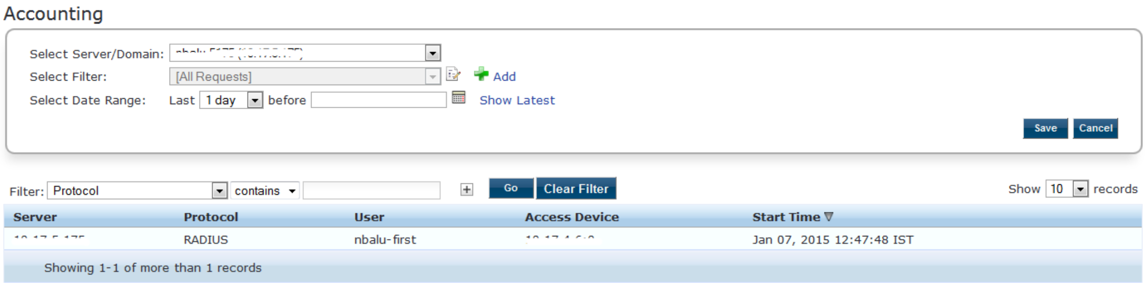
You can filter or modify the information displayed in this table by creating a filter, or selecting a different server, domain, or time range.

To filter the data currently displayed in the **Accounting** page:

1. Navigate to the **Monitoring > Live Monitoring > Accounting** page.
2. Click **Edit**.

   The **Edit Accounting Page** dialog opens.

Figure 77: *Edit Accounting Page Dialog*



Accounting

Select Server/Domain: [illegible]
Select Filter: [All Requests] Add
Select Date Range: Last 1 day before Show Latest

Filter: Protocol contains

Show 10 records

Server	Protocol	User	Access Device	Start Time
[illegible]	RADIUS	nbalu-first	[illegible]	Jan 07, 2015 12:47:48 IST

Showing 1-1 of more than 1 records

3. Specify the **Edit Accounting Page** parameters as described in Table 40:

Table 40: *Edit Accounting Page Parameters*

Parameter	Action/Description
Select Server/ Domain	Select the ClearPass server for the dashboard data to be displayed.
Select Filter	To constrain the data display, select a filter from the drop-down list. You can select one of the following filters: ● Protocol ● User ● Access Device
Modify	To modify a data filter, click the **Modify Data Filter** icon (as shown in Figure 77).
Add	To create a new data filter, click the ✚ Add icon.
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 one day to a week.
Show Latest	To view the latest information, set the date to **Today**.
Select Columns	● To move data between **Available Columns** and **Selected Columns**, click the right or left arrows. ● To rearrange columns, click the **Up** or **Down** buttons.

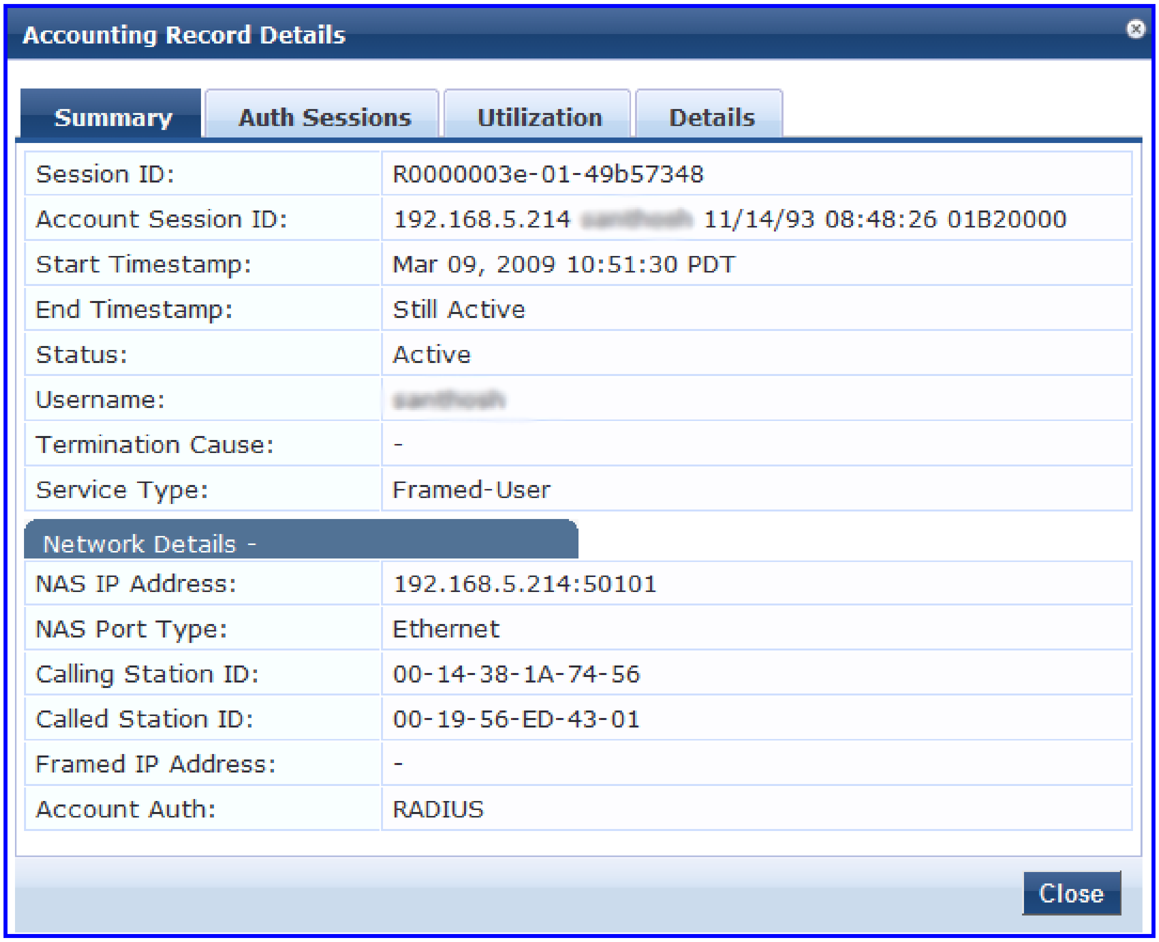
RADIUS Accounting Details > Summary Tab

To drill down and display the corresponding **Accounting Record Details** page for the session, click any row in the **Accounting** page.

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** page:

Figure 78: *RADIUS Accounting Record Details Summary Page*



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

Network Details -

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

The following table describes the configuration parameters on the **RADIUS Accounting Record Details** > **Summary** page:

Table 41: *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 Timestamp End Timestamp	Shows the start time and end time of the session.
Status	Shows the current connection status of the session.
Username	Username associated with this record.
Termination Cause	Specifies the reason for termination of this session.

Table 41: *RADIUS Accounting Record Details Summary Tab Parameters (Continued)*

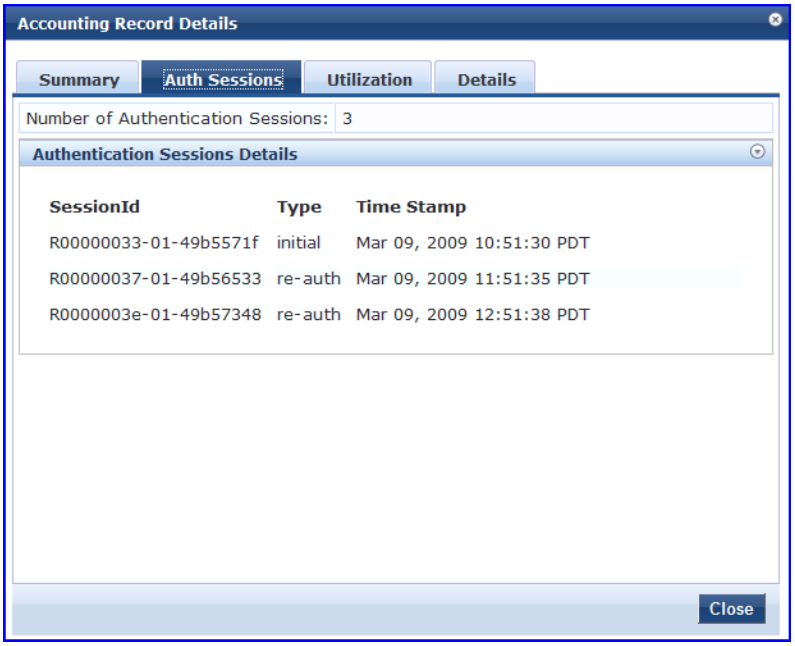
Parameter	Description
Service Type	Shows the value of the standard RADIUS attribute service type.
Network Details	
NAS IP Address	Shows the IP address of the network device.
NAS Port Type	Shows the access methods. For example, Ethernet, or 802.11 Wireless.
Calling Station ID	Specifies the MAC address 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; for example, 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** page:

Figure 79: *RADIUS Accounting Record Details > Auth Sessions Page*



Number of Authentication Sessions: 3

Authentication Sessions Details

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

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

Table 42: *RADIUS Accounting Record Details Auth Sessions Tab Parameters*

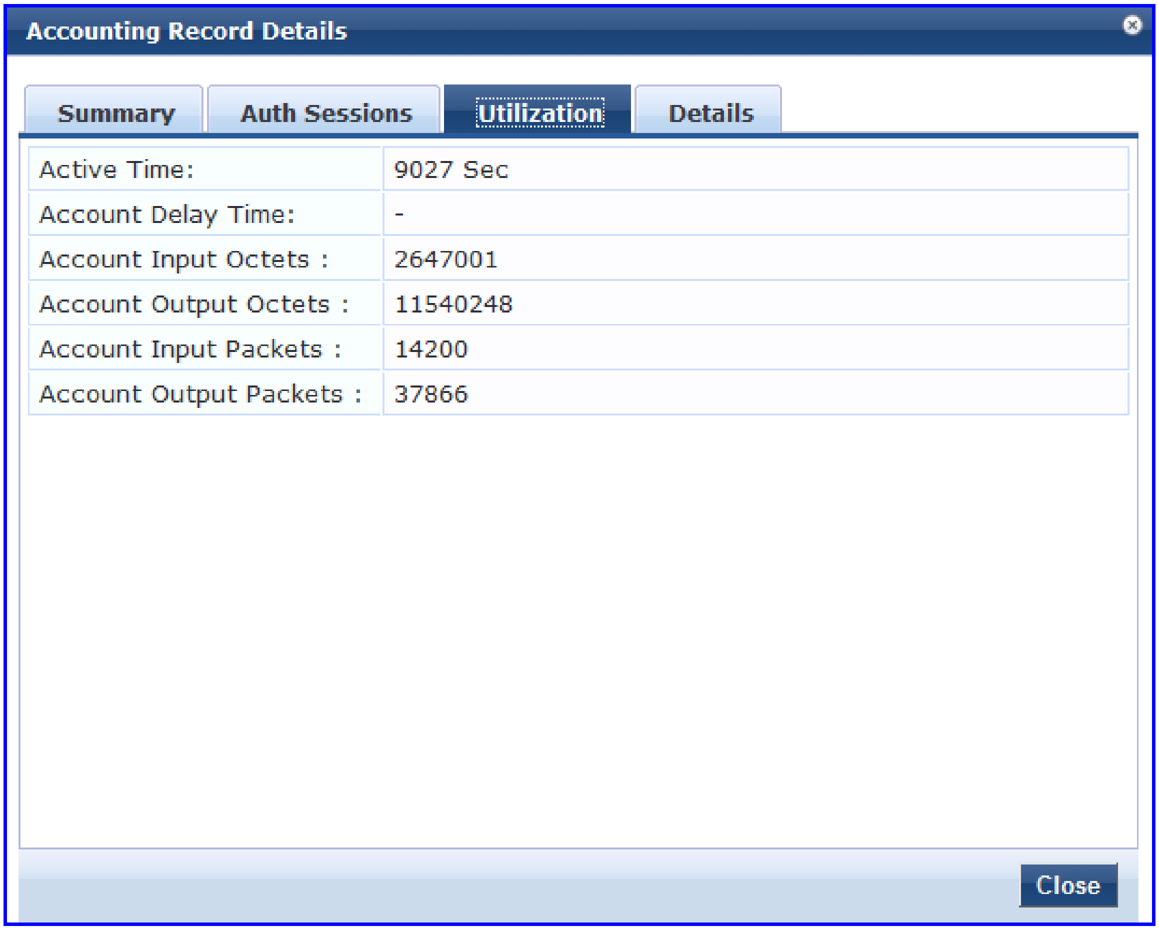
Parameter	Description
Number of Authentication Sessions	Specifies the total number of authentications (always 1) and authorizations in this session.
Authentication Sessions Details	
Session ID	Displays the Policy Manager session ID.
Type	Specifies the type of authentication: Initial authentication or reauthentication.
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** page:

Figure 80: *RADIUS Accounting Record Details > Utilization Page*



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

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

Table 43: *RADIUS Accounting Record Details > Utilization Tab Parameters*

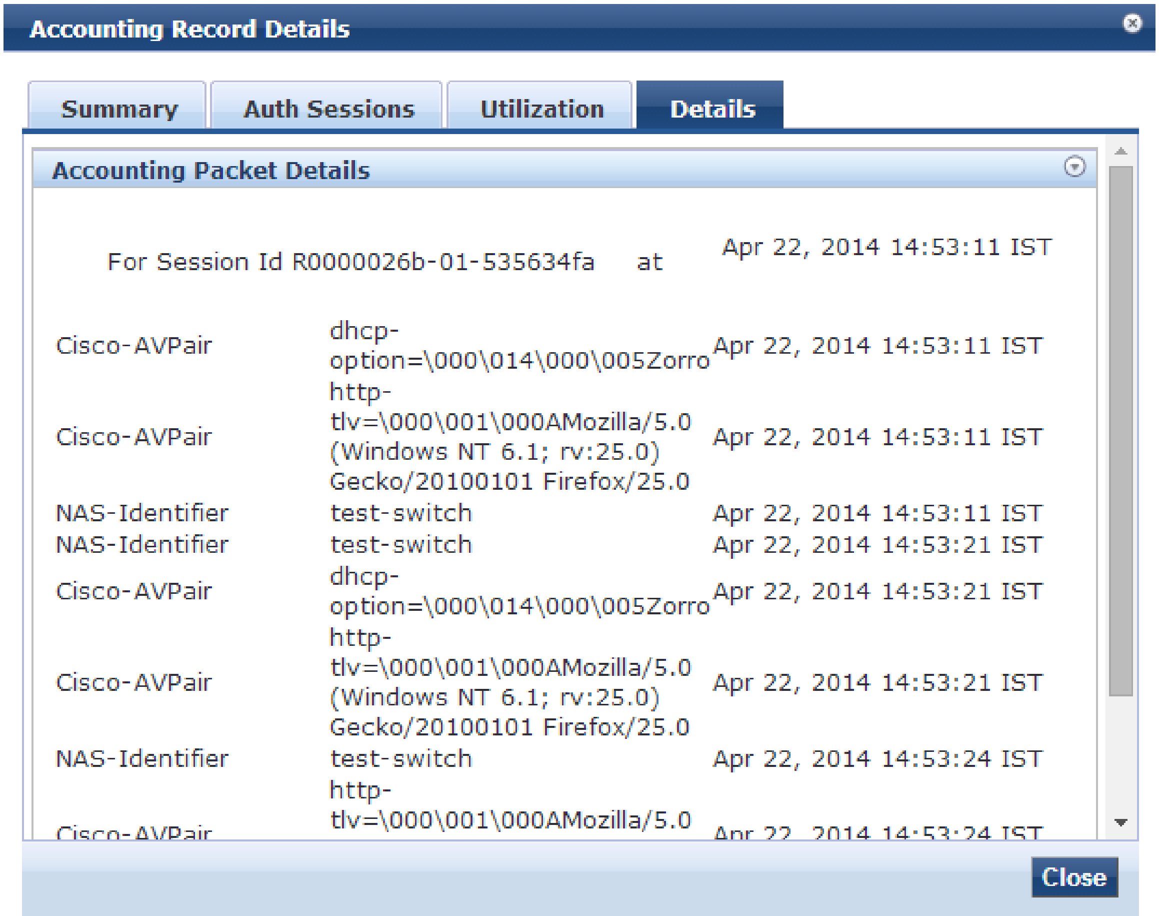
Parameter	Description
Active Time	Displays the duration of the session that was active.
Account Delay Time	Displays how many seconds the network device has been trying to send this record for (subtract from record time stamp to determine the time this record was actually generated by the device).
Account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

Figure 81: *RADIUS Accounting > Details Page*



For Session Id R0000026b-01-535634fa at Apr 22, 2014 14:53:11 IST

Cisco-AVPair	dhcp-option=\000\014\000\005Zorro	Apr 22, 2014 14:53:11 IST
Cisco-AVPair	http-tlv=\000\001\000AMozilla/5.0 (Windows NT 6.1; rv:25.0) Gecko/20100101 Firefox/25.0	Apr 22, 2014 14:53:11 IST
NAS-Identifier	test-switch	Apr 22, 2014 14:53:11 IST
NAS-Identifier	test-switch	Apr 22, 2014 14:53:21 IST
Cisco-AVPair	dhcp-option=\000\014\000\005Zorro	Apr 22, 2014 14:53:21 IST
Cisco-AVPair	http-tlv=\000\001\000AMozilla/5.0 (Windows NT 6.1; rv:25.0) Gecko/20100101 Firefox/25.0	Apr 22, 2014 14:53:21 IST
NAS-Identifier	test-switch	Apr 22, 2014 14:53:24 IST
Cisco-AVPair	http-tlv=\000\001\000AMozilla/5.0	Apr 22, 2014 14:53:24 IST

The following table summarizes the configuration information provided on the **RADIUS Accounting Record Details > Details** page:

Table 44: *RADIUS Accounting Record > Details Page Summary*

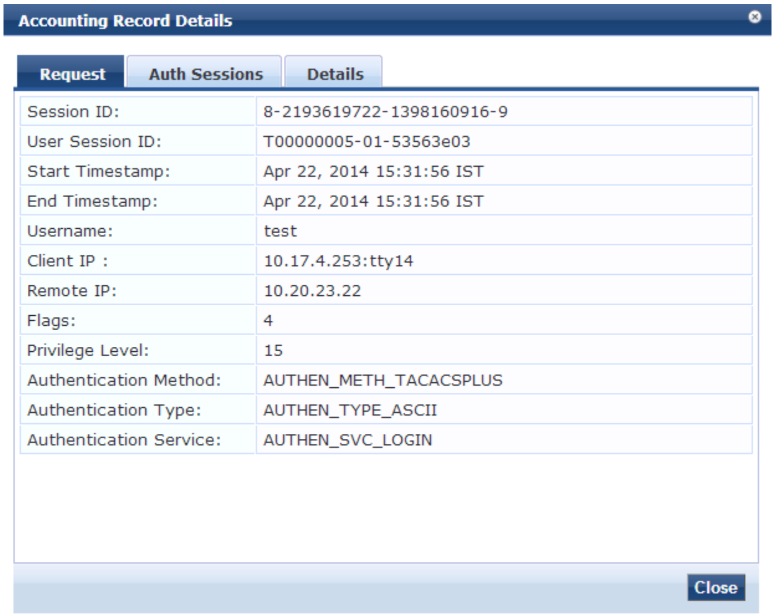
Parameter	Description
Accounting Packet Details	Shows the details of RADIUS attributes sent and received from the network device during an initial authentication and subsequent reauthentications. Each section in the **Details** page corresponds to a session in Policy Manager.

TACACS+ Accounting Record Details > Request Tab

When you navigate to the **Monitoring > Live Monitoring > Accounting** page and select a TACACS+ Accounting record, the **Accounting Record Details** page opens to the **Request** page.

The following figure displays the **TACACS+ Accounting Record Details** > **Request** page:

Figure 82: *TACACS+ Accounting Record Details > Request Page*



Session ID:	8-2193619722-1398160916-9
User Session ID:	T00000005-01-53563e03
Start Timestamp:	Apr 22, 2014 15:31:56 IST
End Timestamp:	Apr 22, 2014 15:31:56 IST
Username:	test
Client IP :	10.17.4.253:tty14
Remote IP:	10.20.23.22
Flags:	4
Privilege Level:	15
Authentication Method:	AUTHEN_METH_TACACSPLUS
Authentication Type:	AUTHEN_TYPE_ASCII
Authentication Service:	AUTHEN_SVC_LOGIN

The following table describes the configuration parameters on the **TACACS+ Accounting Record** > **Request** page:

Table 45: *TACACS+ Accounting Record Request Page Parameters*

Parameter	Description
Session ID	Specifies the **Session ID**, which is a unique ID associated with a request.
User Session ID	Specifies a session ID that correlates authentication, authorization, and accounting records.
Start and End Timestamp	Shows the start and end times of the session.
Username	Shows the username associated with this record.
Client IP	Shows the IP address and tty (text terminal) of the device interface.
Remote IP	Shows the IP address from which the Administrator is logged in.
Flags	Shows the identifier corresponding to starting, stopping, or updating the accounting record.
Privilege Level	Specifies the privilege level of the Administrator. The range is from **1** (lowest) to **15** (highest).

Table 45: *TACACS+ Accounting Record Request Page Parameters (Continued)*

Parameter	Description
Authentication Method	Identifies the authentication method used for network access.
Authentication Type	Identifies the authentication type used for network access.
Authentication Service	Identifies the authentication service used for network access.

TACACS+ Accounting Record Details > Auth Sessions Tab

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

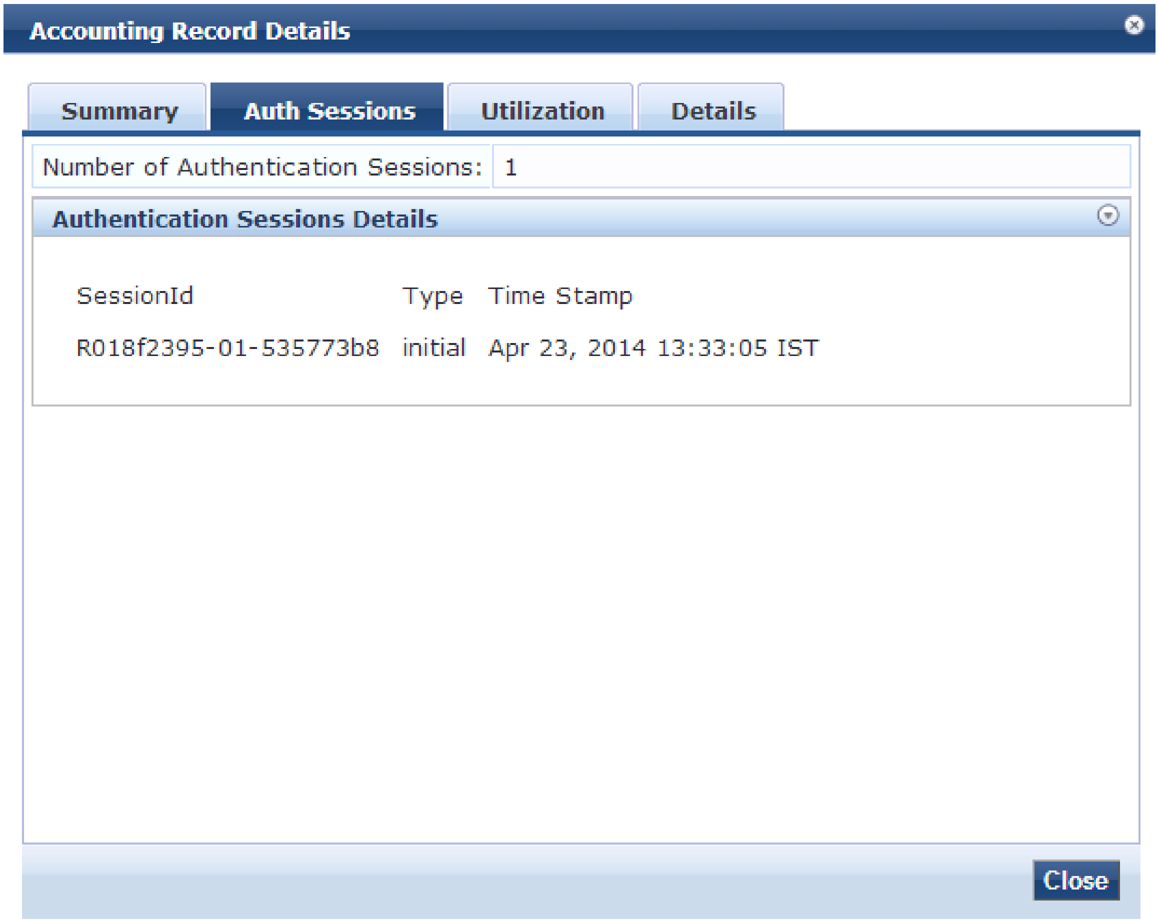
You can click any row in the **Accounting** page to display the corresponding **Accounting Record Details** page for the session.

1. Navigate to the **Monitoring > Live Monitoring > Accounting** page.
2. Select a TACACS+ Accounting record.

   The **Accounting Record Details** page opens.
3. To view the Authentication Sessions details, click the **Auth Sessions** tab.

   The following figure displays the **TACACS+ Accounting Record Details** > **Auth Sessions** page:

Figure 83: *TACACS+ Accounting Record Details > Auth Sessions Page*



Number of Authentication Sessions: 1

Authentication Sessions Details

SessionId	Type	Time Stamp
R018f2395-01-535773b8	initial	Apr 23, 2014 13:33:05 IST

The following table summarizes the information available on the **TACACS+ Accounting Record Details** > **Auth Sessions** page:

Table 46: *TACACS+ Accounting Record Details > Authentication Sessions Page 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** page for the TACACS+ protocol.

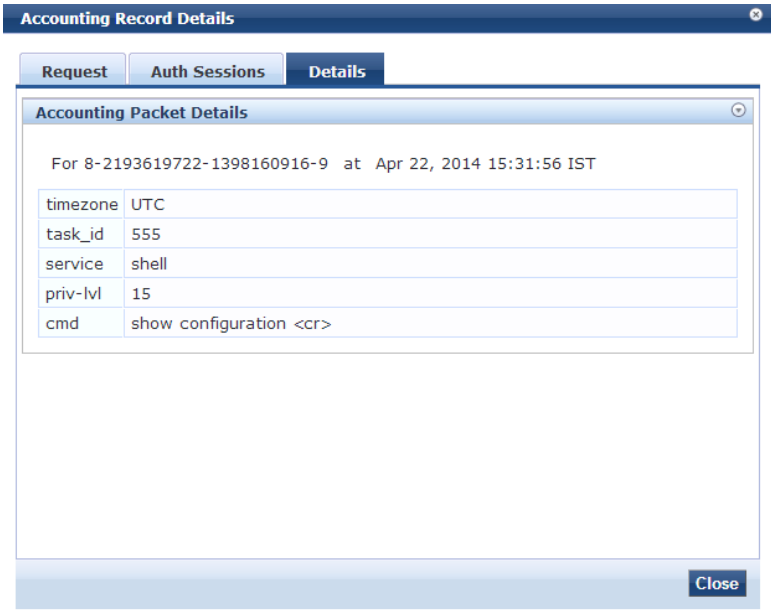
You can click any row in the **Accounting** page to display the corresponding **Accounting Record Details** page for the session.

1. Navigate to the **Monitoring > Live Monitoring > Accounting** page.
2. Select a TACACS+ Accounting record.

   The **Accounting Record Details** page opens.
3. To view the sessions details, click the **Details** tab.

The following figure displays the **TACACS+ Accounting Record Details** > **Details** page:

Figure 84: *TACACS+ Accounting Record Details > Details Page*



For 8-2193619722-1398160916-9 at Apr 22, 2014 15:31:56 IST

timezone	UTC
task_id	555
service	shell
priv-lvl	15
cmd	show configuration <cr>

The following table summarizes the configuration parameters provided on the **TACACS+ Accounting Record** > **Details** tab:

Table 47: *TACACS+ Accounting Record > Details Page Parameters*

Parameter	Description
Accounting Packet Details	Shows command typed (**cmd**), privilege level of the administrator executing the command (**priv-lvl**) and service (**shell**) for each authorization request, as well as the start time, task ID, and the time zone.

Live Monitoring: OnGuard Activity

This section provides the following information:

- About OnGuard Activity
- Bouncing an Agent Using Non-SNMP
- Bouncing a Client Using SNMP
- Broadcasting a Message to Active Endpoints
- Sending a Message to Selected Endpoints

About OnGuard Activity

The **OnGuard Activity** page shows the real-time status of all endpoints that have ClearPass OnGuard persistent agent.

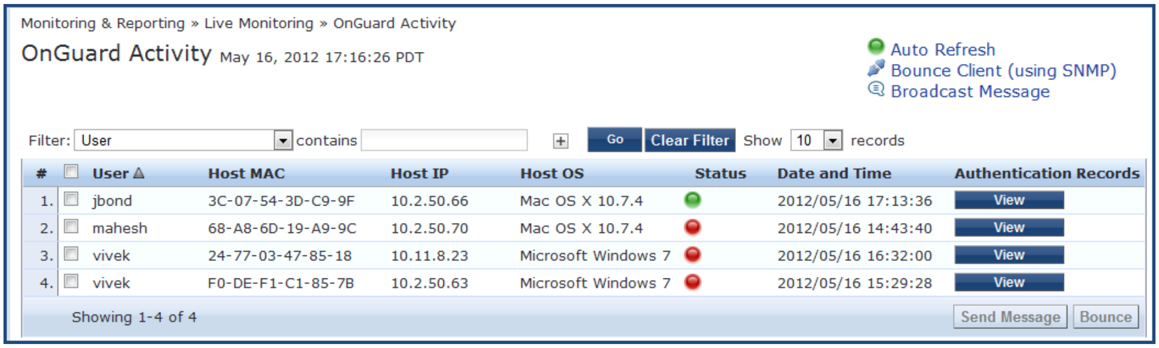
This page also presents configuration tools to bounce an endpoint and to send unicast or broadcast messages to all endpoints running the OnGuard agent.

To access the **OnGuard Activity** page:

1. Navigate to **Monitoring** > **Live Monitoring** > **OnGuard Activity**.

   The **OnGuard Activity** page opens:

Figure 85: *OnGuard Activity Page*



Monitoring & Reporting » Live Monitoring » OnGuard Activity

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

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

Showing 1-4 of 4

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

Table 48: *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 **Authentication Records** > **View** button to see the **Endpoint Authentication Details** page with the authentication records.

Bouncing an Agent Using Non-SNMP

This page is used to initiate a bounce on an endpoint's managed interface.

NOTE

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

Initiating a bounce on the managed interface on the endpoint results in creating tags for the specified endpoint in the **Endpoints** page (navigate to **Configuration** > **Identity** > **Endpoints**).

One or more of the following tags are created:

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

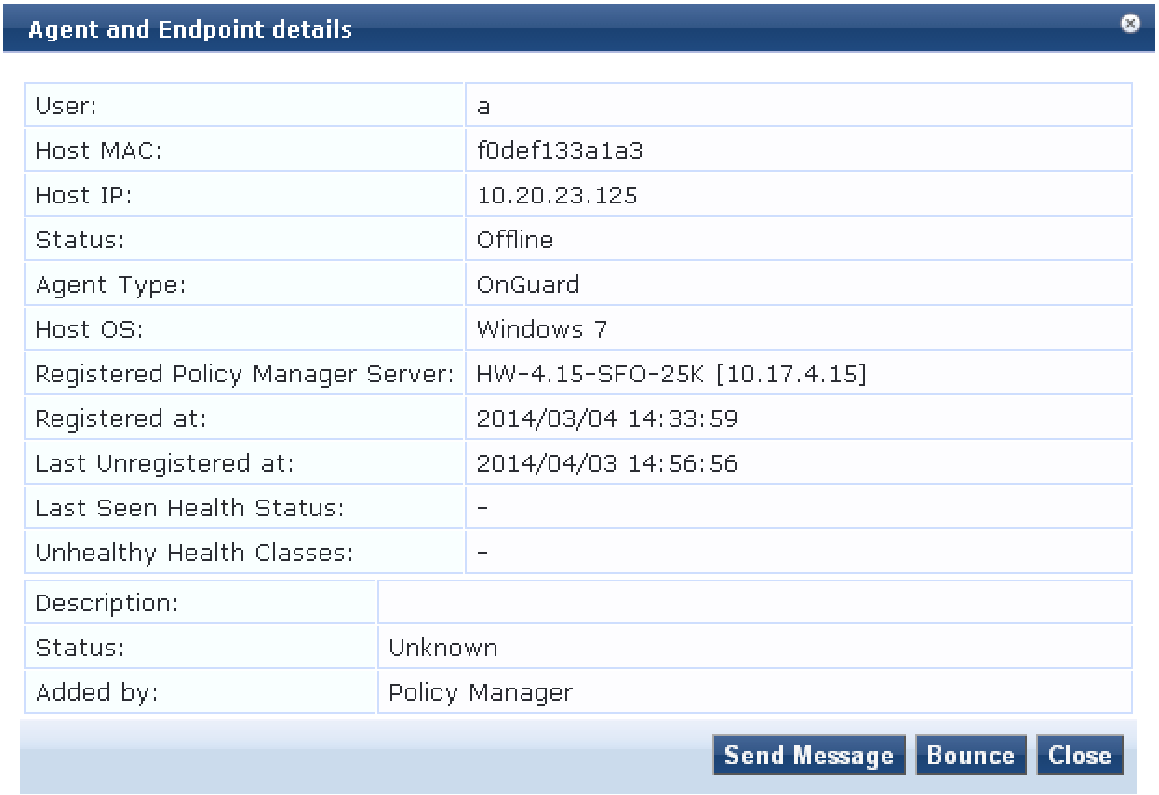
To bounce an agent:

1. Navigate to **Monitoring** > **OnGuard Activity**.

   The **OnGuard Activity** page opens.
2. Click a device listed on the **OnGuard Activity** page.

   The **Agent and Endpoint Details** page opens.

Figure 86: *Agent and Endpoint Details*



Agent and Endpoint details

User:	a
Host MAC:	f0def133a1a3
Host IP:	10.20.23.125
Status:	Offline
Agent Type:	OnGuard
Host OS:	Windows 7
Registered Policy Manager Server:	HW-4.15-SFO-25K [10.17.4.15]
Registered at:	2014/03/04 14:33:59
Last Unregistered at:	2014/04/03 14:56:56
Last Seen Health Status:	-
Unhealthy Health Classes:	-
Description:	
Status:	Unknown
Added by:	Policy Manager

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

Table 49: *Agent and Endpoint Details Parameters*

Parameter	Description
Host MAC	Displays the MAC address of the user.
Description	Optional description of the endpoint.
Status	Displays the status of the endpoint.
Added by	Displays the server name.
MAC Vendor	Vendor name and OS of the endpoint device.
OnGuard Details	
User	Displays the name 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.

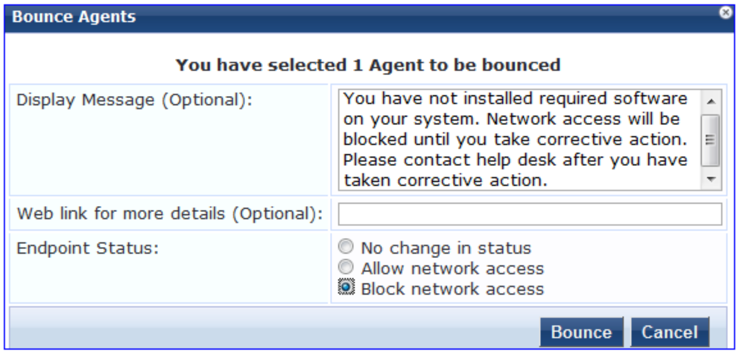
Table 49: *Agent and Endpoint Details Parameters (Continued)*

Parameter	Description
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.
Last Unregistered at	Displays the date and time at which the Policy Manager installation was last unregistered.
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.

3. Click **Bounce**.

   The **Bounce Agents** page opens.

Figure 87: *Bounce Agents Page*



Bounce Agents

You have selected 1 Agent to be bounced

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

Web link for more details (Optional):

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

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

Table 50: *Bounce Agents Page Parameters*

Parameter	Action/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.

Table 50: *Bounce Agents Page Parameters (Continued)*

Parameter	Action/Description
	- **Allow network access**: Allow network access by white-listing this endpoint. Clicking **Allow network access** sets the status of the endpoint as **Known**. **NOTE:** 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**. **NOTE:** You must configure **Enforcement Policy Rules** to allow access to the endpoints with the status **Disabled**.

Bouncing a Client Using SNMP

The **Bounce Client (using SNMP)** dialog is used to initiate a bounce operation using SNMP with wired Ethernet switches.

NOTE

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

Requirements

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

- The network device must be added to Policy Manager and SNMP read and write parameters must be configured.
  - For information about adding a network device to ClearPass Policy Manager, see Adding a Network Device on page 448.
  - For details about configuring SNMP settings, see SNMP Read Settings Parameters on page 450 and SNMP Write Settings Parameters on page 452.
- SNMP traps (link up and/or MAC notification) must be enabled on the switch port (see ClearPass SNMP Traps and OIDs on page 812 and SNMP Trap Details on page 814).
- The DHCP snooper service on a ClearPass server must receive DHCP packets from the endpoint to specify the IP address of the endpoint to bounce.
  - For information about configuring the **DhcpSnooper** service, see ClearPass Network Services Options on page 493.
  - For information about configuring the IP helper address, see DHCP Collector on page 437.

Bouncing a Client

To bounce a client using SNMP:

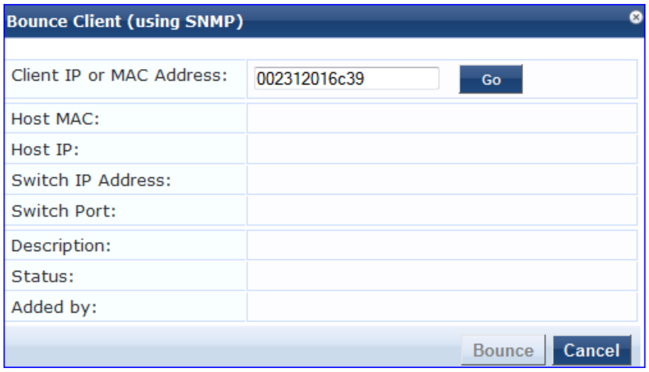
1. Navigate to **Monitoring** > **OnGuard Activity**.

   The **OnGuard Activity** page opens.

2. Click the **Bounce Client (using SNMP)** link on the top-right of the **OnGuard Activity** page.

   The **Bounce Client (using SNMP)** dialog opens.

Figure 88: *Bounce Client (Using SNMP) Dialog*



Bounce Client (using SNMP)

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

3. Enter the client IP or MAC Address.
4. Click **Go**, then click **Bounce**.

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

Table 51: *Bounce Client (Using SNMP) Page Parameters*

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

Broadcasting a Message to Active Endpoints

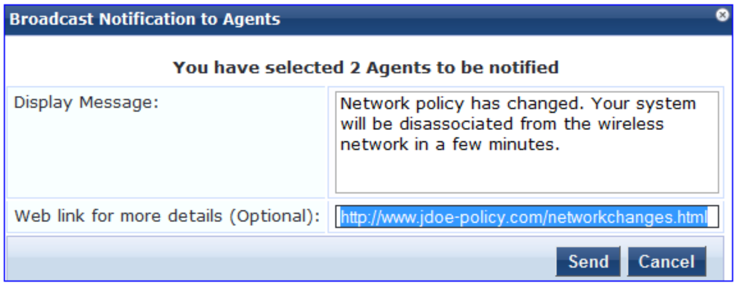
To broadcast a message to selected active endpoints:

1. Navigate to **Monitoring** > **OnGuard Activity**.

   The **OnGuard Activity** page opens.
2. Select the endpoint(s) that you want to broadcast to.
3. Click the **Broadcast Message** link on the top-right of the **OnGuard Activity** page.

   The **Broadcast Notification to Agents** dialog opens.

Figure 89: *Broadcast Notification to Agents Dialog*


Broadcast Notification to Agents

You have selected 2 Agents to be notified

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

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

4. **Display Message**: Enter the text of the message you want to send to the selected active endpoints.
5. **Web link**: Optionally, enter a URL to be included with the **Display Message**.
6. Click **Send**.

Sending a Message to Selected Endpoints

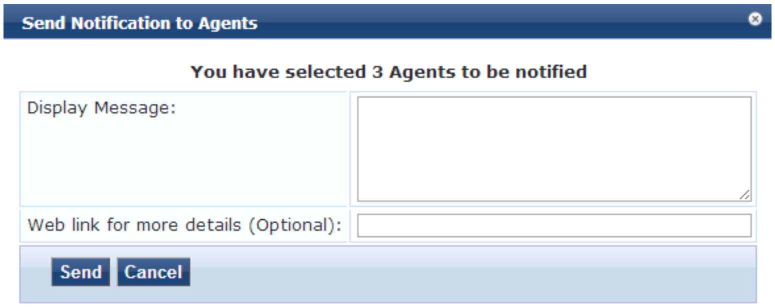
To send a message to selected endpoints:

1. Navigate to **Monitoring** > **OnGuard Activity**.

   The **OnGuard Activity** page opens.
2. Select one or more devices listed on the **OnGuard Activity** page.
3. Click the **Send Message** button.

   The **Send Notification to Agents** dialog opens.

Figure 90: *Send Notifications to Agents*


Send Notification to Agents

You have selected 3 Agents to be notified

Display Message:

Web link for more details (Optional):

4. **Display Message**: Enter a message to be sent to the selected endpoints
5. **Web link**: Optionally, enter a URL to be included with the message.
6. Click **Send**.

Live Monitoring: Analysis and Trending

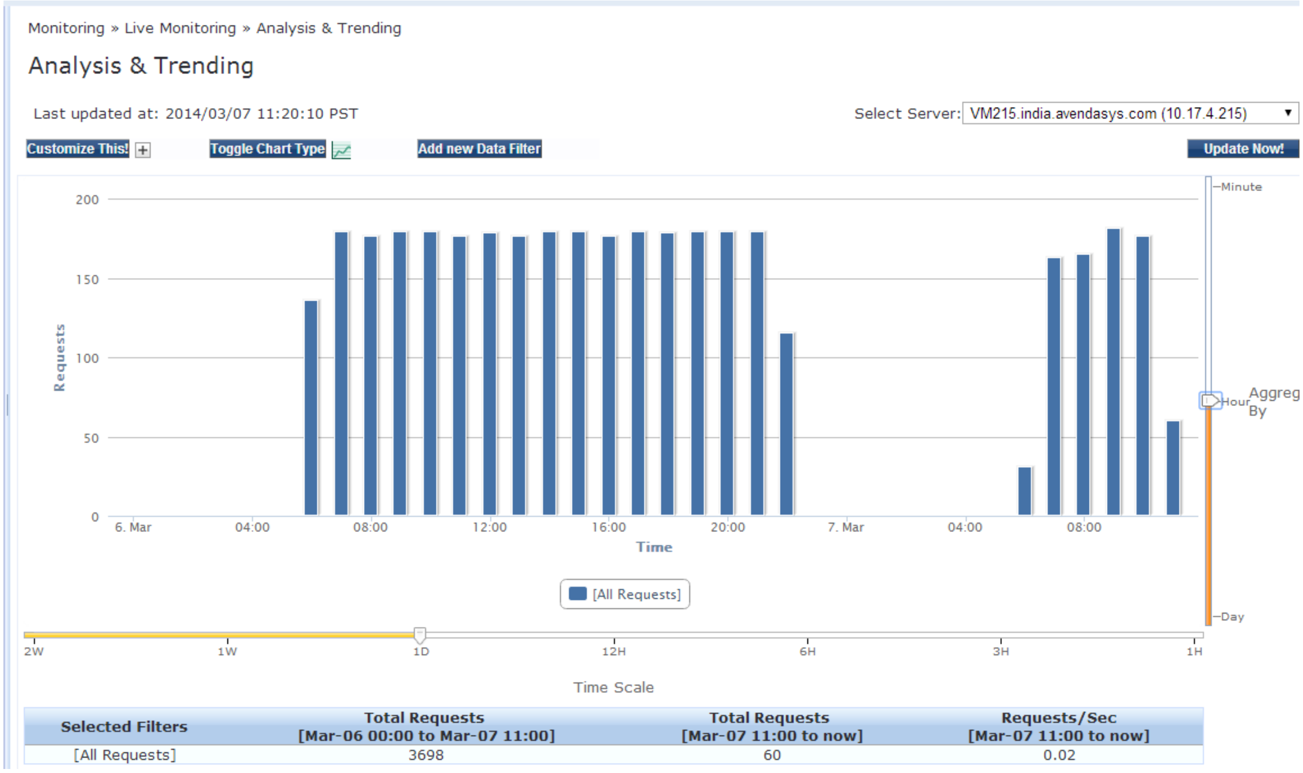
The **Analysis and Trending** page displays requests for the subset of components included in the selected filters over a selected time period: one month, two weeks, one week, one day, 12 hours, 6 hours, 3 hours, or one hour.

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 Access Tracker (see Live Monitoring: Access Tracker on page 99) that shows session data for the specific time-slice and for the specific requests.

To access this page, navigate to **Monitoring** > **Live Monitoring** > **Analysis and Trending**.

Figure 91: *Analysis and Trending*



Monitoring » Live Monitoring » Analysis & Trending

Analysis & Trending

Last updated at: 2014/03/07 11:20:10 PST

Select Server: VM215.india.avendasys.com (10.17.4.215)

Selected Filters	Total Requests [Mar-06 00:00 to Mar-07 11:00]	Total Requests [Mar-07 11:00 to now]	Requests/Sec [Mar-07 11:00 to now]
[All Requests]	3698	60	0.02

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

Component	Action/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 four filters.
Toggle Chart Type	Click to toggle the 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 153.

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 two minutes. You can see the last updated time in the **Last updated at** field in the **System Monitor** page.

- System Monitor Page
- Process Monitor Page

- Network Monitor Page
- ClearPass Monitor Page

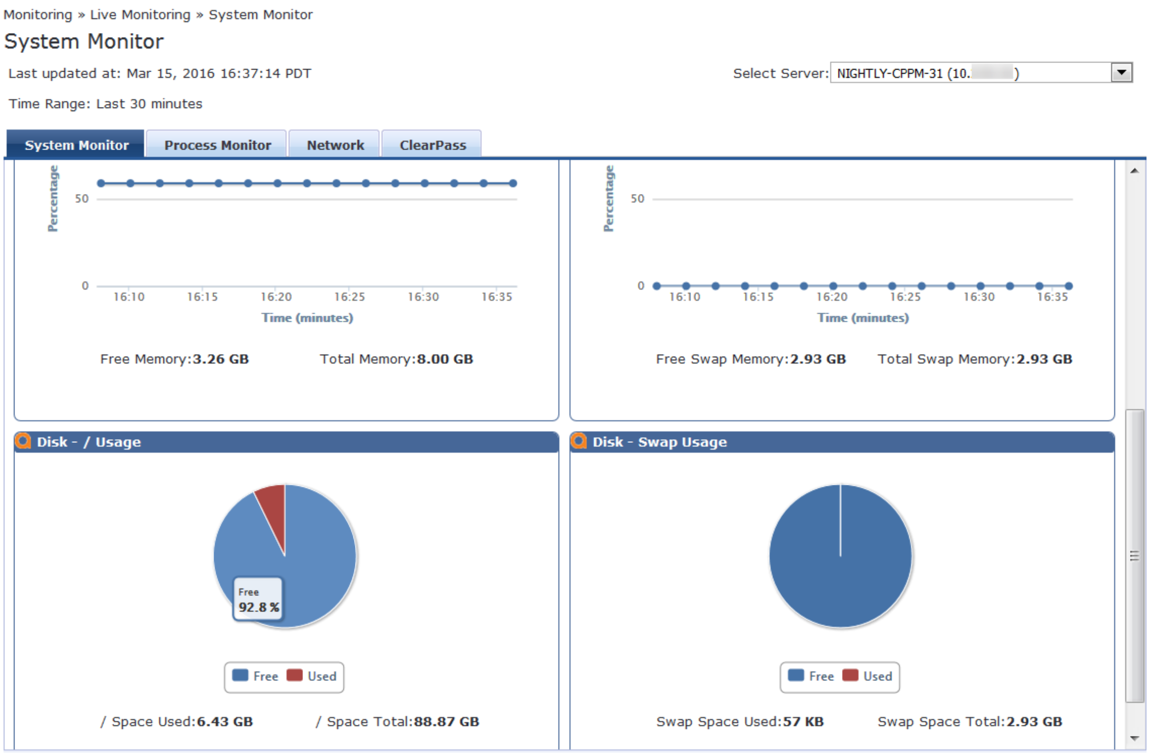
System Monitor Page

The **System Monitor** page displays charts and graphs that display information about CPU load, CPU usage, memory usage, and disk usage for the selected ClearPass server.

To access the **System Monitor** page for the selected ClearPass server:

1. Navigate to **Monitoring > Live Monitoring > System Monitor**.
2. From the **Select Server** drop-down, select the desired ClearPass server.

Figure 92: *System Monitor Page*



Monitoring » Live Monitoring » System Monitor

System Monitor

Last updated at: Mar 15, 2016 16:37:14 PDT

Select Server: NIGHTLY-CPPM-31 (10.[redacted])

Time Range: Last 30 minutes

Free Memory:**3.26 GB** Total Memory:**8.00 GB**

Free Swap Memory:**2.93 GB** Total Swap Memory:**2.93 GB**

/ Space Used:**6.43 GB** / Space Total:**88.87 GB**

Swap Space Used:**57 KB** Swap Space Total:**2.93 GB**

Table 52: *System Monitor Page Report Widgets*

Widget	Description
CPU Usage	Percentage of CPU usage for the following: **System**, **User**, **I/O Wait**, and **Idle** time.
CPU Load	Percentage of CPU load averages in increments of 1, 5, and 15 minutes.
Memory Usage	Percentage of free and total memory in Gigabytes.
Swap Memory Usage	Percentage of free and total swap memory in Gigabytes.
Disk - Usage	Percentage of used and free disk space.
Disk - Swap Usage	Percentage of used and total swap space.

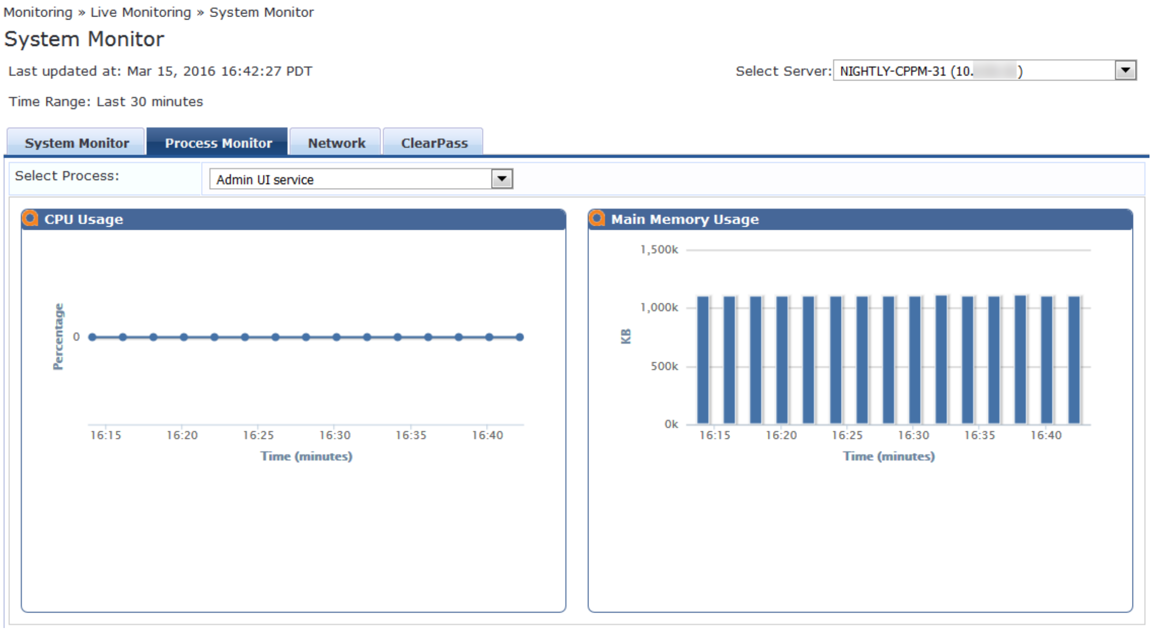
Process Monitor Page

The **Process Monitor** page displays CPU Usage and Main Memory Usage for a selected process or service.

To access the Process Monitor page:

1. Navigate to **Monitoring** > **Live Monitoring** > **System Monitor** > **Process Monitor**.

Figure 93: *System Monitoring: Process Monitor Page*



Monitoring » Live Monitoring » System Monitor

System Monitor

Last updated at: Mar 15, 2016 16:42:27 PDT

Select Server: NIGHTLY-CPPM-31 (10.[redacted])

Time Range: Last 30 minutes

Select Process: Admin UI service

2. To view CPU Usage and Main Memory usage for the selected process or service, click the **Select Process** drop-down list.
3. Select one of the following options :
   - Admin UI service
   - AirGroup notification service
   - Apache web server
   - Async DB write service
   - Async network services
   - ClearPass IPsec service
   - DB change notification server
   - DB replication service
   - Domain service
   - Extensions service
   - Ingress logger service
   - Ingress logrepo 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

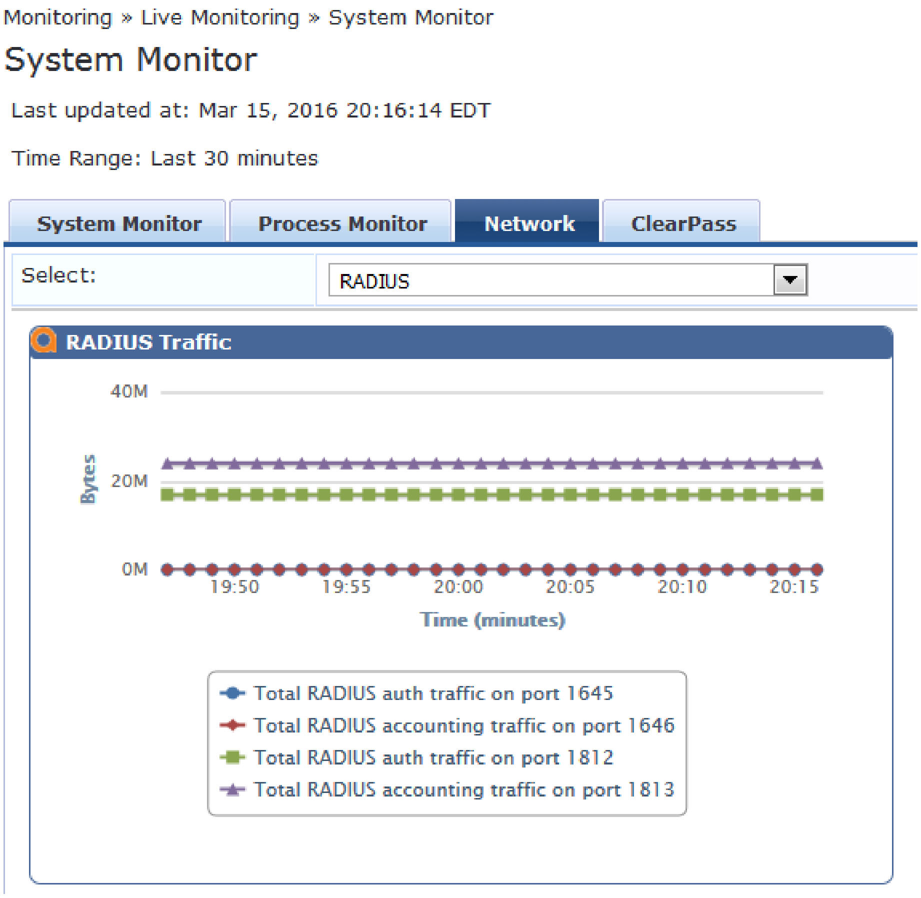
Network Monitor Page

The **Network Monitor** page displays information about the selected network traffic type.

To access the **Network Monitor** page:

1. Navigate to **Monitoring** > **Live Monitoring** > **System Monitor** > **Network** tab.
2. From the **Select** drop-down, select the desired traffic type.

Figure 94: *Network Monitor Page*



Monitoring » Live Monitoring » System Monitor

System Monitor

Last updated at: Mar 15, 2016 20:16:14 EDT

Time Range: Last 30 minutes

Select: RADIUS

System Monitor
Process Monitor
Network
ClearPass
RADIUS Traffic
40M
20M
0M
Bytes
19:50
19:55
20:00
20:05
20:10
20:15
Time (minutes)
Total RADIUS auth traffic on port 1645
Total RADIUS accounting traffic on port 1646
Total RADIUS auth traffic on port 1812
Total RADIUS accounting traffic on port 1813

The **Network Monitor** page displays network activity (in bytes) for the following traffic types:

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

ClearPass Monitor Page

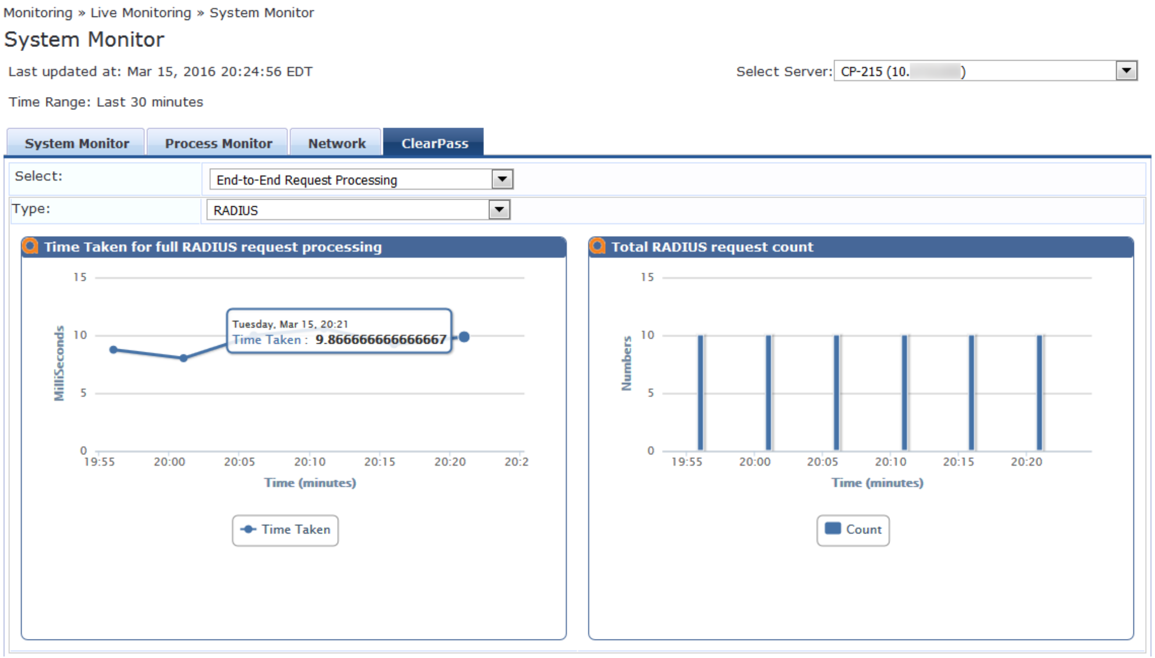
The **ClearPass** Monitoring page displays performance monitoring counters and timers for the last 30 minutes of activity for the following ClearPass components:

- 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

To access the **ClearPass Monitor** page:

1. Navigate to **Monitoring** > **Live Monitoring** > **System Monitor > ClearPass** tab.
2. Click the **Select** drop-down.
3. Select the desired ClearPass performance monitoring counter.

Figure 95: *System Monitoring: ClearPass Monitor Page*



Monitoring » Live Monitoring » System Monitor

System Monitor

Last updated at: Mar 15, 2016 20:24:56 EDT

Select Server: CP-215 (10.[redacted])

Time Range: Last 30 minutes

System Monitor | Process Monitor | Network | ClearPass

Select: End-to-End Request Processing

Type: RADIUS

Profiler and Discovery

This section provides the following information:

- Profiler and Discovery: Endpoint Profiler
- Profiler and Discovery: Network Discovery

Profiler and Discovery: Endpoint Profiler

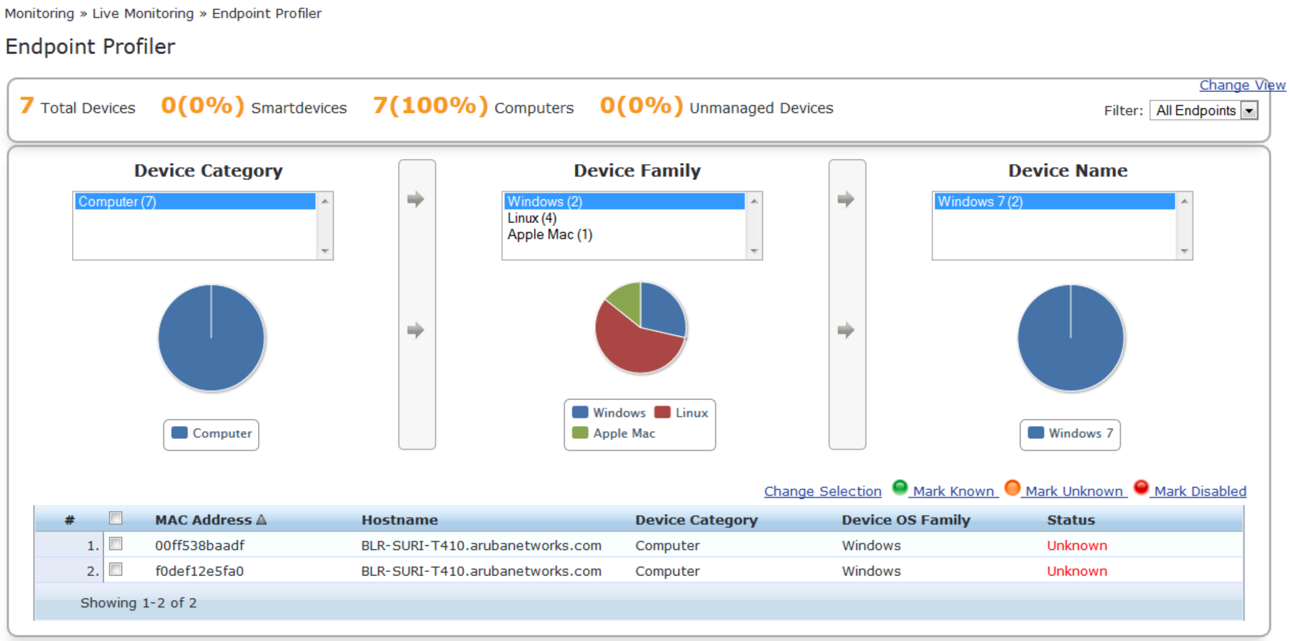
If the Profile license is enabled, a list of the profiled endpoints are visible in the **Endpoints Profiler** page.

1. To access the Endpoint Profiler, navigate to the **Monitoring > Profiler and Discovery > Endpoint Profiler** page.

   The list of endpoints you view is based on the **Device Category**, **Device Family**, and **Device Name** items that you selected.

   Figure 96 shows an example of the graphs available on the **Endpoint Profiler** page:

Figure 96: *Endpoint Profiler Page*



Monitoring » Live Monitoring » Endpoint Profiler

Endpoint Profiler

7 Total Devices 0(0%) Smartdevices 7(100%) Computers 0(0%) Unmanaged Devices

Change View

Filter: All Endpoints

Change Selection Mark Known Mark Unknown Mark Disabled

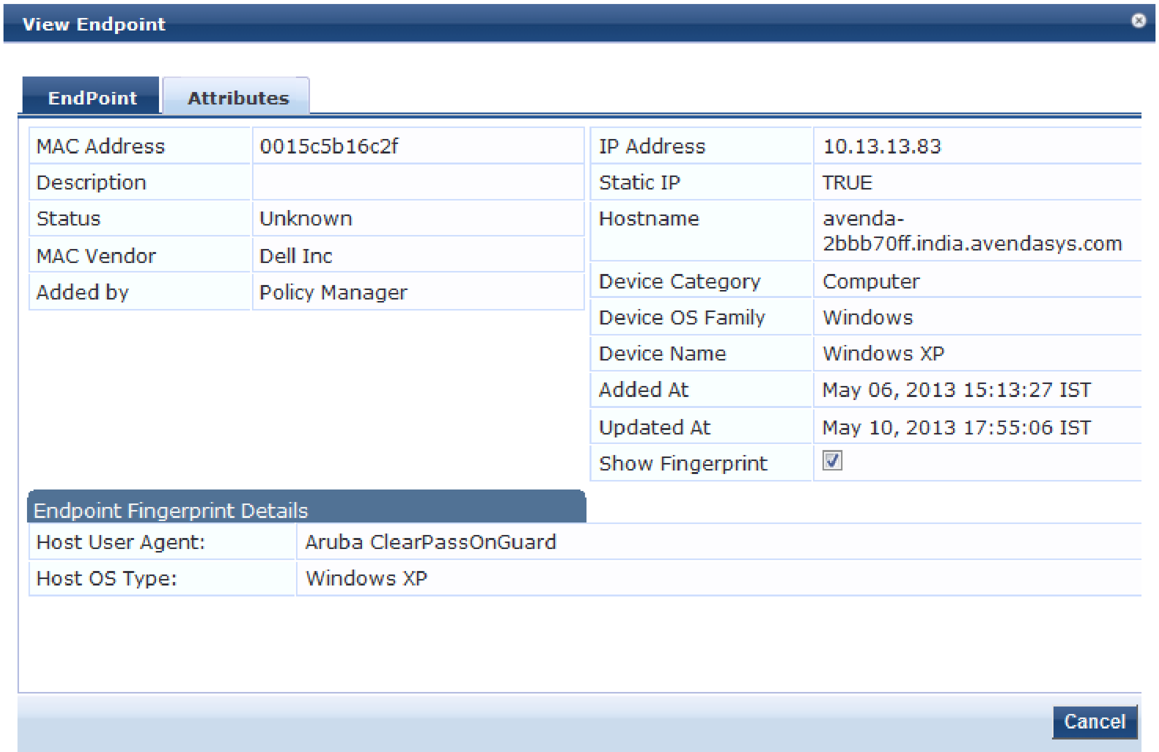
#	□	MAC Address	Hostname	Device Category	Device OS Family	Status
1.	□	00ff538baadf	BLR-SURI-T410.arubanetworks.com	Computer	Windows	Unknown
2.	□	f0def12e5fa0	BLR-SURI-T410.arubanetworks.com	Computer	Windows	Unknown

Showing 1-2 of 2

2. To modify the selection criteria used to list the devices, click **Change Selection**.
3. To see graphs that show information about distribution and update frequency for devices and computers, click **Change View**.
4. To view endpoint details about a specific device, click a device in the table below the graphs.

   The **Endpoint Profiler Details** > **Endpoint** page opens:

Figure 97: *Endpoint Profiler Details*



MAC Address	0015c5b16c2f	IP Address	10.13.13.83
Description		Static IP	TRUE
Status	Unknown	Hostname	avenda-2bbb70ff.india.avendasys.com
MAC Vendor	Dell Inc	Device Category	Computer
Added by	Policy Manager	Device OS Family	Windows
		Device Name	Windows XP
		Added At	May 06, 2013 15:13:27 IST
		Updated At	May 10, 2013 17:55:06 IST
		Show Fingerprint	☑

Endpoint Fingerprint Details

Host User Agent:	Aruba ClearPassOnGuard
Host OS Type:	Windows XP

5. To return to the **Endpoint Profiler** page, select the **Cancel** button.

Profiler and Discovery: Network Discovery

This section provides the following information:

- About Network Discovery
- Adding the Configurations to Query Seed Devices
- SNMP Credentials Configuration
- SSH Credentials Configuration
- SSH Credentials Configuration
- WMI Credentials Configuration
- Initiating a Network Discovery Scan
- About Auto-Refresh
- Importing and Viewing Discovered Network Devices
- Viewing Discovered Endpoints
- Configuring Nmap-Based Endpoint Port Scans

About Network Discovery

Network Discovery uses a configured *seed network device* (typically a switch, router, or controller) to discover endpoints and network devices.

The following information is read from the seed device:

- SNMP information

An SNMP description is necessary for discovering and profiling the network devices. For more information, see SNMP Credentials Configuration on page 135.

- SSH credentials

  For Linux server or network device discovery, specify SSH configuration credentials. For more information, see SSH Credentials Configuration on page 137.

- WMI credentials

  For Windows device discovery, specify WMI (Windows Management Instrumentation) credentials. For more information, see WMI Credentials Configuration on page 139.

- Connected endpoints

  Information about endpoints connected to the network device (typically MAC addresses of endpoints connected to switch ports). These are added as discovered endpoints. For more information, see Viewing Discovered Endpoints on page 146.

- ARP table

  Profiler supports Address Resolution Protocol (ARP) probes for network discovery scans. When this option is enabled, the scan will now also probe all available ARP entries. The ARP table provides information about MAC address > IP associations for endpoints that were recently seen by this device. These endpoints are probed further in an attempt to profile those devices. For more information, see Viewing Discovered Endpoints on page 146.

- Neighbor network devices

  Other network devices connected to the seed device as determined by neighbor discovery protocols such as Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) (if enabled in your network).

  Each of the discovered neighbor network devices are further queried as seed devices; this is repeated for multiple levels in your network up to a specified scan depth. For more information, see Viewing Details on a Discovered Device on page 145.

- Services and processes running on an Endpoint

  During the subnet scan, Network Discovery and the OnConnect domain-joined Windows client will be queried to retrieve all the services and processes running on the endpoint. This information will be displayed in the ClearPass Insight Endpoint reports.

Network Discovery High-Level Tasks

Configuring Network Discovery consists of these major tasks:

1. Add the configurations (SNMP, SSH, or WMI) needed to query all the devices in the target network.
2. Initiate a network discovery scan.
3. Import the discovered network devices into ClearPass.
4. Review the set of discovered devices and view the connected endpoints and neighbors.

Adding the Configurations to Query Seed Devices

You must configure SNMP, SSH, and WMI credentials for the devices that you want to discover as part of the network scan. These credentials are used during Network Discovery or an On-Demand subnet scan to profile Linux servers and machines (SSH credentials), Windows servers and machines (WMI credentials), and network devices (SNMP).

SNMP Credentials Configuration

For network device discovery, specify SNMP Read credentials. An SNMP-based scan sends an SNMP request to retrieve the network device information.

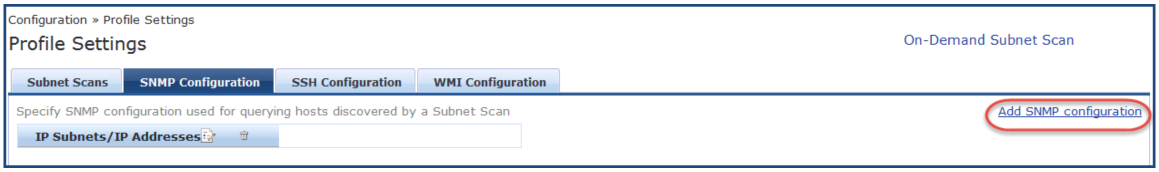
To add the SNMP configuration:

1. Navigate to **Configuration** > **Profile Settings**, then select the **SNMP Configuration** tab.

   The **Profile Settings** > **SNMP Configuration** page opens.

2. Click the **SNMP Configuration** tab.

Figure 98: *Adding an SNMP Configuration*

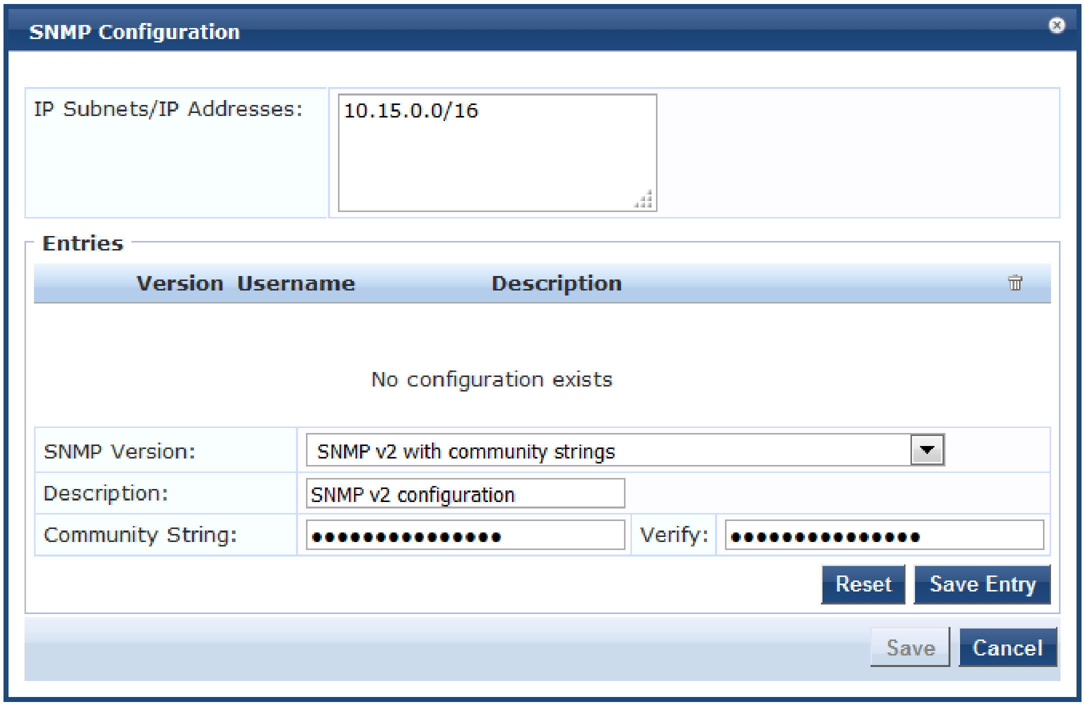


Specify SNMP configuration used for querying hosts discovered by a Subnet Scan

3. Click **Add SNMP Configuration.**

   The SNMP Configuration dialog opens.

Figure 99: *SNMP Configuration Dialog*



IP Subnets/IP Addresses: 10.15.0.0/16

No configuration exists

SNMP Version: SNMP v2 with community strings

Description: SNMP v2 configuration

Community String: ●●●●●●●●●●●●●●● Verify: ●●●●●●●●●●●●●●●

4. Specify the **SNMP Configuration** parameters as described in Table 53. When finished, click **Save Entry**, then click **Save**.

Table 53: *SNMP Configuration Parameters*

Field	Action/Description
IP Subnets/ IP Addresses	1. Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas. When you initiate the network discovery scan, ClearPass will use the SNMP configuration to fetch the network device information for discovered devices.
SNMP Version	2. From the drop-down, select the appropriate SNMP version.
Description	3. Optionally, enter a description of this SNMP configuration (recommended).

Table 53: *SNMP Configuration Parameters (Continued)*

Field	Action/Description
Community String	4. Enter the community string, then reenter the community string in the **Verify** field.

SSH Credentials Configuration

For Linux server or network device discovery, specify SSH (Secure Shell) configuration credentials. When SSH is found for an IP address or subnet, Network Discovery looks for any Linux server or machine associated with that IP address or subnet.

You can configure multiple user names and passwords. These credentials are organized in the order in which they were created.

To configure SSH credentials for a network discovery scan:

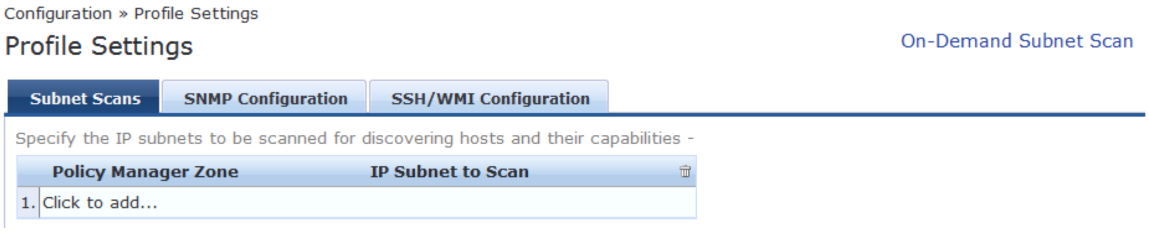
NOTE

The SSH configuration can be for a single IP address or a subnet. These credentials are used when an SSH scan is initiated.

1. Navigate to **Configuration** > **Profile Settings**.

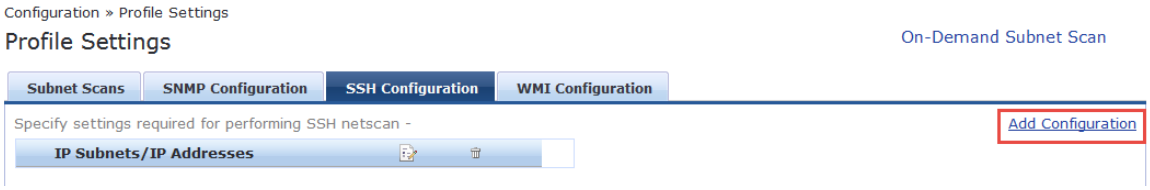
   The **Profile Settings** page opens.

Figure 100: *Profile Settings Page*



2. Select the **SSH Configuration** tab.

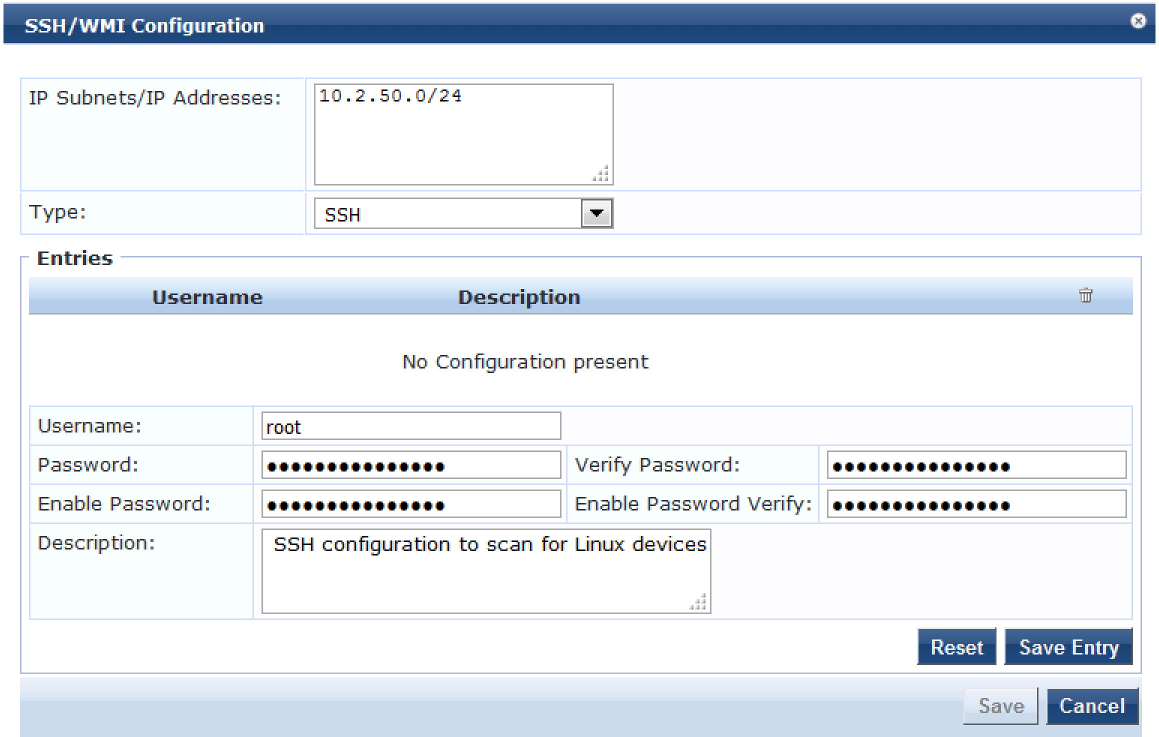
Figure 101: *SSH Configuration Tab*



3. Click **Add Configuration**.

   The **SSH Configuration** page opens.

Figure 102: *SSH Configuration Page*



SSH/WMI Configuration

IP Subnets/IP Addresses:	10.2.50.0/24
Type:	SSH

Entries

Username	Description
No Configuration present	

Username:	root		
Password:	•••••••••••••••	Verify Password:	•••••••••••••••
Enable Password:	•••••••••••••••	Enable Password Verify:	•••••••••••••••
Description:	SSH configuration to scan for Linux devices		

4. Specify the parameters in the **SSH Configuration** dialog as described in the following table, then click **Save Entry**.

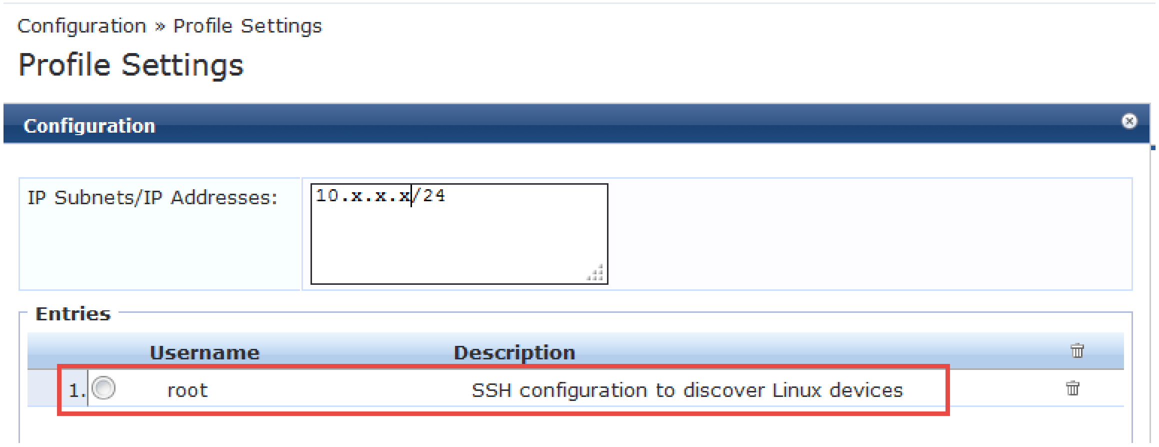
Table 54: *SSH Configuration Parameters*

Field	Action/Description
IP Subnets/ IP Addresses	1. Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas.
Username	2. Enter the username for the device or subnet specified.
Password	3. Enter the password for the device or subnet specified.
Enable Password	4. Enter the Enable password, then reenter the password in the **Enable Password Verify** field.
Description	5. Optionally, enter a description of this SNMP configuration (recommended).

6. Repeat this procedure for additional entries if needed.
7. When finished, click **Save**.

   You return to the **Profile Settings** page, where you can see that the SSH configuration has been added successfully (see Figure 103).

Figure 103: *SSH Configuration Added Successfully*



IP Subnets/IP Addresses: 10.x.x.x/24

Entries

	Username	Description	
1. ○	root	SSH configuration to discover Linux devices	

WMI Credentials Configuration

For Windows device discovery, specify WMI (Windows Management Instrumentation) configuration credentials. WMI configuration is necessary to discover Windows systems and device fingerprint details.

WMI a key part of the Windows operating system. It is used to gather system statistics, monitor system health, and manage system components. To work properly, WMI relies on the WMI service. This service must be running and properly configured for your environment.

For WMI, the login format for **username** is usually **domain\username**. Whatever domain you provide, it will be prepended to the username before logging into that machine.

Suppose you have provided an IP subnet address:

- ClearPass first checks to see if WMI is configured for that subnet/IP address.
- If WMI is configured, ClearPass checks to see if port 135 is open.
- If port 135 is open, ClearPass attempts the WMI login with those credentials.

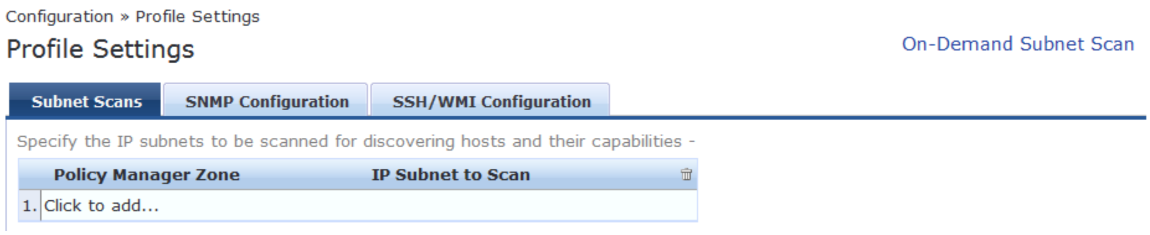
  If you provide just one IP address, the WMI login is performed for that particular IP address only.

To configure WMI credentials for a network discovery scan:

1. Navigate to **Configuration** > **Profile Settings**.

   The **Profile Settings** page opens.

Figure 104: *Profile Settings Page*

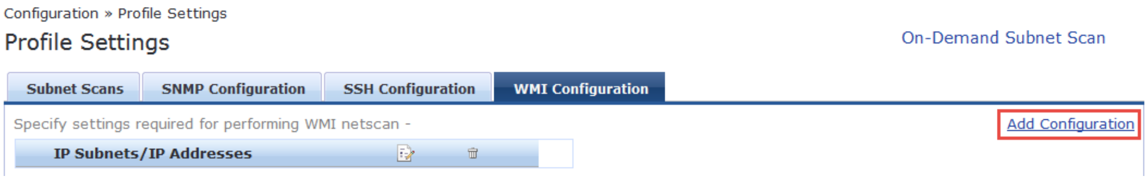


Specify the IP subnets to be scanned for discovering hosts and their capabilities -

	Policy Manager Zone	IP Subnet to Scan
1.	Click to add...	

2. Select the **WMI Configuration** tab.

Figure 105: *WMI Configuration Tab*



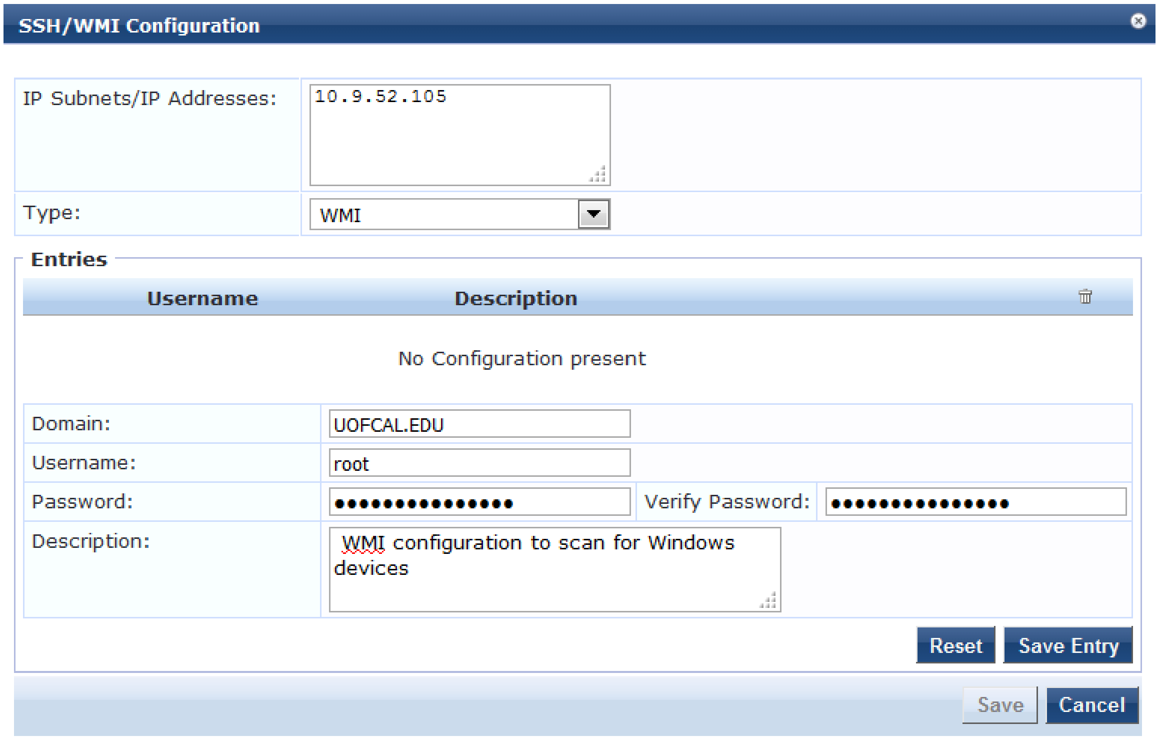
Specify settings required for performing WMI netscan -

IP Subnets/IP Addresses

3. Click **Add Configuration**.

   The **WMI Configuration** page opens.

Figure 106: *WMI Configuration Page*



IP Subnets/IP Addresses: 10.9.52.105

Type: WMI

Entries

Username	Description
No Configuration present	

Domain: UOFCAL.EDU

Username: root

Password: ●●●●●●●●●●●●●●● Verify Password: ●●●●●●●●●●●●●●●

Description: WMI configuration to scan for Windows devices

4. Specify the **WMI Configuration** parameters as described in Table 55, then click **Save Entry**.

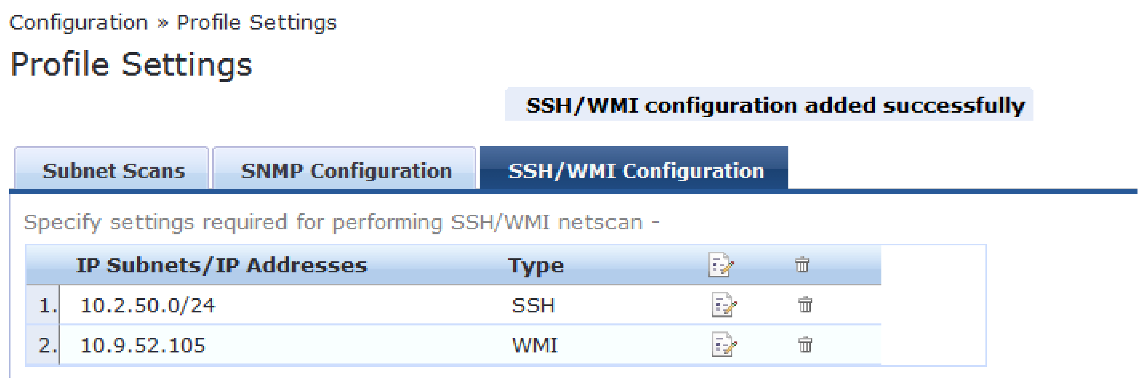
Table 55: *WMI Configuration Parameters*

Field	Action/Description
IP Subnets/ IP Addresses	1. Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas. **NOTE:** The WMI configuration can be for a single IP address or a subnet. These credentials are used when a WMI scan is initiated.
Domain	2. Enter the name of the Windows domain for logging into the device(s) that you are scanning.
Username	3. Enter the username for the device or subnet specified.
Password	4. Enter the password for the device or subnet specified.
Description	5. Optionally, enter a description of this SNMP configuration (recommended).

6. Repeat this procedure for additional entries if needed.
7. When finished, click **Save**.

   You return to the **Profile Settings** page, where you can see that the WMI configuration has been added successfully (see Figure 107).

Figure 107: *WMI Configuration Added Successfully*



Configuration » Profile Settings

Profile Settings

SSH/WMI configuration added successfully

Specify settings required for performing SSH/WMI netscan -

	IP Subnets/IP Addresses	Type		
1.	10.2.50.0/24	SSH		
2.	10.9.52.105	WMI		

Initiating a Network Discovery Scan

Seed devices are the initial IP addresses provided by the network administrator to start the network scan. When you initiate a network discovery scan and specify the seed devices, network discovery uses SNMP to:

- Find any other devices connected to the seed devices.
- Profile the connected devices.
- ClearPass uses that information to detect more devices in the network. The network discovery scan will proceed to the network depth specified by the **Scan Depth** parameter (described in Table 56 below).
- You can go to those devices and see their neighbor devices.

CAUTION

Running a network discovery scan on seed devices is a time- and resource-consuming operation. Depending on the number of devices associated with the seed device, a complete scan can take more than an hour.

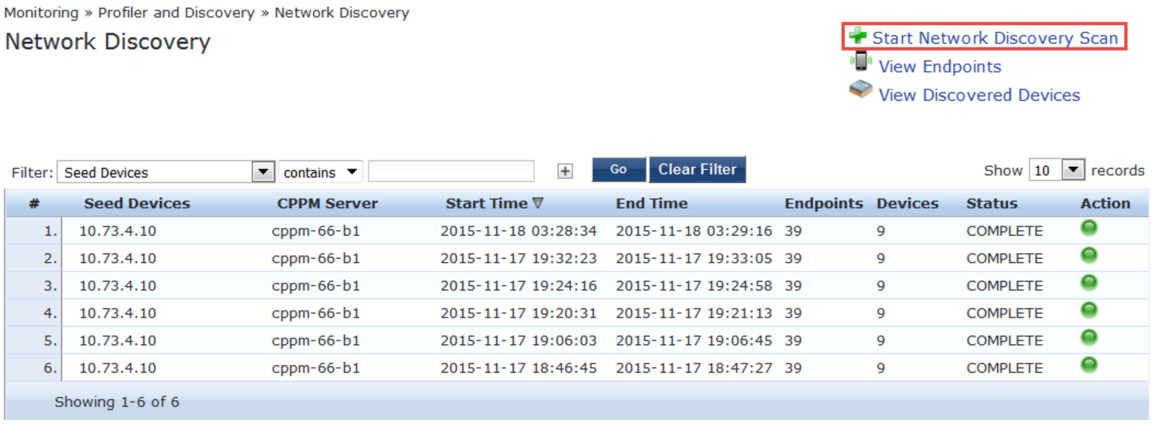
It is recommended that the network scan should be done outside of normal business hours or performed on a ClearPass node that is not servicing core authentications.

To initiate a Network Discovery Scan:

1. Navigate to **Monitoring** > **Profiler and Discovery > Network Discovery**.

   The **Network Discovery** page opens.

Figure 108: *Network Discovery Page*



Monitoring » Profiler and Discovery » Network Discovery

Network Discovery

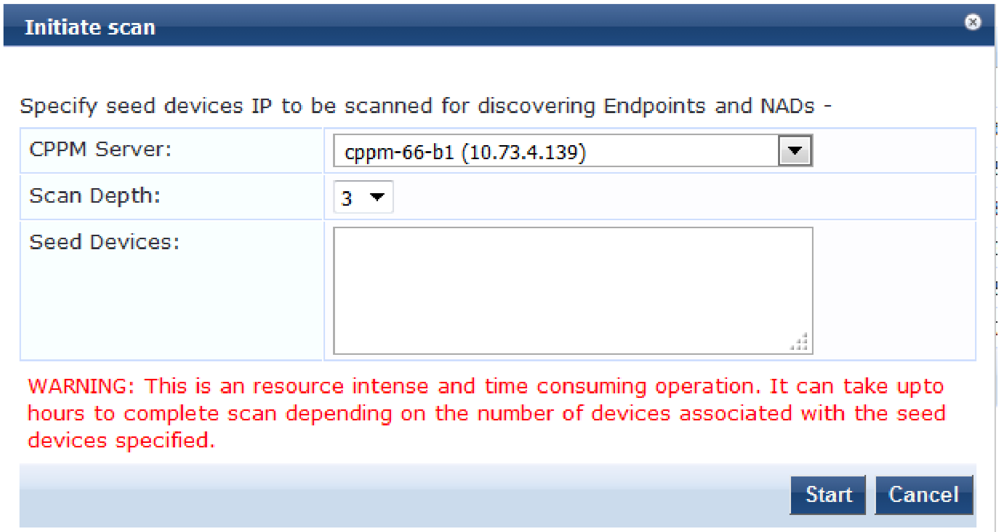
#	Seed Devices	CPPM Server	Start Time	End Time	Endpoints	Devices	Status	Action
1.	10.73.4.10	cppm-66-b1	2015-11-18 03:28:34	2015-11-18 03:29:16	39	9	COMPLETE	●
2.	10.73.4.10	cppm-66-b1	2015-11-17 19:32:23	2015-11-17 19:33:05	39	9	COMPLETE	●
3.	10.73.4.10	cppm-66-b1	2015-11-17 19:24:16	2015-11-17 19:24:58	39	9	COMPLETE	●
4.	10.73.4.10	cppm-66-b1	2015-11-17 19:20:31	2015-11-17 19:21:13	39	9	COMPLETE	●
5.	10.73.4.10	cppm-66-b1	2015-11-17 19:06:03	2015-11-17 19:06:45	39	9	COMPLETE	●
6.	10.73.4.10	cppm-66-b1	2015-11-17 18:46:45	2015-11-17 18:47:27	39	9	COMPLETE	●

Showing 1-6 of 6

2. Click **Start Network Discovery Scan**.

   The **Initiate Scan** dialog opens.

Figure 109: *Initiating the Seed Devices Scan*



Initiate scan

Specify seed devices IP to be scanned for discovering Endpoints and NADs -

CPPM Server: cppm-66-b1 (10.73.4.139)

Scan Depth: 3

Seed Devices:

WARNING: This is an resource intense and time consuming operation. It can take upto hours to complete scan depending on the number of devices associated with the seed devices specified.

3. Enter the appropriate information in the **Initiate Scan** dialog as described in Table 56.

Table 56: *Initiating Network Discovery Scan Parameters*

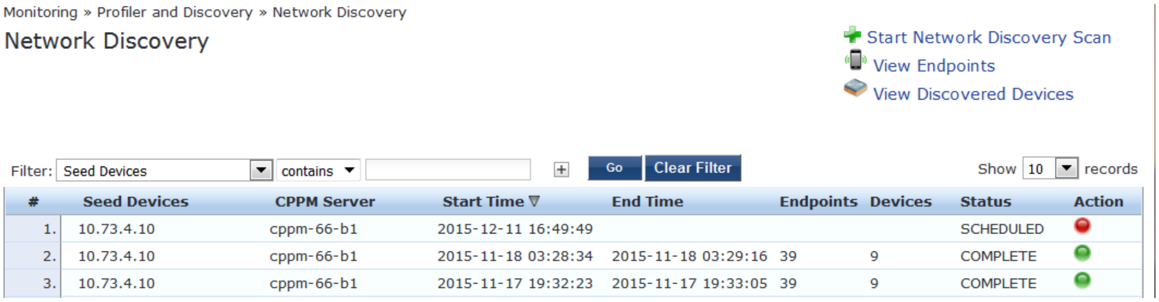
Field	Action/Description
Server	1. From the drop-down list, select the ClearPass Policy Manager server. If the ClearPass server is in a cluster, the list will display the cluster node IP addresses that you can choose. **NOTE:** Once you select the node, the network discovery scan starts with that node.
Scan Depth	2. Specify the **Scan Depth** by selecting the desired number from **1** to **5**. The **Scan Depth** numbers indicate the levels of the network you want to scan. The default is **Scan Depth 3**. The seed devices are, by default, at **Scan Depth 1**. Starting from the seed device, the next device level is **Scan Depth 2**, and so on, until the scan reaches the scan depth specified here.
Seed Devices	3. Enter the IP addresses of one or more seed devices from which the network scan should proceed. Separate multiple device IP addresses with commas.

4. Click **Start**.

   You return to the **Network Discovery** page, which now indicates the following:

   - The **Start Time** and **End Time** for the seed device scan.
   - The number of **Endpoints** and **Devices** connected to the seed device.
   - The **Status** of the scan operation, which shows initally as **"Scheduled**," then "**In Progress**," and finally, "**Completed**."

Figure 110: *Seed Device Successfully Scanned*



Monitoring » Profiler and Discovery » Network Discovery

Network Discovery

Start Network Discovery Scan
View Endpoints
View Discovered Devices

Filter: Seed Devices ▾ contains ▾ [+] Go Clear Filter Show 10 ▾ records

#	Seed Devices	CPPM Server	Start Time ▽	End Time	Endpoints	Devices	Status	Action
1.	10.73.4.10	cppm-66-b1	2015-12-11 16:49:49				SCHEDULED	🔴
2.	10.73.4.10	cppm-66-b1	2015-11-18 03:28:34	2015-11-18 03:29:16	39	9	COMPLETE	🟢
3.	10.73.4.10	cppm-66-b1	2015-11-17 19:32:23	2015-11-17 19:33:05	39	9	COMPLETE	🟢

5. You can stop a scheduled seed device scan or restart a completed scan:
   a. To stop the scan operation, click the **Red Action** button, then click **Yes** to confirm the stop operation.
   b. To restart a completed scan, click the **Green Action** button.

About Auto-Refresh

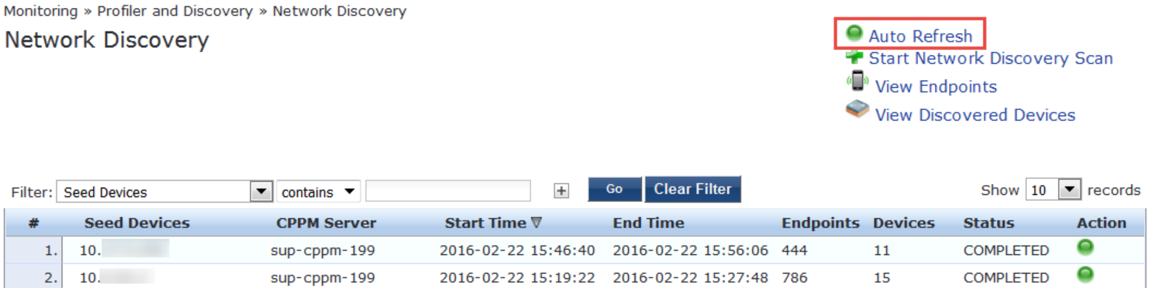
When **Auto-Refresh** is enabled (it is enabled by default), ClearPass fetches fresh data every few seconds to ensure that the network discovery scan status is always current.

When **Auto-Refresh** is enabled, the button is green. You can disable **Auto-Refresh** by clicking the button, which will then turn red to indicate this feature is disabled.

To enable or disable Auto Refresh:

1. Navigate to **Monitoring** > **Profiler and Discovery** > **Network Discovery**.

Figure 111: *Network Discovery > Auto Refresh*



Monitoring » Profiler and Discovery » Network Discovery

Network Discovery

Auto Refresh
Start Network Discovery Scan
View Endpoints
View Discovered Devices

Filter: Seed Devices ▾ contains ▾ [+] Go Clear Filter Show 10 ▾ records

#	Seed Devices	CPPM Server	Start Time ▽	End Time	Endpoints	Devices	Status	Action
1.	10.[redacted]	sup-cppm-199	2016-02-22 15:46:40	2016-02-22 15:56:06	444	11	COMPLETED	🟢
2.	10.[redacted]	sup-cppm-199	2016-02-22 15:19:22	2016-02-22 15:27:48	786	15	COMPLETED	🟢

2. Click the **Auto Refresh** link.

   Every **Auto-Refresh** operation accesses the database and reads the data. When there is no network scan occurring, you can disable **Auto-Refresh** as there is no need to access the database every time.

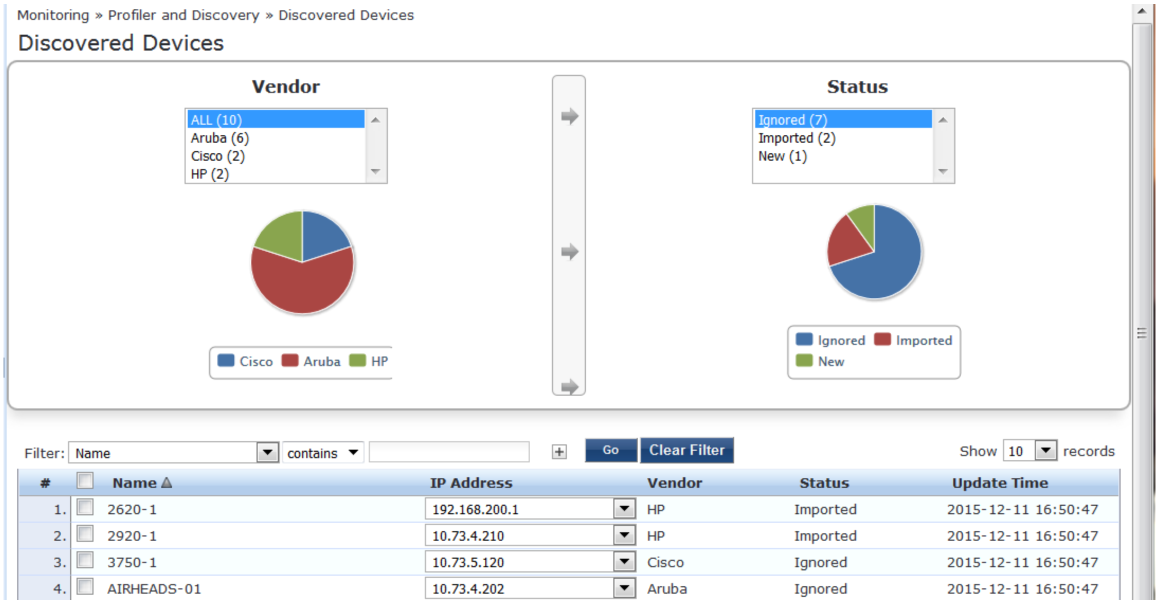
Importing and Viewing Discovered Network Devices

To import and view discovered network devices:

1. Navigate to **Monitoring** > **Profiler and Discovery** > **Discovered Devices**.

   The **Discovered Devices** page opens.

Figure 112: *Discovered Devices Page*



#	□ Name △	IP Address	Vendor	Status	Update Time
1.	□ 2620-1	192.168.200.1	HP	Imported	2015-12-11 16:50:47
2.	□ 2920-1	10.73.4.210	HP	Imported	2015-12-11 16:50:47
3.	□ 3750-1	10.73.5.120	Cisco	Ignored	2015-12-11 16:50:47
4.	□ AIRHEADS-01	10.73.4.202	Aruba	Ignored	2015-12-11 16:50:47

Importing Network Devices

The devices that you import are added to the set of network devices known to ClearPass.

NOTE

You can import devices from the Publisher node only.

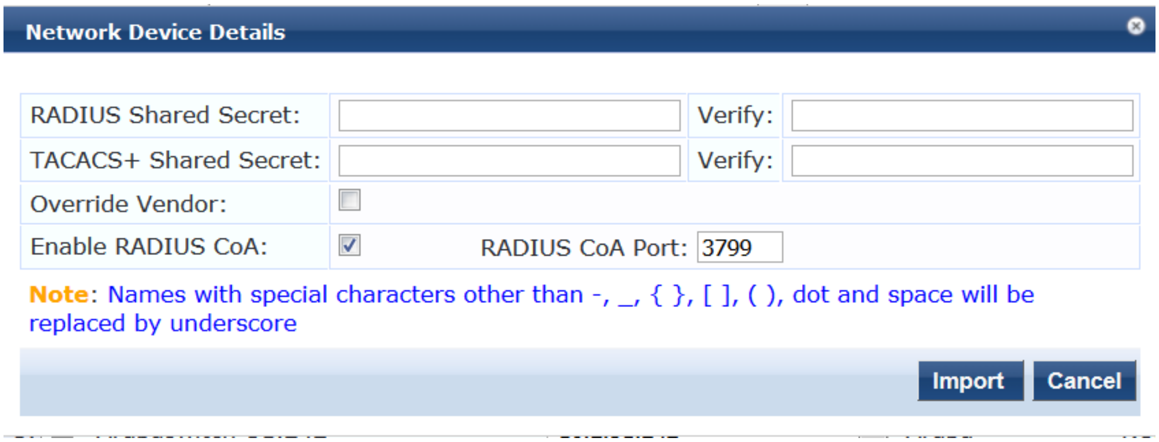
To import and add discovered devices to the set of ClearPass Network Devices:

1. From the list of discovered devices, select a device you wish to import (as shown in Figure 112).

   You can select all of the discovered devices at once by clicking the **Name** check box.
2. Click the **Import** button.

   The **Network Device Details** dialog opens.

Figure 113: *Importing a Network Device*


Network Device Details

RADIUS Shared Secret:		Verify:	
TACACS+ Shared Secret:		Verify:	
Override Vendor:	□		
Enable RADIUS CoA:	☑	RADIUS CoA Port:	3799

Note: Names with special characters other than -, _, { }, [ ], ( ), dot and space will be replaced by underscore

3. Enter the appropriate information in the **Network Device Details** dialog as described in Table 57.

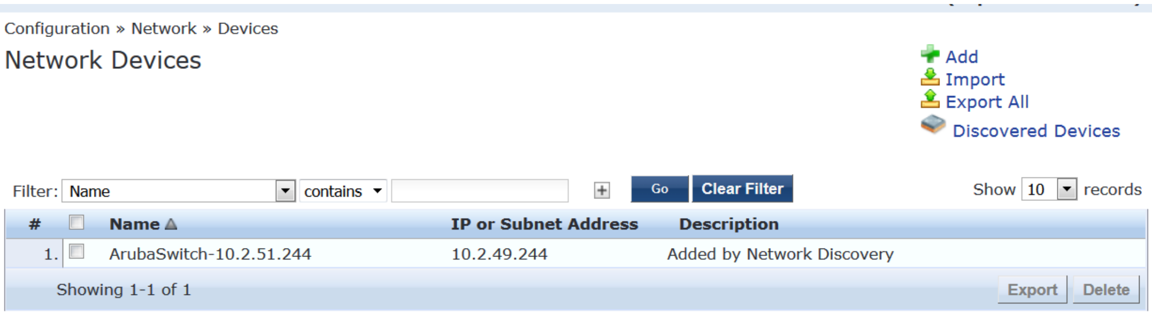
Table 57: *Specifying Network Device Details for Importing Devices*

Field	Action/Description
RADIUS Shared Secret	1. If using RADIUS, enter the RADIUS Shared Secret for the selected discovered device.
TACACS+ Shared Secret	2. If using TACACS+, enter the TACACS+ Shared Secret for the selected discovered device.
Override Vendor	3. Optionally, to override the discovered vendor type, select this check box.
Vendor	This field is displayed when you select **Override Vendor**. 4. From the **Vendor** drop-down, select the name of the vendor type to override the discovered vendor type.
Enable RADIUS CoA	5. Select this check box to enable RADIUS CoA (Change of Authorization).
RADIUS CoA Port	The default RADIUS CoA port is **3799**. 6. To change the RADIUS CoA port number, enter the new port number.

7. Click **Import**.

   The selected network device has been added to ClearPass. To see the network device listed, navigate to **Configuration** > **Network** > **Devices**.

Figure 114: *Network Device Added to ClearPass*



Configuration » Network » Devices

Network Devices

#	Name	IP or Subnet Address	Description
1.	ArubaSwitch-10.2.51.244	10.2.49.244	Added by Network Discovery

Showing 1-1 of 1

Viewing Details on a Discovered Device

To view detailed information about a discovered network devices, including a list of its neighbors in the network:

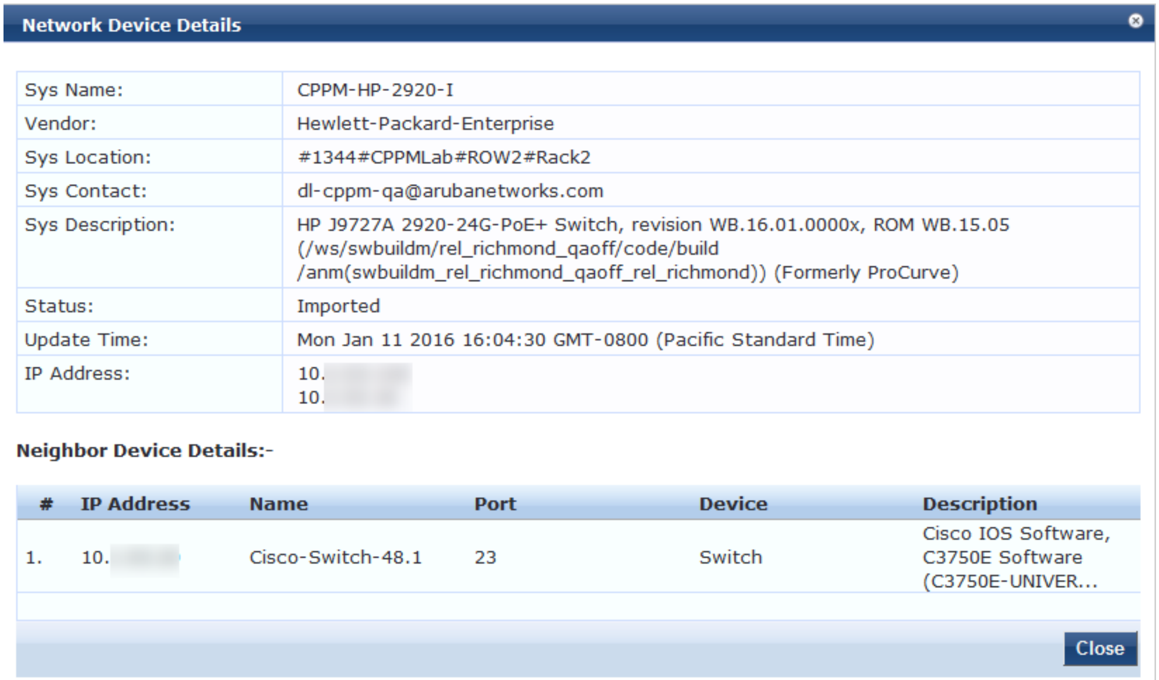
1. Navigate to **Monitoring** > **Profiler and Discovery** > **Discovered Devices**.

   The **Discovered Devices** page opens.

2. Click the name of the device of interest.

   The **Network Device Details** page opens.

Figure 115: *Viewing Details fora Discovered Device*



Network Device Details

Sys Name:	CPPM-HP-2920-I
Vendor:	Hewlett-Packard-Enterprise
Sys Location:	#1344#CPPMLab#ROW2#Rack2
Sys Contact:	dl-cppm-qa@arubanetworks.com
Sys Description:	HP J9727A 2920-24G-PoE+ Switch, revision WB.16.01.0000x, ROM WB.15.05 (/ws/swbuildm/rel_richmond_qaoff/code/build /anm(swbuildm_rel_richmond_qaoff_rel_richmond)) (Formerly ProCurve)
Status:	Imported
Update Time:	Mon Jan 11 2016 16:04:30 GMT-0800 (Pacific Standard Time)
IP Address:	10.[redacted] 10.[redacted]

Neighbor Device Details:-

#	IP Address	Name	Port	Device	Description
1.	10.[redacted]	Cisco-Switch-48.1	23	Switch	Cisco IOS Software, C3750E Software (C3750E-UNIVER...

3. When finished, click **Close**.

Viewing Discovered Endpoints

To view all the discovered endpoints that are connected to the network:

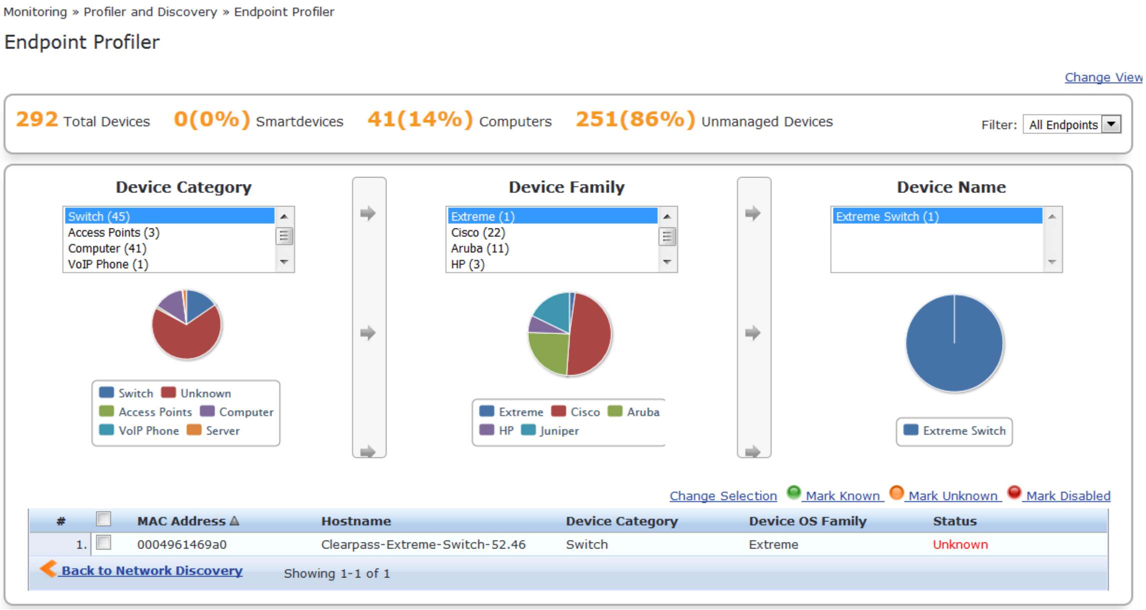
1. Navigate to **Monitoring** > **Profiler and Discovery** > **Network Discovery.**

   The **Network Discovery** page opens.

2. Click **View Endpoints**.

   The Endpoint Profiler opens.

Figure 116: *Viewing the Discovered Endpoints Information*



Monitoring » Profiler and Discovery » Endpoint Profiler

Endpoint Profiler

292 Total Devices **0(0%)** Smartdevices **41(14%)** Computers **251(86%)** Unmanaged Devices

Filter: All Endpoints

#	□	MAC Address ▲	Hostname	Device Category	Device OS Family	Status
1.	□	0004961469a0	Clearpass-Extreme-Switch-52.46	Switch	Extreme	Unknown

Back to Network Discovery   Showing 1-1 of 1

3. When finished, click **Back to Network Discovery**.

Configuring Nmap-Based Endpoint Port Scans

The Network Discovery scan feature supports running an Nmap-based scan on a host to detect open ports and also to fingerprint the service(s) running behind those ports. This information is used in the device profile.

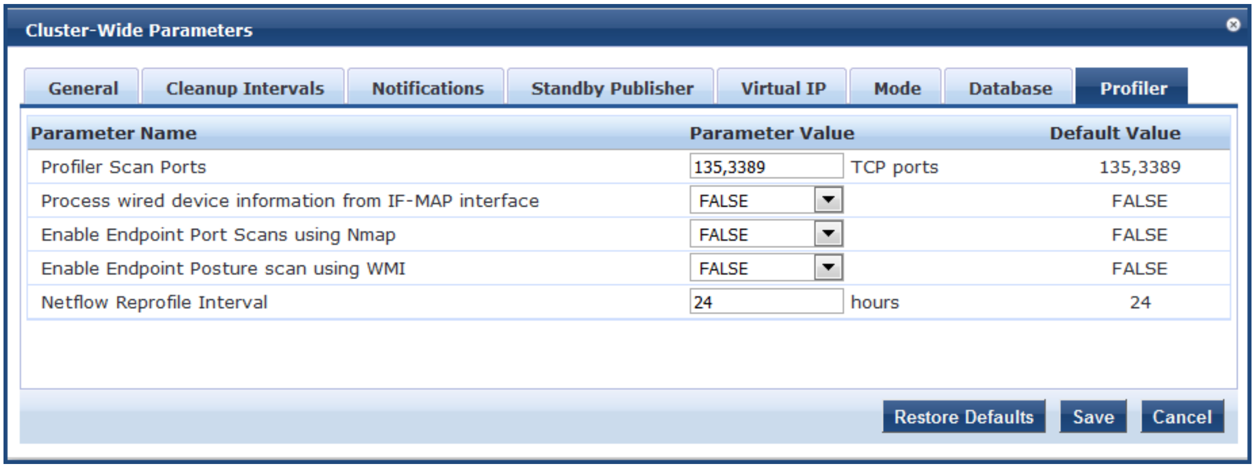
The steps to fully configure endpoint port scans using Nmap are as follows:

1. Enable Nmap-based endpoint port scans.
   a. Navigate to **Administration** > **Server Manager** > **Server Configuration** > **Cluster-Wide Parameters**.

      The **Cluster-Wide Parameters** page opens.

   b. Select the **Profiler** tab.

Figure 117: *Cluster-Wide Parameters > Profiler Dialog*



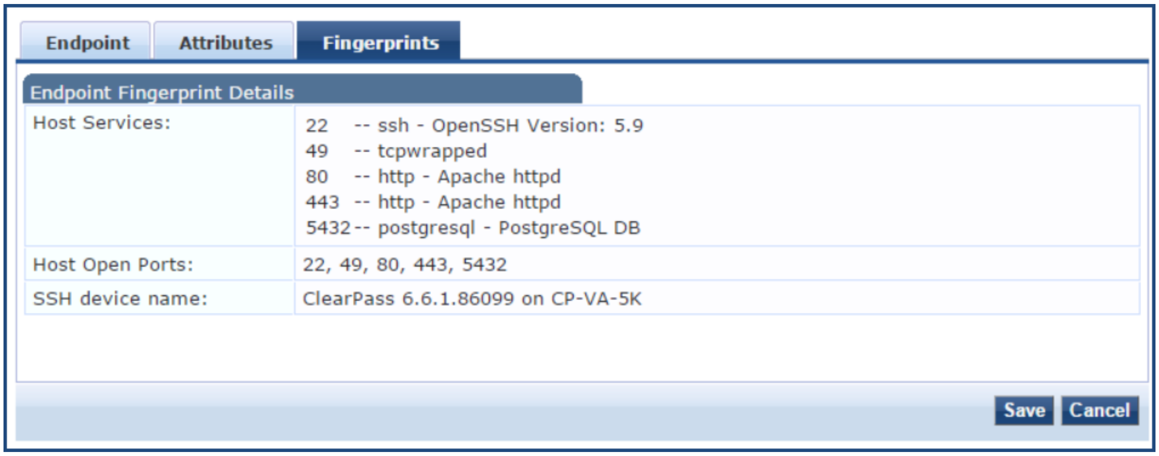
Parameter Name	Parameter Value		Default Value
Profiler Scan Ports	135,3389	TCP ports	135,3389
Process wired device information from IF-MAP interface	FALSE		FALSE
Enable Endpoint Port Scans using Nmap	FALSE		FALSE
Enable Endpoint Posture scan using WMI	FALSE		FALSE
Netflow Reprofile Interval	24	hours	24

   c. Set the **Enable Endpoint Port Scans using Nmap** parameter to **TRUE**.

      For more information, see Profiler Parameters on page 542.

2. Configure SNMP, SSH, WMI settings for the subnets.
   a. Navigate to **Configuration** > **Profile Settings**.
   b. Configure SNMP, SSH, WMI settings for the subnets (see Adding the Configurations to Query Seed Devices on page 135).
3. Initiate a network discovery scan configuring a seed device with **Probe ARP** entries enabled (see Initiating a Network Discovery Scan on page 141).
4. When the Network Discovery scan is completed, select an endpoint (see Viewing the List of Authentication Endpoints on page 243).
   a. Navigate to **Configuration** > **Identity** > **Endpoints**.
   b. Select the endpoint of interest.
5. To view the list of host services and the list of open ports returned by the network discovery scan for the selected host/endpoint, select the **Fingerprints** tab (see Figure 118).

Figure 118: *Endpoint Fingerprint Details with Nmap Data*



Endpoint Fingerprint Details

Host Services:	22 -- ssh - OpenSSH Version: 5.9 49 -- tcpwrapped 80 -- http - Apache httpd 443 -- http - Apache httpd 5432 -- postgresql - PostgreSQL DB
Host Open Ports:	22, 49, 80, 443, 5432
SSH device name:	ClearPass 6.6.1.86099 on CP-VA-5K

Audit Viewer

This section provides the following information:

- Introduction
- Audit Viewer
- Audit Viewer
- Audit Viewer

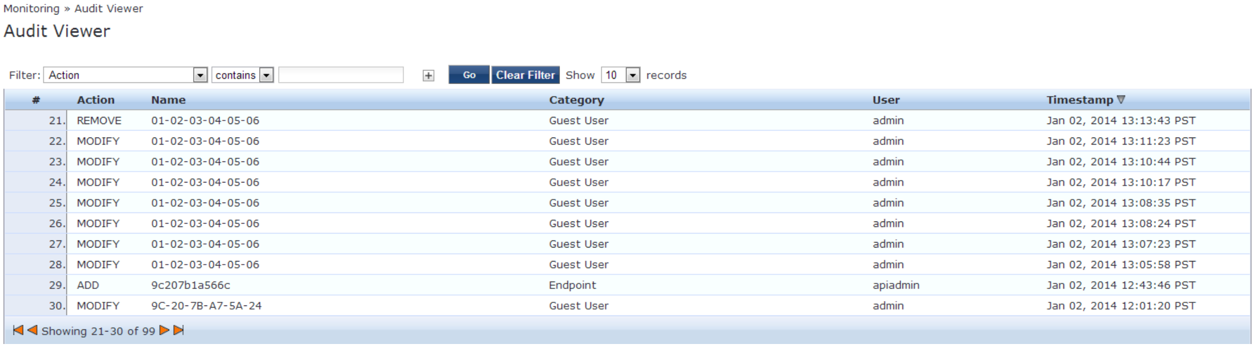
Introduction

The **Audit Viewer** page provides a dynamic report on actions, device name, category of Policy Manager component, user, and timestamp. To access the Audit Viewer:

1. Navigate to **Monitoring** > **Audit Viewer**.

   The **Audit Viewer** page opens.

Figure 119: *Audit Viewer Page*



Filter: Action contains Show 10 records

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

Showing 21-30 of 99

2. To display detailed information about the selected event, click any row in the audit viewer.

   The **Audit Row Details** page opens (see).

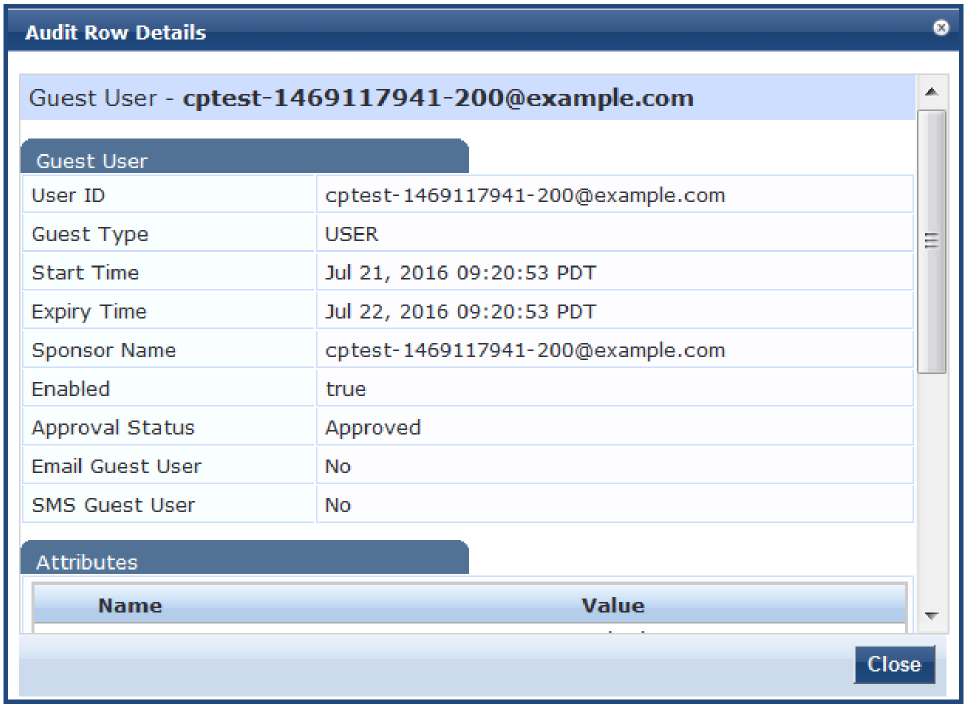
   The content in the **Audit Row Details** page varies, depending upon type of event you select.

Add Events

To display additional details that are specific to the new policy component, click a row with the **Add** action type.

The **Audit Row Details** page opens.

Figure 120: *Audit Row Details for Add Event*



Guest User - **cptest-1469117941-200@example.com**

Guest User

User ID	cptest-1469117941-200@example.com
Guest Type	USER
Start Time	Jul 21, 2016 09:20:53 PDT
Expiry Time	Jul 22, 2016 09:20:53 PDT
Sponsor Name	cptest-1469117941-200@example.com
Enabled	true
Approval Status	Approved
Email Guest User	No
SMS Guest User	No

Attributes

Name	Value

For example, if a TACACS enforcement profile is added, the **Audit Row Details** page displays detailed information about that profile.

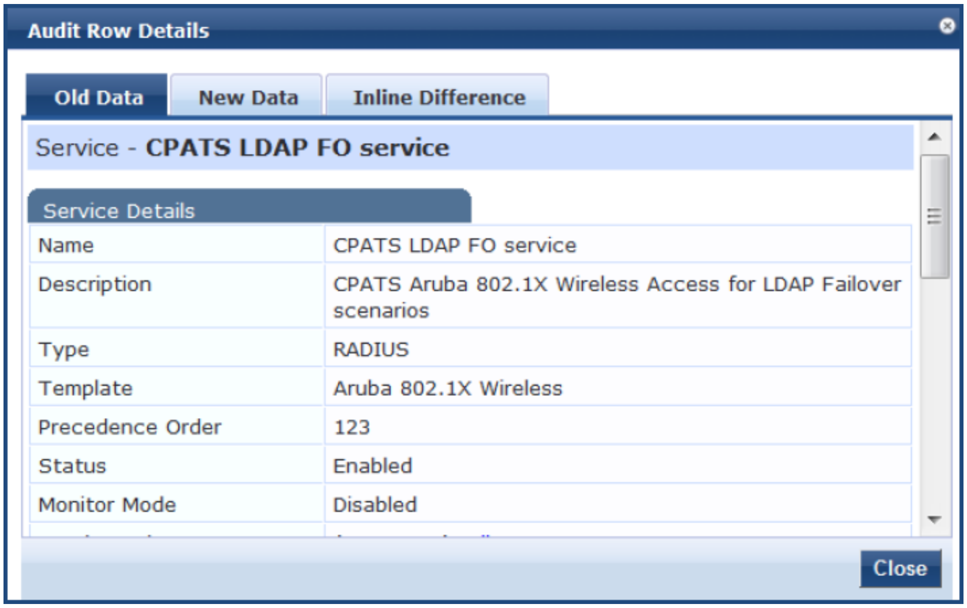
If a policy is created, the **Audit Row Details** page displays information about the policy.

Modify Events

To display additional details information about the change, including the previous values, the latest, updated values, and the differences between the two, click a row with the **Modify** action type.

Figure 121 shows the **Audit Row Details** page for a **Modify Event**.

Figure 121: *Audit Row Details for Modify Event*



Service - **CPATS LDAP FO service**

Service Details

Name	CPATS LDAP FO service
Description	CPATS Aruba 802.1X Wireless Access for LDAP Failover scenarios
Type	RADIUS
Template	Aruba 802.1X Wireless
Precedence Order	123
Status	Enabled
Monitor Mode	Disabled

When you view a modify event, the **Audit Row Details** window contains the following three tabs:

Table 58: *Audit Row Details > Modify Event Page*

Parameter	Description
Old Data	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.
New Data	Displays a summary of details about the new data values. ● The **Profile** section shows a summary of the profile values. ● The **Attributes** section shows data about the original attributes and values.
Inline Difference	Displays information about what changed. The information is color-coded to indicate the following types of changes: ● Modified ● Added ● Deleted ● Moved up ● Moved down

Remove Events

To display details about attributes that were removed, click a row with the **Remove** action type.

Event Viewer

This section provides the following information:

- About the Event Viewer
- Creating an Event Viewer Report Using Default Values
- Creating an Event Viewer Report Using Custom Values
- Viewing Report Details

About the Event Viewer

The **Event Viewer** page provides reports about system-level events. All attempted upgrade, patch, and hotfix installations are logged in the Event Viewer, including failed system installation attempts.

Session Idle time-out values for Admin WebUI session time-out and CLI session time-out events generate Event Viewer messages with a description that includes the client IP address and session ID when necessary.

Unsupported Admin Access Attempts Logged to the Event Viewer

If an attempt is made to access ClearPass Policy Manager administration command-line interface (CLI) with unsupported SSH protocol versions, or unsupported encryption or cryptographic hash algorithms, ClearPass logs those alerts in the Event Viewer. This feature requires the **Ingress Event Engine** option and services to be enabled (for details, see Enabling Ingress Events Processing on page 708).

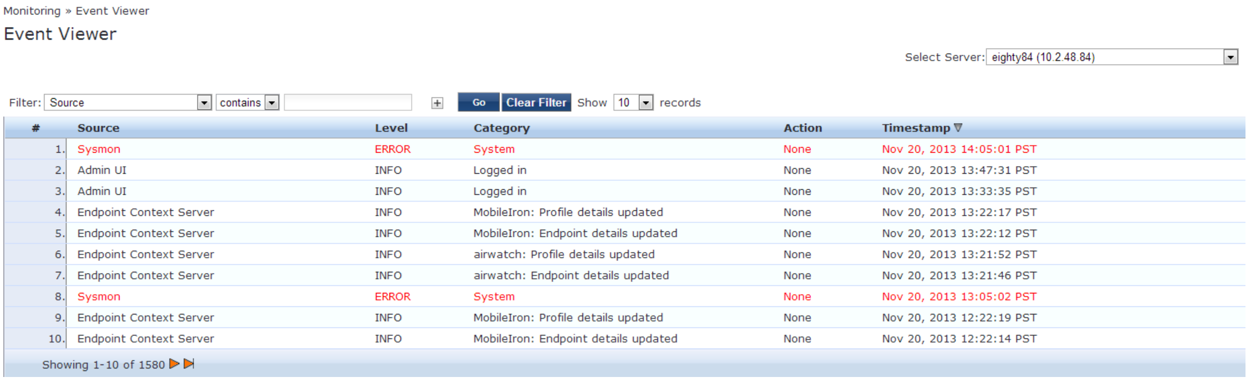
If an attempt is made to access ClearPass Policy Manager administration WebUI with unsupported SSL protocol versions, or unsupported ciphers, ClearPass logs those alerts in the Event Viewer. This feature requires the **Ingress Event Engine** option and services to be enabled for the ClearPass server (for details, see Enable Ingress Events Processing on page 484).

To access the Event Viewer:

1. Navigate to **Monitoring** > **Event Viewer**.

   The **Event Viewer** page opens.

Figure 122: *Event Viewer Page*



Monitoring » Event Viewer

Event Viewer

Select Server: eighty84 (10.2.48.84)

Filter: Source contains Go Clear Filter Show 10 records

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

Showing 1-10 of 1580

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

Table 59: *Event Viewer Page Parameters*

Parameter	Description
Source	Displays the source of the event. For example, AdminUI or ClearPass Updater.
Level	Displays the level of the event from the following options: ● INFO ● WARN ● ERROR
Category	Displays the category of the event. For example, Logged in, System, or AV/AS Updates.

Table 59: *Event Viewer Page Parameters (Continued)*

Parameter	Description
Action	Displays the status of the event action. For example, Success, Failed, Unknown, and None.
Timestamp	Displays the date and time when the event occurred.

Creating an Event Viewer Report Using Default Values

1. In the **Filter** field, select **Source** as the filter parameter.
2. Click **Go**.

   ClearPass returns all event records.

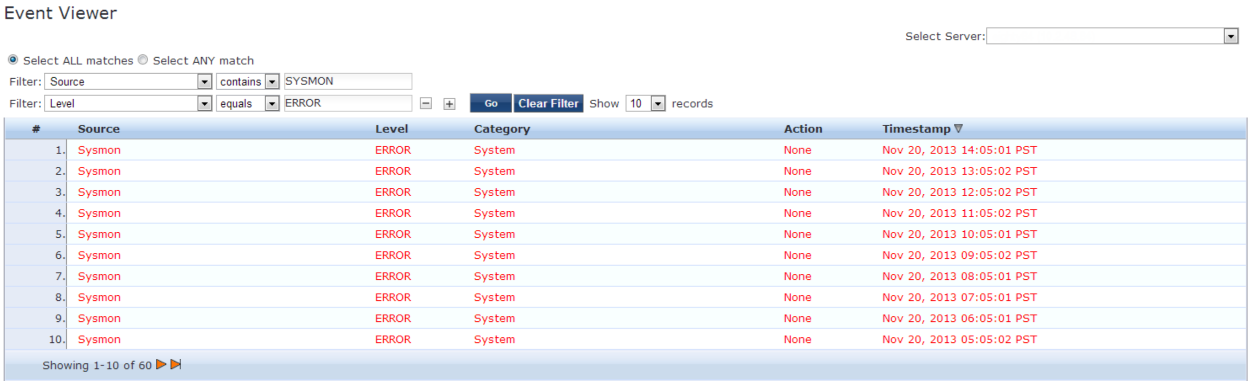
Creating an Event Viewer Report Using Custom Values

1. Click the ⊞ icon.

   A new filter is added. You can add up to four filters.
2. Click **Select ANY match**.
3. In the first **Filter** field, select **Level**.
4. Leave the search term set to **contains**.
5. Enter **ERROR** in the text field.
6. In the second **Filter** field, select **Source**.
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 123: *Event Viewer Report with Customized Filter*



Event Viewer

Select Server:

● Select ALL matches ○ Select ANY match

Filter: Source | contains | SYSMON

Filter: Level | equals | ERROR ⊟ ⊞ Go Clear Filter Show 10 records

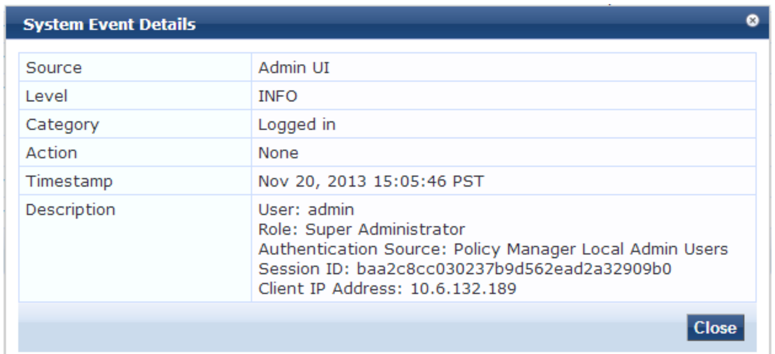
#	Source	Level	Category	Action	Timestamp ▽
1.	Sysmon	ERROR	System	None	Nov 20, 2013 14:05:01 PST
2.	Sysmon	ERROR	System	None	Nov 20, 2013 13:05:02 PST
3.	Sysmon	ERROR	System	None	Nov 20, 2013 12:05:02 PST
4.	Sysmon	ERROR	System	None	Nov 20, 2013 11:05:02 PST
5.	Sysmon	ERROR	System	None	Nov 20, 2013 10:05:01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

Showing 1-10 of 60 ▶ ⏭

Viewing Report Details

To display the **System Event Details** page, click a row in the **Event Viewer** page.

Figure 124: *System Event Details Page*



System Event Details

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

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

Table 60: *System Event Details Page Parameters*

Parameter	Description
Source	Displays the source of the event. For example, Admin UI, 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, including the session ID, client IP address when pertinent, and the session inactive expiry time.

Data Filters

This section provides the following information:

- About Data Filters
- Adding a Data Filter

About Data Filters

The **Data Filters** page provides a way to limit the number of rows of data shown by defining custom criteria or rules in the following components in Policy Manager:

- Live Monitoring: Access Tracker on page 99
- Syslog Export Filters on page 567
- Live Monitoring: Analysis and Trending on page 127

- Live Monitoring: Accounting on page 111

Preconfigured Data Filters

Policy Manager is preconfigured with the following data filters:

Table 61: *Access Tracker Edit Page Parameters*

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

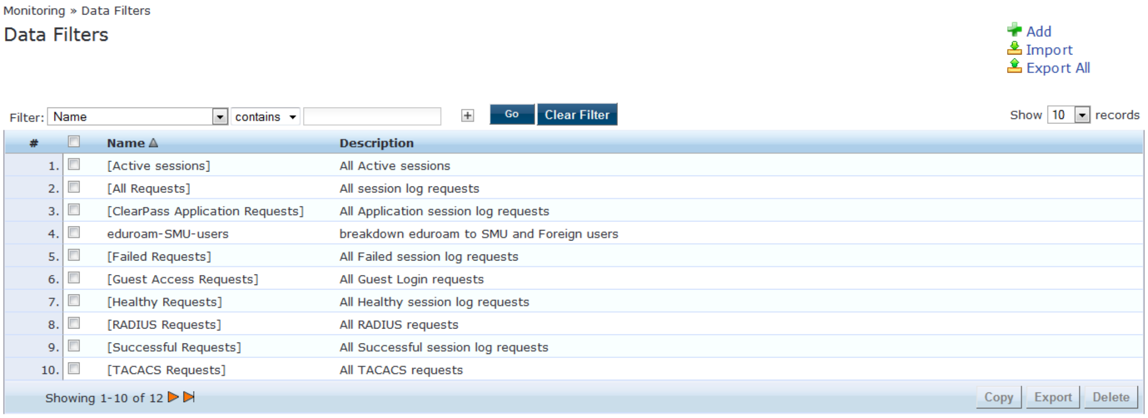
Accessing the Data Filters Page

To access the **Data Filters** page:

1. Navigate to **Monitoring** > **Data Filters**.

   The **Data Filters** page opens.

Figure 125: *Data Filters Page*



Monitoring » Data Filters

Data Filters

Add
Import
Export All

Filter: Name contains Go Clear Filter Show 10 records

#	□	Name ▲	Description
1.	□	[Active sessions]	All Active sessions
2.	□	[All Requests]	All session log requests
3.	□	[ClearPass Application Requests]	All Application session log requests
4.	□	eduroam-SMU-users	breakdown eduroam to SMU and Foreign users
5.	□	[Failed Requests]	All Failed session log requests
6.	□	[Guest Access Requests]	All Guest Login requests
7.	□	[Healthy Requests]	All Healthy session log requests
8.	□	[RADIUS Requests]	All RADIUS requests
9.	□	[Successful Requests]	All Successful session log requests
10.	□	[TACACS Requests]	All TACACS requests

Showing 1-10 of 12 ▶ ▶|

Copy Export Delete

Adding a Data Filter

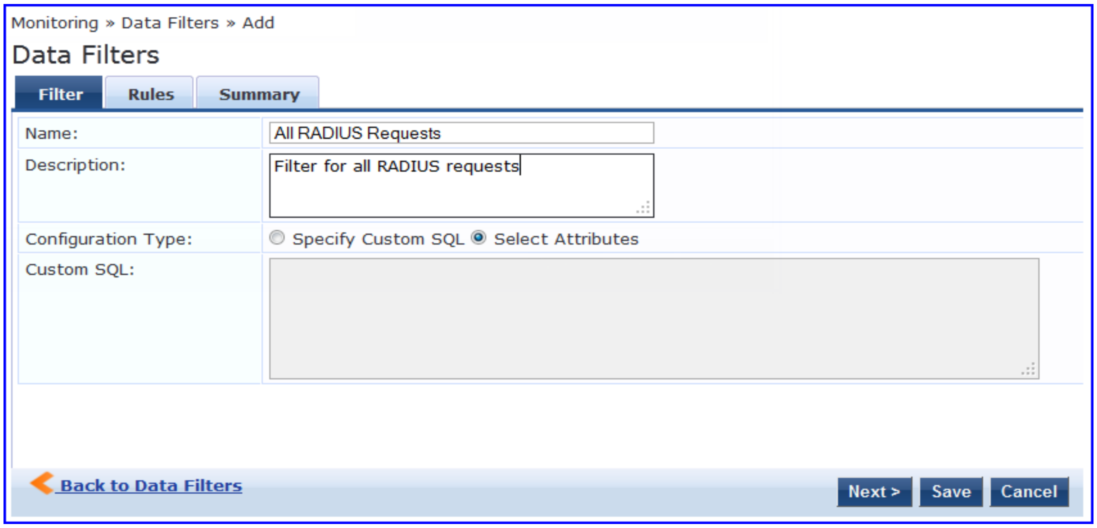
To add a data filter:

1. Click the **Add** link in the top-right corner of the page.

   The **Add Data Filters** page opens to the **Filter** tab.

   Figure 126 shows the **Filter** dialog when you choose **Select Attributes**.

Figure 126: *Add Data Filter > Filter Tab > Select Attributes*



Monitoring » Data Filters » Add

Data Filters

Filter | Rules | Summary

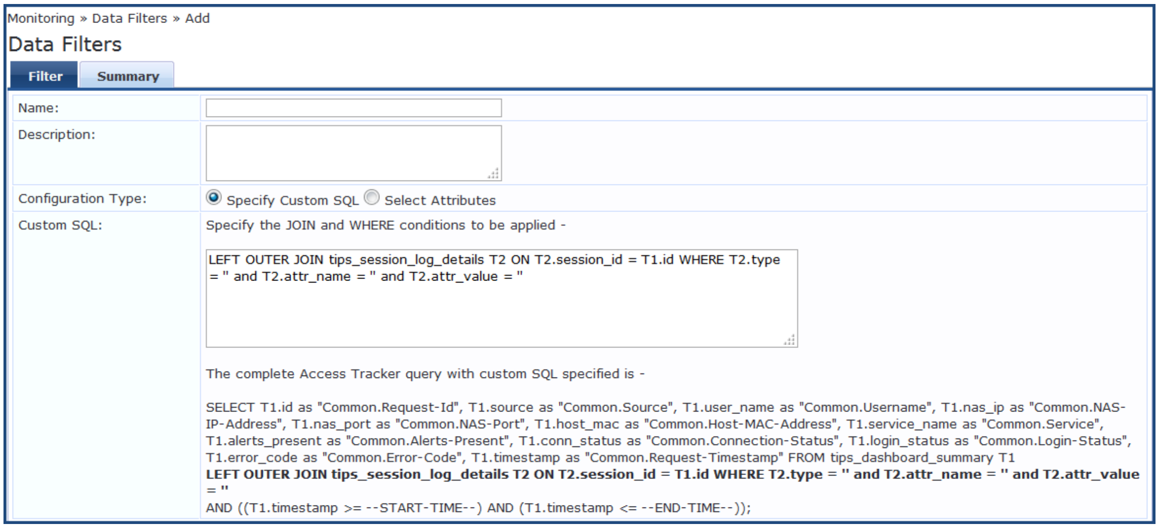
Name:	All RADIUS Requests
Description:	Filter for all RADIUS requests
Configuration Type:	○ Specify Custom SQL ● Select Attributes
Custom SQL:	

Back to Data Filters

Next > Save Cancel

Figure 127 shows the **Filter** dialog when you choose **Specify Custom SQL**.

Figure 127: *Add Data Filter > Filter Tab > Specify Custom SQL*



Monitoring » Data Filters » Add

Data Filters

Name:	
Description:	
Configuration Type:	● Specify Custom SQL ○ Select Attributes
Custom SQL:	Specify the JOIN and WHERE conditions to be applied -

```
LEFT OUTER JOIN tips_session_log_details T2 ON T2.session_id = T1.id WHERE T2.type
= '' and T2.attr_name = '' and T2.attr_value = ''
```

The complete Access Tracker query with custom SQL specified is -

```
SELECT T1.id as "Common.Request-Id", T1.source as "Common.Source", T1.user_name as "Common.Username", T1.nas_ip as "Common.NAS-
IP-Address", T1.nas_port as "Common.NAS-Port", T1.host_mac as "Common.Host-MAC-Address", T1.service_name as "Common.Service",
T1.alerts_present as "Common.Alerts-Present", T1.conn_status as "Common.Connection-Status", T1.login_status as "Common.Login-Status",
T1.error_code as "Common.Error-Code", T1.timestamp as "Common.Request-Timestamp" FROM tips_dashboard_summary T1
LEFT OUTER JOIN tips_session_log_details T2 ON T2.session_id = T1.id WHERE T2.type = '' and T2.attr_name = '' and T2.attr_value
= ''
AND ((T1.timestamp >= --START-TIME--) AND (T1.timestamp <= --END-TIME--));
```

2. Specify the **Add Data Filters** parameters as described in the following table.

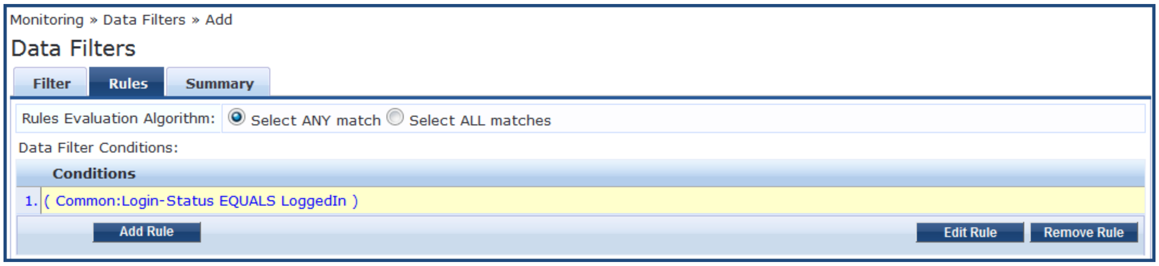
Table 62: *Add Data Filters Page > Filter Tab Parameters*

Parameter	Action/Description
Name	Enter a name for the data filter.
Description	Optionally,enter a description of this data filter (recommended).
Configuration Type	Choose one of the following configuration types: ● **Select Attributes** ● **Specify Custom SQL**
Select Attributes	This option is selected by default. When you specify **Select Attributes**, the **Rules** tab appears. Use the **Rules** tab to configure rules for this filter.
Specify Custom SQL	When you choose **Specify Custom SQL**, a default SQL template is displayed. In the text entry field, enter the attributes for the type, attribute name, and attribute value. **NOTE:** Aruba does not recommend that you enable this option without first consulting Support (navigate to **Administration** > **Support** > **Contact Support**).

Rules Tab

The **Rules** tab displays when you choose the **Select Attributes** configuration type on the **Filter** dialog.

Figure 128: *Add Data Filter > Rules Dialog*



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

Data Filter Conditions:

	Conditions
1.	(Common:Login-Status EQUALS LoggedIn)

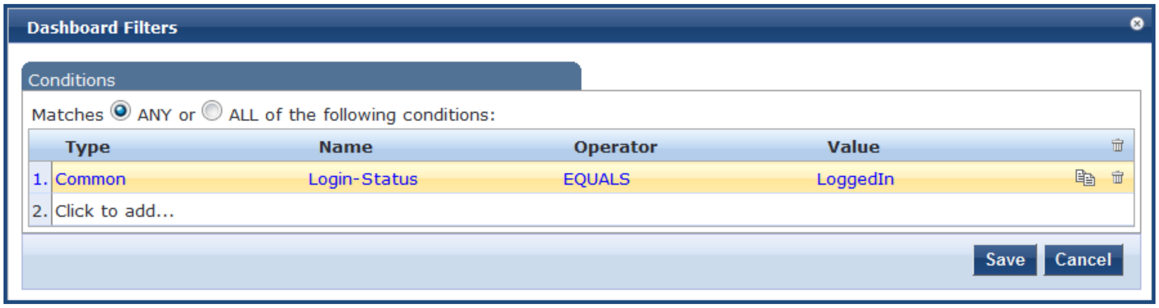
[Table 63](#) describes the **Add Filter** > **Rules** tab parameters:

Table 63: *Add Filter > Rules Tab*

Parameter	Action/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.
Edit Rule	Edit an existing rule.
Remove Rule	When you select an existing rule and click **Remove Rule**, the selected Rule is deleted immediately (no confirmation prompt appears).

When you click **Add Rule** or **Edit Rule**, the **Dashboard Filter Rules Editor** dialog opens.

Figure 129: *Dashboard Filters > Rules Editor*



Matches ● ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Common	Login-Status	EQUALS	LoggedIn
2.	Click to add...			

Table 64 describes the **Dashboard Filters** > **Rules Editor** parameters:

Table 64: *Dashboard Filters > Rules Editor Configuration Parameters*

Parameter	Action/Description
Matches	Specify the match conditions: - **ANY** matches one of the configured conditions. - **ALL** specifies to match all of the configured conditions.
Type	Select the type of data filter. - **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	Select the name of the attribute from the **Name** drop-down list. The **Name** list varies according to which **Type** you selected.
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.

Restoring Blacklisted Users to the Network

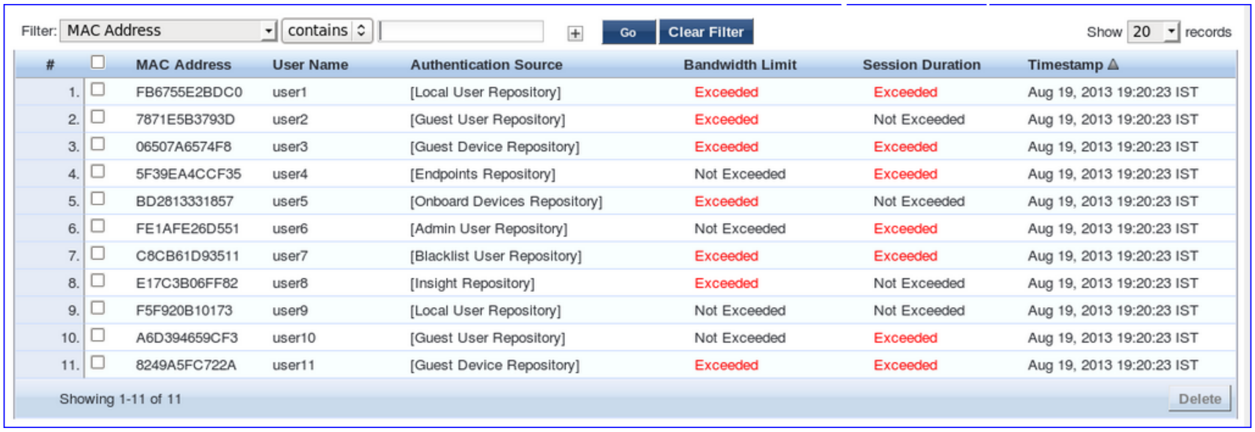
The **Blacklisted Users** page lists the MAC address and user name of all blacklisted users, the authentication source for that user, and indicates whether the bandwidth limit or session duration limits were exceeded by each blacklisted user.

After a user entry is removed from the blacklisted users list, the user is eligible to access the network.

To access the **Blacklisted Users** page:

1. Navigate to **Monitoring** > **Blacklisted Users**.

Figure 130: *Blacklisted Users Page*



Filter: MAC Address contains

Show 20 records

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

Showing 1-11 of 11

2. To delete a user from this blacklist, select the user row and click **Delete**.

   The deleted Blacklisted user is now eligible to access the network.

Authentication Methods and Sources

This section provides the following information:

Supported Authentication Methods

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 161.

ClearPass Policy Manager supports the following authentication methods:

Tunneled EAP Authentication Methods

- 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 Methods

- EAP Message Digest 5 (EAP-MD5)
- EAP Microsoft Challenge Handshake Authentication Protocol version 2 (EAP- MSCHAPv2)
- EAP Generic Token Card (EAP-GTC)
- Challenge Handshake Authentication Protocol (CHAP)
- Password Authentication Protocol (PAP)
- Microsoft CHAP version 1 and 2
- MAC authentication method (MAC-AUTH)
- Authorize authentication

Authentication and Authorization Architecture and Flow

This section includes the following information:

- Authentication Method
- Authentication Source
- Authorization Source
- Authentication and Authorization Flow of Control

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 the following possible outcomes:

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

NOTE

An authentication method is configurable only for some service types. For more information, see Configuring Policy Manager Services on page 70. All 802.1X wired and wireless services have an associated authentication method.

Authentication Source

In Policy Manager, an authentication source is the identity store (Active Directory, LDAP directory, SQL DB, token server, etc.) 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 Managerthen 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.

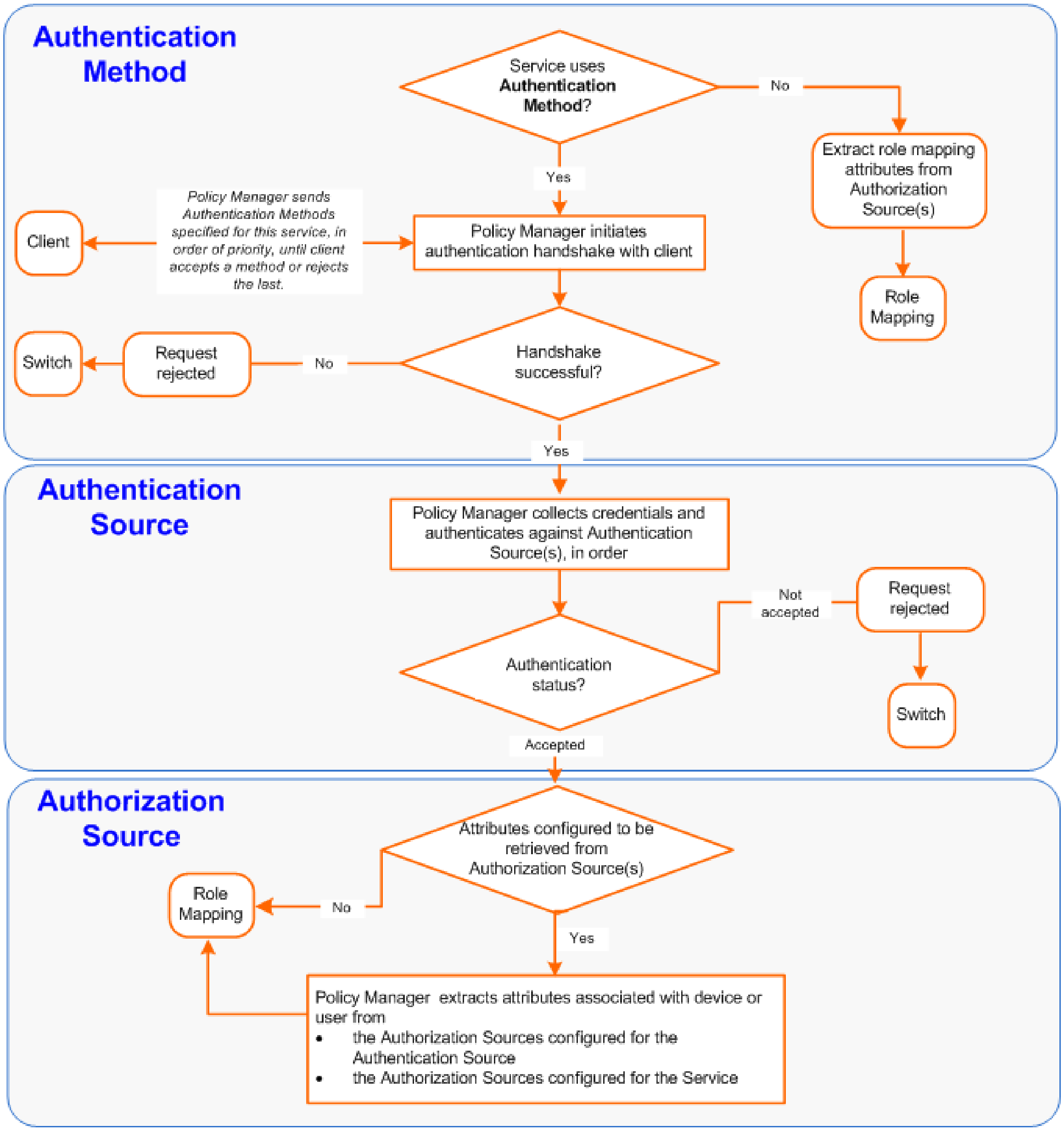
Authorization Source

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.

Authentication and Authorization Flow of Control

The flow of control for authentication takes these components in sequence:

Figure 131: *Authentication and Authorization Flow of Control*



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

Configuring Authentication Methods for an Existing Service

To add or modify an authentication method or source for an existing service:

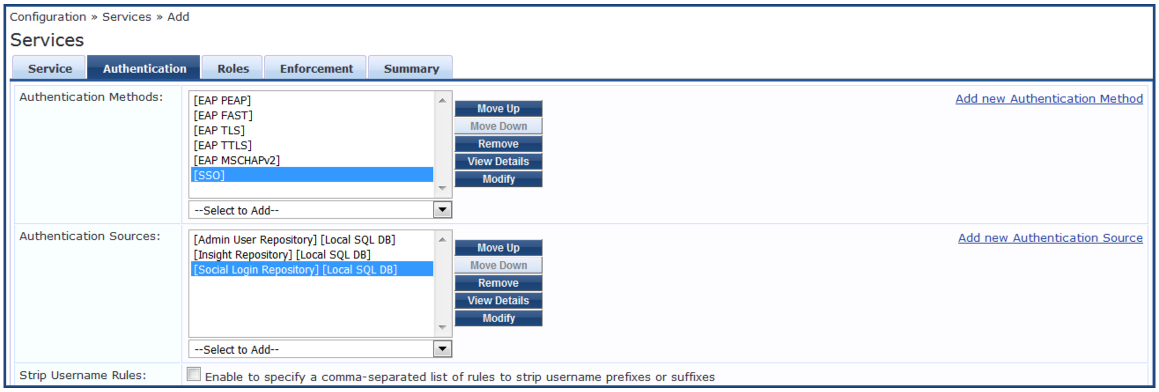
1. Navigate to the **Configuration > Services** page, then click **Add**.

   The **Add Services** page opens.

2. Select the **Authentication** tab.

   The **Add Services** > **Authentication** dialog opens:

Figure 132: *Specifying Authentication Methods and Sources for a Selected Service*



Authentication Methods: [EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] [EAP MSCHAPv2] [SSO]

Authentication Sources: [Admin User Repository] [Local SQL DB] [Insight Repository] [Local SQL DB] [Social Login Repository] [Local SQL DB]

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

3. Specify the Authentication methods and sources for the selected service as described in the following table.

You can open an authentication method or source from the **Configuration > Authentication > Methods** or **Configuration > Authentication > Sources** page.

Table 65: *Authentication Configuration at the Service Level*

Component	Configuration Steps
Sequence of Authentication Methods	• Select a method, then select **Move Up**, **Move Down**, or **Remove**. • Select **View Details** to view the details of the selected method. • Select **Modify** to modify the selected authentication method. This displays a popup with the edit widgets for the select authentication method. ▪ To add a previously configured authentication method, select from the **Select to Add** drop-down list. ▪ To configure a new method, click the **Add new Authentication Method** link. For more information about authentication methods, see Adding and Configuring Authentication Methods on page 165. **NOTE:** An authentication method is only configurable for some service types. For more information, refer to Configuring Policy Manager Services on page 70.
Sequence of Authentication Sources	• Select a source, then select **Move Up**, **Move Down**, or **Remove**. • Select **View Details** to view the details of the selected authentication source. • Select **Modify** to modify the selected authentication source. This displays the **Authentication Source Configuration** wizard for the selected authentication source. • To add a previously configured authentication source, select from the **Select to Add** drop-down list. • To configure a new authentication source, click the **Add new Authentication Source** link. For more information about authentication sources, see Adding and Configuring Authentication Sources on page 190.
Whether to standardize the form in which usernames are present	Select the **Enable to specify a comma-separated list of rules to strip usernames** check box to pre-process the user name and to remove prefixes and suffixes before authenticating it to the authentication source.

Adding and Configuring Authentication Methods

This section provides the following information:

- Adding a New Authentication Method
- Modifying an Existing Authentication Method

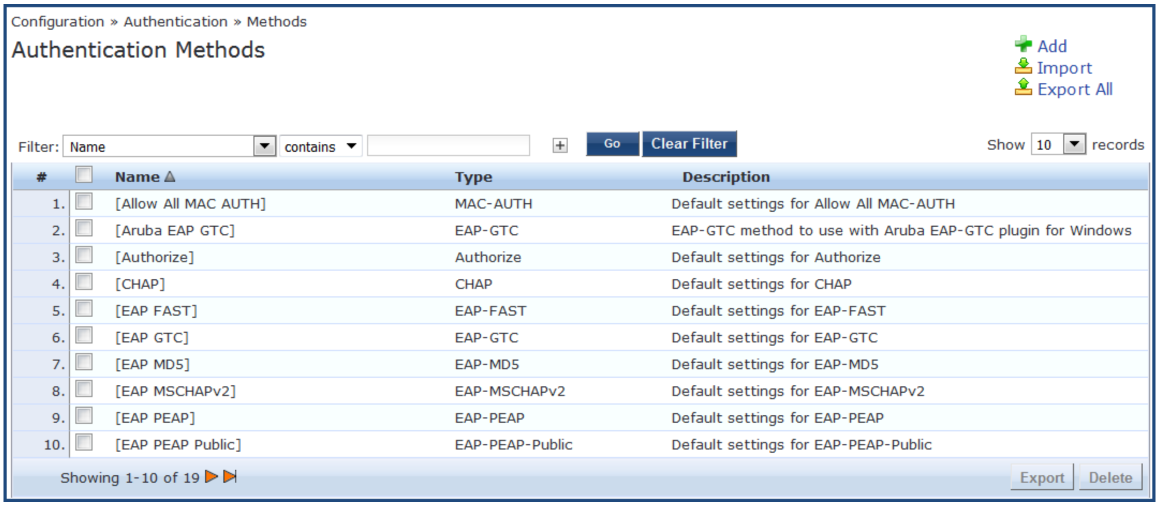
Adding a New Authentication Method

To add a new authentication method:

1. Navigate to **Configuration** > **Authentication** > **Methods**.

   The **Authentication Methods** page opens.

Figure 133: *Authentication Methods Page*

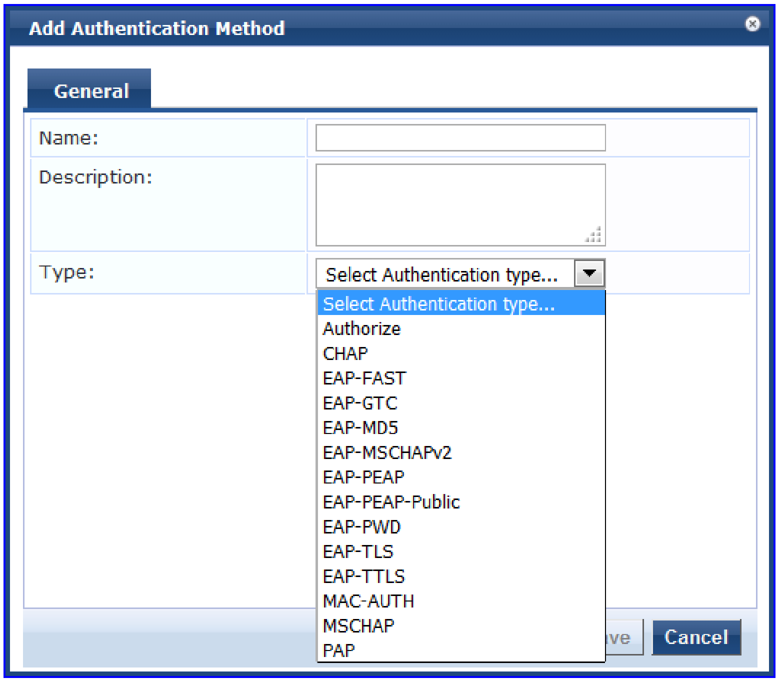


#	□	Name	Type	Description
1.	□	[Allow All MAC AUTH]	MAC-AUTH	Default settings for Allow All MAC-AUTH
2.	□	[Aruba EAP GTC]	EAP-GTC	EAP-GTC method to use with Aruba EAP-GTC plugin for Windows
3.	□	[Authorize]	Authorize	Default settings for Authorize
4.	□	[CHAP]	CHAP	Default settings for CHAP
5.	□	[EAP FAST]	EAP-FAST	Default settings for EAP-FAST
6.	□	[EAP GTC]	EAP-GTC	Default settings for EAP-GTC
7.	□	[EAP MD5]	EAP-MD5	Default settings for EAP-MD5
8.	□	[EAP MSCHAPv2]	EAP-MSCHAPv2	Default settings for EAP-MSCHAPv2
9.	□	[EAP PEAP]	EAP-PEAP	Default settings for EAP-PEAP
10.	□	[EAP PEAP Public]	EAP-PEAP-Public	Default settings for EAP-PEAP-Public

2. Click **Add**.

   The **Add Authentication Method** page opens.

Figure 134: *Add Authentication Method Page*



Add Authentication Method

General

Name:

Description:

Type: Select Authentication type...

3. Enter the name and description of the new authentication method.
4. From the **Type** drop-down, select the type of authentication type.

   You can select from the following list of Authentication types:

   - Authorize
   - CHAP (Challenge Handshake Authentication Protocol)
   - EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)
   - EAP-GTC (EAP-Generic Token Card)
   - EAP-MD5 (EAP-Message Digest 5)
   - EAP-MSCHAPv2 (EAP-Microsoft Challenge Handshake Authentication Protocol version 2)
   - EAP-PEAP (EAP-Protected Extensible Authentication Protocol)
   - EAP-PEAP-Public
   - EAP-PWD (EAP-Password)
   - EAP-TLS (EAP-Transport Layer Security)
   - EAP-TTLS (EAP-Tunneled Transport Layer Security)
   - MAC-AUTH (MAC Address Authentication)
   - MSCHAP (Microsoft Challenge Handshake Authentication Protocol version 1)
   - PAP (Password Authentication Protocol)
5. Configure the Authentication Method of interest as described in the following sections:
   - Authorize Authentication Method on page 168
   - CHAP and EAP-MD5 Authentication Methods on page 168
   - EAP-FAST Authentication Method on page 169
   - EAP-GTC Authentication Method on page 174
   - EAP-MSCHAPv2 on page 176
   - EAP-PEAP on page 176
   - EAP-PEAP-Public on page 179

- EAP-PWD on page 182
- EAP-TLS on page 183
- EAP-TTLS on page 185
- MAC-AUTH Authentication Method on page 187
- MSCHAP on page 188
- PAP on page 189

Modifying an Existing Authentication Method

To modify an existing authentication method:

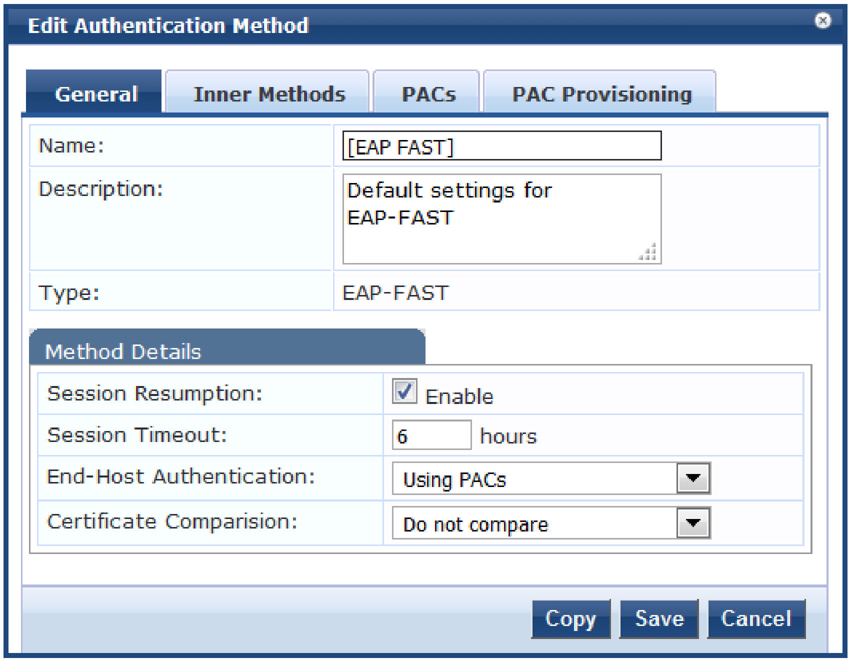
1. Navigate to **Configuration** > **Authentication** > **Methods**.

   The **Authentication Methods** page opens.

2. Click the authentication method of interest.

   The **Edit Authentication Method** page opens.

Figure 135: *Edit Authentication Method Page (EAP-FAST)*



Name:	[EAP FAST]
Description:	Default settings for EAP-FAST
Type:	EAP-FAST

Method Details

Session Resumption:	☑ Enable
Session Timeout:	6 hours
End-Host Authentication:	Using PACs
Certificate Comparision:	Do not compare

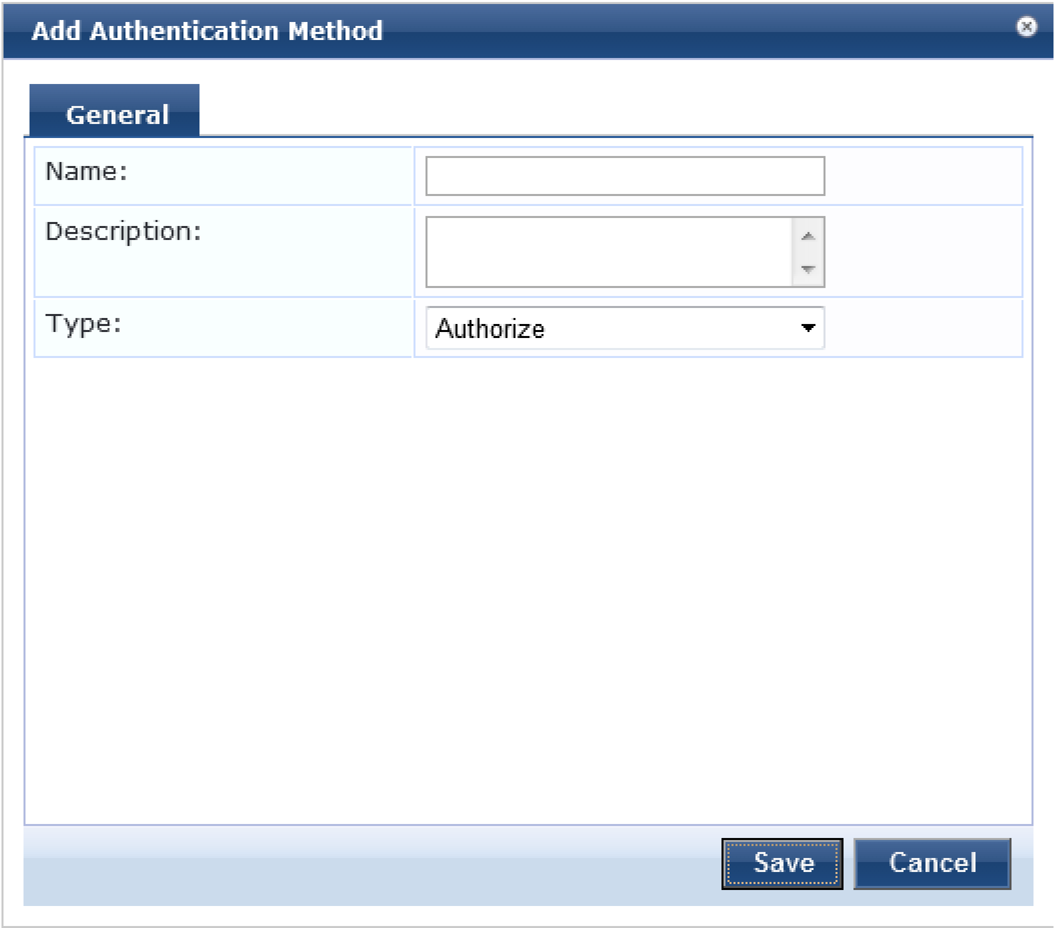
3. Modify the selected authentication method(s) as necessary, then click **Save**.

Authorize Authentication Method

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

The following figure displays the **Authentication Method** configuration dialog:

Figure 136: *Add Authorize Authentication Method Configuration Dialog*



Name:

Description:

Type: Authorize

Specify the **Authorize Authentication Method** parameters as described in the following table:

Table 66: *Authorize Authentication Method Parameters*

Parameter	Action/Description
Name	Specify the label of the authentication method.
Description	Provide additional information that helps to identify the authentication method.
Type	Select authentication method type **Authorize.**

CHAP and EAP-MD5 Authentication Methods

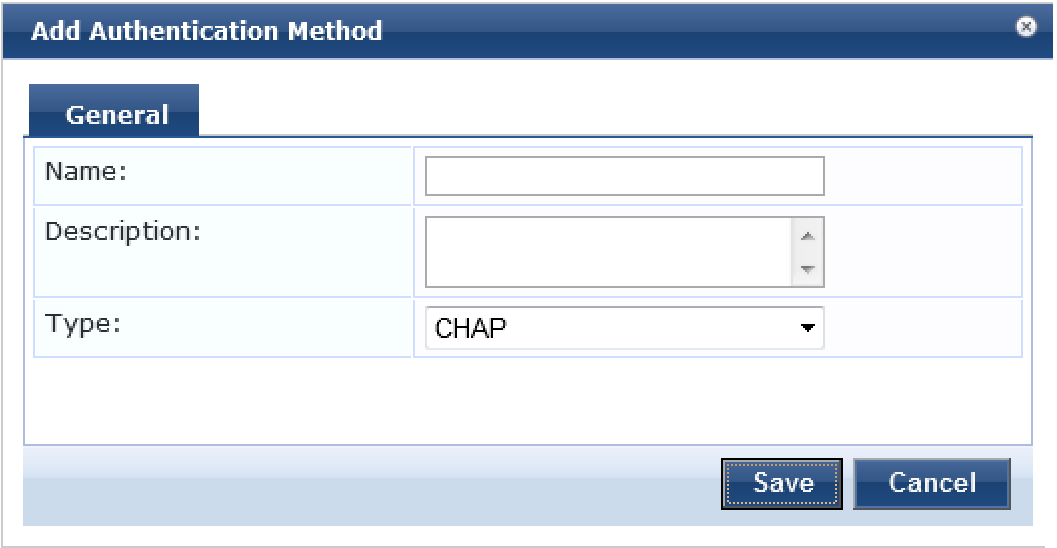
Policy Manager is packaged with **CHAP** and **EAP-MD5** authentication methods. You can create one or more instances of CHAP and EAP-MD5 authentication methods by assigning a customized name to each one. These methods can also be associated to a service as authentication methods.

NOTE

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

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

Figure 137: *Adding CHAP Authentication Method*



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

Table 67: *CHAP and EAP-MD5 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 Authentication Method

This section includes the following information:

- General Tab on page 169
- Inner Methods Tab on page 171
- PACs Tab on page 172
- PAC Provisioning Tab on page 173

EAP-EAP-FAST (Flexible Authentication through Secure Tunneling) is an authentication method that encrypts EAP transactions within a TLS (Transport Layer Security) tunnel.

General Tab

To add the EAP-FAST authentication method to ClearPass:

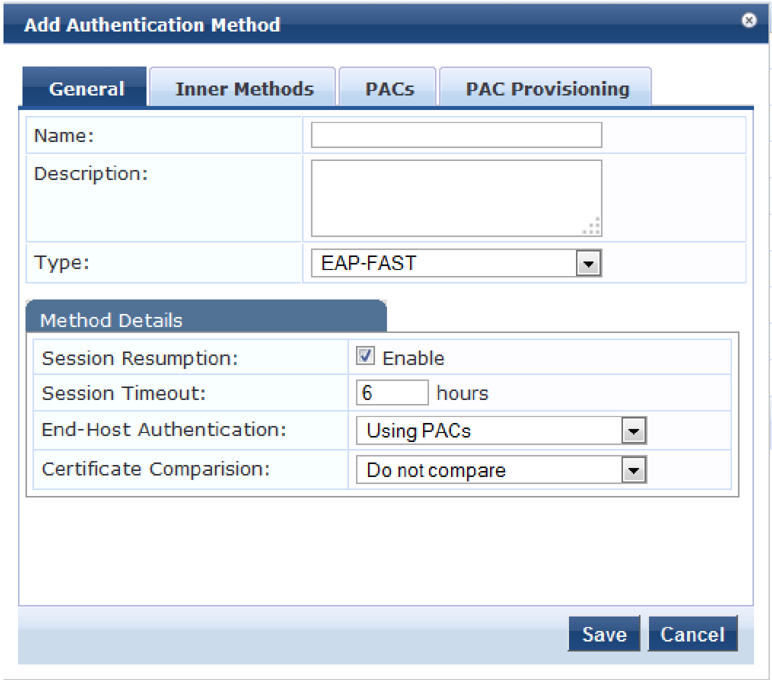
1. Navigate to **Configuration** > **Authentication** > **Methods**.

   The **Authentication Methods** page opens.

2. Select the **Add** link.

   The **Add Authentication Method** dialog opens to the **General** tab.

Figure 138: *Adding the EAP-FAST Authentication Method*



Name:

Description:

Type: EAP-FAST

Session Resumption: ☑ Enable

Session Timeout: 6 hours

End-Host Authentication: Using PACs

Certificate Comparision: Do not compare

3. Configure the EAP-FAST authentication service as described in Table 68, then click **Save**.

Table 68: *Specifying the EAP_FAST > General Parameters*

Parameter	Action/Description
Name	1. Specify the name of the authentication method.
Description	2. Provide the additional information that helps to identify the authentication method.
Type	3. Select **EAP_FAST**.
Session Resumption	4. Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to the ClearPass server within the session-timeout interval. By default, this option is enabled.

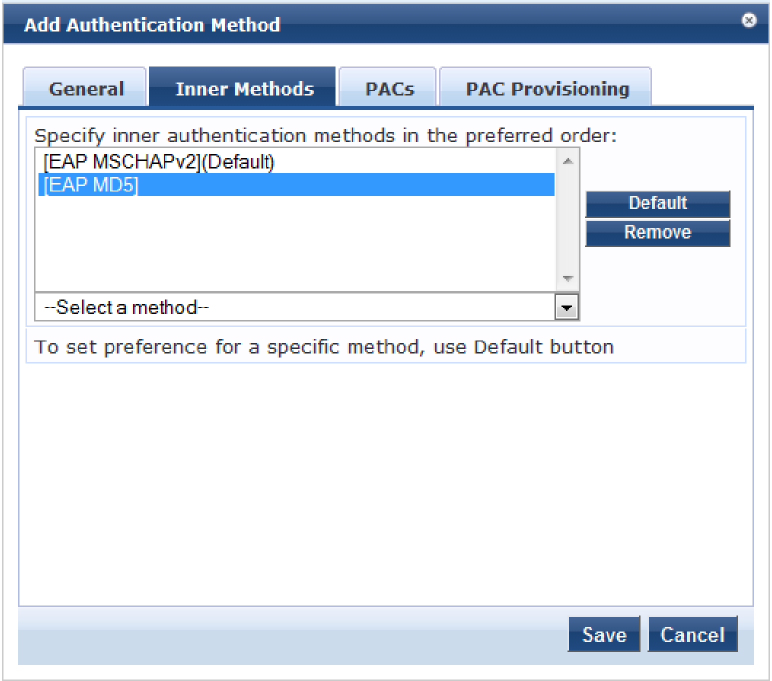
Table 68: *Specifying the EAP_FAST > General Parameters (Continued)*

Parameter	Action/Description
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. 5. Specify the **Session Timeout** in the number of hours. The default is **6** hours. If the **Session Timeout** value is set to **0**, the cached sessions are not purged.
End-Host Authentication	6. Specify one of the following end-host authentication methods: ■ Using PACS (Protected Access Credentials) ■ Using Client Certificate **NOTE:** The PACs and PAC Provisioning tabs are available only when you select **Using PACs**.
Certificate Comparison	7. Specify one of the following Certificate Comparison actions: ■ Do not compare ■ Compare Distinguished Name (DN) ■ Compare Common Name (CN) ■ Compare Subject Alternate Subject Name (SAN) ■ Compare CN or SAN ■ Compare Binary

Inner Methods Tab

The following figure displays the **EAP-FAST** > **Inner Methods** dialog:

Figure 139: *EAP-FAST Authentication Method > Inner Methods Dialog*



Specify inner authentication methods in the preferred order:

[EAP MSCHAPv2](Default)
[EAP MD5]

--Select a method--

To set preference for a specific method, use Default button

The EAP-MD5 authentication method is not supported when you use ClearPass Policy Manager in FIPS mode.

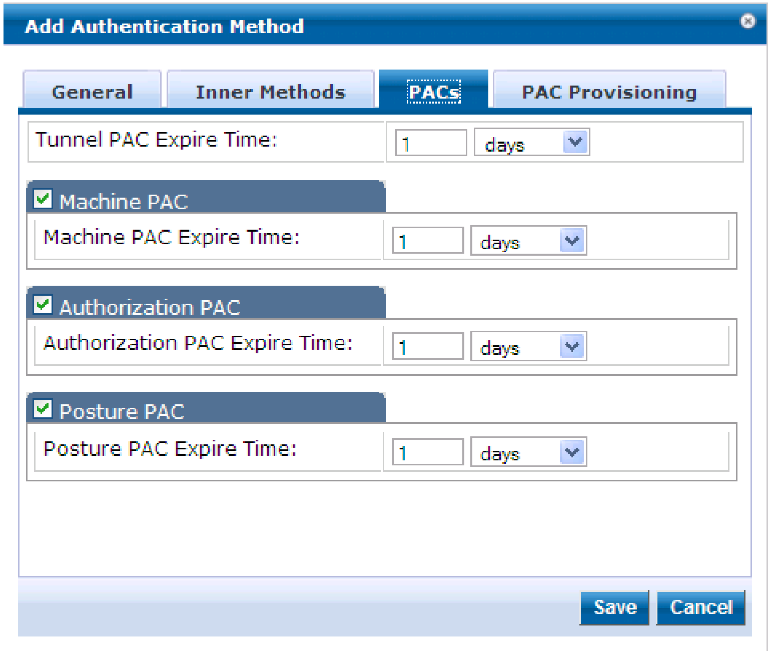
Table 69: *EAP-FAST > Inner Methods Tab Parameters*

Parameter	Action/Description
Specify inner authentication methods in the preferred order	1. Select a method from the drop-down list: ■ Aruba EAP GTC ■ EAP GTC ■ EAP MD5 ■ EAP MSCHAPV2 (Default) ■ EAP PWD ■ EAP TLS with OSCP Enabled ■ EAP TLS 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** dialog enables or disables Protected Access Credential (PAC) types. The following figure displays the **EAP-FAST** > **PACs** dialog:

Figure 140: *EAP_FAST PACs Dialog*



Tunnel PAC Expire Time: 1 days

☑ Machine PAC

Machine PAC Expire Time: 1 days

☑ Authorization PAC

Authorization PAC Expire Time: 1 days

☑ Posture PAC

Posture PAC Expire Time: 1 days

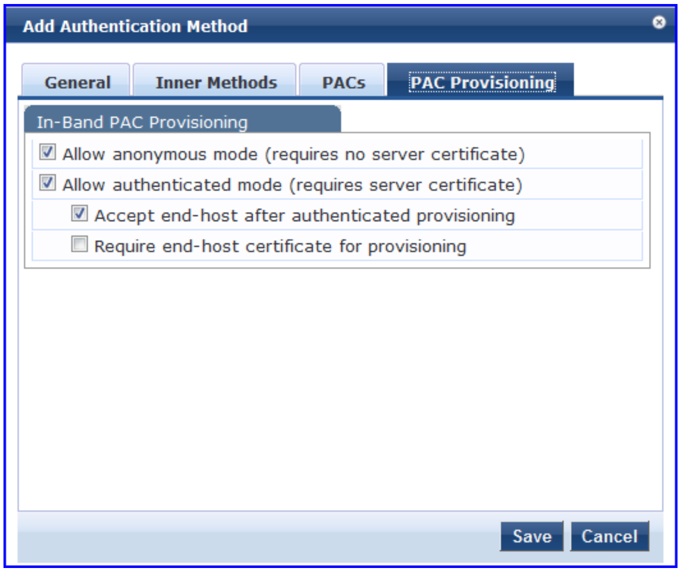
1. Specify the **Expiration Time** (number of **hours**, **days**, **weeks**, **months**, or **years**) for each of the Protected Access Credentials:
   a. Tunnel PAC Expire Time
   b. Machine PAC Expire Time
   c. Authorization PAC Expire Time
   d. Posture PAC Expire Time

2. Select the **PAC Provisioning** tab.

PAC Provisioning Tab

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

Figure 141: *EAP_FAST PAC Provisioning Dialog*



Add Authentication Method

In-Band PAC Provisioning

☑ Allow anonymous mode (requires no server certificate)
☑ Allow authenticated mode (requires server certificate)
☑ Accept end-host after authenticated provisioning
☐ Require end-host certificate for provisioning

1. Configure the PAC Provisioning parameters as described in Table 70.
2. When finished, click **Save**.

Table 70: *EAP_FAST PAC Provisioning Parameters*

Parameter	Action/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. **NOTE:** This mode is not as secure as the authenticated mode. After an outer tunnel is established, the 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	

Table 70: *EAP_FAST PAC Provisioning Parameters (Continued)*

Parameter	Action/Description	Considerations
	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 the 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, which results 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 Authentication Method

EAP-Generic Token Card (GTC) enables the exchange of clear-text authentication credentials across the network. EAP-GTC carries a text challenge from the authentication server and a reply generated by a security token.

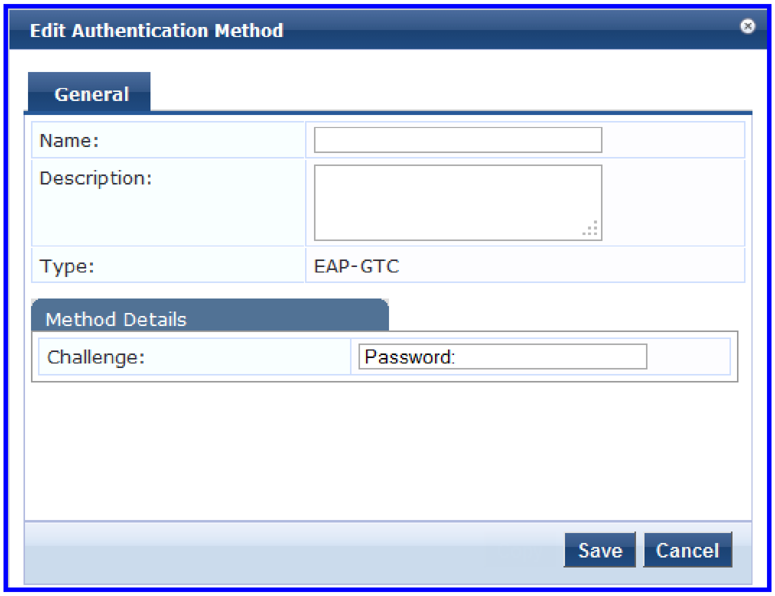
To modify the EAP-GTC authentication method:

1. Navigate to **Configuration** > **Authentication** > **Methods**.

   The **Authentication Methods** page opens.
2. From the list of Authentication Methods, select **EAP GTC**.

   The **Edit Authentication Method** dialog for **EAP-GTC** opens:

Figure 142: *Edit EAP-GTC Authentication Method*



Edit Authentication Method

General

Name:	
Description:	
Type:	EAP-GTC

Method Details

Challenge:	Password:

3. Specify the **EAP-GTC General** parameters as described in the following table, then click **Save**:

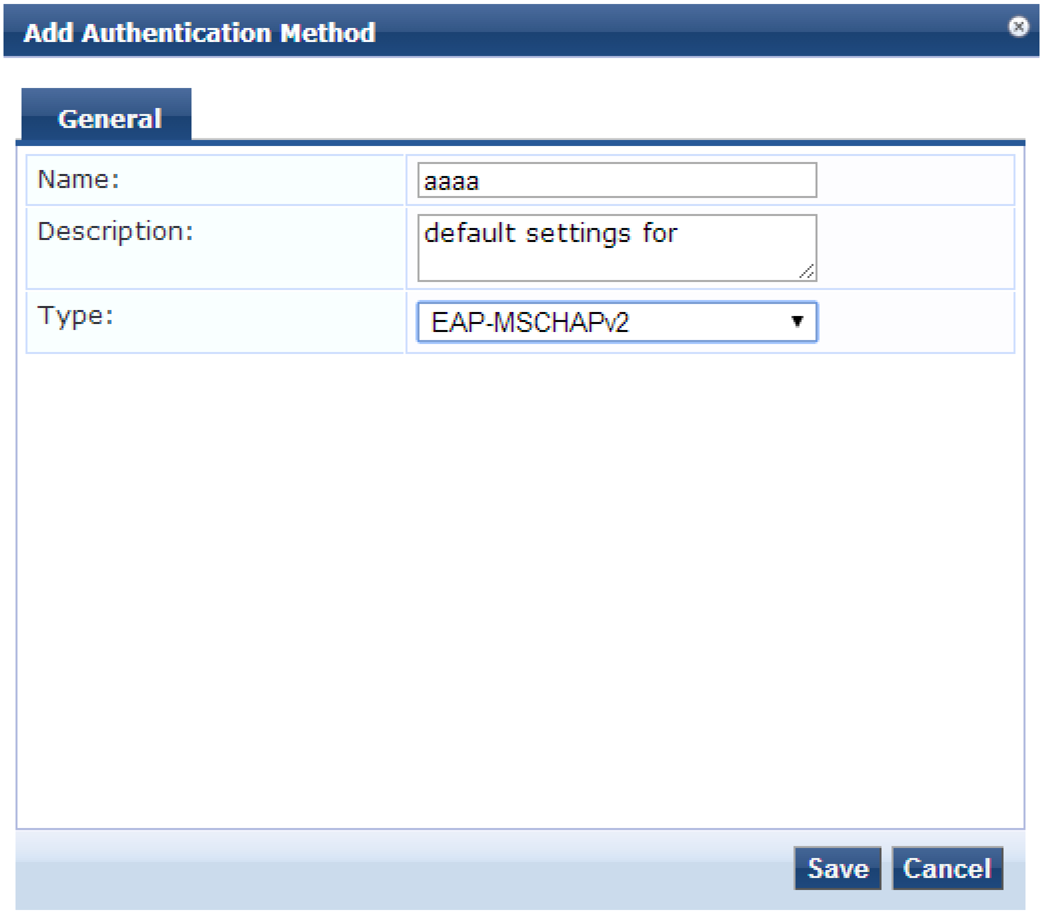
Table 71: *EAP-GTC Authentication Method Parameters*

Parameter	Action/Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method.
Type	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 143: *EAP-MSCHAPv2 - General Tab*



Name: aaaa

Description: default settings for

Type: EAP-MSCHAPv2

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

Table 72: *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.

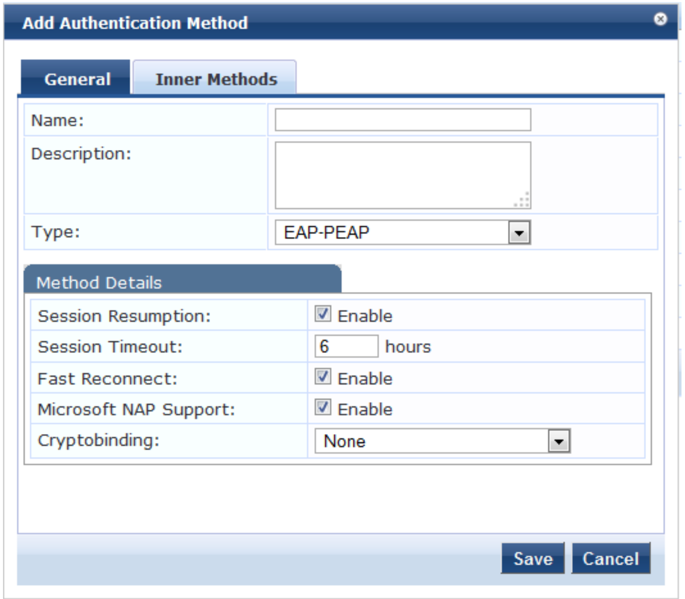
The **EAP-PEAP** authentication method contains the following two tabs:

- General Tab on page 177
- Inner Methods Tab on page 178

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 144: *EAP-PEAP - General Tab*



Name:

Description:

Type: EAP-PEAP

Session Resumption: ☑ Enable

Session Timeout: 6 hours

Fast Reconnect: ☑ Enable

Microsoft NAP Support: ☑ Enable

Cryptobinding: None

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

Table 73: *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	

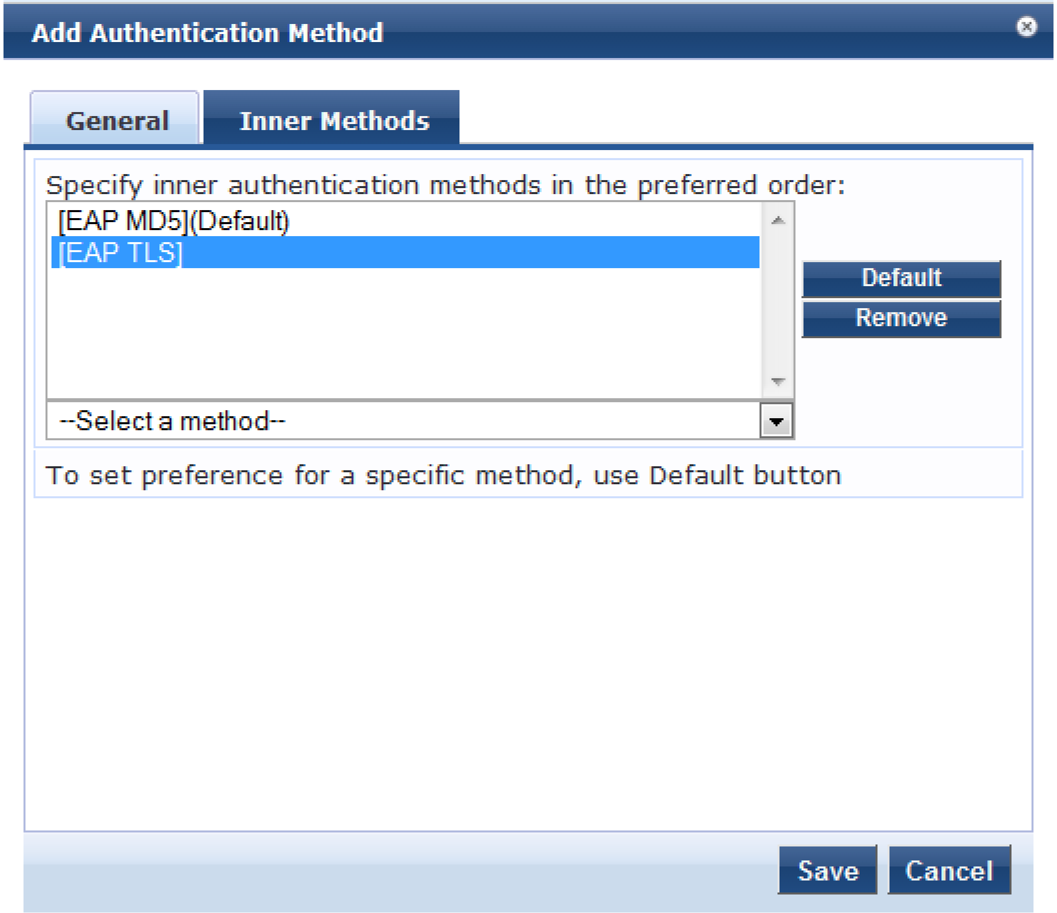
Table 73: *EAP-PEAP - General Tab Parameters (Continued)*

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 145: *EAP-PEAP - Inner Methods Tab*



Specify inner authentication methods in the preferred order:

[EAP MD5](Default)
[EAP TLS]

--Select a method--

To set preference for a specific method, use Default button

NOTE

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

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

Table 74: *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.

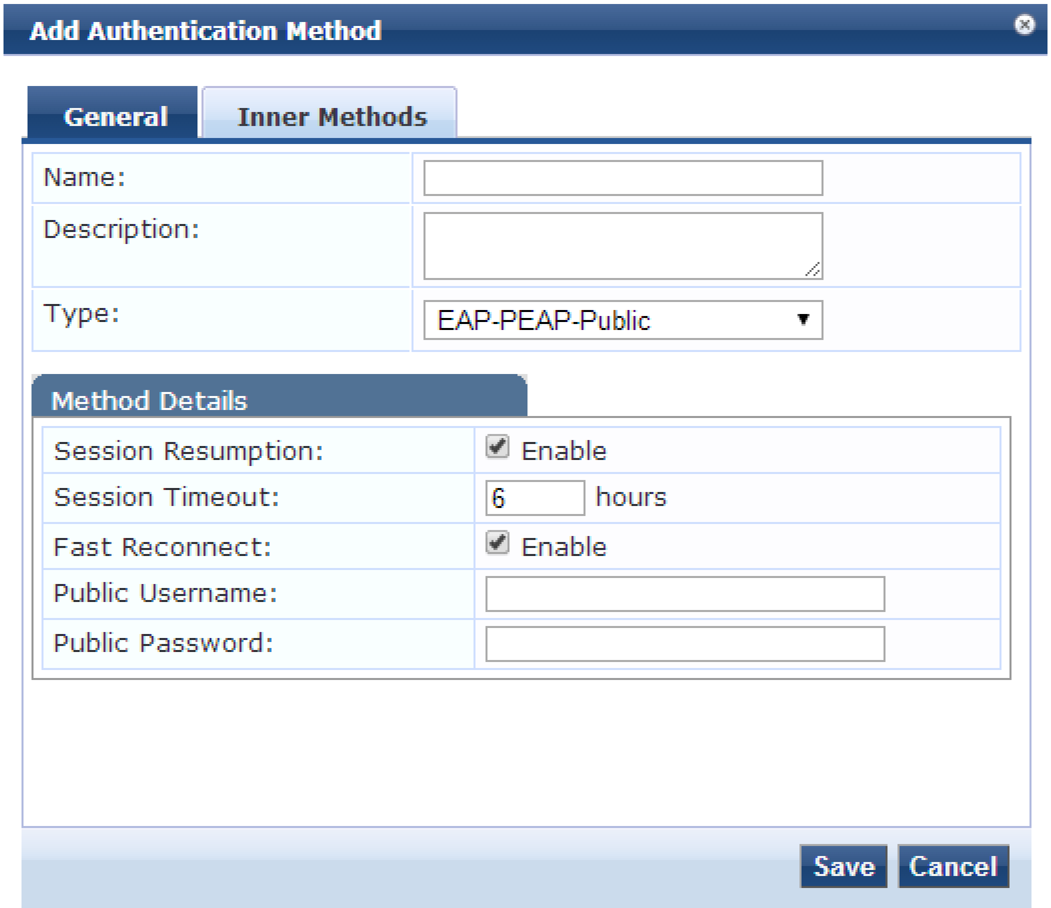
The **EAP-PEAP-Public** method contains the following two tabs:

- General on page 180
- Inner Methods on page 181

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 146: *EAP-PEAP-Public - General Tab*



Name:

Description:

Type: EAP-PEAP-Public

Session Resumption: ☑ Enable

Session Timeout: 6 hours

Fast Reconnect: ☑ Enable

Public Username:

Public Password:

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

Table 75: *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.

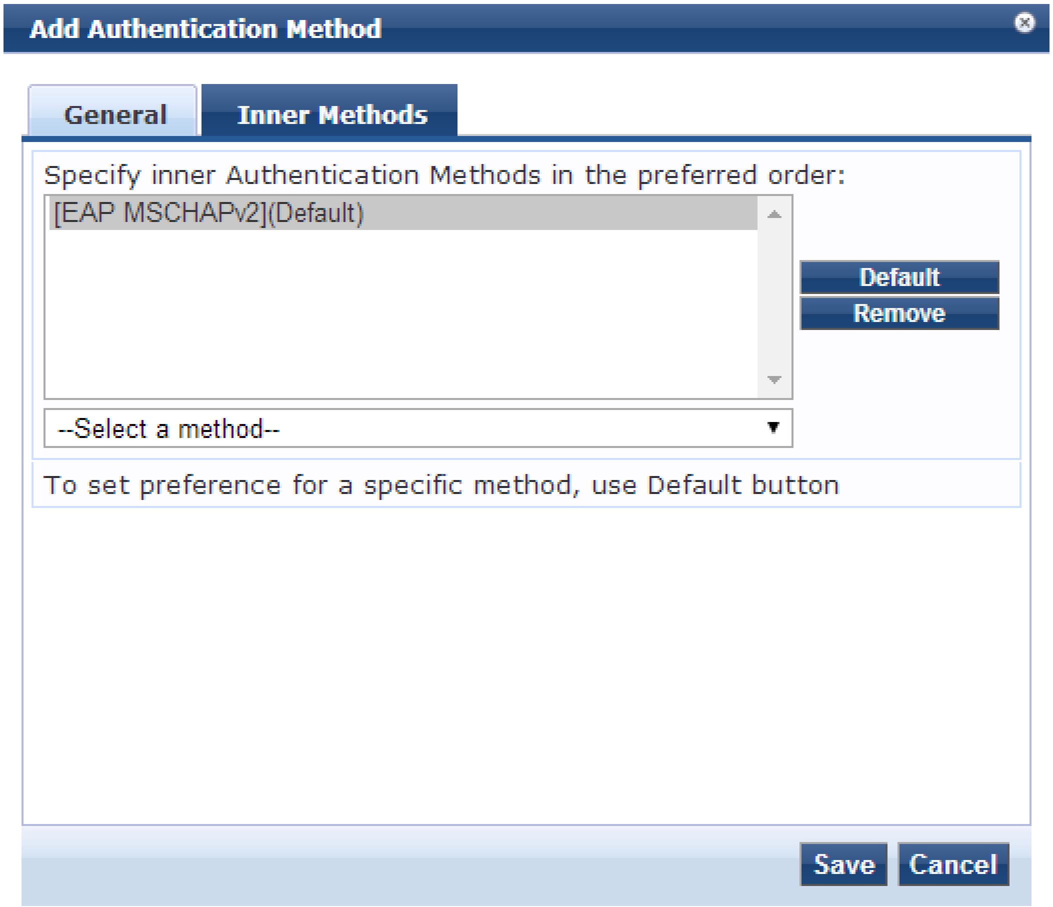
Table 75: *EAP-PEAP-Public - General Tab Parameters (Continued)*

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 147: *EAP-PEAP-Public - Inner Methods Tab*


Add Authentication Method
General
Inner Methods
Specify inner Authentication Methods in the preferred order:
[EAP MSCHAPv2](Default)
Default
Remove
--Select a method--
To set preference for a specific method, use Default button
Save
Cancel

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

Table 76: *EAP-PEAP-Public Inner Methods Tab Parameters*

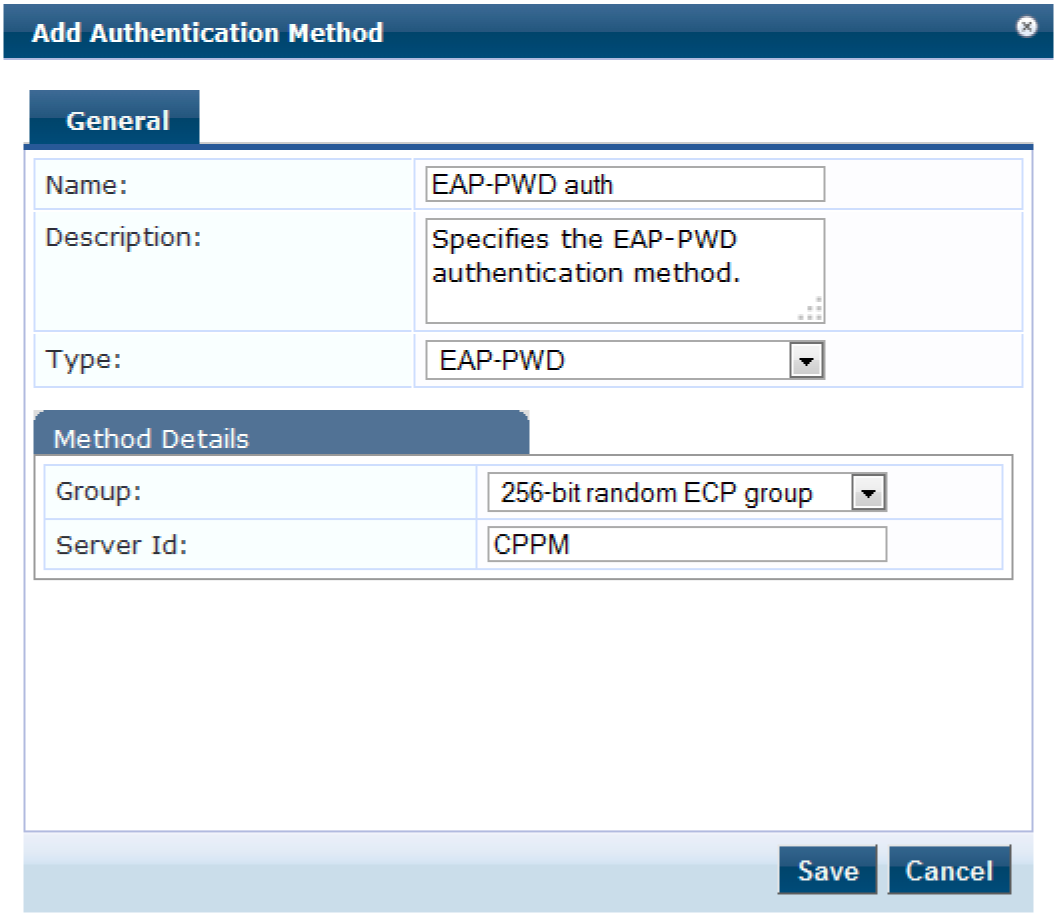
Parameter	Description
Specify inner authentication methods in the preferred order	Select the inner authentication method available from the drop-down list. In this context, only the EAP-MSCHAPv2 method is available. The following functions are available in this tab: ● To append an inner method to the 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 148: *EAP-PWD - General Tab*



Name:	EAP-PWD auth
Description:	Specifies the EAP-PWD authentication method.
Type:	EAP-PWD

Group:	256-bit random ECP group
Server Id:	CPPM

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

Table 77: *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.

To add the EAP-TLS authentication method:

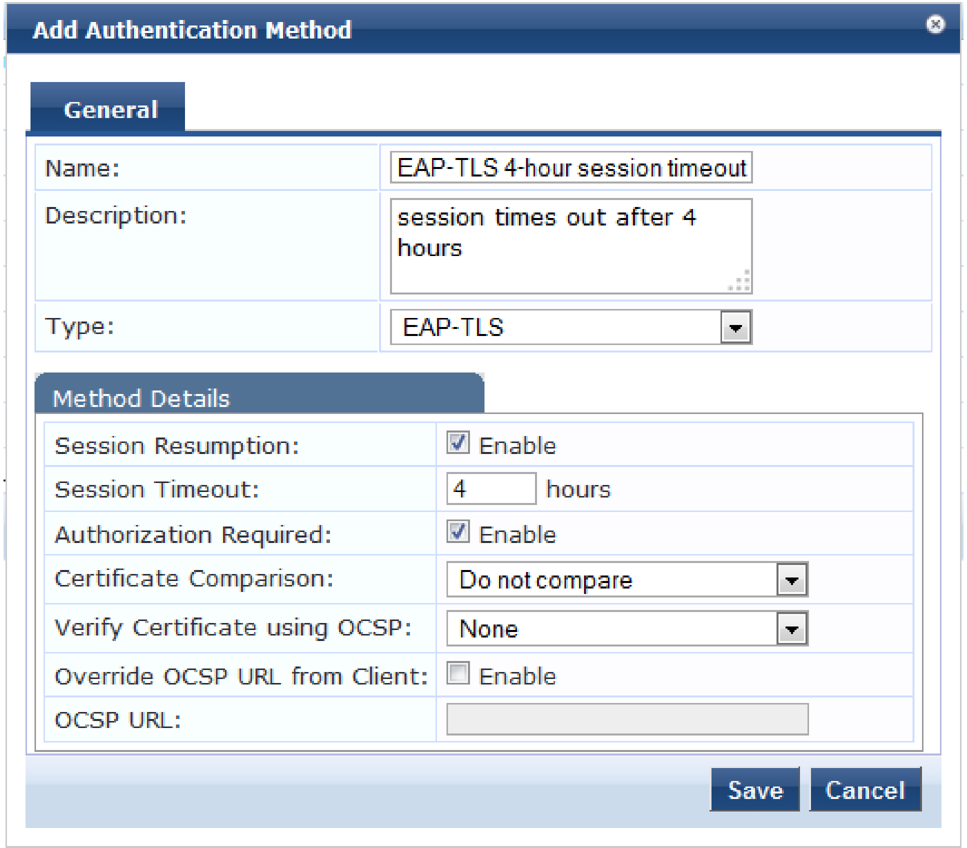
1. Navigate to **Configuration** > **Authentication** > **Methods**.

   The **Authentication Methods** page opens.

2. Click **Add**.

   The **Add Authentication Method** dialog opens.

Figure 149: *EAP-TLS Authentication Method Dialog*



Name: EAP-TLS 4-hour session timeout

Description: session times out after 4 hours

Type: EAP-TLS

Session Resumption: ☑ Enable

Session Timeout: 4 hours

Authorization Required: ☑ Enable

Certificate Comparison: Do not compare

Verify Certificate using OCSP: None

Override OCSP URL from Client: □ Enable

OCSP URL:

3. Specify the **Add Authentication Method** parameters as described in the following table, then click **Save**.

Table 78: *EAP_TLS Authentication Method Parameters*

Parameter	Action/Description
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method (recommended).
Method Details	
Type	Select **EAP_TLS**.
Session Resumption	This option is enabled by default. Caches EAP-TLS 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 cached EAP-TLS sessions to be retained. The default is 6 hours.
Authorization Required	This parameter is enabled by default. Specify whether to perform an authorization check.

Table 78: *EAP_TLS Authentication Method Parameters (Continued)*

Parameter	Action/Description
Certificate Comparison	Specify the type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate: ● To skip the certificate comparison, choose **Do not compare.** ● To compare specific attributes, choose **Compare Common Name (CN)**, **Compare Subject Alternate Name (SAN)**, or **Compare CN or SAN**. ● To perform a binary comparison of the stored (in the client record in Active Directory or another LDAP-compliant directory) and presented certificates, choose **Compare Binary**.
Verify Certificate using OCSP	● If the certificate is to be verified by the Online Certificate Status Protocol (OCSP), select **Optional** or **Required**. ● To not verify the certificate, select **None**.
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, 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.

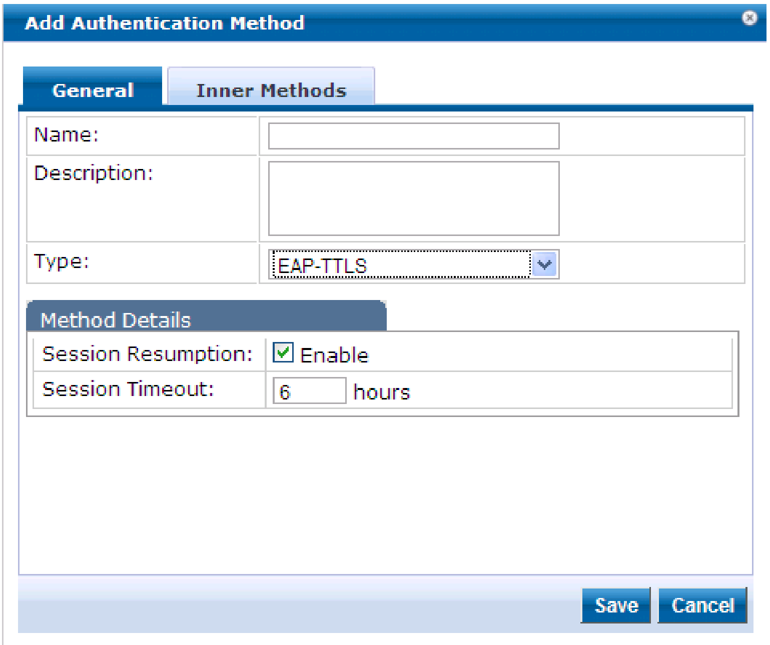
The **EAP-TTLS** method contains the following two tabs:

- General Tab on page 186
- Inner Methods Tab on page 187

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 150: *EAP-TTLS - General Tab*



Name:

Description:

Type: EAP-TTLS

Session Resumption: ☑ Enable

Session Timeout: 6 hours

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

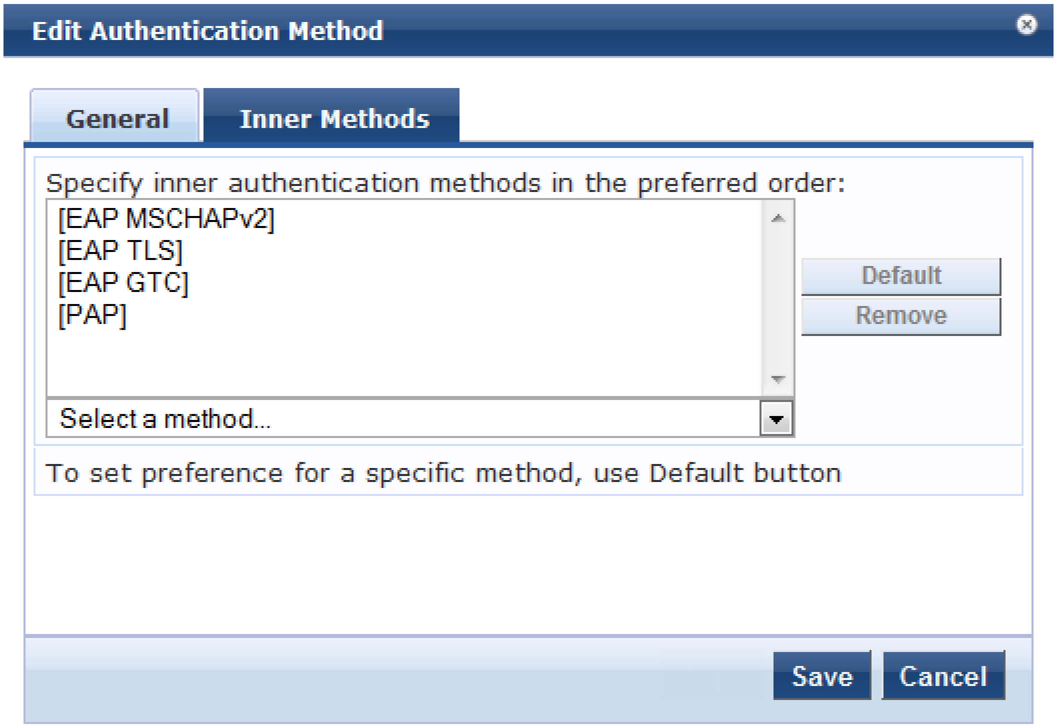
Table 79: *EAP-TTLS - General Tab Parameters*

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 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 151: *EAP_TTLS - Inner Methods Tab*



Specify inner authentication methods in the preferred order:

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

Select a method...

To set preference for a specific method, use Default button

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

Table 80: *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 ClearPass Policy Manager in the FIPS (**Administration** > **Server Manager** > **Server Configuration** > **FIPS** tab) mode.

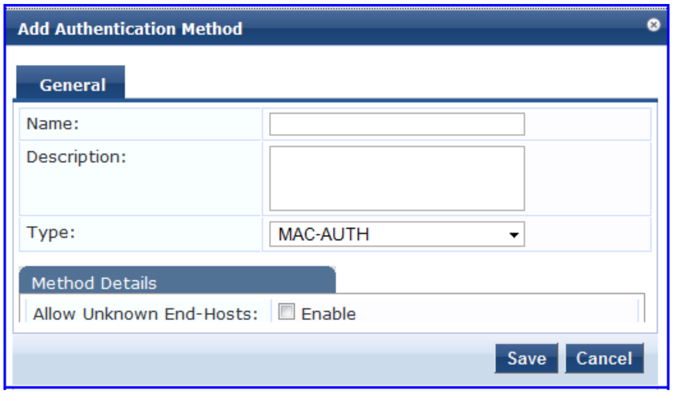
MAC-AUTH Authentication Method

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.

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

Figure 152: *Adding MAC-AUTH Authentication Method*



Add Authentication Method

General

Name:

Description:

Type: MAC-AUTH

Method Details

Allow Unknown End-Hosts: □ Enable

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

Table 81: *MAC-Auth Parameters*

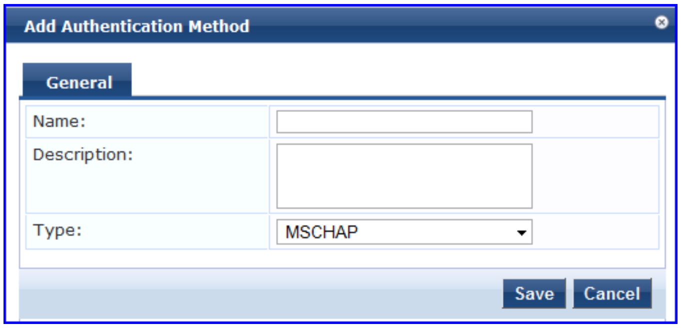
Parameter	Action/Description
General	
Name	Specify the name of the authentication method.
Description	Provide the additional information that helps to identify the authentication method (recommended).
Type	Select the **MAC-AUTH** type of authentication.
Method Details	
Allow Unknown End-Hosts	Select this check box to enable 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 338), 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 153: *MSCHAP - General Tab*



Name:	
Description:	
Type:	MSCHAP

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

Table 82: *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**.

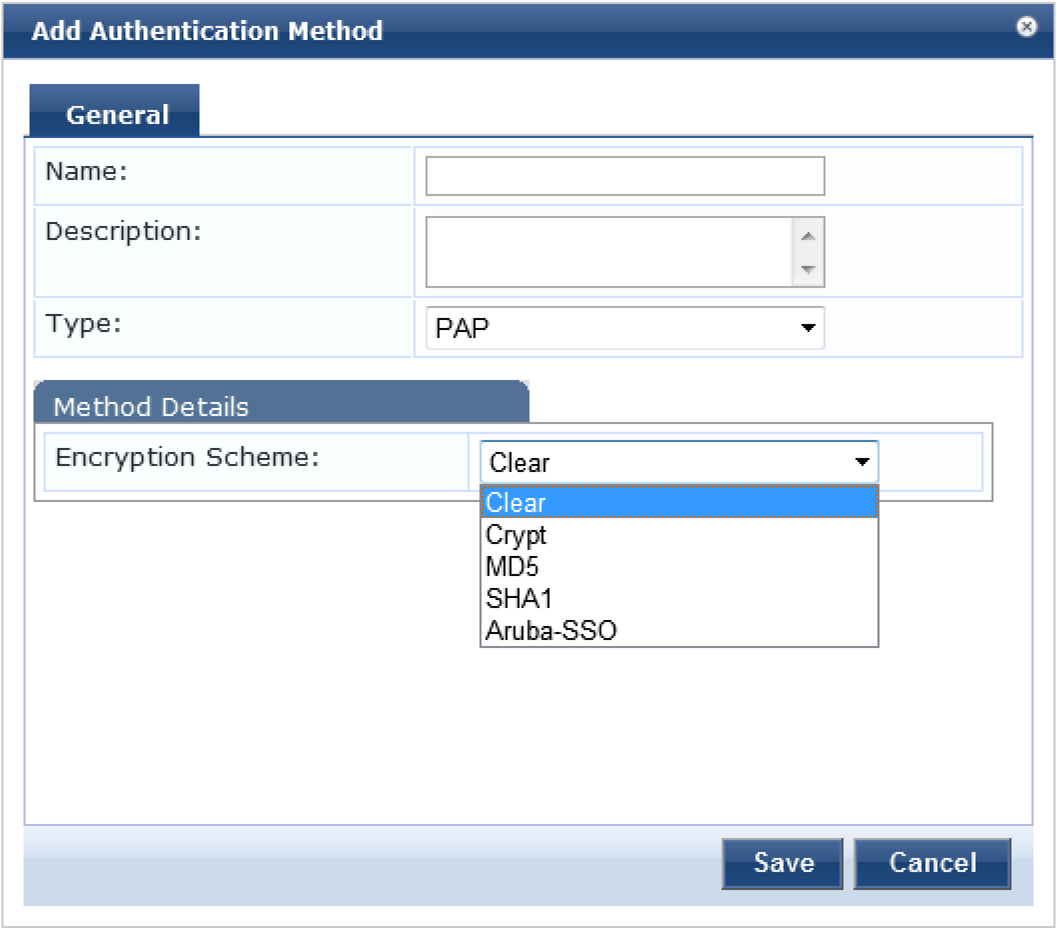
PAP

The Password Authentication Protocol (PAP) is an authentication protocol in which the user name and password are sent to the remote access server in unencrypted form.

The **Add Authentication Method** dialog identifies the authentication method—in this example, PAP—and defines the method details.

displays the **Add Authentication Method** > **PAP** dialog.

Figure 154: *Adding the PAP Authentication Method*



Add Authentication Method

General

Name:

Description:

Type: PAP

Method Details

Encryption Scheme: Clear

Table 83 describes the **PAP** parameters:

Table 83: *PAP Authentication Method Parameters*

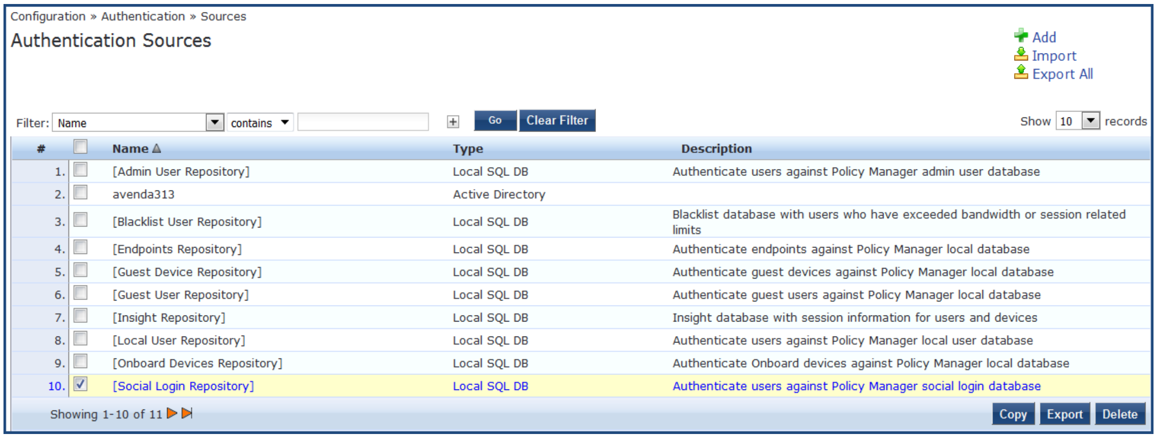
Parameter	Action/Description
Name	1. Specify the name of the authentication method.
Description	2. Provide the additional information that helps to identify the authentication method.
Type	3. Select **PAP** as the **Type** of authentication.
Method Details	
Enable Aruba-SSO	4. Enable or disable **Aruba-SSO** (Single Sign-On) by specifying **True** or **False**. The default is **False**.

Adding and Configuring Authentication Sources

To configure an authentication source for a new service:

1. Navigate to **Configuration** > **Authentication** > **Sources**.

Figure 155: *Authentication Sources Page*



Configuration » Authentication » Sources

Authentication Sources

Filter: Name contains

Show 10 records

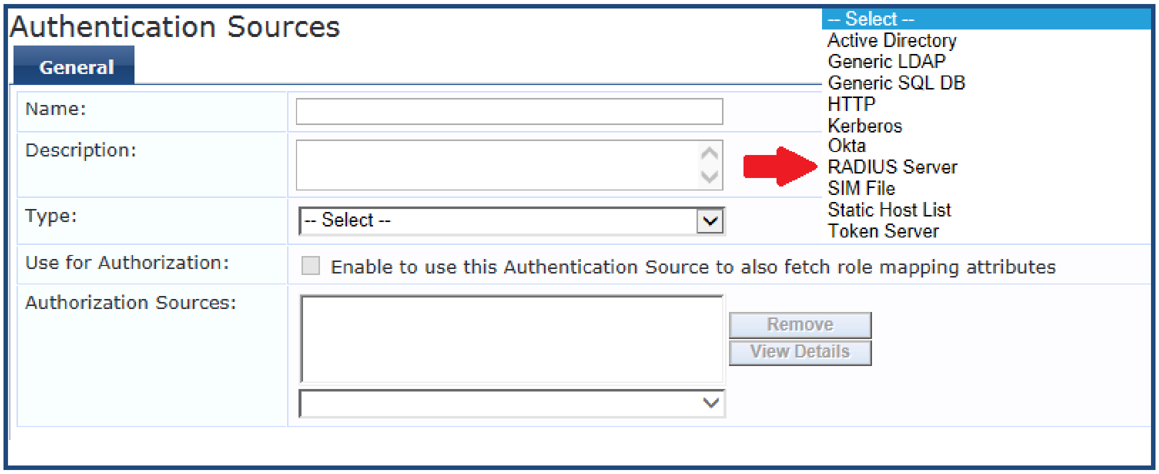
#		Name	Type	Description
1.	□	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	□	avenda313	Active Directory	
3.	□	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
4.	□	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
5.	□	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
6.	□	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
7.	□	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
8.	□	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
9.	□	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
10.	☑	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database

Showing 1-10 of 11

2. Click **Add**.

   The **Add Authentication Sources** page opens. Different tabs and fields appear, depending on the authentication source selected.

Figure 156: *Add Authentication Source Page*



Authentication Sources

Name:	
Description:	
Type:	-- Select --
Use for Authorization:	□ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	

Refer to the following sections to configure these authentication sources:

- Generic LDAP and Active Directory
- Generic SQL DB
- HTTP
- Kerberos
- Okta
- RADIUS Server
- Adding a Static Host List as an Authentication Source
- Token Server

Generic LDAP and Active Directory

This section includes the following information:

- General Configuration on page 192
- Primary Server Configuration on page 194
- Attributes Configuration on page 196

- Summary Information on page 204

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 configuration details, see Adding and Modifying Role-Mapping Policies on page 258.

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

General Configuration

To add a new Generic LDAP and Active Directory:

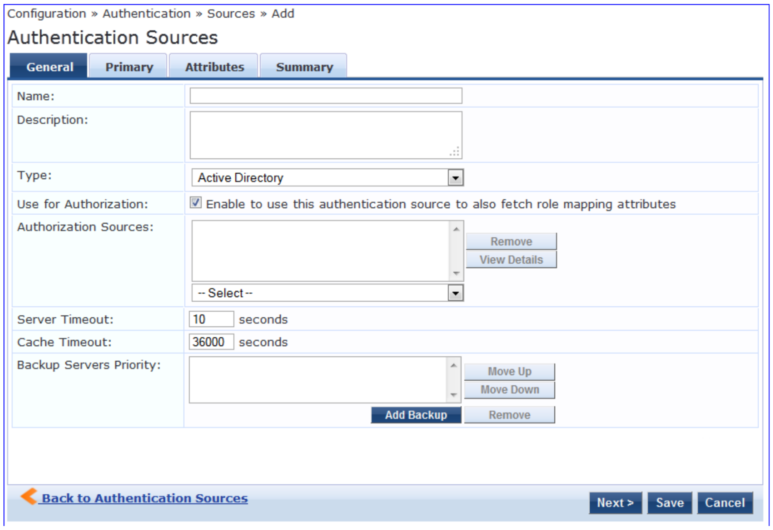
Navigate to **Configuration** > **Authentication** > **Sources**.

The **Authentication Sources** page opens.

Click **Add**.

The **Add Authentication Sources** dialog opens.

Figure 157: *Active Directory or Generic LDAP Configuration Dialog*



Configuration » Authentication » Sources » Add

Authentication Sources

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

Specify the **Generic Active Directory** or **LDAP > General** parameters as described in the following table:

Table 84: *Active Directory or GEneric LDAP Authentication Source> General Parameters*

Parameter	Action/Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source (recommended).
Type	Select **Active Directory** or **Generic LDAP**.
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

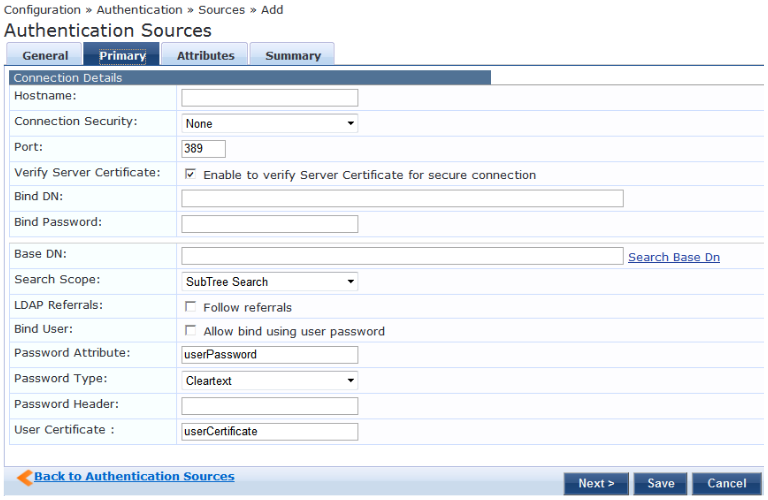
Table 84: *Active Directory or GEneric LDAP Authentication Source> General Parameters (Continued)*

Parameter	Action/Description
	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 checked (enabled) by default.
Authorization Sources	Specify additional sources from which role-mapping attributes are to be fetched. 1. Select a previously configured authentication source from the drop-down list. 2. To add the authentication source to the list of authorization sources, click **Add**. - To remove the authentication source from the list, click **Remove**. If Policy Manager authenticates the user or device from this authentication source, then also fetches role-mapping attributes from these additional authorization sources. **NOTE:** You can specify additional authorization sources at the service level. Policy Manager fetches role-mapping attributes regardless of which authentication source the user or device was authenticated against.
Server Timeout	Specify the duration in number of seconds that Policy Manager waits before considering this server unreachable. If multiple backup servers are available, 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	Specify the duration in number of seconds for which the attributes are cached. Policy Manager caches attributes fetched for an authenticating entity.
Backup Servers Priority	- To add a backup server, click **Add Backup**. When the **Backup 1** tab appears, you can specify connection details for a backup server. - To remove a backup server, select the server name and click **Remove**. - To change the server priority of the backup servers, select a server, then select **Move Up** or **Move Down**. This is the order in which Policy Manager attempts to connect to the backup servers if the primary server is unreachable.

Primary Server Configuration

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

Figure 158: *Generic LDAP or Active Directory > Primary Tab*



Hostname:	
Connection Security:	None
Port:	389
Verify Server Certificate:	☑ Enable to verify Server Certificate for secure connection
Bind DN:	
Bind Password:	
Base DN:	
Search Scope:	SubTree Search
LDAP Referrals:	□ Follow referrals
Bind User:	□ Allow bind using user password
Password Attribute:	userPassword
Password Type:	Cleartext
Password Header:	
User Certificate :	userCertificate

Specify the **Active Directory** or **Generic LDAP > Primary** parameters as described in the following table:

Table 85: *Active Directory or Generic LDAP > Primary Parameters*

Parameter	Action/Description
Hostname	Specify the hostname or the IP address of the LDAP or Active Directory server.
Connection Security	- For a default nonsecure connection (usually port 389), select **None**. - For a secure connection that is negotiated over the standard LDAP port, select **StartTLS**. This is the preferred way to connect to an LDAP directory securely. - To choose the legacy way of securely connecting to an LDAP directory, select **LDAP over SSL** or **AD over SSL**. You must use port **636** for this type of connection.
Port	Specify 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 check box to verify the server certificate as part of authentication.
Bind DN	Specify the DN (Distinguised Name) 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.

Table 85: *Active Directory or Generic LDAP > Primary Parameters (Continued)*

Parameter	Action/Description
	NOTE: This setting is available only for Active Directory.
Base DN	Enter the DN (Distinguished Name) of the node in your directory tree from which to start searching for records. 1. 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. 2. Click on any node in the tree structure that is displayed to select it as a base DN. Note that the base DN is displayed at the top of the LDAP browser. **NOTE:** This is also a method to test the connectivity to your LDAP or AD directory. If the values entered for the primary server attributes are correct, you can browse the directory hierarchy by clicking **Search Base Dn**.
Search Scope	Select the scope of the search you want to perform, starting at the base DN. - **Base Object Search** allows you to search at the level specified by the base DN. - **One Level Search** allows you to search up to one level lesser to the immediate children of the base DN. - **Subtree Search** allows you to search the entire subtree under the base DN (including at the base DN level).
LDAP Referral	Enable this check box to automatically follow referrals returned by your directory server in search results. Refer to your directory documentation for more information on referrals.
Bind User	Enable this check box 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 clear text.
Password Attribute	Enter the name of the attribute in the user record from which user password can be retrieved. **NOTE:** This is available only for **Generic LDAP** and is not available for Active Directory.
Password Type	Specify whether the password type is Cleartext, NT Hash, or LM Hash. **NOTE:** This is available only for **Generic LDAP**.

Table 85: *Active Directory or Generic LDAP > Primary Parameters (Continued)*

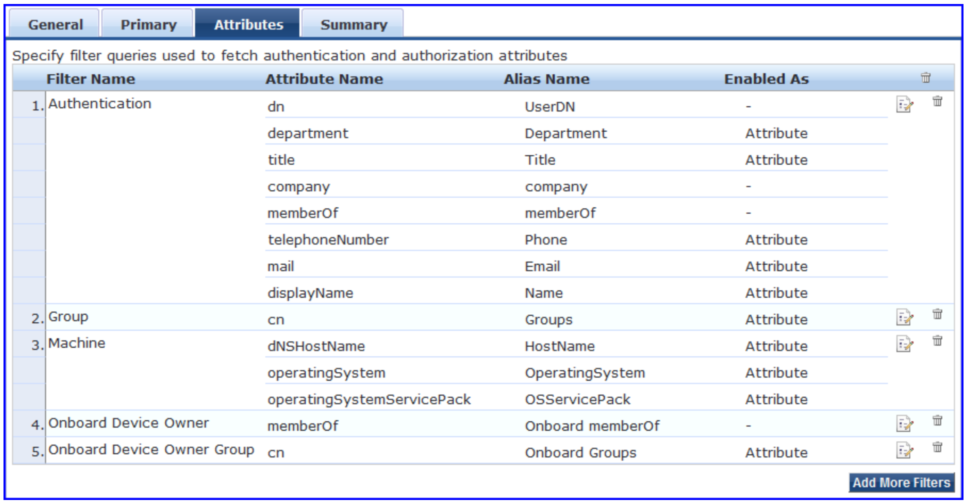
Parameter	Action/Description
Password Header	Specify Oracle's LDAP implementation that prepends a header to a hashed password string. If using Oracle LDAP, enter the header in this field to correctly identify and read the password. **NOTE:** This is available only for **Generic LDAP** and is not available for Active Directory.
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 the NetBIOS name instead of the domain part in the username for authentication. **NOTE:** This field is available only if you select **Active Directory** as an authentication source.

Attributes Configuration

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

The following figures are the examples of the **Active Directory** > **Attributes** tab and the **Generic LDAP Directory** > **Attributes** tab:

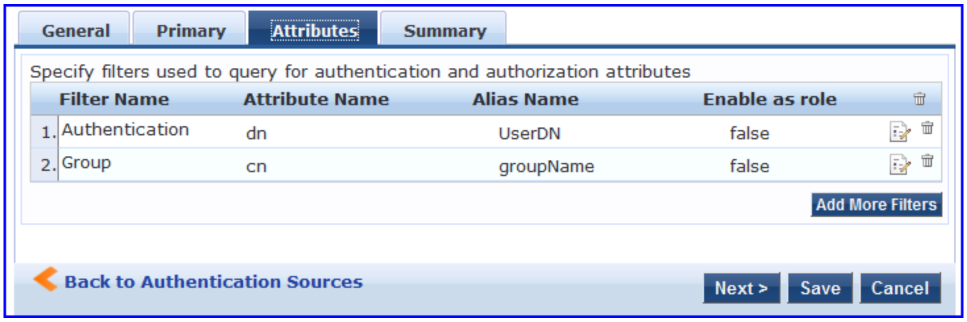
Figure 159: *Active Directory Attributes Dialog*



Specify filter queries used to fetch authentication and authorization attributes

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

Figure 160: *Generic LDAP Directory > Attributes Dialog*



Specify filters used to query for authentication and authorization attributes

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

Specify the **Active Directory** or **LDAP Attributes > Filter Listing Screen** parameters as described in the following table:

Table 86: *Active Directory or Generic LDAP Attributes > Filter Listing Parameters*

Parameter	Action/Description
Filter Name	Specify the name of the filter.
Attribute Name	Specify the name of the LDAP or Active Directory 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 87: *Active Directory/Generic 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:

Table 87: *Active Directory/Generic LDAP Default Filters (Continued)*

Directory	Default Filters
	- **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}))` - 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.

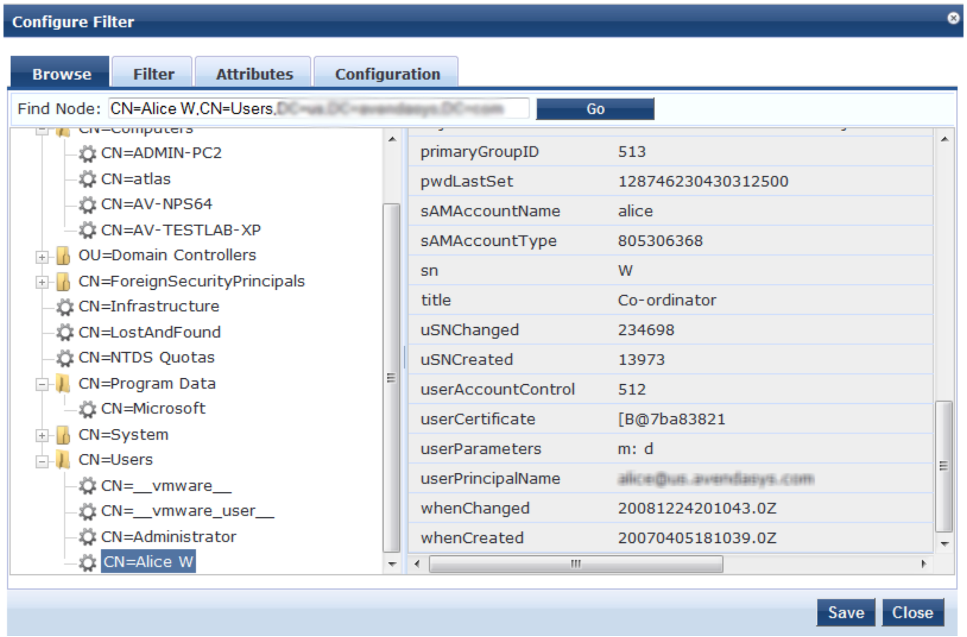
Browse Configuration

The **Browse** tab shows an LDAP browser from which you can browse the nodes in the LDAP or Active Directory 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 figure is an example of the **Active Directory** or **Generic LDAP Configure Filter** > **Browse** dialog:

Figure 161: *Active Directory or Generic LDAP Configure Filter > Browse Dialog*



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

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

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

Specify the **Active Directory** or **Generic LDAP Configure Filter Page > Browse** tab parameter as described in the following table:

Table 88: *Active Directory or Generic LDAP Configure Filter Page > Browse Tab Parameter*

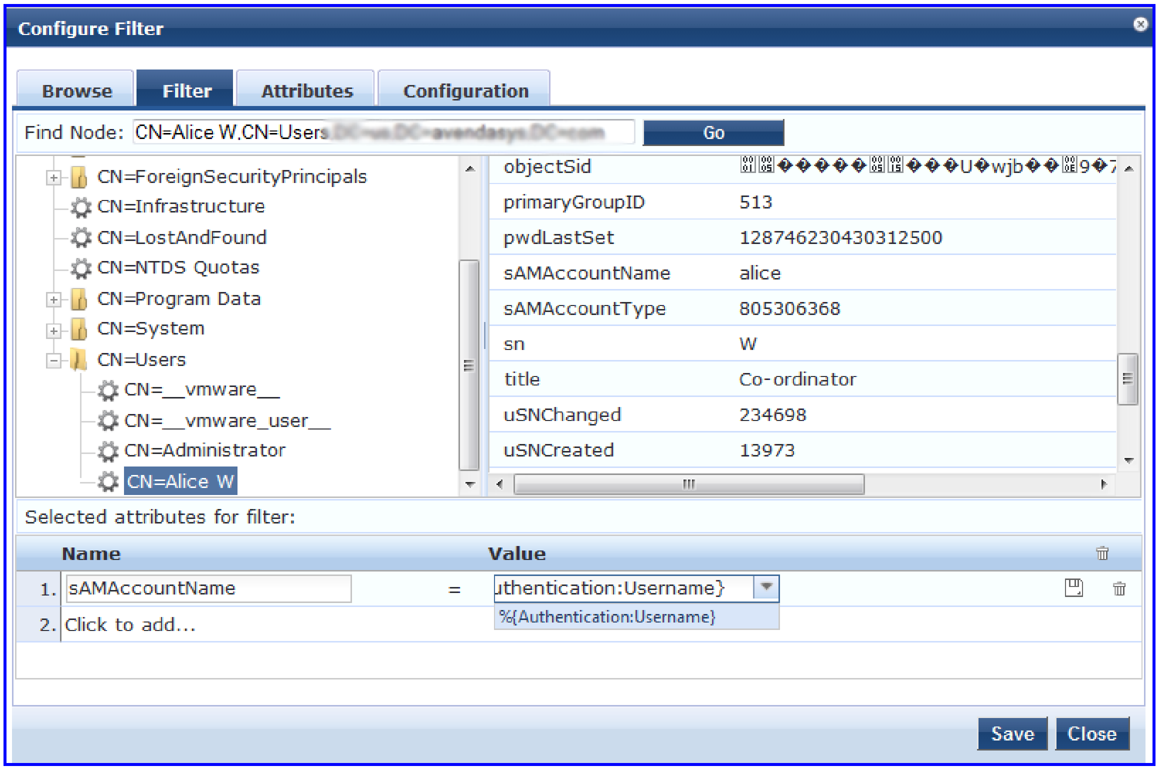
Navigation	Action/Description
Find Node	To find the node, enter the DN, then click the **Go** button.

Filter Configuration

The **Filter** tab provides an LDAP browser interface to define the filter search query.

The following figure is an example of the **Active Directory** or **Generic LDAP Create Filter Page** > **Filter** configuration dialog:

Figure 162: *Active Directory or Generic LDAP Create Filter Page > Filter Dialog*



Configure Filter

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

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

objectSid	������U�wjb��9�7
primaryGroupID	513
pwdLastSet	128746230430312500
sAMAccountName	alice
sAMAccountType	805306368
sn	W
title	Co-ordinator
uSNChanged	234698
uSNCreated	13973

Selected attributes for filter:

	Name		Value
1.	sAMAccountName	=	uthentication:Username}
2.	Click to add...		

%{Authentication:Username}

Policy Manager is preconfigured 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.

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 89: *Configure Filter Page > Filter Tab Parameters*

Parameter	Action/Description
Find Node	To find a node, enter the DN, then click 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 find a user or device connecting to the network in LDAP or Active Directory. 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. Select the attributes that help Policy Manager 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).

   After Step 2, you can have values for a specific record (in this example, Alice's record).

3. Change the value to a dynamic session attribute that helps Policy Manager associate a session with a specific record in LDAP/Active Directory.

   For example, if you selected the **sAMAccountName** attribute in Active Directory, click 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.

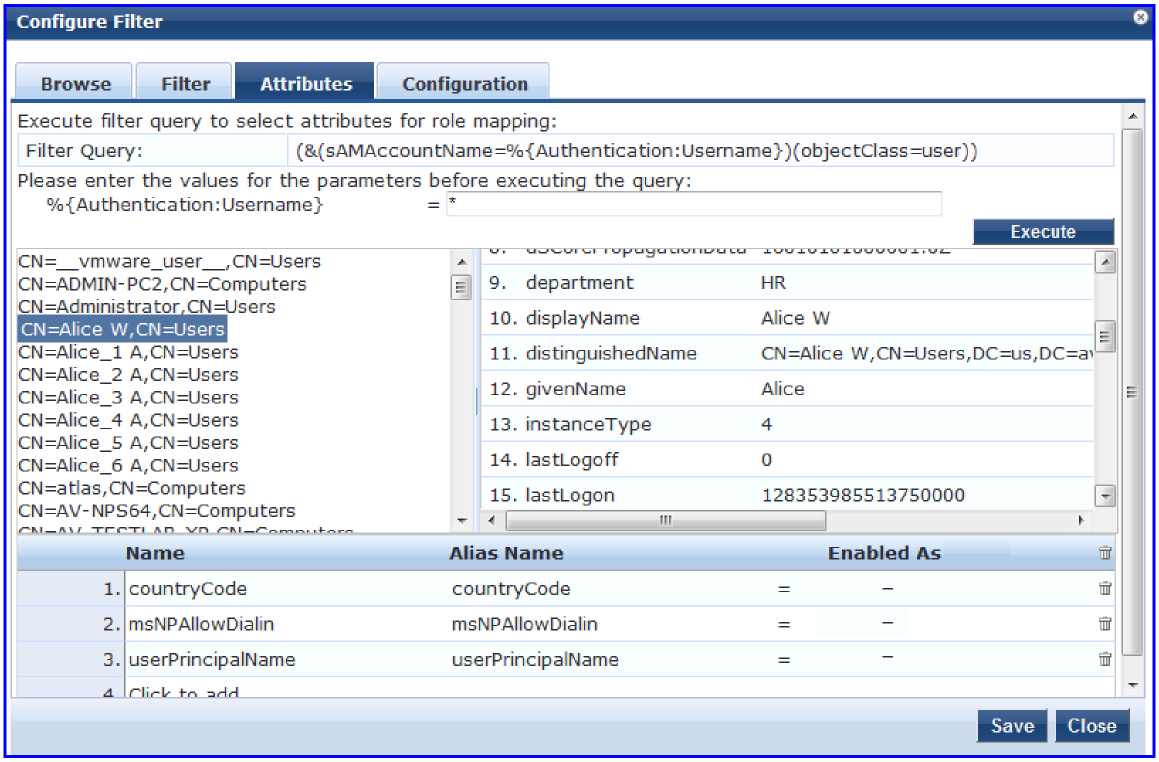
Attributes Configuration

The **Attributes** tab defines the attributes to be fetched from the Active Directory or LDAP directory.

You can also enable each attribute 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 355.

The following figure displays the **Active Directory** or **Generic LDAP Configure Filter > Attributes** tab:

Figure 163: *Active Directory or Generic LDAP Configure Filter > Attributes Dialog*



Execute filter query to select attributes for role mapping:

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

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

%{Authentication:Username} = *

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

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

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

Specify the **Active Directory/LDAP Configure Filter Page > Attributes** tab parameters as described in the following table:

Table 90: *Active Directory/LDAP Configure Filter Page > Attributes Parameters*

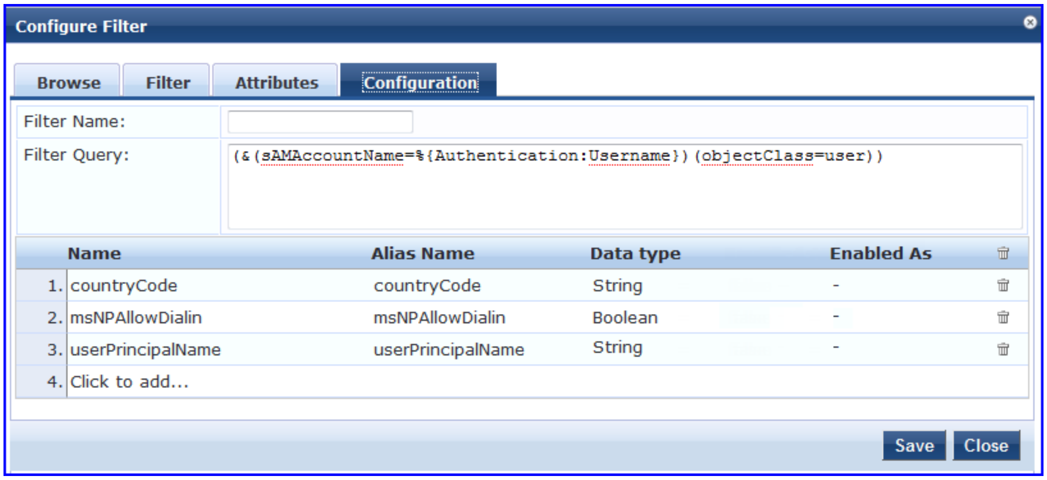
Parameter	Action/Description
Enter values for parameters	Policy Manager parses the filter query (created in the **Filter** tab and shown at the top of the **Attributes** tab) and prompts to enter the values for all dynamic session parameters in the query. For example, if you have **%{Authentication:Username}** 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	1. 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. 2. Click on one of the entries (nodes) to view the list of attributes for that node. 3. 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 check box 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 the attributes to be fetched.

The following figure displays the **Configure Filter > Configuration** dialog:

Figure 164: *Configure Filter > Configuration Dialog*



Filter Name:

Filter Query:

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

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

Modify Default Filters

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

To modify these predefined filters:

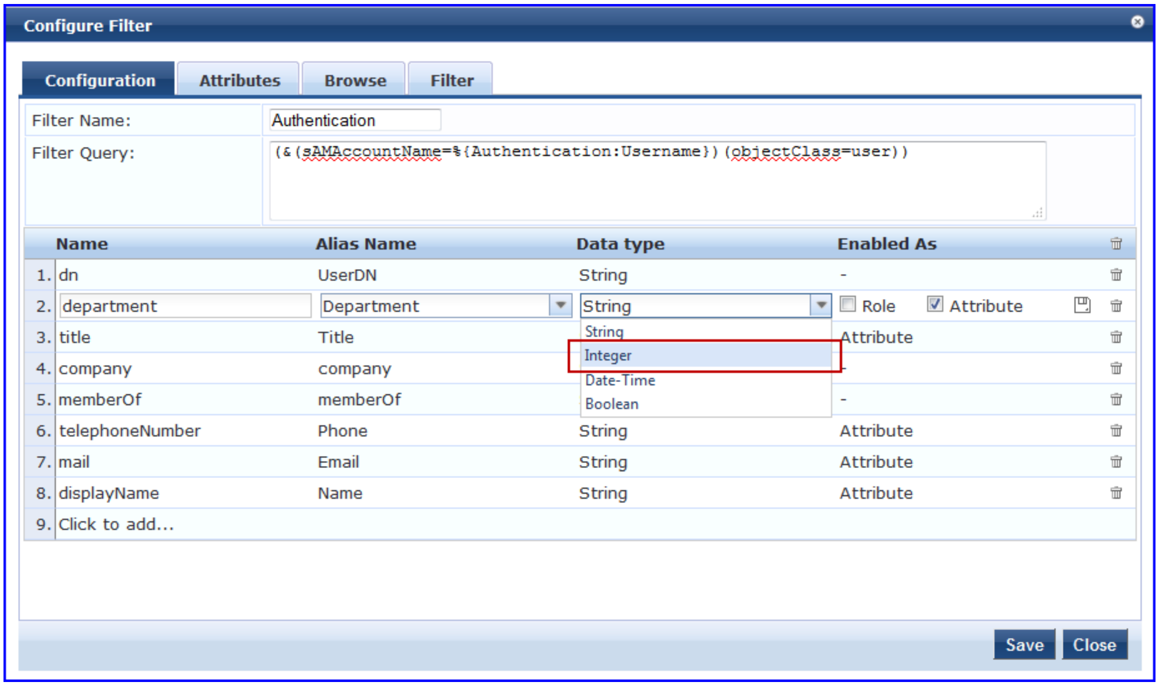
1. Select a filter on the **Authentication > Sources > Attributes** dialog.

   The **Configure Filter** page for the specified filter opens.

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 165: *Modify Default Filters > Configuration Dialog*



Filter Name: Authentication

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

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

The attributes that are defined for the authentication source display as attributes in role-mapping policy Rules Editor under the authorization source namespace.

2. From the **Configure Filter** > **Configuration** dialog, select the attribute you wish to modify.
3. Change the attribute operator values as needed, then click **Save**.

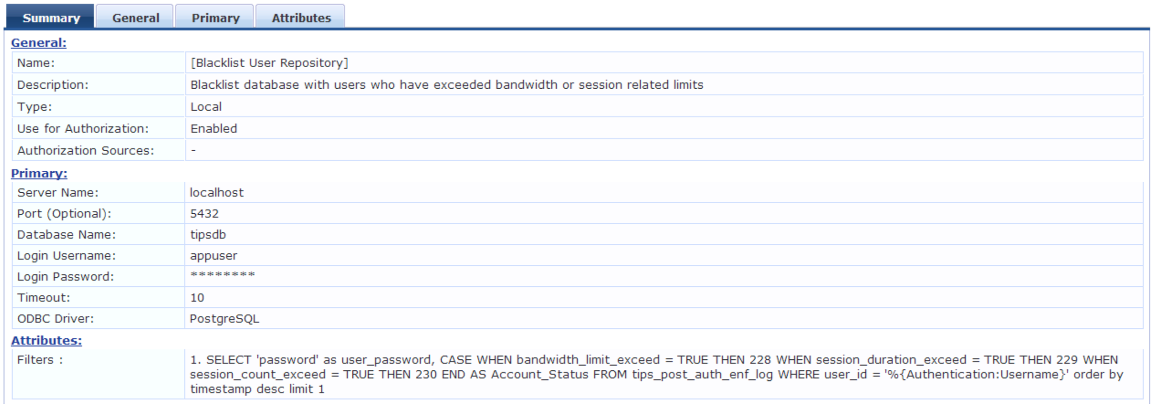
   The operator values that display are based on the **Data Type** specified here.

   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 Information

You can use the **Summary** tab to view configured parameters. The following figure is an example of the **Active Directory** > **Summary** information:

Figure 166: *Active Directory Authentication Source > Summary Information*



General:

Name:	[Blacklist User Repository]
Description:	Blacklist database with users who have exceeded bandwidth or session related limits
Type:	Local
Use for Authorization:	Enabled
Authorization Sources:	-

Primary:

Server Name:	localhost
Port (Optional):	5432
Database Name:	tipsdb
Login Username:	appuser
Login Password:	********
Timeout:	10
ODBC Driver:	PostgreSQL

Attributes:

Filters :	1. SELECT 'password' as user_password, CASE WHEN bandwidth_limit_exceed = TRUE THEN 228 WHEN session_duration_exceed = TRUE THEN 229 WHEN session_count_exceed = TRUE THEN 230 END AS Account_Status FROM tips_post_auth_enf_log WHERE user_id = '%{Authentication:Username}' order by timestamp desc limit 1

Generic SQL DB

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 205
- Primary Tab on page 207
- Attributes Tab on page 208
- Summary Tab on page 209

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.

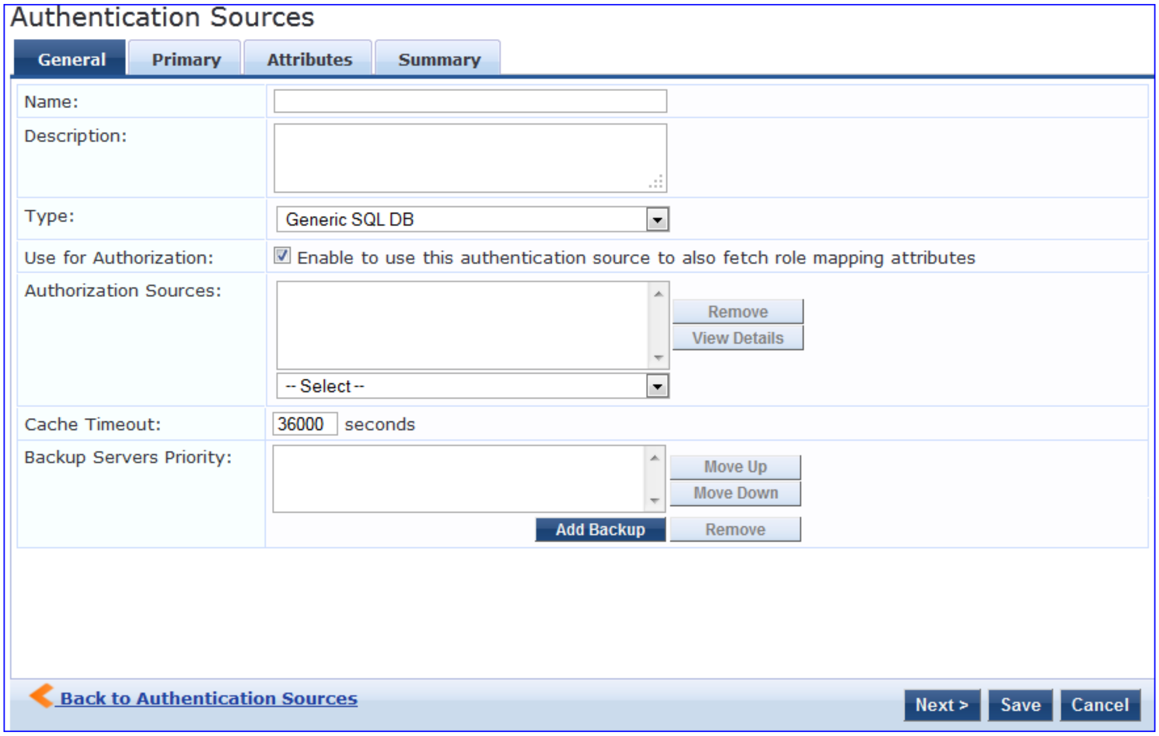
The **Configuration > Authentication > Sources > Add** page includes two configuration options for managing existing Generic SQL DB authentication source:

- The **Clear Cache** option clears the attributes cached by Policy Manager for all entities that authorize against this server.
- 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.

Figure 167: *Generic SQL DB > General Tab*



Authentication Sources

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

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

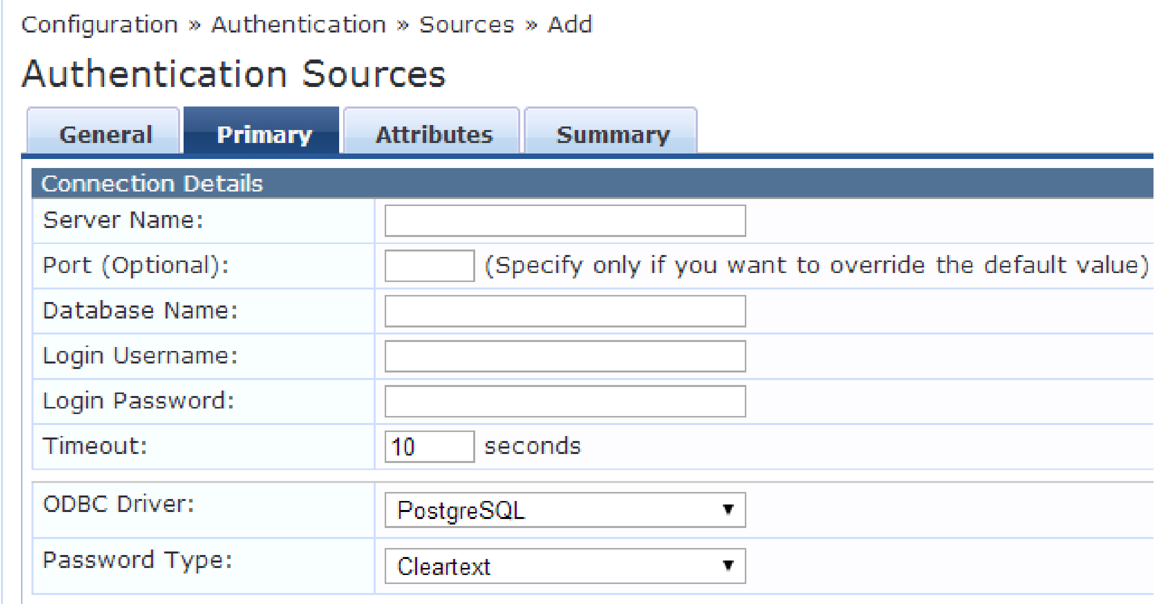
Table 91: *General SQL DB > General Tab Parameters*

Parameter	Action/Description
Name	Specify the name of the authentication source.
Description	Provide the additional information that helps to identify the authentication source.
Type	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.
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:** 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 168: *General SQL DB > Primary Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Connection Details

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

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

Table 92: *Generic SQL DB > Primary Tab Parameters*

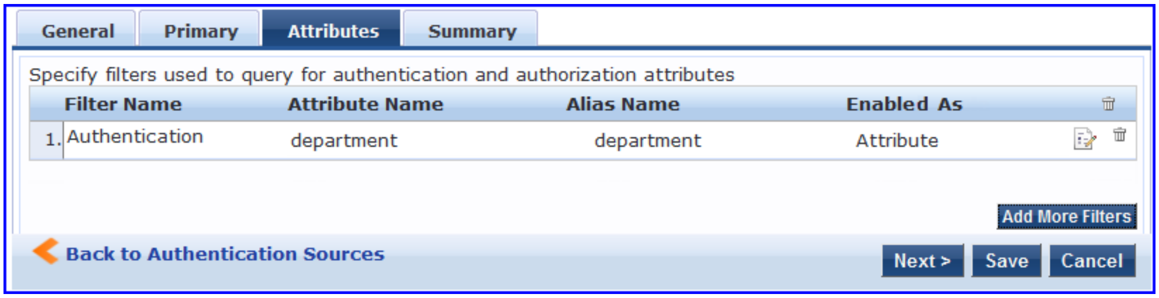
Parameter	Action/Description
Server Name	Enter the hostname or IP address of the database server.
Port (Optional)	Specify a port value to override the default port.
Database Name	Enter the name of the database from which records can be retrieved.
Login Username	Enter the name of the user used to log 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.

Parameter	Action/Description
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. Aruba does not ship MySQL drivers by default. If you require MySQL, contact Aruba support to get the required patch. This patch does not persist across upgrades. 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 : Stored as clear, unencrypted text. ● NT Hash: Stored with an NT hash using MD4. ● LM Hash : Stored with a LAN Manager Hash using DES. ● SHA: Stored with a Secure Hash Algorighm (SHA) hash. ● SHA256: 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 169: *Generic SQL DB > Attributes Tab*



Specify filters used to query for authentication and authorization attributes

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

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

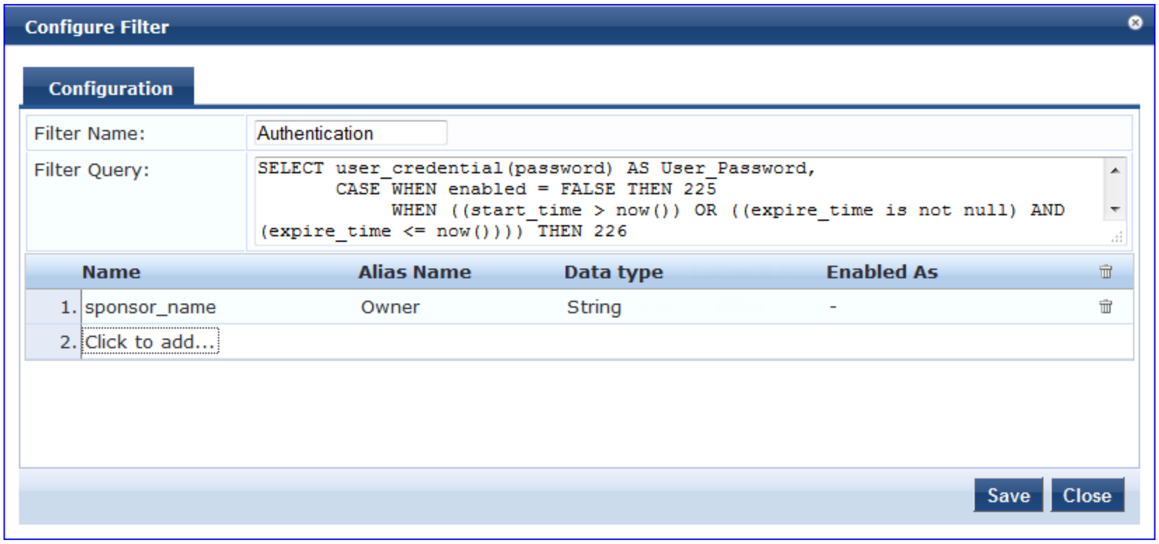
Table 93: *Generic SQL DB > Attributes Tab (Filter List) Parameters*

Parameter	Action/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.

Parameter	Action/Description
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 170 displays the **Generic SQL DB > Configure Filter** page.

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

Figure 170: *Generic SQL DB > Configure Filter Page*



Filter Name: Authentication

Filter Query:

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

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

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

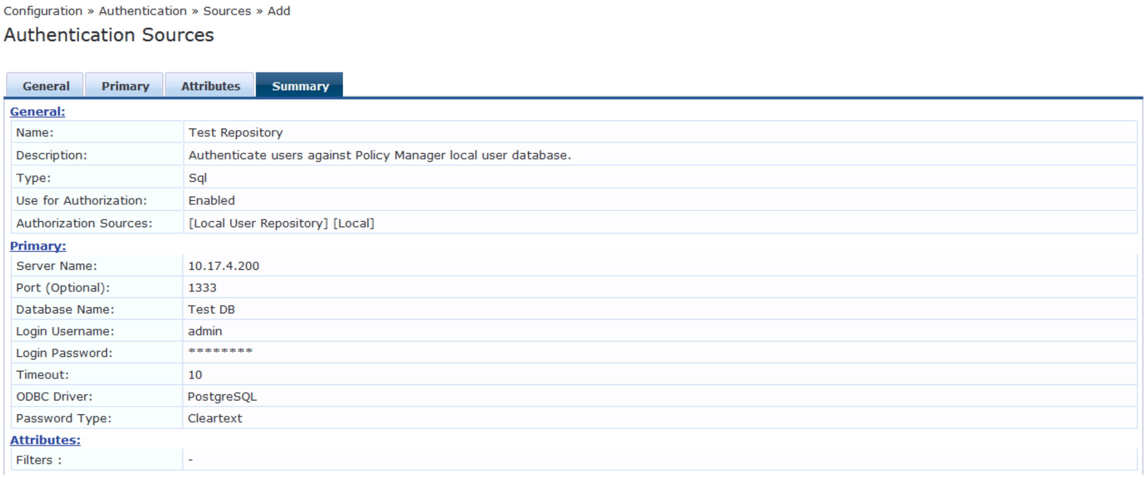
Table 94: *Generic SQL DB > Configure Filter Page Parameters*

Parameter	Action/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 171: *Generic SQL DB > Summary Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

General:

Name:	Test Repository
Description:	Authenticate users against Policy Manager local user database.
Type:	Sql
Use for Authorization:	Enabled
Authorization Sources:	[Local User Repository] [Local]

Primary:

Server Name:	10.17.4.200
Port (Optional):	1333
Database Name:	Test DB
Login Username:	admin
Login Password:	********
Timeout:	10
ODBC Driver:	PostgreSQL
Password Type:	Cleartext

Attributes:

Filters :	-

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.

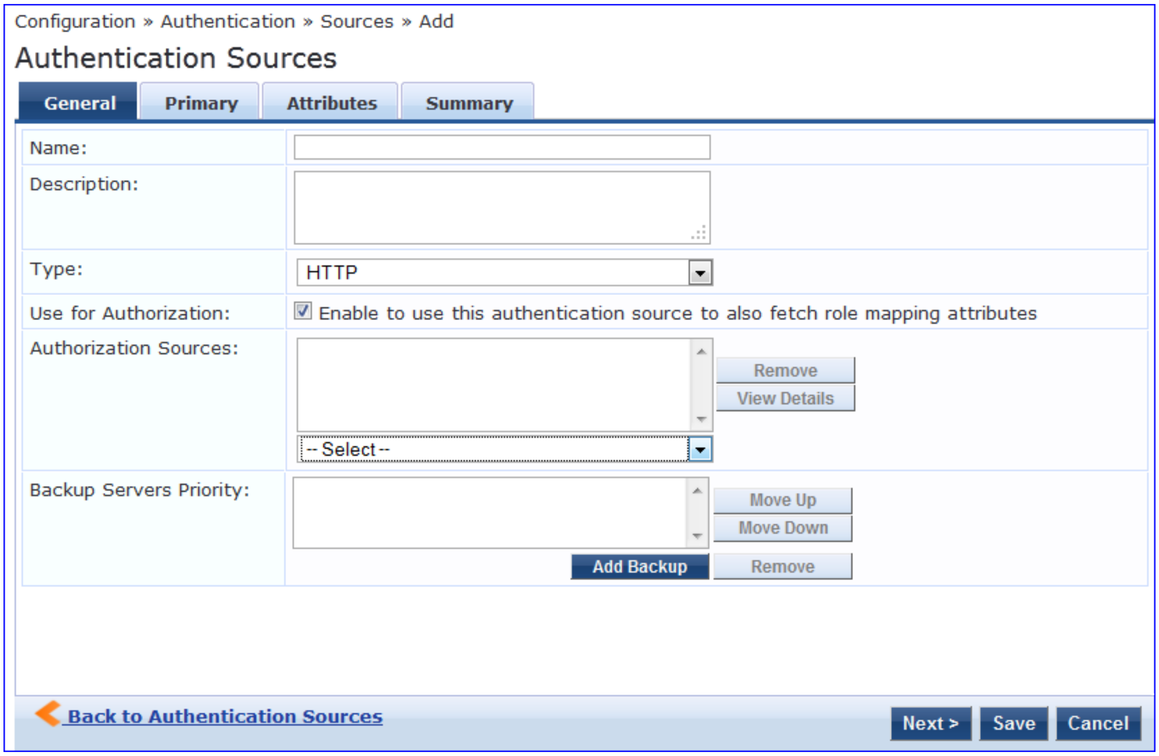
Configure primary and backup servers, session details, filter query, and role mapping attributes to fetch HTTP authentication sources using the following tabs:

- General Tab on page 211
- Primary Tab on page 212
- Attributes Tab on page 213
- Summary Tab on page 215

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 172: *HTTP - General Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Name:

Description:

Type: HTTP

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

Authorization Sources: -- Select --

Backup Servers Priority:

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

Table 95: *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**.

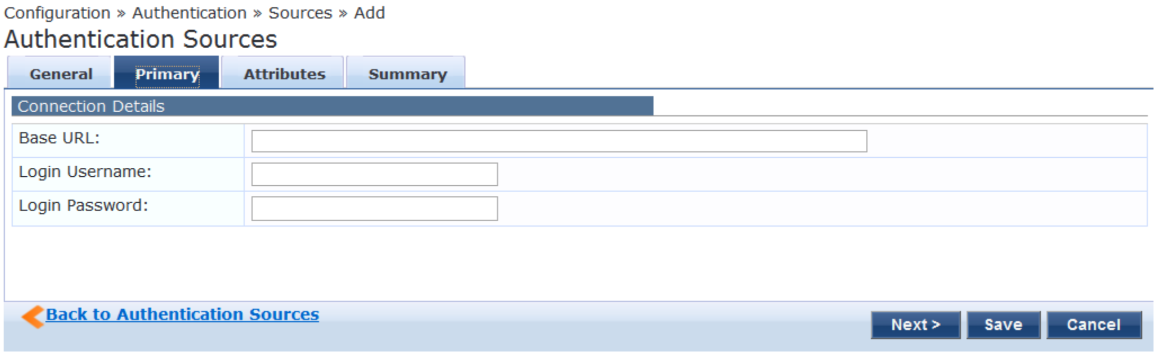
Table 95: *HTTP - General Tab Parameters (Continued)*

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:** 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 173: *HTTP - Primary Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Connection Details

Base URL:	
Login Username:	
Login Password:	

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

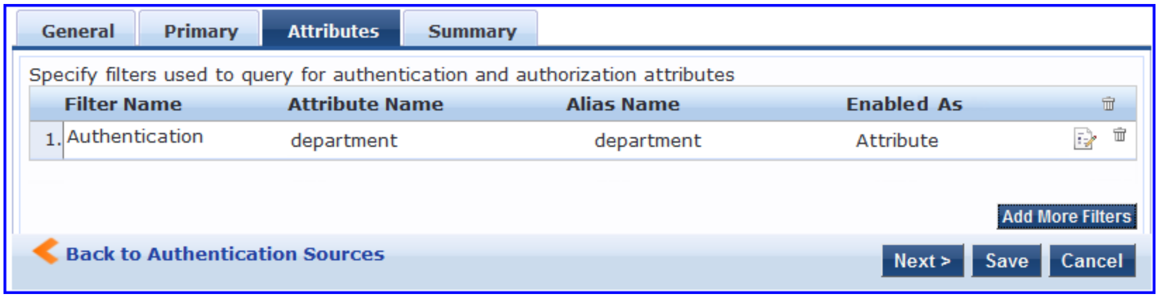
Table 96: *HTTP - Primary Tab Parameters*

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 174: *HTTP - Attributes Tab*



Specify filters used to query for authentication and authorization attributes

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

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

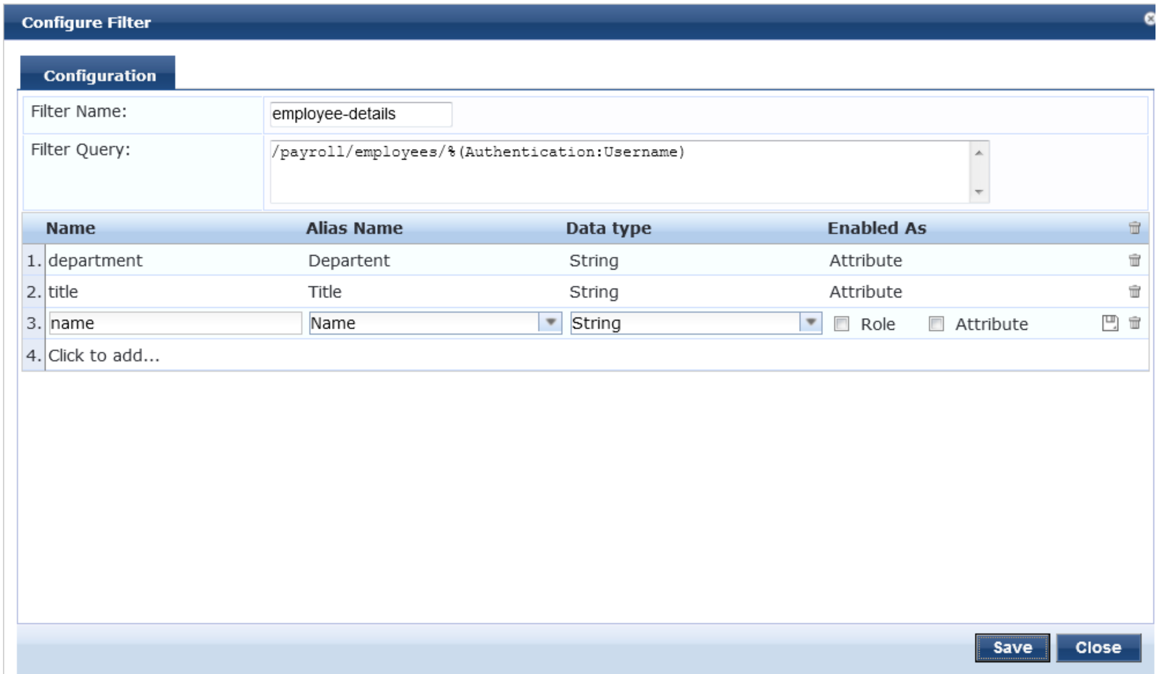
Table 97: *HTTP - Attributes tab (Filter List) Parameters*

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 214.

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 175: *HTTP Filter Configure Page*



Filter Name: employee-details

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

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

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

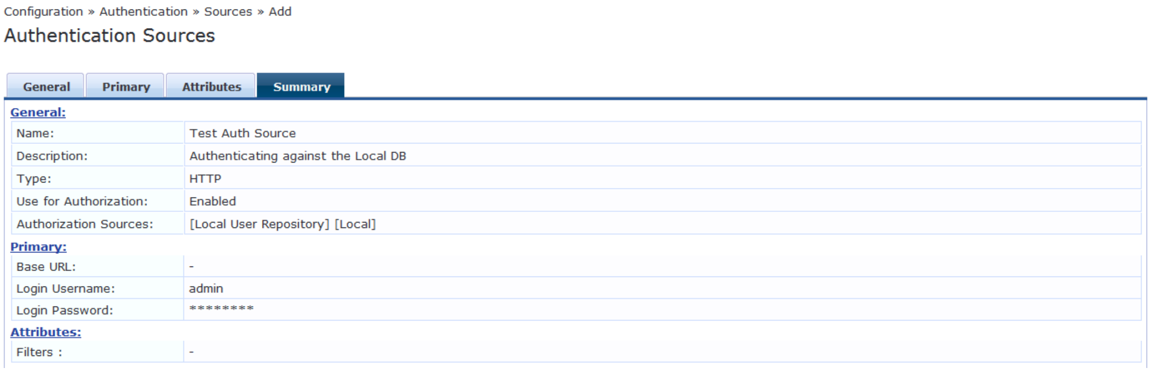
Table 98: *HTTP Configure Filter Page Parameters*

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 176: *HTTP - Summary Tab*



Authentication Sources

General:

Name:	Test Auth Source
Description:	Authenticating against the Local DB
Type:	HTTP
Use for Authorization:	Enabled
Authorization Sources:	[Local User Repository] [Local]

Primary:

Base URL:	-
Login Username:	admin
Login Password:	********

Attributes:

Filters :	-

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.

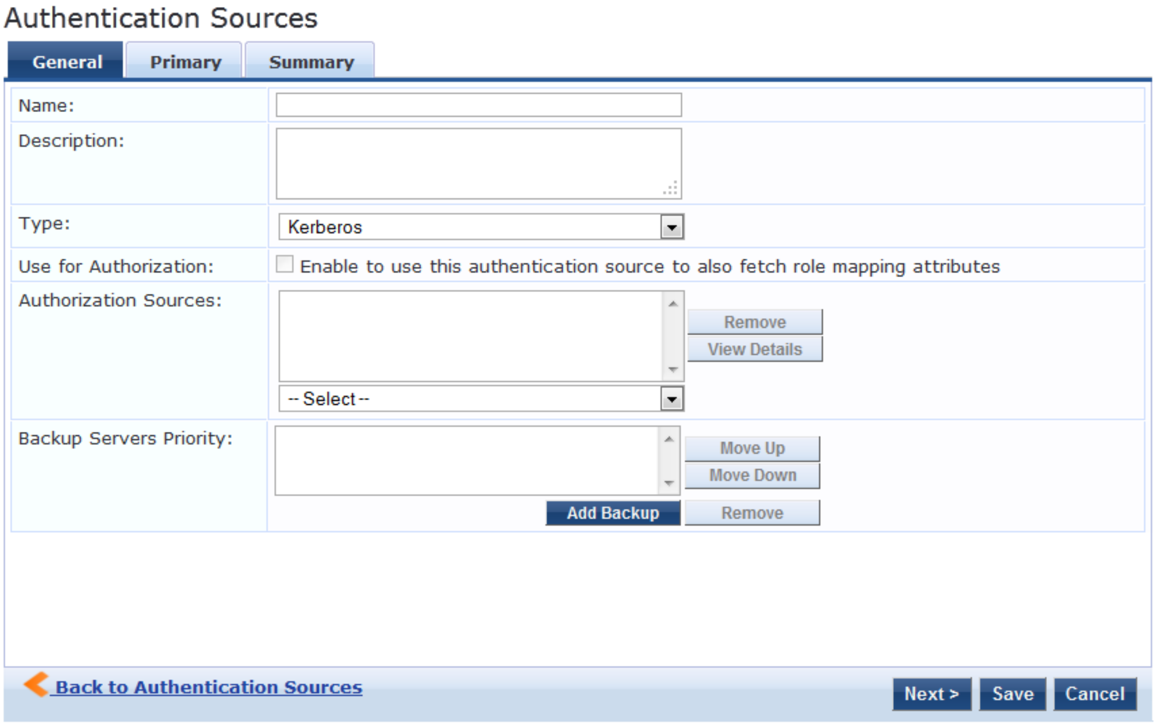
You can configure Kerberos authentication sources using the following tabs:

- General Tab on page 216
- Primary Tab on page 217
- Summary Tab on page 218

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 177: *Kerberos - General Tab*



Authentication Sources

Name:

Description:

Type: Kerberos

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

Authorization Sources: -- Select --

Backup Servers Priority:

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

Table 99: *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**.

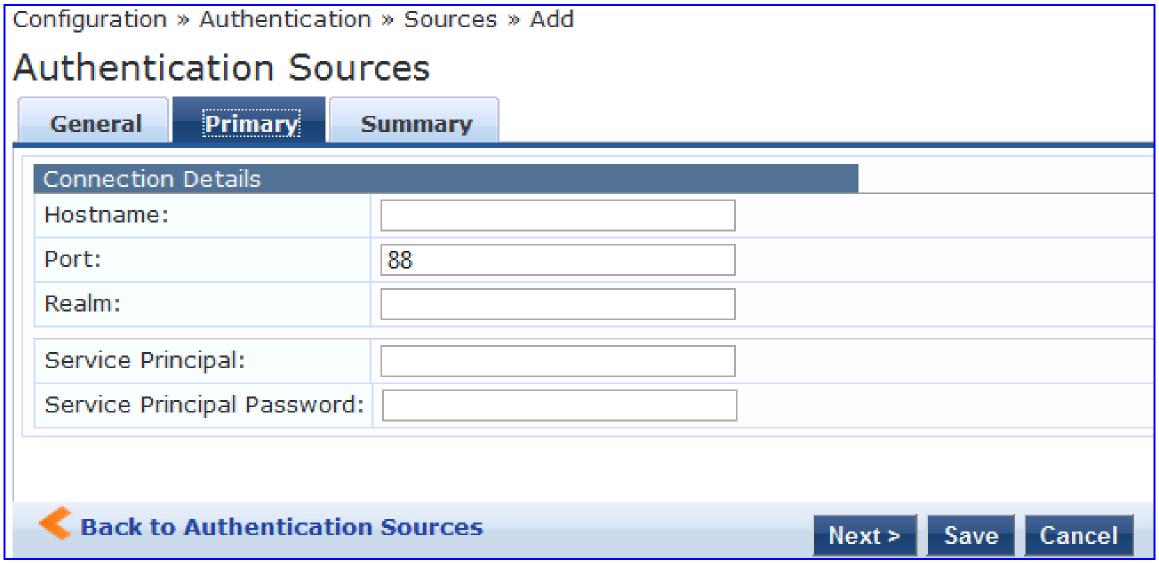
Table 99: *Kerberos - General Tab Parameters (Continued)*

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:** 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 178: *Kerberos - Primary Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Connection Details

Hostname:	
Port:	88
Realm:	
Service Principal:	
Service Principal Password:	

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

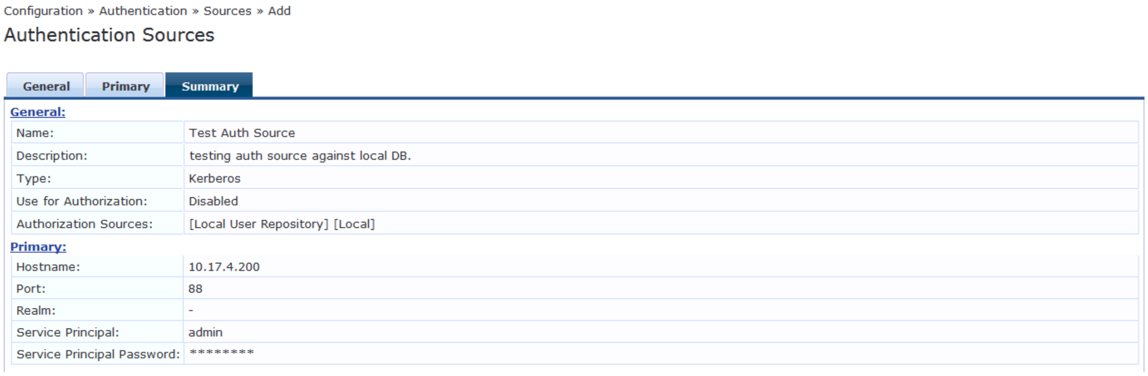
Table 100: *Kerberos - Primary Tab Parameters*

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 179: *Kerberos - Summary Tab*



General:

Name:	Test Auth Source
Description:	testing auth source against local DB.
Type:	Kerberos
Use for Authorization:	Disabled
Authorization Sources:	[Local User Repository] [Local]

Primary:

Hostname:	10.17.4.200
Port:	88
Realm:	-
Service Principal:	admin
Service Principal Password:	********

Okta

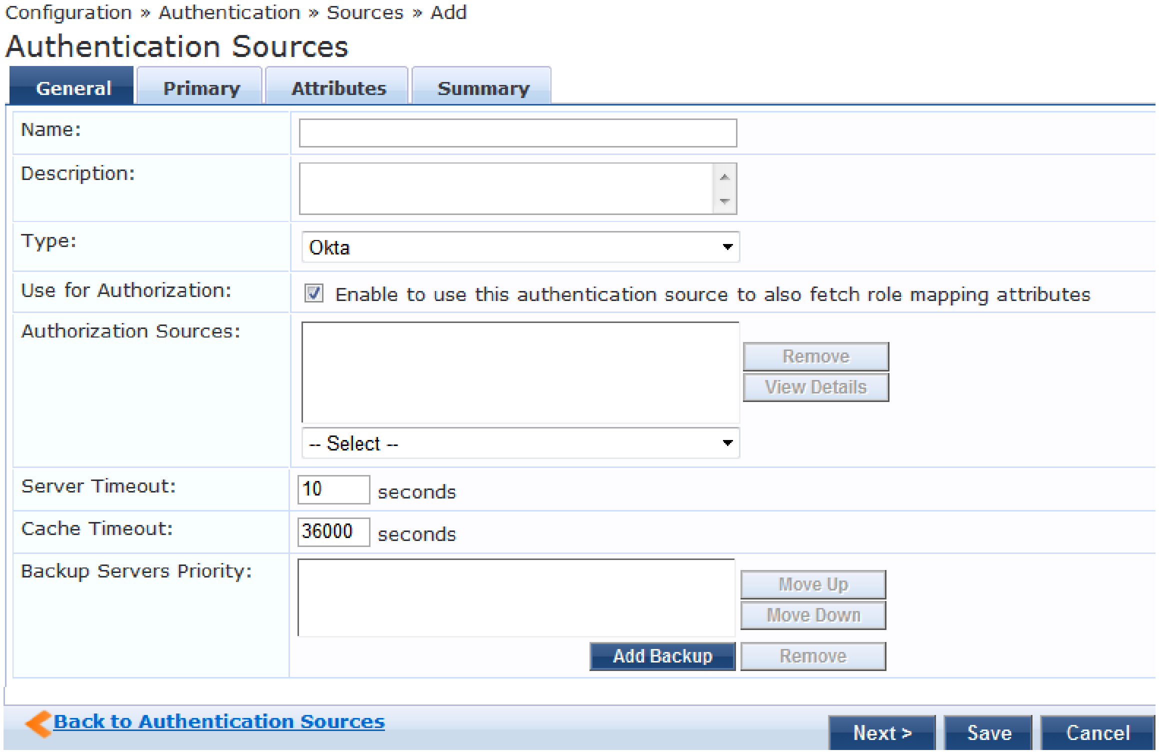
You can use Okta as an authentication source only for servers of the type Aruba Application Authentication. Configure Okta authentication sources on the following tabs:

- General Tab on page 219
- Primary Tab on page 220
- Attributes Tab on page 221
- Summary Tab on page 223

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 180: *Okta - General Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

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

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

Table 101: *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.

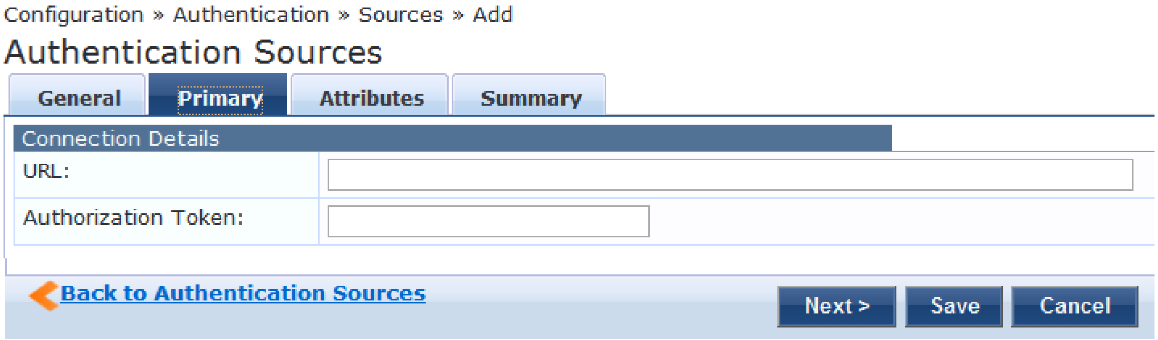
Table 101: *Okta - General Tab Parameters (Continued)*

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 181: *Okta - Primary Tab*



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

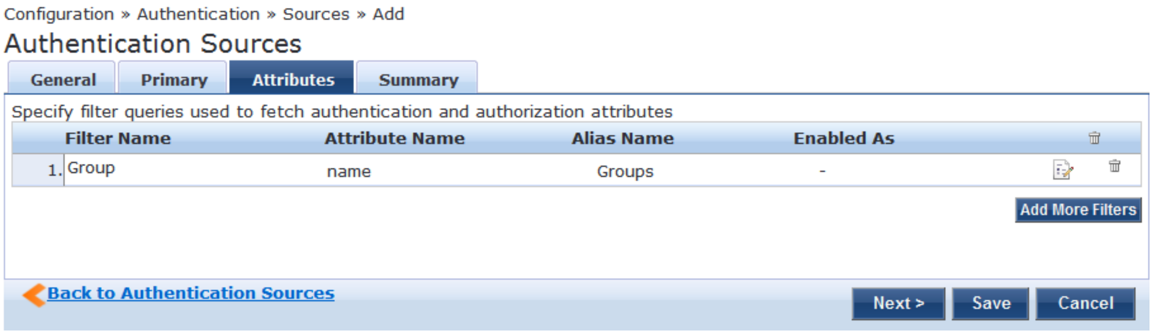
Table 102: *Okta - Primary Tab Parameters*

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 182: *Okta - Attributes Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Group	name	Groups	-

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

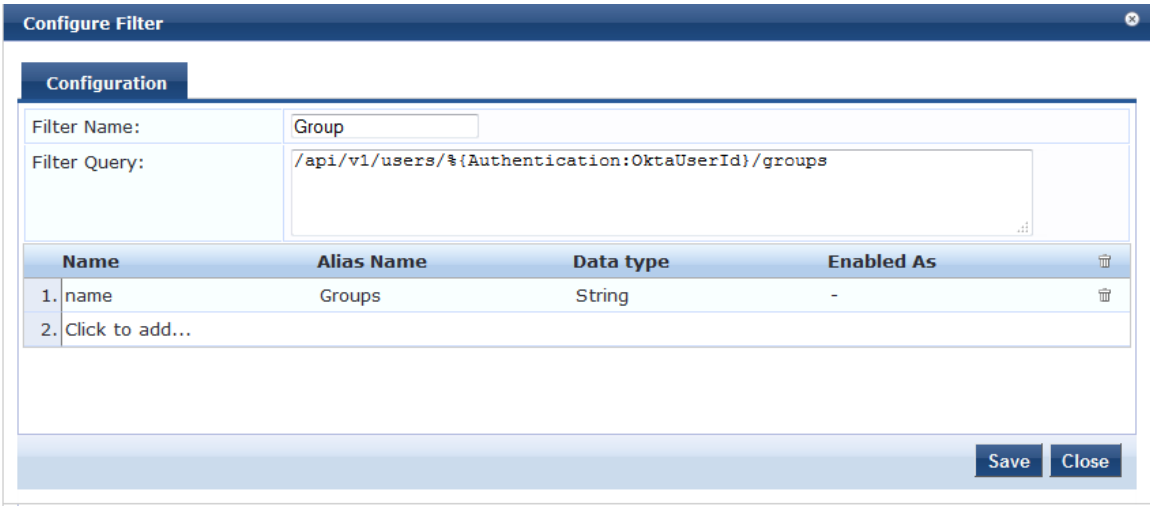
Table 103: *Okta - Attributes Tab Parameters*

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 222.

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 183: *Okta - Configure Filter Page*



Filter Name: Group

Filter Query: /api/v1/users/%{Authentication:OktaUserId}/groups

	Name	Alias Name	Data type	Enabled As
1.	name	Groups	String	-
2.	Click to add...			

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

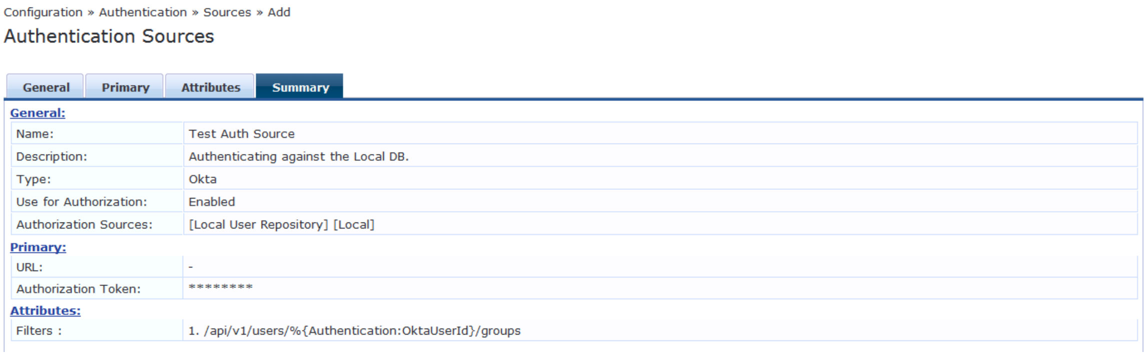
Table 104: *Okta Configure Filter Page*

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 184: *Okta - Summary Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

General:

Name:	Test Auth Source
Description:	Authenticating against the Local DB.
Type:	Okta
Use for Authorization:	Enabled
Authorization Sources:	[Local User Repository] [Local]

Primary:

URL:	-
Authorization Token:	********

Attributes:

Filters :	1. /api/v1/users/%{Authentication:OktaUserId}/groups

RADIUS Server

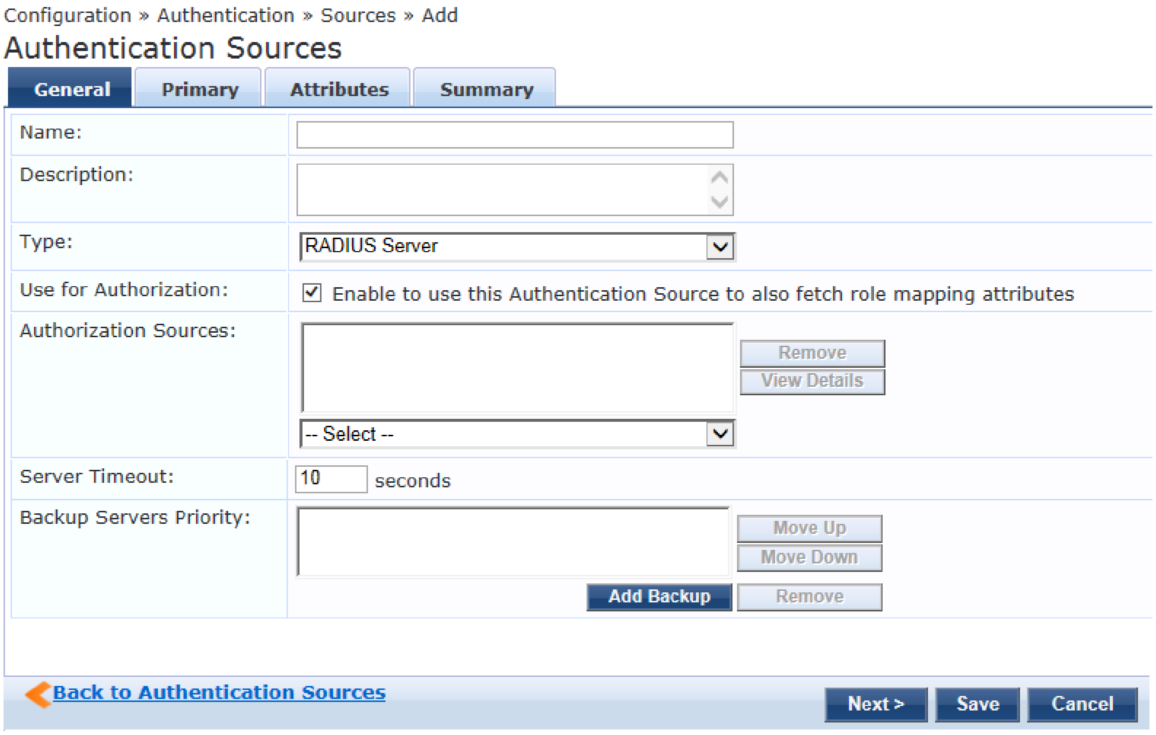
You can use the **RADIUS Server** as an authentication source to allow ClearPass to query a third-party **RADIUS Serve**r for authentication. Configure **RADIUS Server** authentication sources on the following tabs:

- General Tab on page 223
- Primary Tab on page 224
- Attributes Tab on page 225
- Summary Tab on page 226

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 185: *RADIUS Server - General Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

Name:	
Description:	
Type:	RADIUS Server
Use for Authorization:	☑ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Backup Servers Priority:	

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

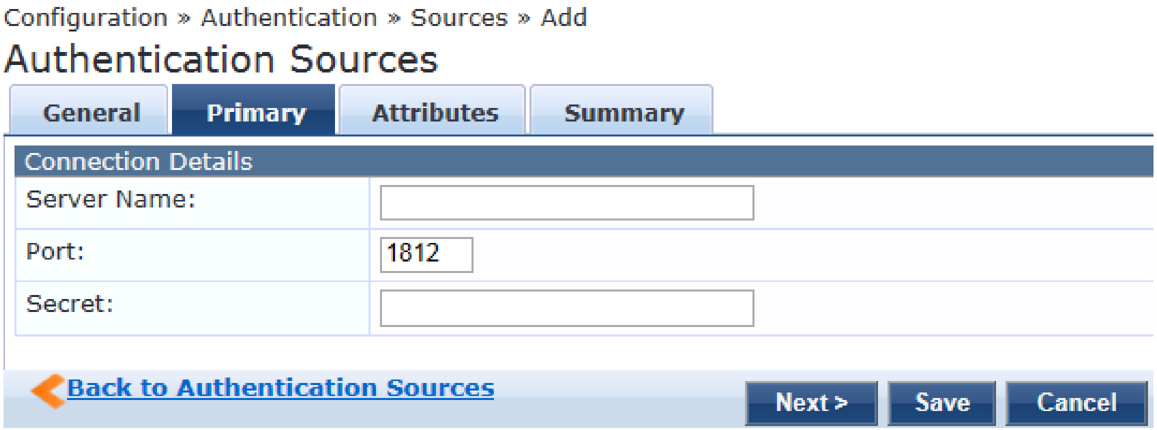
Table 105: *Radius Server - General Tab Parameters*

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 186: *RADIUS Server - Primary Tab*


Configuration » Authentication » Sources » Add
Authentication Sources
General
Primary
Attributes
Summary
Back to Authentication Sources
Next >
Save
Cancel

Connection Details

Server Name:	
Port:	1812
Secret:	

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

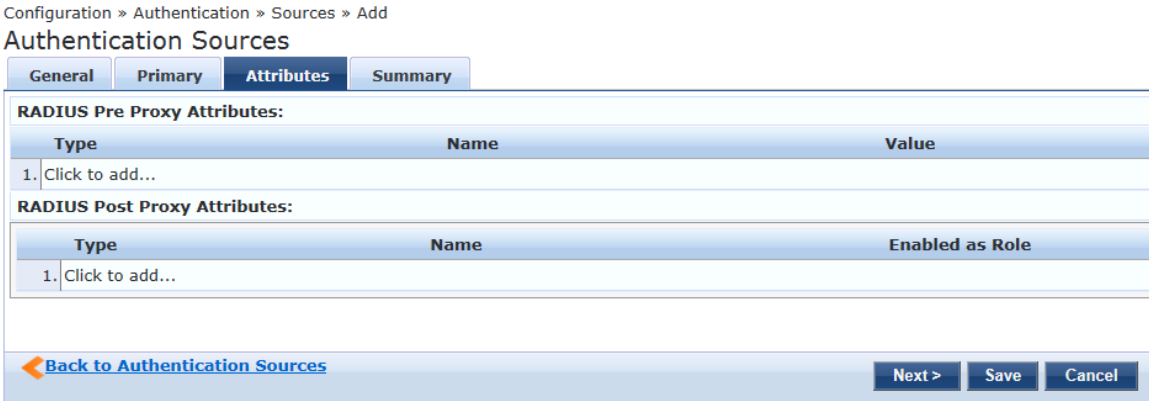
Table 106: *RADIUS Server - Primary Tab Parameters*

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 187: *RADIUS Server - Attributes Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

RADIUS Pre Proxy Attributes:

	Type	Name	Value
1.	Click to add...		

RADIUS Post Proxy Attributes:

	Type	Name	Enabled as Role
1.	Click to add...		

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

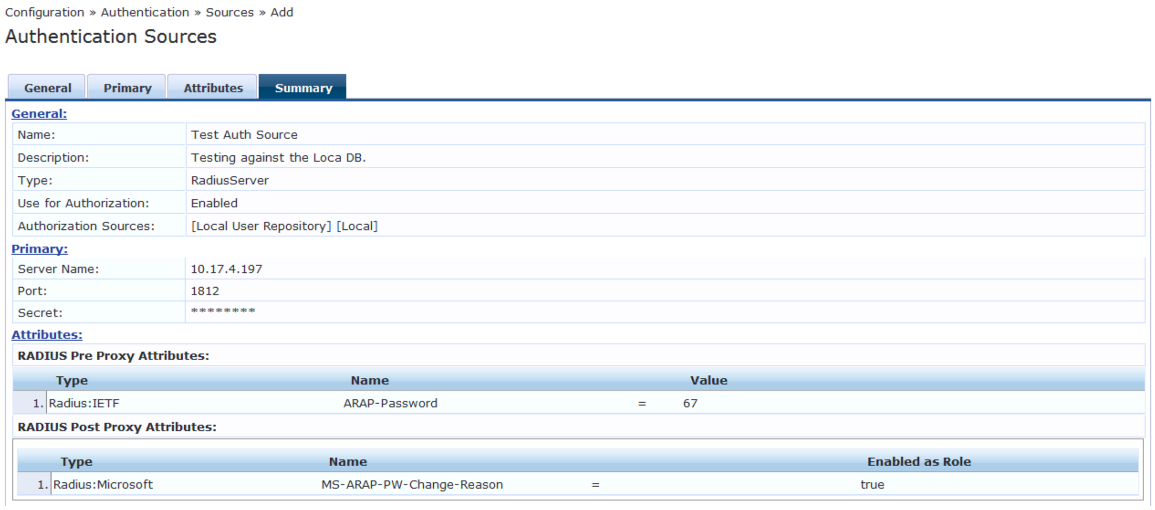
Table 107: *RADIUS Server - Attributes Tab Parameters*

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 188: *RADIUS Server - Summary Tab*



General:

Name:	Test Auth Source
Description:	Testing against the Loca DB.
Type:	RadiusServer
Use for Authorization:	Enabled
Authorization Sources:	[Local User Repository] [Local]

Primary:

Server Name:	10.17.4.197
Port:	1812
Secret:	********

Attributes:

RADIUS Pre Proxy Attributes:

	Type	Name		Value
1.	Radius:IETF	ARAP-Password	=	67

RADIUS Post Proxy Attributes:

	Type	Name		Enabled as Role
1.	Radius:Microsoft	MS-ARAP-PW-Change-Reason	=	true

Adding a Static Host List as an Authentication Source

This section provides the following information:

- About Static Host Lists
- Adding a Static Host List as an Authentication Source

About Static Host Lists

You can configure primary and backup servers, session details, and the list of static hosts for **Static Host List** authentication sources.

A static host list often functions, in the context of the service, as a white list or a black list. Therefore, static host lists are configured independently at the global level.

A static host list comprises a named list of MAC addresses 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.

For more information about static host lists, see Managing Static Host Lists on page 252.

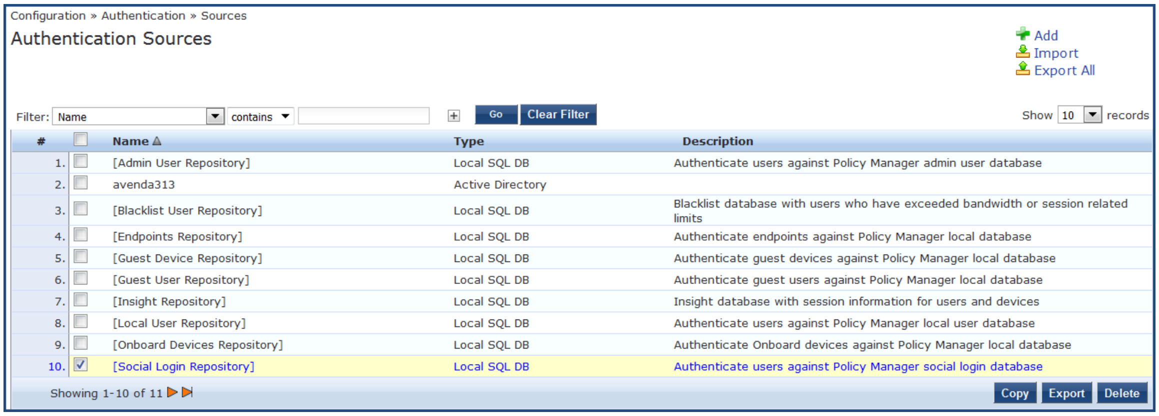
Adding a Static Host List as an Authentication Source

To add a static host list as an authentication source:

1. Navigate to **Configuration** > **Authentication** > **Sources**.

   The **Authentication Sources** page appears.

Figure 189: *Authentication Sources Page*



Configuration » Authentication » Sources

Authentication Sources

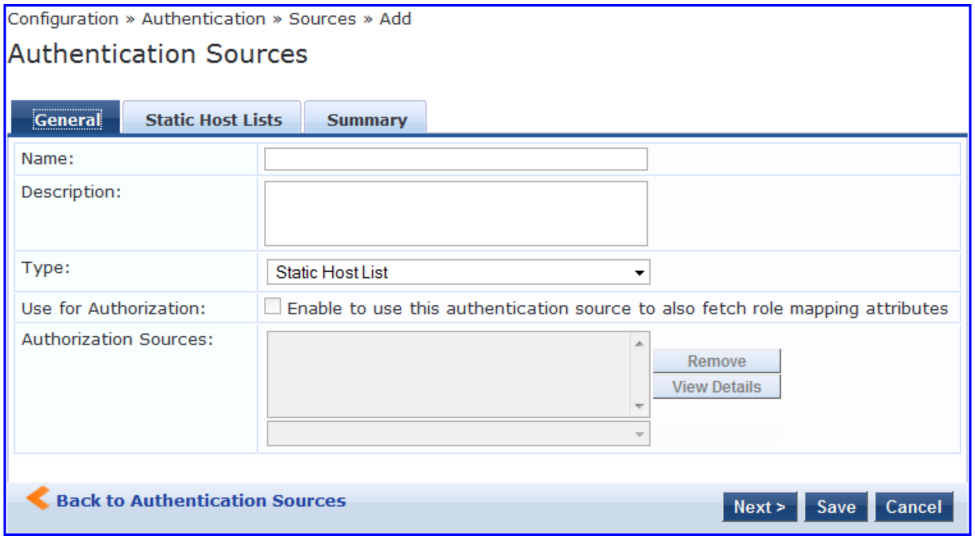
#	☐	Name	Type	Description
1.	☐	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	☐	avenda313	Active Directory	
3.	☐	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
4.	☐	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
5.	☐	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
6.	☐	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
7.	☐	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
8.	☐	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
9.	☐	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
10.	☑	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database

Showing 1-10 of 11

2. Click the **Add** link.

   The **Add Authentication Sources** dialog opens.

Figure 190: *Specifying a Static Host List as Authentication Source*



Configuration » Authentication » Sources » Add

Authentication Sources

Name:

Description:

Type: Static Host List

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

Authorization Sources:

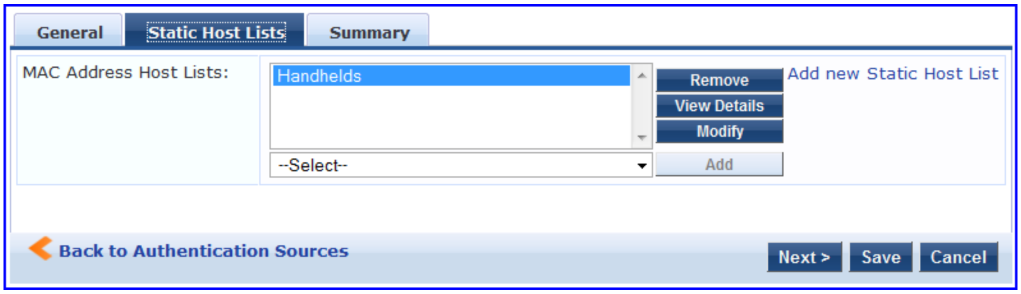
3. Enter the name and description of the static host list.
4. In the **Type** field, select **Static Host List**.

   In this context, the **Use for Authorization** and **Authorization Sources** fields are not configurable.
5. Click **Next**.

   The **Static Hosts Lists** dialog appears.
6. From the **Static Host Lists** tab, select a static host list from the drop-down list.

   The selected static host list is added to the MAC Address Host Lists (see Figure 191).

Figure 191: *Existing Static Host List Added*



Only static host lists of type **MAC Address Host Lists** or **MAC Address Regular Expression** can be configured as authentication sources.

a. To remove the selected static host list, click **Remove**.

b. To view the contents of the selected static host list, click **View Details**.

c. To modify the selected static host list, click **Modify**.

7. Click **Save**.

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 875.

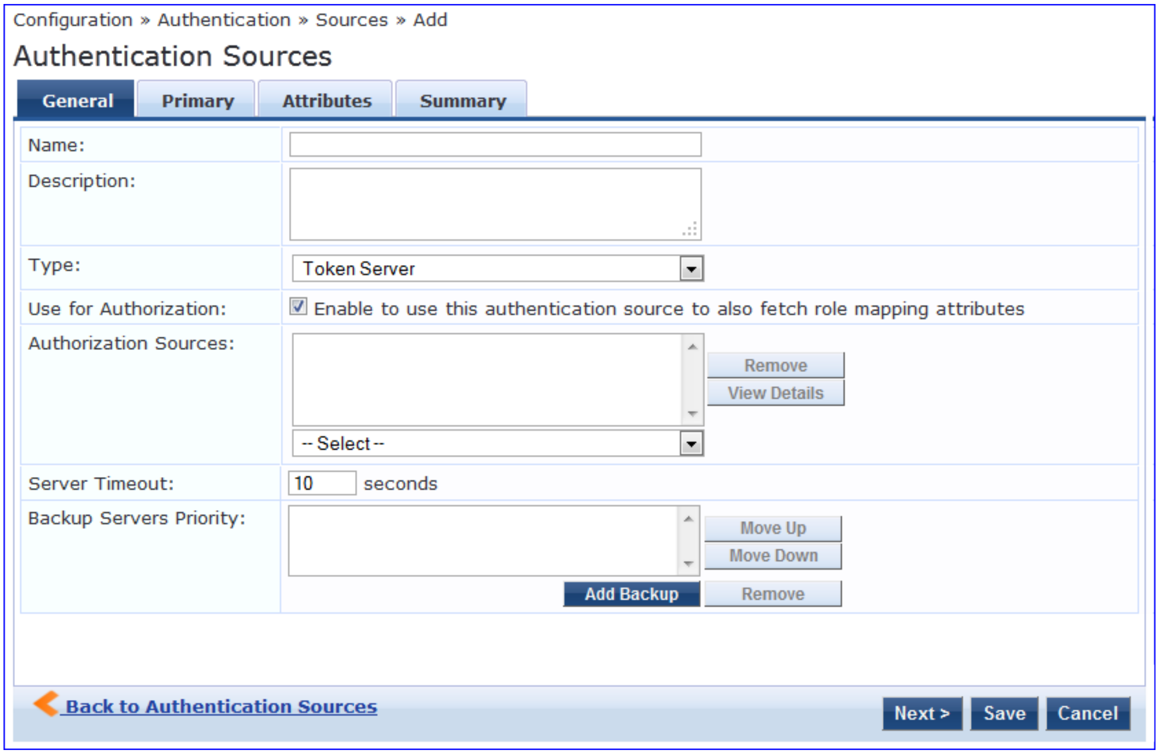
You configure primary and backup servers, session details, and the filter query and role mapping attributes to fetch for token server authentication sources on the following tabs:

- General Tab on page 229
- Primary Tab on page 230
- Attributes Tab on page 230
- Summary Tab on page 231

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 192: *Token Server - General Tab*



Configuration » Authentication » Sources » Add

Authentication Sources

General | Primary | Attributes | Summary

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

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

Table 108: *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.

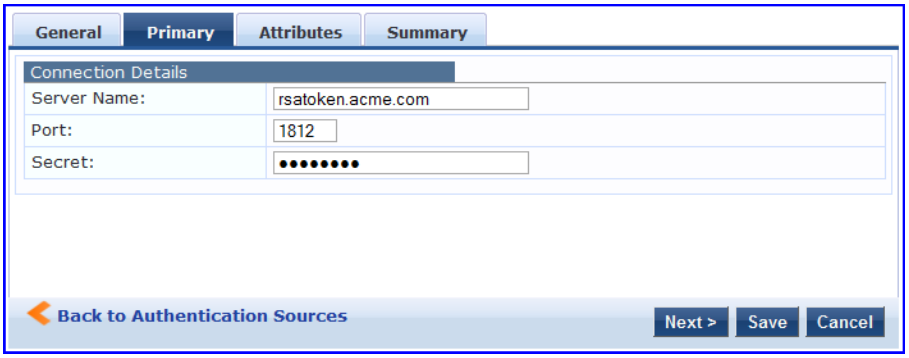
Table 108: *Token Server - General Tab Parameters (Continued)*

Parameter	Description
	NOTE: 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 193: *Token Server - Primary Tab*



Server Name: rsatoken.acme.com

Port: 1812

Secret: ●●●●●●●●

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

Table 109: *Token Server - Primary Tab Parameters*

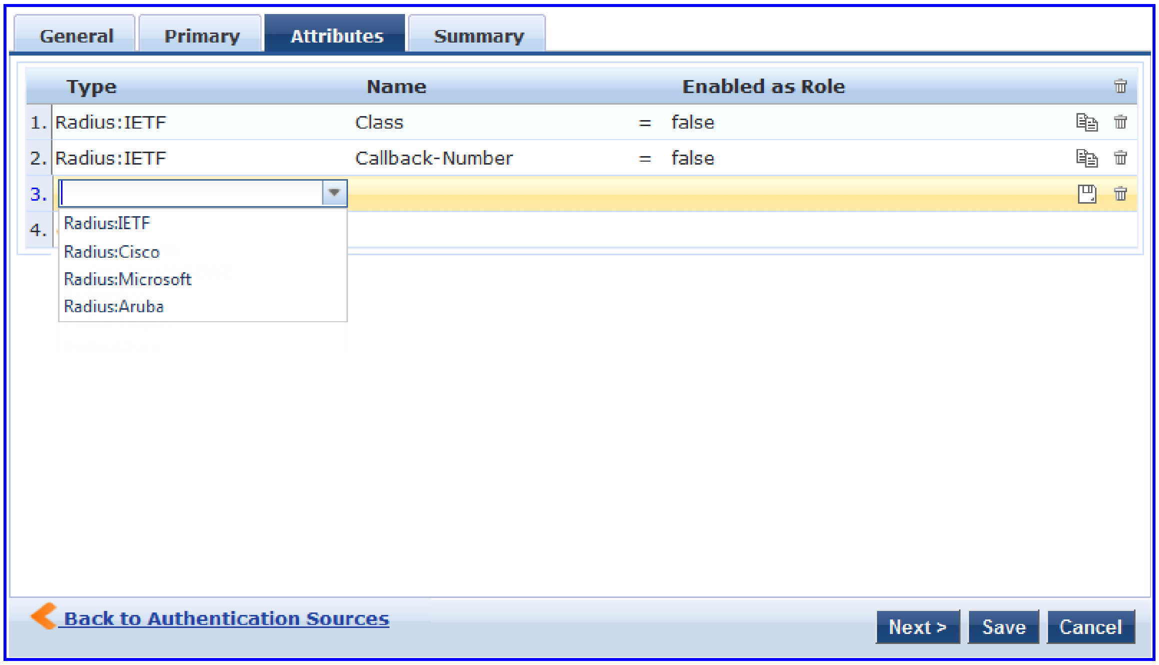
Parameter	Description
Server Name	Displays the host name or the IP address of the token server,
Port	Specifies the UDP port at which the token server listens for RADIUS connections. The default port is 1812.
Secret	Specify the RADIUS shared secret to connect to the token server.

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 194: *Token Server - Attributes Tab*



	Type	Name		Enabled as Role
1.	Radius:IETF	Class	=	false
2.	Radius:IETF	Callback-Number	=	false
3.				
4.				

See Configuring a Role and Role-Mapping Policy on page 255 for more information. The following table describes the **Token Server - Attribute** parameters:

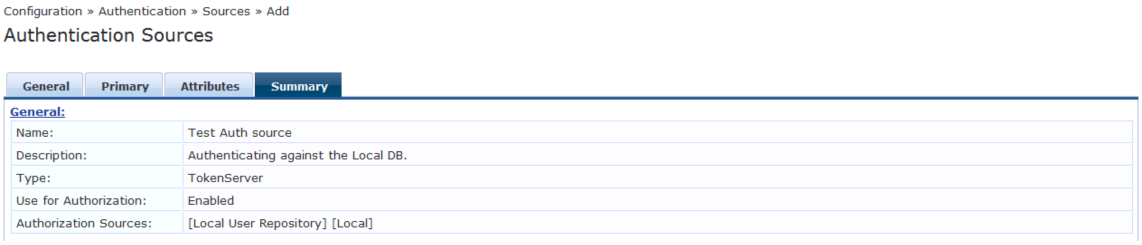
Table 110: *Token Server - Attribute Tab Parameters*

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 195: *Token Servers - Summary Tab*



General:

Name:	Test Auth source
Description:	Authenticating against the Local DB.
Type:	TokenServer
Use for Authorization:	Enabled
Authorization Sources:	[Local User Repository] [Local]

Chapter 5
Configuring Identity Settings

This chapter provides information on the following topics:

- Configuring Single Sign-On
- Managing Local Users
- Adding and Modifying Endpoints
- Managing Static Host Lists
- Configuring a Role and Role-Mapping Policy

This chapter provides details on the settings required to configure ClearPass Policy Manager Identify settings.

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

NOTE

To authenticate local users from a particular service, include **Local User Repository** among the authentication sources.

Configuring Single Sign-On

This section provides the following information:

- SAML Service Provider (SP) Configuration
- SAML Identity Provider (IdP) Configuration

The Single Sign-On (SSO) settings on the **Single Sign-On** page allows ClearPass users that have signed in to ClearPass Policy Manager to access the Onboard, Guest, and Insight applications and Policy Manager administration settings without reauthenticating. ClearPass provides single sign-on support using the Security Assertion Markup Language (SAML).

This feature also provides differentiated single sign-on access for Guest web login and Guest Operator login (see Table 111 for details).

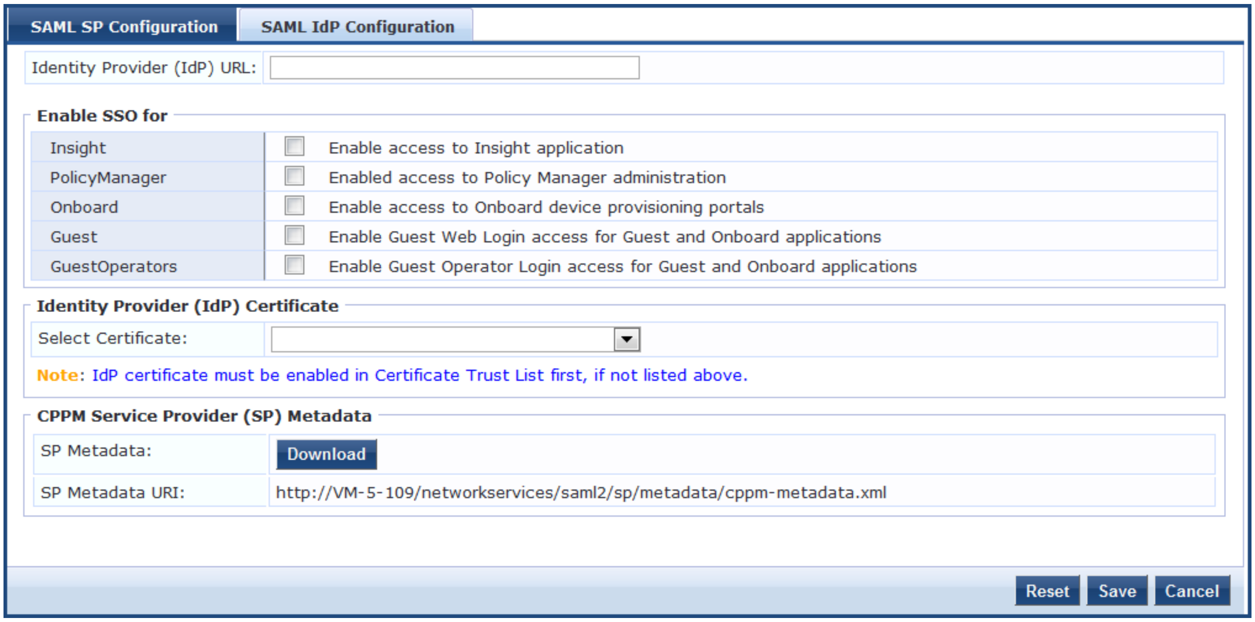
SAML Service Provider (SP) Configuration

To configure single sign-on service provider settings:

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

   The **Single Sign-On** > **SAML SP Configuration** dialog opens.

Figure 196: *Configuring Single Sign-On > SAML Service Provider Parameters*



Identity Provider (IdP) URL:

Enable SSO for

Insight	□	Enable access to Insight application
PolicyManager	□	Enabled access to Policy Manager administration
Onboard	□	Enable access to Onboard device provisioning portals
Guest	□	Enable Guest Web Login access for Guest and Onboard applications
GuestOperators	□	Enable Guest Operator Login access for Guest and Onboard applications

Identity Provider (IdP) Certificate

Select Certificate:

Note: IdP certificate must be enabled in Certificate Trust List first, if not listed above.

CPPM Service Provider (SP) Metadata

SP Metadata:

SP Metadata URI: http://VM-5-109/networkservices/saml2/sp/metadata/cppm-metadata.xml

2. Select the application(s) you want users to access with single sign-on.

   To complete this task, specify the **SAML SP Configuration** tab parameters as described in Table 111.

3. Create trusted relationships between a Service Provider and Identity Provider by providing the Identity Provider (IdP) URL and IdP certificate.

   To complete this task, specify the **SAML IdP Configuration** tab parameters as described in Table 112.

Table 111: *Single Sign-On Service Provider Configuration Settings*

Parameter	Action/Description
Identity Provider (IdP) URL	1. Enter the URL of the identity provider.
Enable SSO For	2. Select the applications to be enabled for single sign-on: ▪ Insight ▪ Policy Manager ▪ Onboard device provisioning portals ▪ Guest and Onboard Web Login ▪ Guest and Onboard Guest Operator Login ● If you select only the **Guest Operator Login**, SSO will be enabled for Operator logins only, and Web logins will use standard non-SSO authentication. ● If you select only the **Guest Web Login** option, SSO will be enabled for Web logins only, and Operator logins will use standard non-SSO authentication. ● If you select both the **Guest Operator Login** and the **Guest Web Login** options, Operator logins and Web logins will both use SSO authentication.
Select Certificate	3. Select the Identity Provider (IdP) certificate to use for single sign-on. When you select a certificate, the page displays the following information about the certificate: ▪ Subject DN ▪ Issuer DN ▪ Issue Date/Time ▪ Expiry Date/Time

Table 111: *Single Sign-On Service Provider Configuration Settings (Continued)*

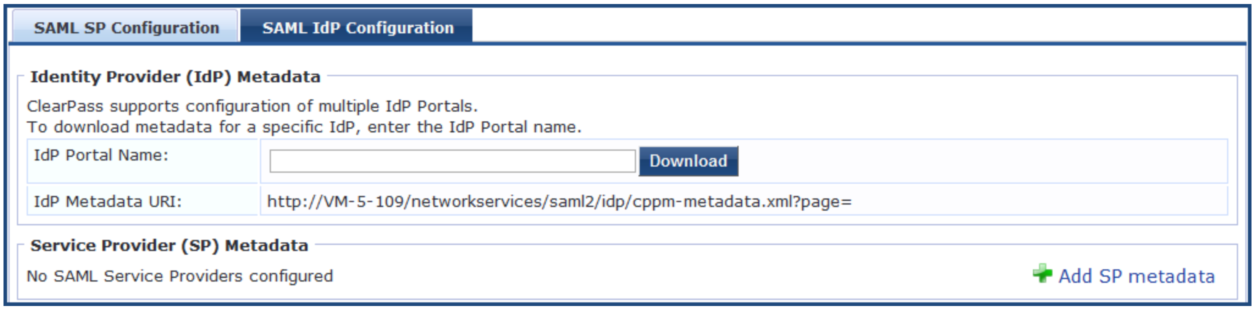
Parameter	Action/Description
	■ Validity Status ■ Signature Algorithm ■ Public Key Format ■ Serial Number ■ Enabled This field only displays certificates that are enabled in the certificate trust list. See also Certificate Trust List on page 659.
CPPM Service Provider (SP) Metadata	**SP Metadata**: 4. To download and view an XML file containing metadata for the Service Provider Uniform Resource Identifier (URI), click **Download**. **Metadata URI** : 5. View the Uniform Resource Identifier (URI) for the Service Provider metadata resource.

SAML Identity Provider (IdP) Configuration

To configure single sign-on identity provider settings:

1. Navigate to **Configuration** > **Identity** > **Single Sign-On**.
2. Select the **SAML IdP Configuration** tab.

Figure 197: *Configuring Single Sign-On > Identity Provider Parameters*



Identity Provider (IdP) Metadata

ClearPass supports configuration of multiple IdP Portals.
To download metadata for a specific IdP, enter the IdP Portal name.

IdP Portal Name:

IdP Metadata URI: http://VM-5-109/networkservices/saml2/idp/cppm-metadata.xml?page=

Service Provider (SP) Metadata

No SAML Service Providers configured

3. Specify the **SAML IdP Configuration** parameters as described in the following table:

Table 112: *Single Sign-On Identity Provider Configuration Settings*

Parameter	Action/Description
IdP Portal Name	1. Enter the name of the identity provider portal. 2. To download and view an XML file containing metadata for the Identity Provider Uniform Resource Identifier (URI), click **Download**.
IdP Metadata URI	3. View the Uniform Resource Identifier (URI) for the IdP metadata resource.
Service Provider (SP) Metadata	4. If you upload metadata for an SAML Service Providers, ClearPass can upload the SP metadata for validation during the single-sign on process. a. Click **Add SP Metadata**. b. Enter the name of the service provider. c. Upload the service provider metadata file.

Table 112: *Single Sign-On Identity Provider Configuration Settings (Continued)*

Parameter	Action/Description
CPPM Service Provider (SP) Metadata	**SP Metadata** section: 5. To download and view an XML file containing metadata for the Service Provider Uniform Resource Identifier (URI), click **Download**. **The Metadata URI**: 6. View the location of this metadata file.

Managing Local Users

This section provides the following information:

- Adding a Local User
- Modifying a Local User Account
- Importing and Exporting Local Users
- Setting Password Policy for Local Users
- Disabling Local User Accounts

ClearPass Policy Manager lists all local users in the **Local Users** page.

You can also add, import, export, set password policies, and configure the conditions for disabling accounts for the local users using the links provided at the top-right corner of the **Local Users** page.

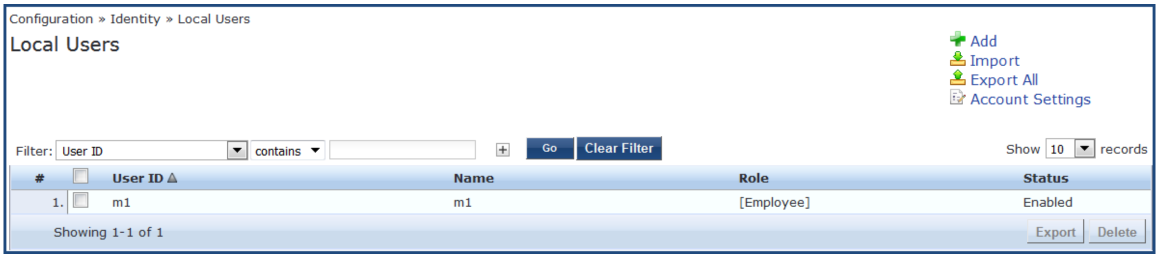
Adding a Local User

To add a local user in the **Local Users** table:

1. Navigate to **Configuration** > **Identity** > **Local Users**.

   The **Local Users** page opens.

Figure 198: *Local Users Page*



Configuration » Identity » Local Users

Local Users

Filter: User ID contains

Show 10 records

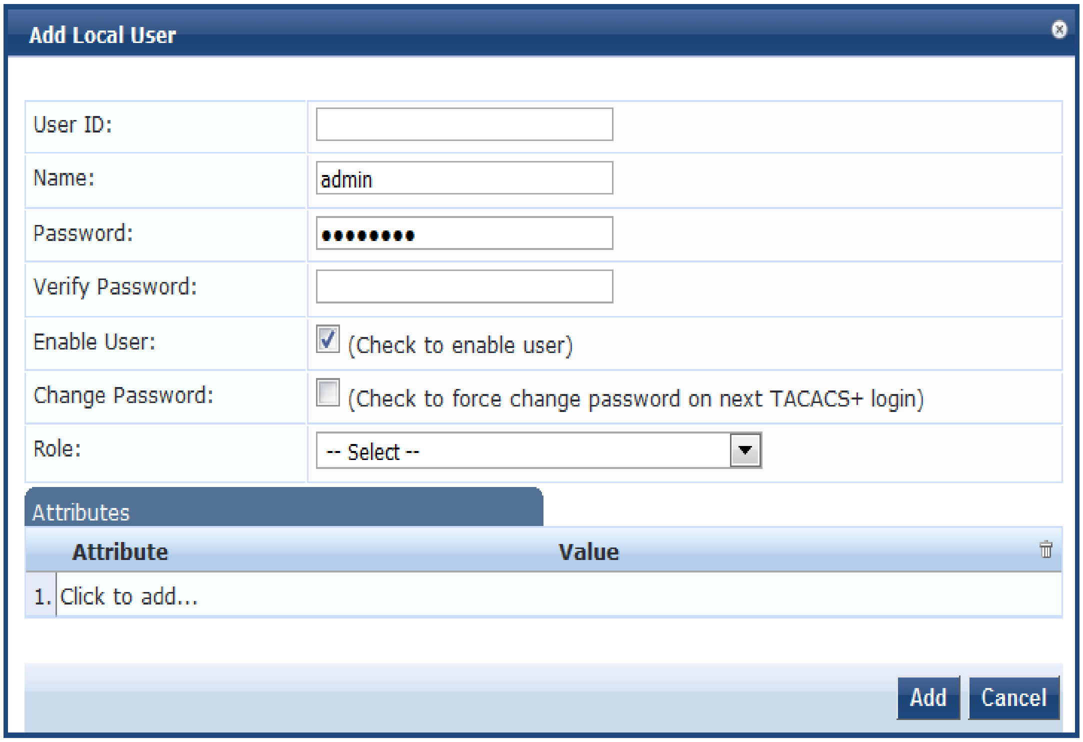
#	☐	User ID	Name	Role	Status
1.	☐	m1	m1	[Employee]	Enabled

Showing 1-1 of 1

2. Click the **Add** link at the top-right corner the page.

   The **Add Local User** page opens (see Figure 199).

Figure 199: *Adding a Local User*



Add Local User

User ID:	
Name:	admin
Password:	••••••••
Verify Password:	
Enable User:	☑ (Check to enable user)
Change Password:	□ (Check to force change password on next TACACS+ login)
Role:	-- Select --

Attributes

	Attribute	Value
1.	Click to add...	

3. Specify the **Add Local User** parameters as described in the following table, then click **Add**:

Table 113: *Adding a Local User Parameters*

Parameter	Action/Description
User ID	1. Specify the local user's user ID.
Name	2. Enter the local user's name.
Password/ Verify Password	3. Specify a password for the local user, then verify the password.
Enable User	4. You must enable this check box to enable the local user account. Otherwise, the local user account is disabled.
Change Password	5. Enable this check box to allow the user to change the password at the next TACACS+ login (after authenticating with the old password). Once the password is changed successfully, this option is automatically disabled. **NOTE:** The option to change the password on the next login is applicable for network device administration logins using TACACS+ only.

Table 113: *Adding a Local User Parameters (Continued)*

Parameter	Action/Description
Role	6. Select a static role to be assigned to the user from the **Role** drop-down list.
Attributes	
	7. To add attributes for the local users, click **Click to add...** A new row is created with a drop-down list in the **Attribute** column. This field is optional. The list of local user attributes are: ■ Department ■ Designation ■ Email ■ Phone ■ Sponsor ■ Title a. To add a custom attribute in the **Attribute** column, select an attribute from the drop-down list or enter any string. **NOTE:** 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. **NOTE:** All attributes entered for a local user are available in the role-mapping rules editor under the **LocalUser** namespace. When you click **Add**, you return to the **Local User** page where the following message is displayed: *User <username> added successfully*

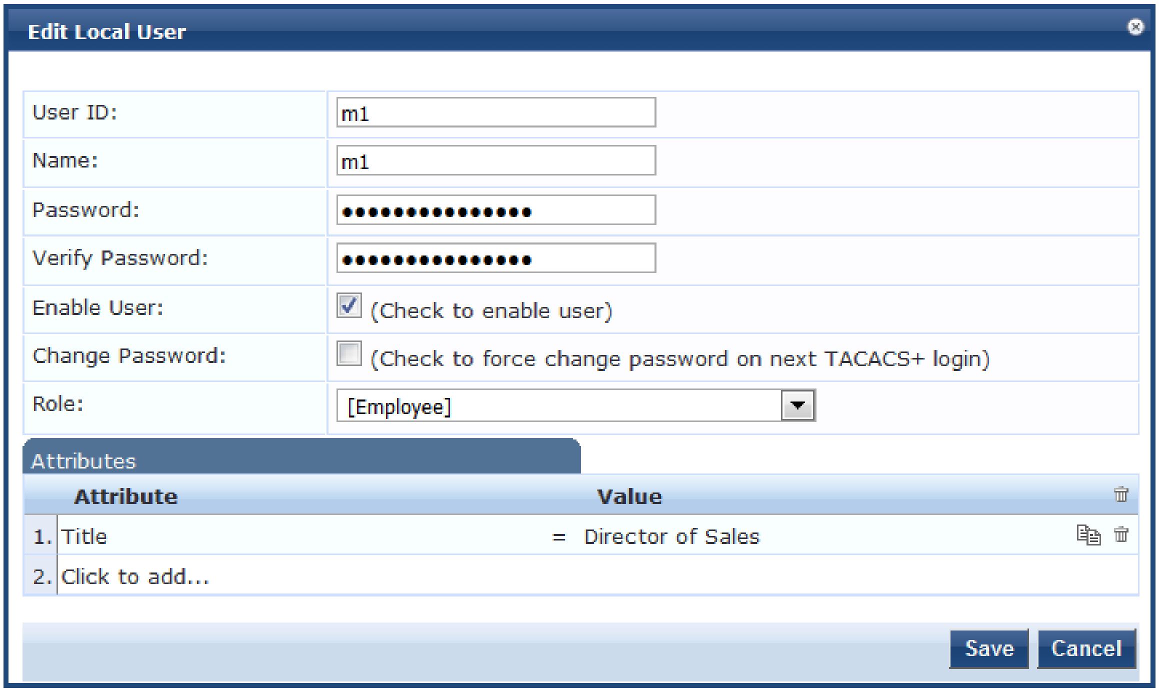
Modifying a Local User Account

To modify a local user account:

1. Navigate to the **Configuration > Identity > Local Users** page.
2. Click the **User ID** row that you want to edit.

   The **Edit Local User** window opens.

Figure 200: *Modifying a Local User*



Edit Local User

User ID:	m1
Name:	m1
Password:	•••••••••••••••
Verify Password:	•••••••••••••••
Enable User:	☑ (Check to enable user)
Change Password:	☐ (Check to force change password on next TACACS+ login)
Role:	[Employee]

Attributes

	Attribute		Value
1.	Title	=	Director of Sales
2.	Click to add...		

3. Modify any values as necessary in the **Edit Local User** dialog.
4. Click **Save**.

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.

For more information, see Importing and Exporting Information on page 31.

After selecting one or more user accounts from the list, you can also export specific user accounts by clicking the **Export** button .

NOTE

The passwords of the local user accounts are not stored in clear text when exported to an XML file.

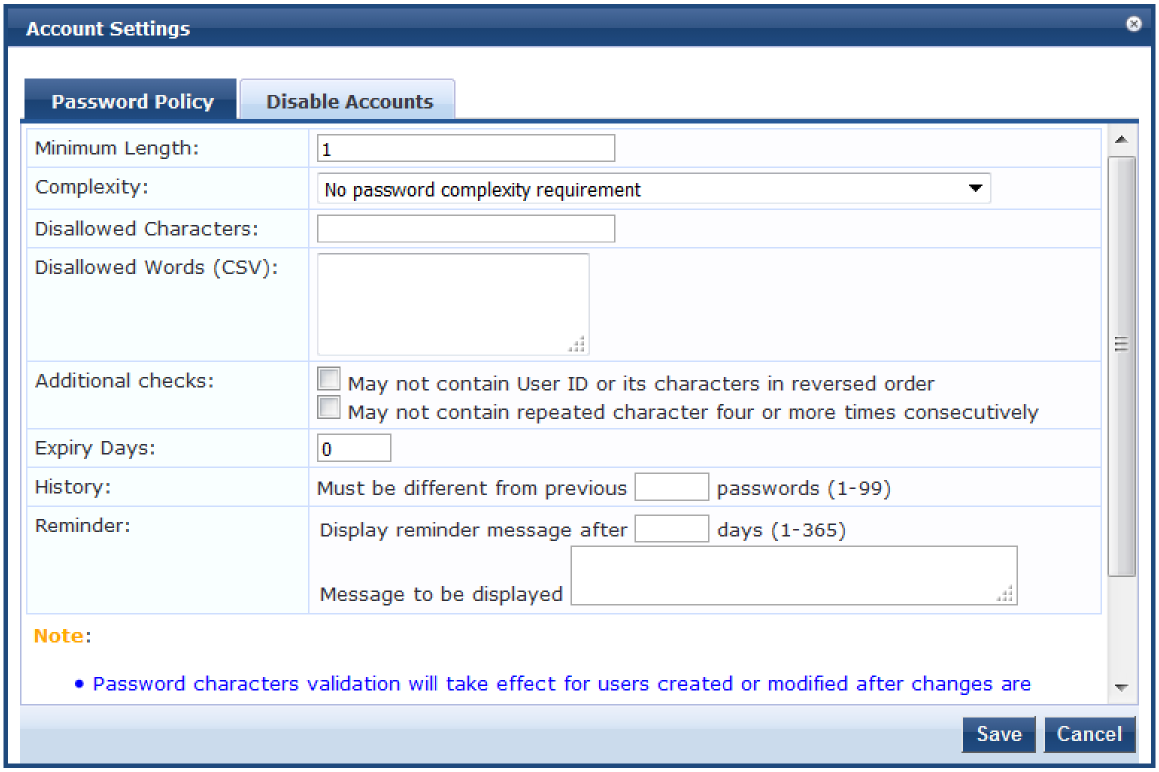
Setting Password Policy for Local Users

To set password policies for the local users:

1. Navigate to the **Configuration > Identity > Local Users** page.
2. Click the **Account Settings** link.

   The **Account Settings** page opens.

Figure 201: *Account Settings > Password Policy Settings Dialog*



Minimum Length:	1
Complexity:	No password complexity requirement
Disallowed Characters:	
Disallowed Words (CSV):	
Additional checks:	□ May not contain User ID or its characters in reversed order □ May not contain repeated character four or more times consecutively
Expiry Days:	0
History:	Must be different from previous passwords (1-99)
Reminder:	Display reminder message after days (1-365) Message to be displayed

Note:

- Password characters validation will take effect for users created or modified after changes are

3. Specify the **Password Policy** parameters as described in Table 114, then click **Save**.

Table 114: *Password Policy Parameters*

Parameter	Action/Description
Minimum Length	1. Specify the minimum length required for the password.
Complexity	2. 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
Disallowed Characters	3. Specify the characters not to be allowed in the password. **NOTE:** Password characters validation takes effect for users created or modified after changes are saved.
Disallowed Words (CSV)	4. Specify the words not to be allowed in the password. Separate the disallowed words with commas.
Additional Checks	5. Select any additional checks, if required. The options are:

Table 114: *Password Policy Parameters (Continued)*

Parameter	Action/Description
	■ May not contain User ID or its characters in reversed order. ■ May not contain a repeated character four or more times consecutively.
Expiry Days	6. Set the password expiration time for local users. The allowed range is **0** to **500** days. The default value is **0**. **NOTE:** If the value is set to **0**, the password never expires. For any other value, local users are forced to reset the expired password when they log in. ClearPass alerts users five days before the password expires.
History	7. Specify the number of previous passwords for this user to be compared against. This option prevents users from setting a password that was used recently. Valid options are from 1 to 99.
Reminder	8. Configure the reminder message. Setting this option displays a reminder after n days to change the password. The valid options are from 1 to 365. When set, this option only displays a reminder; it does not prompt for a new password. The message to be displayed can be set accordingly. **NOTE:** The **Reminder** parameter is applicable for TACACS+ authentication only. The other settings are applied to all users.

Disabling Local User Accounts

Disabling a local user account can happen in two ways:

- When a local user tries to log in with an invalid password for a configured number of times defined by the **Failed attempts count** parameter, the local user account is locked.

NOTE

If the mechanism for logging in to ClearPass Policy Manager is Certificate + Password, the local user is allowed to enter the password even if the certificate is invalid.

- When the local user tries to log in with an invalid user certificate for a configured number of times defined by the **Failed attempts count** parameter, the local user account is disabled.

NOTE

A local user's failed login attempts are counted only when the Password_Mismatch, Password_Not_Available, and User_Authentication_Failed error messages occur.

- To reset the **Failed attempts count** and enable a disabled local user account, click the **Reset** button (see Table 115).
- For Local users whose accounts are locked due to account settings validations, and whose accounts are enabled again after being locked out, entries are logged in both the Audit Viewer (see Audit Viewer on page 148) and the Event Viewer (see Event Viewer on page 150).

The **Disable Account** check occurs every day at midnight, except for the **Failed attempts count**. Other local user configuration settings are applied to all local users.

To specify the conditions for disabling local user accounts:

1. Navigate to **Configuration** > **Identity** > **Local Users**.

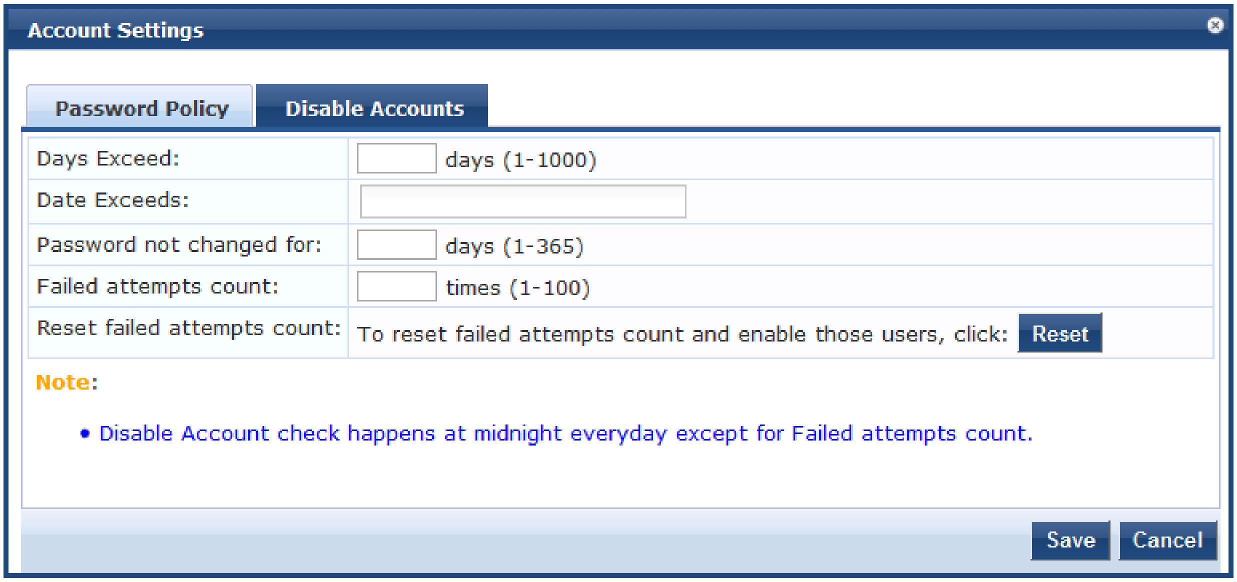
2. Click the **Account Settings** link.

   The **Account Settings** page opens.

3. Select the **Disable Accounts** tab.

   The **Disable Accounts** dialog opens.

Figure 202: *Disable Accounts Dialog*



Days Exceed:	days (1-1000)
Date Exceeds:	
Password not changed for:	days (1-365)
Failed attempts count:	times (1-100)
Reset failed attempts count:	To reset failed attempts count and enable those users, click: Reset

Note:

- Disable Account check happens at midnight everyday except for Failed attempts count.

4. Specify the **Disable Accounts** parameters as described in Table 115, then click **Save**.

Table 115: *Disable Accounts Parameters*

Parameter	Action/Description
Days Exceed	1. Specify the number of days before the account is disabled. The range is from **1** to **100** days.
Date Exceeds	2. Specify the date when local users are disabled when the current date exceeds the configured date. The configured date can either be the current system date or a future date. Entering a date prior to the current date is not supported.
Password not changed for	3. Specify the number of days allowed before the password must be changed The range is from **1** to **365** days.
Failed attempts count	4. Specify the number of failed log-in attempts are allowed before the account is disabled. The range is from **1** to **100** attempts.
Reset failed attempts count	5. To reset the failed attempts count to zero and reenable those local users who were disabled after exceeding the failed attempts count, click **Reset**.

Adding and Modifying Endpoints

This section provides the following information:

- Viewing the List of Authentication Endpoints

- Viewing Endpoint Authentication Details
- Performing Bulk Updates of Endpoint Attributes
- Triggering Actions to Be Performed on Endpoints
- Updating Device Fingerprints From a Hosted Portal
- Manually Adding an Endpoint
- Modifying an Endpoint

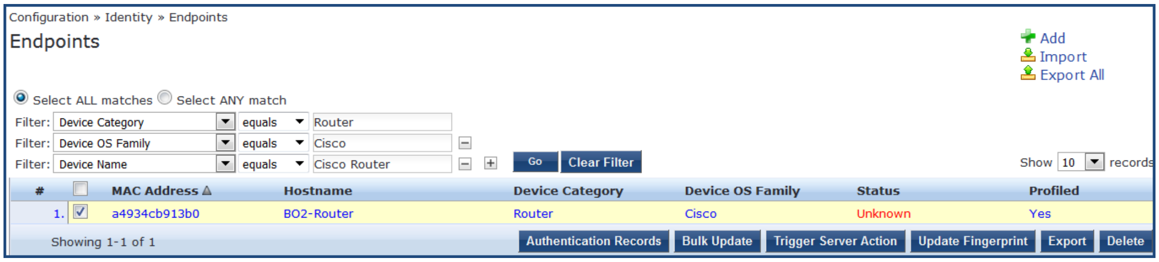
For related information, see:

- Configuring Endpoint Context Server Actions on page 590
- Adding Vendor-Specific Endpoint Context Servers on page 595

Viewing the List of Authentication Endpoints

ClearPass Policy Manager automatically lists all the endpoints that are authenticated in the **Configuration > Identity > Endpoints** page.

Figure 203: *Endpoints Page*



Configuration » Identity » Endpoints

Endpoints

● Select ALL matches ○ Select ANY match

Filter: Device Category equals Router

Filter: Device OS Family equals Cisco

Filter: Device Name equals Cisco Router

#	□	MAC Address ▲	Hostname	Device Category	Device OS Family	Status	Profiled
1.	☑	a4934cb913b0	BO2-Router	Router	Cisco	Unknown	Yes

Showing 1-1 of 1

Table 116: *Endpoint Page Parameters*

Parameter	Action/Description
Filters	You can choose to select **ALL matches** or **ANY matches**. Then you can specify from one to three device filters to refine the endpoint information you wish to view.
MAC Address	Displays the MAC address of the endpoint.
Hostname	Specifies the host name of the endpoint.
Device Category	Indicates the category of the profiled device. For example, Access Points, Computer, SmartDevice, VoIP phone, and so on.
Device OS Family	Specifies the operating system that the device runs on. For example, when the category is Computer, ClearPass shows a Device OS Family of *Windows*, *Linux*, or *Mac OS X*.
Status	Displays the status of the endpoint: - Unknown - Known client - Unknown client - Disabled client
Profiled	Indicates whether the device has been added to the ClearPass Profile.

Viewing Endpoint Authentication Details

To view the authentication details of an endpoint:

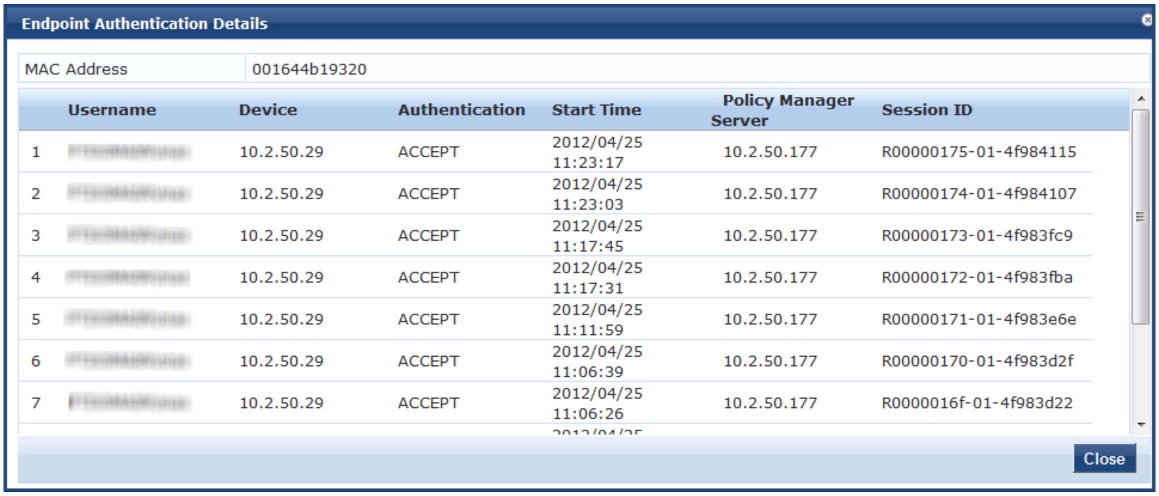
1. From the **Configuration** > **Identity** > **Endpoints** page, select an endpoint by the clicking the corresponding check box.

   The **Authentication Records** button is now enabled.

2. Click the **Authentication Records** button.

   The **Endpoint Authentication Details** page opens.

Figure 204: *Endpoint Authentication Details*



Endpoint Authentication Details

MAC Address	001644b19320

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

Performing Bulk Updates of Endpoint Attributes

You can perform bulk updates of endpoint attributes, either for a single endpoint or for multiple endpoints simultaneously.

To perform bulk updates of endpoint attributes:

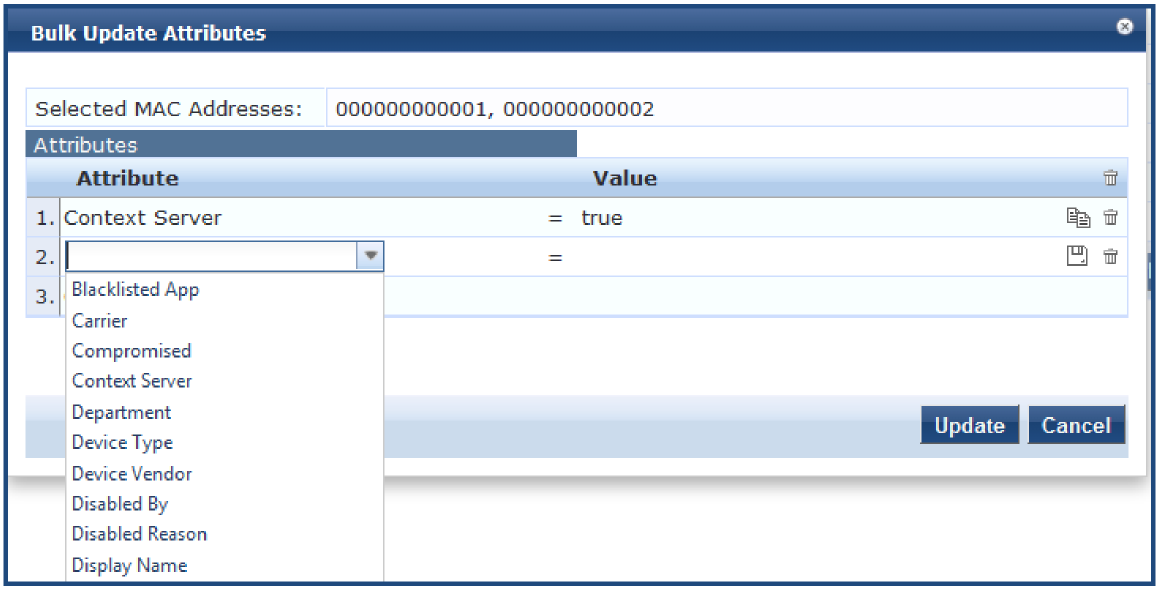
1. From the **Configuration** > **Identity** > **Endpoints** page, select one or more endpoints by the clicking the corresponding check boxes.

   The **Bulk Update** button is now enabled.

2. Click the **Bulk Update** button.

   The **Bulk Update Attributes** dialog opens.

Figure 205: *Bulk Update Attributes*



Bulk Update Attributes

Selected MAC Addresses:	000000000001, 000000000002

Attributes

	Attribute		Value
1.	Context Server	=	true
2.		=	
3.			

3. To select an attribute you want to update, select **Click to add**, select the attribute from the **Attribute** list, and then specify its **Value**.
4. Repeat the selection process for all the attributes you want to update, then click **Update**.

Triggering Actions to Be Performed on Endpoints

You can trigger endpoint actions for a single endpoint or for multiple endpoints simultaneously.

To trigger actions that are to be performed on selected endpoints:

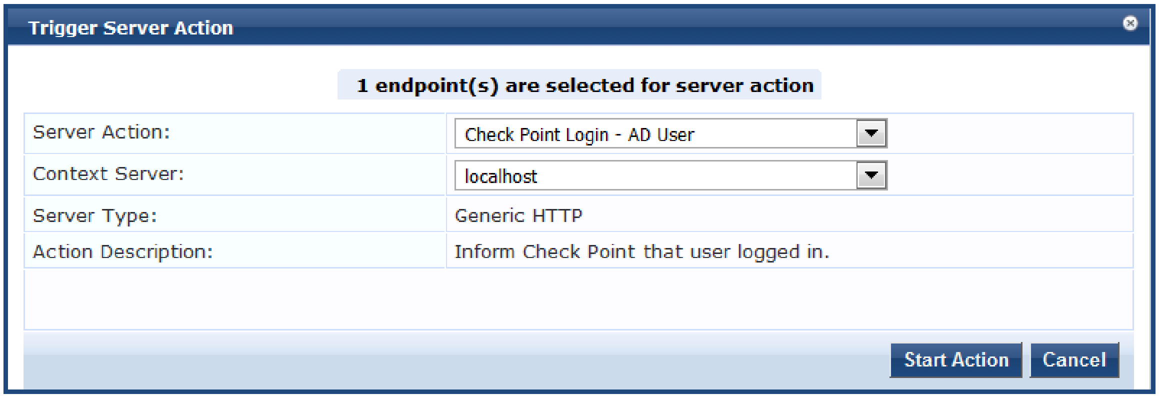
1. From the **Configuration** > **Identity** > **Endpoints** page, select one or more endpoints from the **Endpoints** page by clicking the corresponding check boxes.

   The **Trigger Server Action** button is now enabled.

2. Click the **Trigger Server Action** button.

   The **Trigger Server Action** page opens:

Figure 206: *Endpoints > Trigger Server Action Page*



Trigger Server Action

1 endpoint(s) are selected for server action

Server Action:	Check Point Login - AD User
Context Server:	localhost
Server Type:	Generic HTTP
Action Description:	Inform Check Point that user logged in.

3. Specify the **Trigger Server Action** page parameters as described in the following table, then click **Start Action**:

Table 117: *Trigger Server Action Page Parameters*

Parameter	Action/Description
Server Action	Select the server action from the drop-down list. The available server actions are as follows: - Check Point Login - AD User - Check Point Logout - Guest User - Fortinet Login - Fortinet Logout - Handle AirGroup Time Sharing - Infoblox Login - Nmap Scan - SNMP Scan
Context Server	Enter a valid context server name. You can enter an IP address or domain name.
Server Type	Indicates the server type specified when the server was configured.
Action Description	Describes the action that will take place on the endpoint; for example, "Inform Check Point that user logged in."

Updating Device Fingerprints From a Hosted Portal

You can update device fingerprints for a single endpoint or for multiple endpoints simultaneously.

To update device fingerprints from a hosted portal:

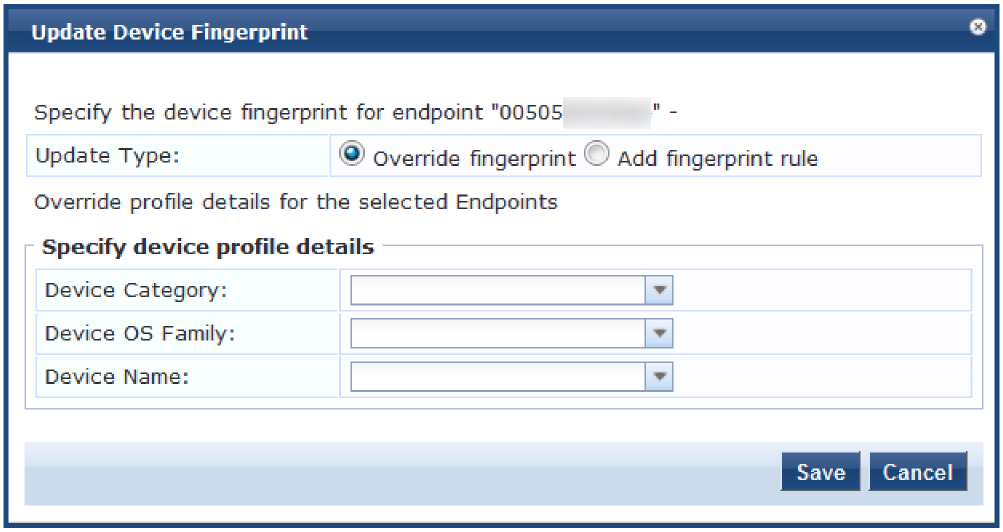
1. From the **Configuration** > **Identity** > **Endpoints** page, select one or more endpoints by clicking the corresponding check boxes.

   The **Update Fingerprint** button is now enabled.

2. Click the **Update Fingerprint** button.

   The **Update Device Fingerprint** page opens. By default, the **Update Type** is set to **Override fingerprint** (see Figure 207).

Figure 207: *Update Device Fingerprint Page: Override Fingerprint*



Update Device Fingerprint

Specify the device fingerprint for endpoint "00505[redacted]" -

Update Type:	● Override fingerprint ○ Add fingerprint rule

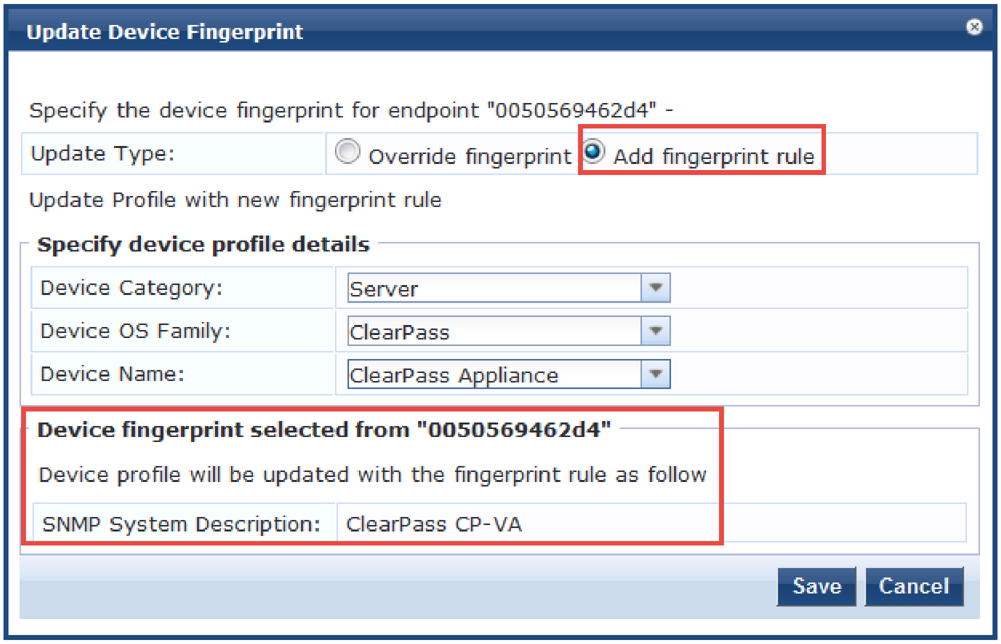
Override profile details for the selected Endpoints

Specify device profile details

Device Category:	
Device OS Family:	
Device Name:	

Figure 208 shows the **Update Device Fingerprint** page when you set the **Update Type** to **Add fingerprint rule**.

Figure 208: *Update Device Fingerprint Page: Add Fingerprint Rule*



Update Device Fingerprint

Specify the device fingerprint for endpoint "0050569462d4" -

Update Type: ○ Override fingerprint ● Add fingerprint rule

Update Profile with new fingerprint rule

Specify device profile details

Device Category:	Server
Device OS Family:	ClearPass
Device Name:	ClearPass Appliance

Device fingerprint selected from "0050569462d4"

Device profile will be updated with the fingerprint rule as follow

SNMP System Description:	ClearPass CP-VA

3. Specify the **Update Device Fingerprint** page parameters as described in the following table, then click **Save**:

Table 118: *Update Device Fingerprint Parameters*

Parameter	Action/Description
Update Type	Select one of the following update types: ● **Override fingerprint**: Update the device profile details (device category, device OS family, and device name) for the selected endpoint. ● **Add fingerprint rule**: Update the device profile with a new fingerprint rule. This information is displayed at the bottom of the **Update Device Fingerprint** page, as shown in Figure 208.
Specify Device Profile Details	
Device Category	Select the category the profiled device belongs to.
Device OS Family	Select the operating system configured on the device.
Device Name	Enter the name of the device. You can select the name of the device from the list.

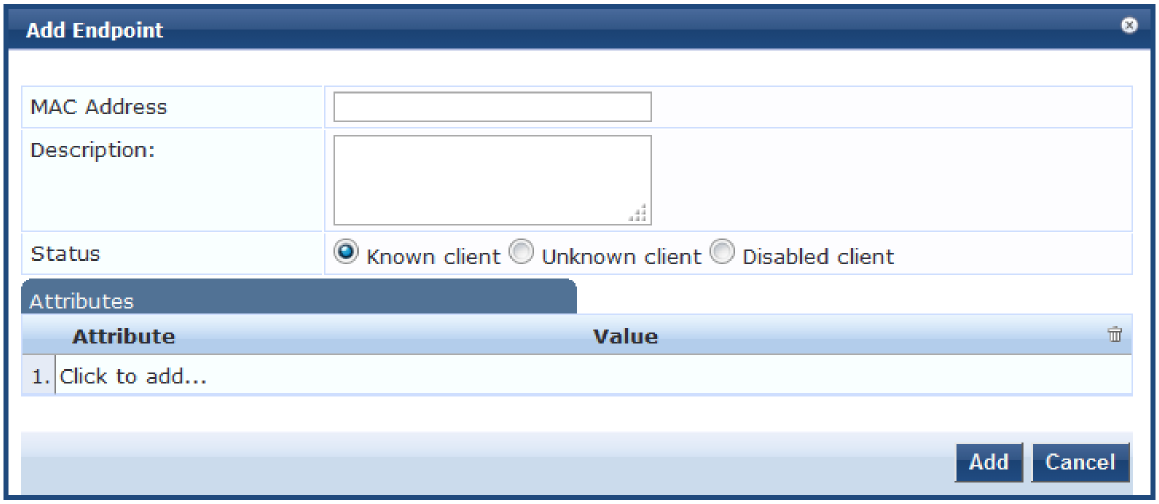
Manually Adding an Endpoint

To manually add an endpoint:

1. From the **Configuration** > **Identity** > **Endpoints** page, click **Add**.

   The **Add Endpoint** page opens.

Figure 209: *Add Endpoint Page*



Add Endpoint

MAC Address	
Description:	
Status	● Known client ○ Unknown client ○ Disabled client

Attributes

	Attribute	Value
1.	Click to add...	

2. Specify the **Add Endpoint** page parameters as described in the following table, then click **Save**:

Table 119: *Add Endpoint Page Parameters*

Parameter	Action/Description
MAC Address	Specify the MAC address of the endpoint.
Description	Enter a description that provides additional information about the endpoin (recommended).
Status	Specify the client status as: ● Known client ● Unknown client ● Disabled client ■ You can use the **Known client** and **Unknown client** status in role-mapping rules by specifying 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 Profiler.
Attributes	Add custom attributes for this endpoint. Select 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.

Modifying an Endpoint

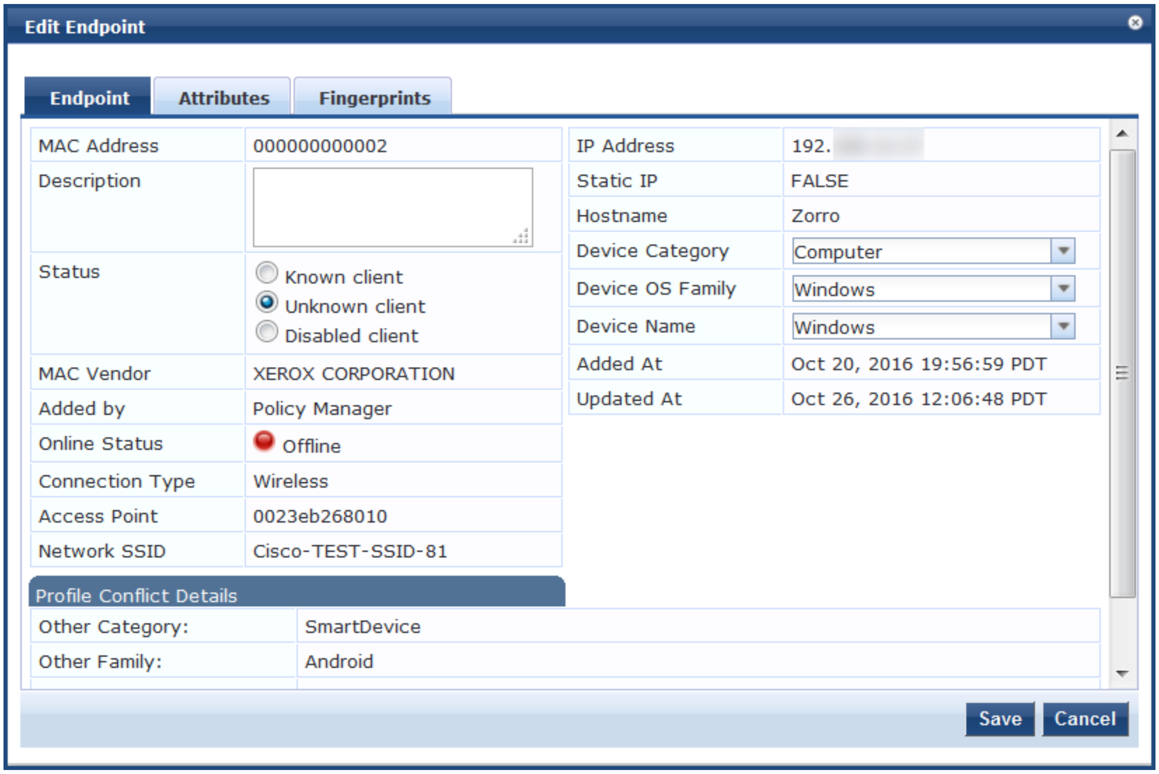
To modify an endpoint:

1. From the **Configuration** > **Identity** > **Endpoints** page, click the endpoint of interest from the list of endpoints.

   The **Edit Endpoint** page opens.

Modifying an Endpoint

Figure 210: *Edit Endpoint Page*



Edit Endpoint

MAC Address	000000000002
Description	
Status	○ Known client ● Unknown client ○ Disabled client
MAC Vendor	XEROX CORPORATION
Added by	Policy Manager
Online Status	● Offline
Connection Type	Wireless
Access Point	0023eb268010
Network SSID	Cisco-TEST-SSID-81

IP Address	192.[redacted]
Static IP	FALSE
Hostname	Zorro
Device Category	Computer
Device OS Family	Windows
Device Name	Windows
Added At	Oct 20, 2016 19:56:59 PDT
Updated At	Oct 26, 2016 12:06:48 PDT

Profile Conflict Details

Other Category:	SmartDevice
Other Family:	Android

2. Specify the **Edit Endpoint** page parameters as described in the following table, then click **Save**:

Table 120: *Edit Endpoint Page Parameters*

Parameter	Action/Description
MAC Address	Displays the MAC address of the endpoint.
Description	Enter a description that provides additional information about the endpoint (recommended).
Status	Indicate the status of the selected endpoint as: - **Known client** - **Unknown client** - **Disabled client** - You can use the **Known** client and **Unknown** client status in role-mapping rules by applying 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 Profiler.
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:

Table 120: *Edit Endpoint Page Parameters (Continued)*

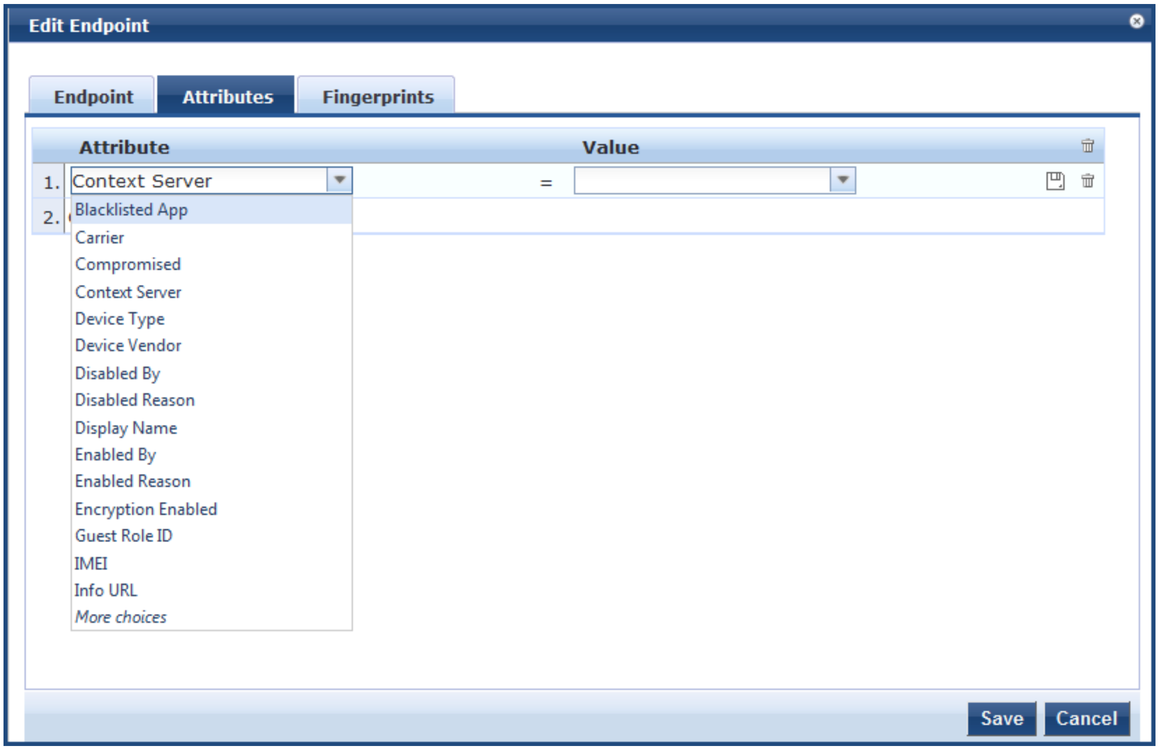
Parameter	Action/Description
	- Green button: **Online** - Red button: **Offline**
Connection Type	Indicates the connection type; for example, **Wireless**. If the connection type is not known, the connection type is displayed as *Unknown*.
Access Point	Indicates the access point with which the endpoint device is associated.
Network SSID	Indicates the SSID of the network in which the endpoint is deployed.
IP Address	Displays the IP address that is associated with the endpoint.
Static IP	Indicates whether the IP address of the endpoint is a static IP address (**True** or **False**).
Hostname	Displays the host name or the IP address of the endpoint.
Device Category	Select the device category that the endpoint belongs to from the drop-down list.
Device OS Family	Specify the operating system that the endpoint runs on.
Device Name	Select the name of the device from the drop-down list.
Added At	Displays the date and time at which the endpoint was added.
Updated At	Displays the date and time at which the endpoint was updated.

Configuring the Attributes for the Selected Endpoint

To configure the endpoint attributes for the selected endpoint:

1. From the **Edit Endpoint** page, select the **Attributes** tab.

Figure 211: *Adding Endpoint Attributes*



2. To add attributes for the selected endpoint, click **Click to add...**

   A new row is created with a drop-down list in the **Attribute** column.

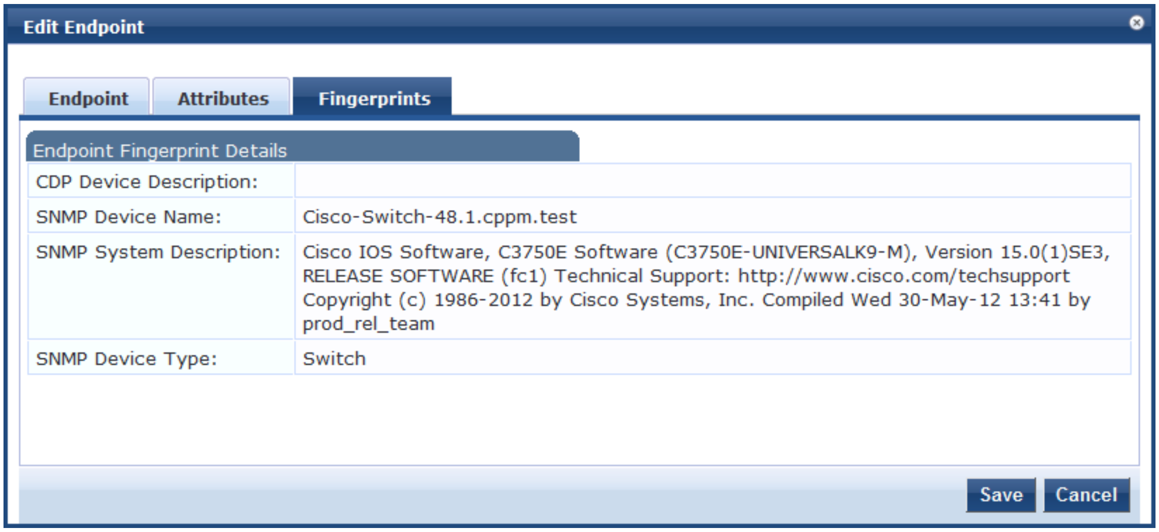
3. To add an attribute to the endpoint, select one or more attributes from the drop-down list , then click **Save**.

Viewing the Endpoint Fingerprint Details

The information displayed in the **Edit Endpoint** > **Fingerprints** page varies depending on what type of device is selected and whether an Nmap-based network discovery scan has been run (see Configuring Nmap-Based Endpoint Port Scans on page 147).

As shown in Figure 212, the Fingerprints details page shows the active and inactive Windows services and processes for the selected Windows endpoint. Service names are listed alphabetically.

Figure 212: *Endpoint Fingerprint Details Page*



Endpoint Fingerprint Details

CDP Device Description:	
SNMP Device Name:	Cisco-Switch-48.1.cppm.test
SNMP System Description:	Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE3, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Wed 30-May-12 13:41 by prod_rel_team
SNMP Device Type:	Switch

Additional Endpoint Tasks

- **Delete an endpoint**: Select the desired endpoint, then click **Delete**.
- **Export an endpoint**: Select the desired endpoint, then click **Export**.
- **Export all endpoints**: Click the **Export All** link in the upper-right corner of the page.
- **Import endpoints**: Click the **Import** link in the upper-right corner of the page.

Managing Static Host Lists

This section provides the following information:

- About Static Host Lists
- Adding a Static Host List
- Static Hosts Lists Configuration Summary
- Editing a Static Host List
- Importing and Exporting Static Host Lists

About Static Host Lists

You can configure primary and backup servers, session details, and the list of static hosts for **Static Host List** authentication sources.

A static host list often functions, in the context of the service, as a white list or a black list. Therefore, static host lists are configured independently at the global level.

A static host list comprises a named list of MAC addresses 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. For more information, see Adding a Static Host List as an Authentication Source on page 226.

NOTE

Only static host lists of type **MAC address** are available as authentication sources.

Internal Relational Database

An internal relational database stores the ClearPass Policy Manager configuration data as well as locally configured user and device accounts.

The following predefined authentication sources represent the 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.

Role Statically Assigned

For a user account created in a 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 account (local or guest) in the local database, these can be used in role-mapping policies.

Preconfigured Filter

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.

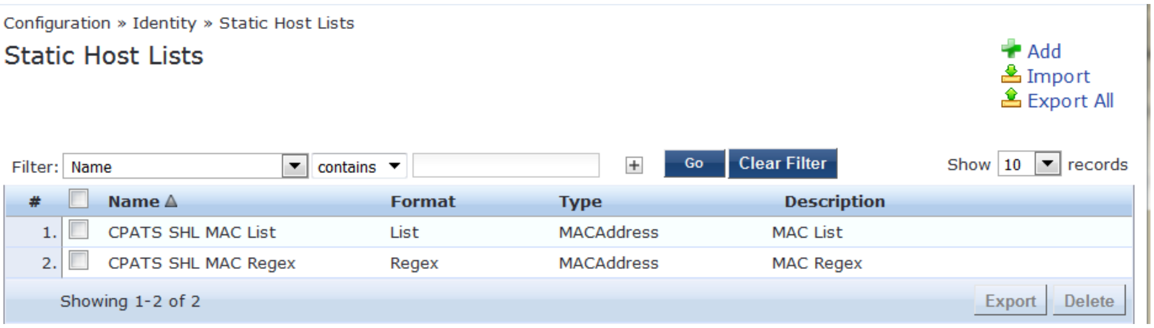
Adding a Static Host List

To add a static host list to ClearPass:

1. Navigate to the **Configuration > Identity > Static Host Lists** page.

   The **Static Hosts Lists** page opens.

Figure 213: *Static Host Lists Page*



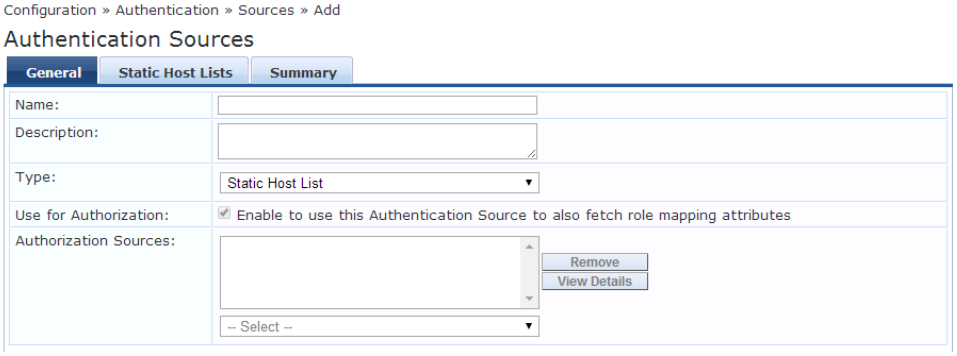
#		Name	Format	Type	Description
1.	□	CPATS SHL MAC List	List	MACAddress	MAC List
2.	□	CPATS SHL MAC Regex	Regex	MACAddress	MAC Regex

Showing 1-2 of 2

2. Click **Add**.

   The **Add Static Host List** dialog opens.

Figure 214: *Adding a Static Host List*



Name:	
Description:	
Type:	Static Host List
Use for Authorization:	☑ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	-- Select --

3. Specify the parameters to add a static host list as described in Table 121, then click **Save**.

Table 121: *Add Static Host List Parameters*

Parameter	Action/Description
Name	1. Enter the name of the static host list.
Description	2. Enter the description that provides additional information about the static host list.
Host Format	3. Select a format for expression of the address: ● **Subnet** ● **Regular Expression** ● **List**

Table 121: *Add Static Host List Parameters (Continued)*

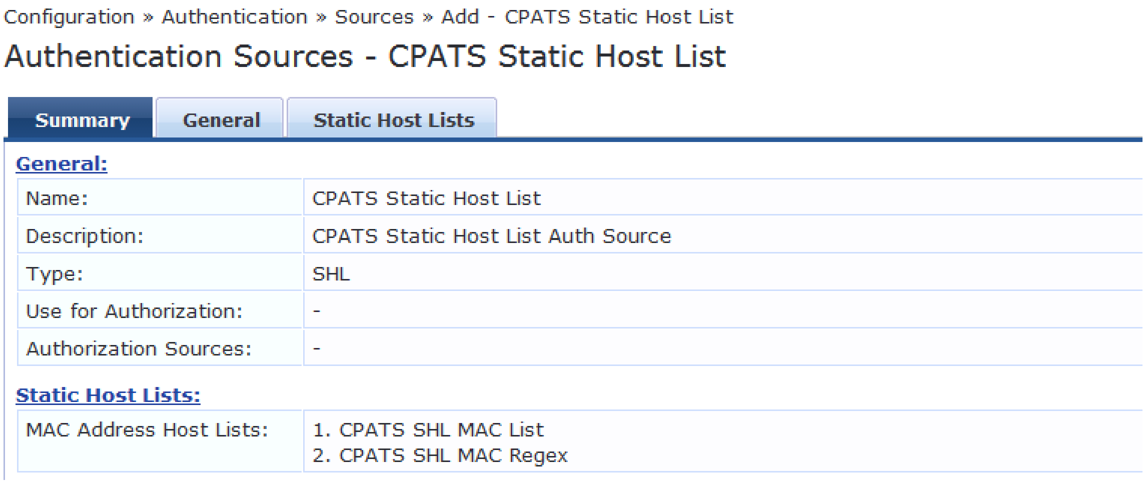
Parameter	Action/Description
Host Type	4. Select a host type: ● **IP Address** ● **MAC Address**
Subnet	5. Enter the subnet address.

The new static host list is now available to be added as an authentication source. For details, see Adding a Static Host List as an Authentication Source on page 227.

Static Hosts Lists Configuration Summary

You can use the **Summary** tab to view the static host list's configuration information.

Figure 215: *Static Hosts Lists Configuration Summary*



Configuration » Authentication » Sources » Add - CPATS Static Host List

Authentication Sources - CPATS Static Host List

General:

Name:	CPATS Static Host List
Description:	CPATS Static Host List Auth Source
Type:	SHL
Use for Authorization:	-
Authorization Sources:	-

Static Host Lists:

MAC Address Host Lists:	1. CPATS SHL MAC List 2. CPATS SHL MAC Regex

Editing a Static Host List

To edit a static host list:

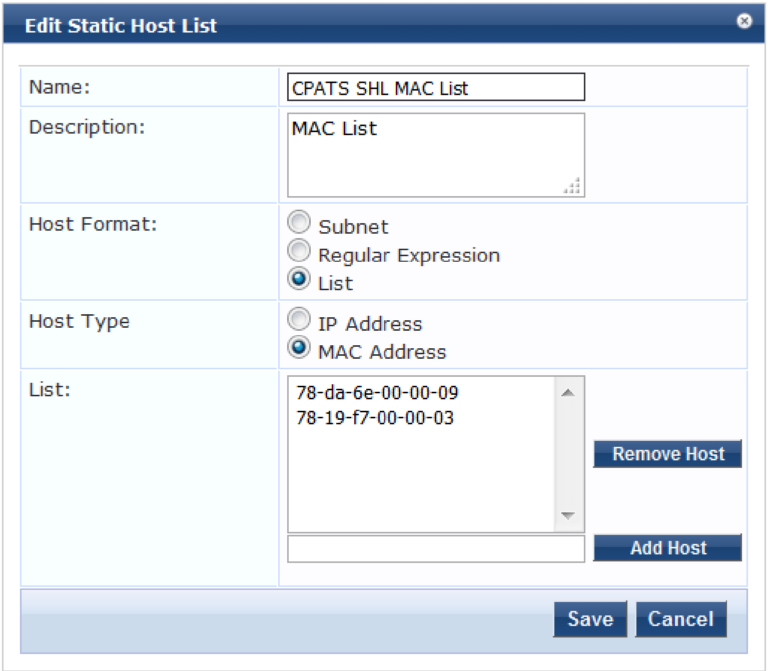
1. Navigate to the **Configuration > Identity > Static Host Lists** page .

   The **Static Hosts Lists** page opens.

2. Click on the name of the static hosts list you want to edit.

   The **Edit Static Host List** dialog opens.

Figure 216: *Edit Static Host List Dialog*



Edit Static Host List

Name:	CPATS SHL MAC List
Description:	MAC List
Host Format:	○ Subnet ○ Regular Expression ● List
Host Type	○ IP Address ● MAC Address
List:	78-da-6e-00-00-09 78-19-f7-00-00-03

3. Make any required changes, then click **Save**.

Importing and Exporting Static Host Lists

You can import static host lists into ClearPass or export them to a file.

1. Navigate to the **Configuration > Identity > Static Host Lists** page .

   The **Static Hosts Lists** page opens.
2. Click on the name of the static hosts list you want to import or export.
3. To import a static host list into ClearPass, click the **Import** link.
4. To export a static host list to a file, click the **Export All** link.

   For further details, see Importing and Exporting Information on page 31.

Configuring a Role and Role-Mapping Policy

This section includes the following information:

- Preconfigured Roles
- Adding and Modifying Roles on page 257
- Adding and Modifying Role-Mapping Policies on page 258

After authenticating a request, a Policy Manager service invokes its role-mapping policy, resulting in assignment of a role(s) to the client. This role becomes the identity component of enforcement policy decisions.

NOTE

A service can be configured without a role-mapping policy, but only one role-mapping policy can be configured for each service.

Preconfigured Roles

Policy Manager provides the following preconfigured roles:

- [AirGroup v1]: Role for an AirGroup protocol version 1 request.

- [AirGroup v2]: Role for an AirGroup protocol version 2 request.
- [Aruba TACACS read-only Admin]: Default role for read-only\ access to Aruba device.
- [Aruba TACACS root Admin]: Default role for root access to Aruba device.
- [BYOD Operator]: Operators with this profile can view and manage their own provisioned devices.
- [Contractor]: Default role for a contractor
- [Device Registration]: Operators with this profile can self-provision their devices for MAC authentication and AirGroup sharing.
- [Employee]: Default role for an employee.
- [Guest]: Default role for guest access.
- [MAC Caching]: Default role applied during MAC caching.
- [Onboard Android]: Role for an Android device being provisioned.
- [Onboard Chromebook]: Role for a Chromebook device being provisioned.
- [Onboard iOS]: Role for an iOS device being provisioned.
- [Onboard Linux]: Role for a Linux device being provisioned.
- [Onboard Mac OS X]: Role for a Mac OS X device being provisioned.
- [Onboard Windows]: Role for a Windows device being provisioned.
- [Other]: Default role for another 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 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 user interface screens

Identity Roles Architecture and Workflow

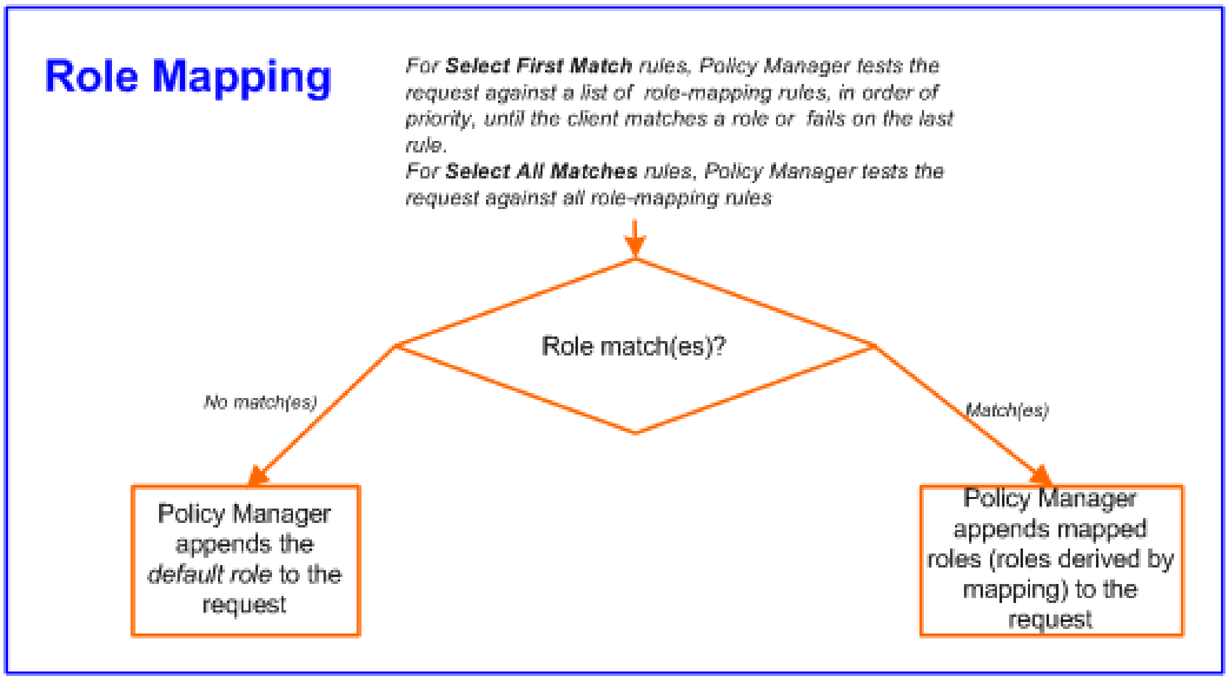
Roles can range in complexity from a simple user group (for example, Finance, Engineering, or Human Resources) to a combination of a user group with some dynamic constraints (for example, “Night Shift Worker,” an employee in the Engineering department who logs in through the network device between 8:00 p.m. and 5:00 a.m on weekdays). It can also apply to a list of users.

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

For more information, see Configuring a Role and Role-Mapping Policy on page 255.

Figure 217 illustrates the role-mapping process and workflow.

Figure 217: *Role-Mapping Process*


Role Mapping
For **Select First Match** rules, Policy Manager tests the request against a list of role-mapping rules, in order of priority, until the client matches a role or fails on the last rule.
For **Select All Matches** rules, Policy Manager tests the request against all role-mapping rules
Role match(es)?
No match(es)
Match(es)
Policy Manager appends the *default role* to the request
Policy Manager appends mapped roles (roles derived by mapping) to the request

A role can be:

- Authenticated through predefined single sign-on rules.
- Associated directly with a user in the Policy Manager *local user* database.
- Authenticated based on predefined allowed endpoints.
- Associated directly with a *static host list*, again through *role mapping*.
- Discovered by Policy Manager through *role mapping*.

  Roles are typically discovered by Policy Manager by retrieving attributes from the *authentication source*.

  Filter rules associated with the authentication source tell Policy Manager where to retrieve these attributes.
- Assigned automatically when retrieving attributes from the *authentication source*. Any attribute in the authentication source can be mapped directly to a role.

Adding and Modifying Roles

Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.

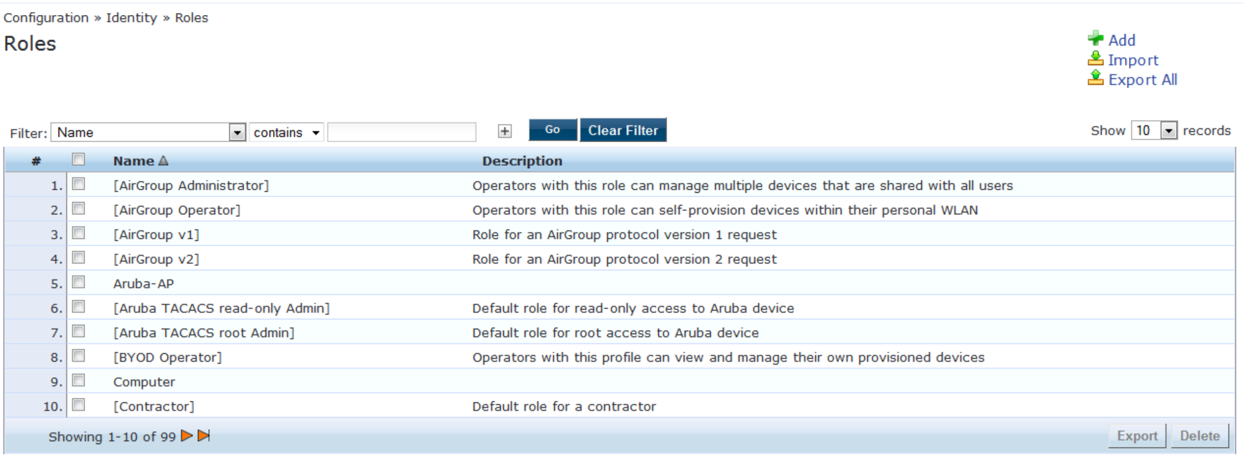
Policy Manager lists all available roles in the **Roles** page.

To add a role:

1. Navigate to **Configuration** > **Identity** > **Roles**.

   The **Roles** page opens.

Figure 218: *Roles Page*



Configuration » Identity » Roles

Roles

#		Name	Description
1.	□	[AirGroup Administrator]	Operators with this role can manage multiple devices that are shared with all users
2.	□	[AirGroup Operator]	Operators with this role can self-provision devices within their personal WLAN
3.	□	[AirGroup v1]	Role for an AirGroup protocol version 1 request
4.	□	[AirGroup v2]	Role for an AirGroup protocol version 2 request
5.	□	Aruba-AP	
6.	□	[Aruba TACACS read-only Admin]	Default role for read-only access to Aruba device
7.	□	[Aruba TACACS root Admin]	Default role for root access to Aruba device
8.	□	[BYOD Operator]	Operators with this profile can view and manage their own provisioned devices
9.	□	Computer	
10.	□	[Contractor]	Default role for a contractor

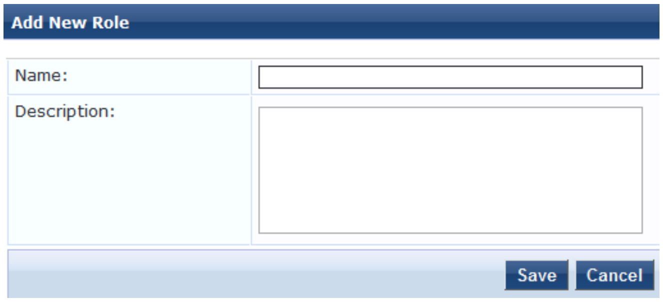
Showing 1-10 of 99

You can also configure a role from within a role-mapping policy (**Add New Role**).

2. Click **Add**.

   The **Add New Role** page opens.

Figure 219: *Add New Role Page*



3. Define the **Add New Role** parameters as described in the following table, then click **Save**.

Table 122: *Add New Role Page Parameters*

Parameter	Action/Description
Name	Enter the name of the role.
Description	Optionally, enter the description that provides additional information about the new role (recommended).

Adding and Modifying Role-Mapping Policies

This section includes the following information:

- Adding a Role-Mapping Policy
- Mapping Rules
- Modifying a Role-Mapping Policy

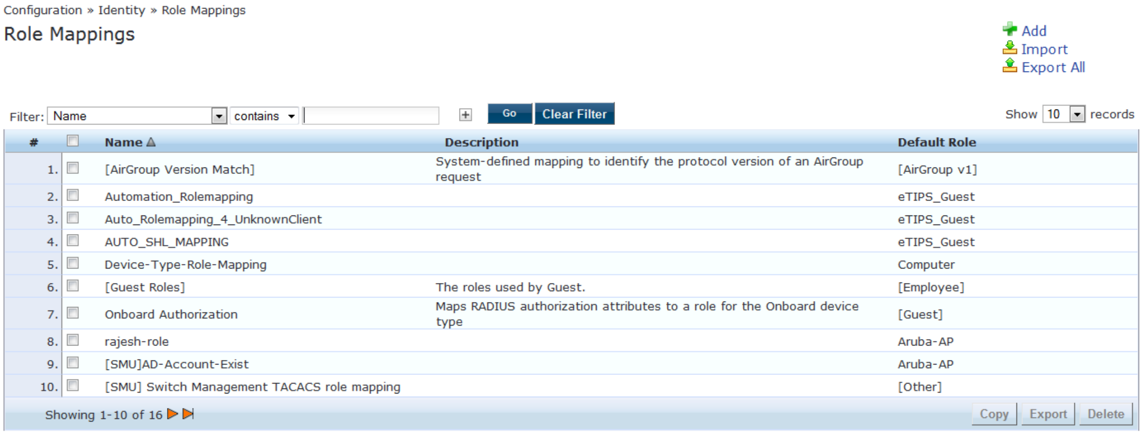
Adding a Role-Mapping Policy

To add a role-mapping policy:

1. Navigate to the **Configuration > Identity > Role Mappings** page.

   The **Role Mappings** page opens:

Figure 220: *Role Mappings Page*



Configuration » Identity » Role Mappings

Role Mappings

#	□	Name	Description	Default Role
1.	□	[AirGroup Version Match]	System-defined mapping to identify the protocol version of an AirGroup request	[AirGroup v1]
2.	□	Automation_Rolemapping		eTIPS_Guest
3.	□	Auto_Rolemapping_4_UnknownClient		eTIPS_Guest
4.	□	AUTO_SHL_MAPPING		eTIPS_Guest
5.	□	Device-Type-Role-Mapping		Computer
6.	□	[Guest Roles]	The roles used by Guest.	[Employee]
7.	□	Onboard Authorization	Maps RADIUS authorization attributes to a role for the Onboard device type	[Guest]
8.	□	rajesh-role		Aruba-AP
9.	□	[SMU]AD-Account-Exist		Aruba-AP
10.	□	[SMU] Switch Management TACACS role mapping		[Other]

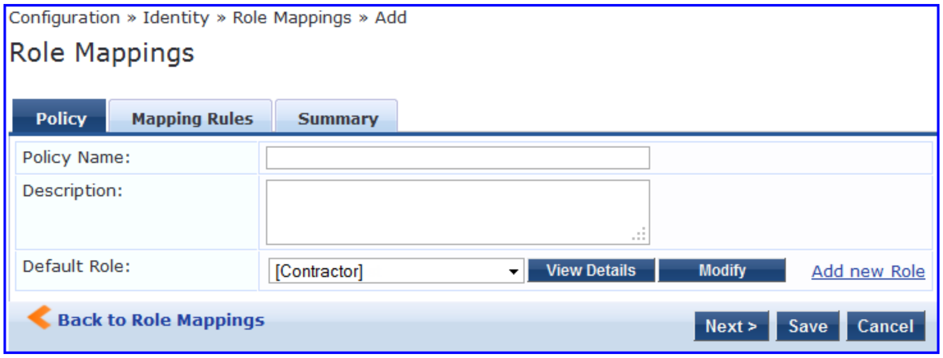
Showing 1-10 of 16

2. Click **Add**.

   The **Add Role-Mappings** page opens to the **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 role-mapping policy does not produce a match for a given request.

Figure 221: *Role Mappings > Policy Tab*



Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Name:

Description:

Default Role: [Contractor]

3. Specify the **Role Mappings > Policy** parameters as described in the following table:

Table 123: *Role Mappings > Policy Parameters*

Parameter	Action/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 a match.

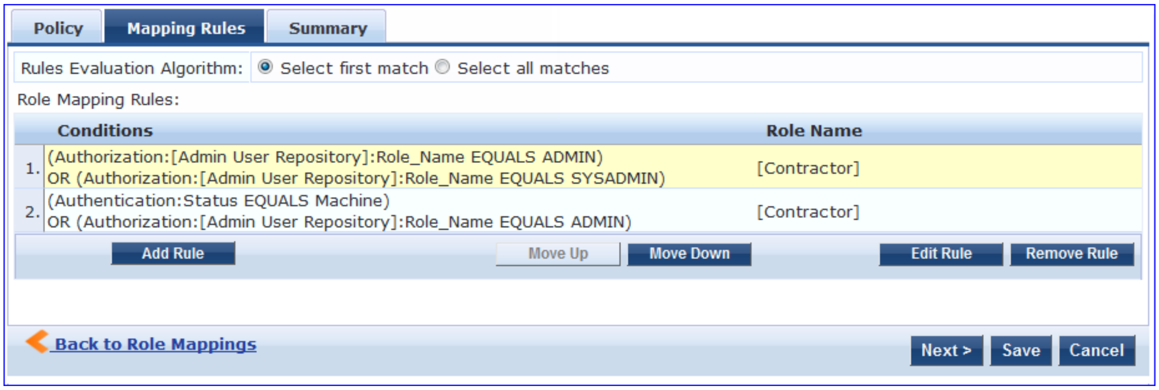
Table 123: *Role Mappings > Policy Parameters (Continued)*

Parameter	Action/Description
View Details	To view the details of the default role, click **View Details**.
Modify	To modify the default role, click **Modify**.
Add New Role	To add a new role, click **Add New Role**.

Mapping Rules

The **Mapping Rules** tab selects the evaluation algorithm to add, edit, remove, and reorder rules (see Figure 222).

Figure 222: *Role Mapping > Mapping Rules Page*



Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Role Mapping Rules:

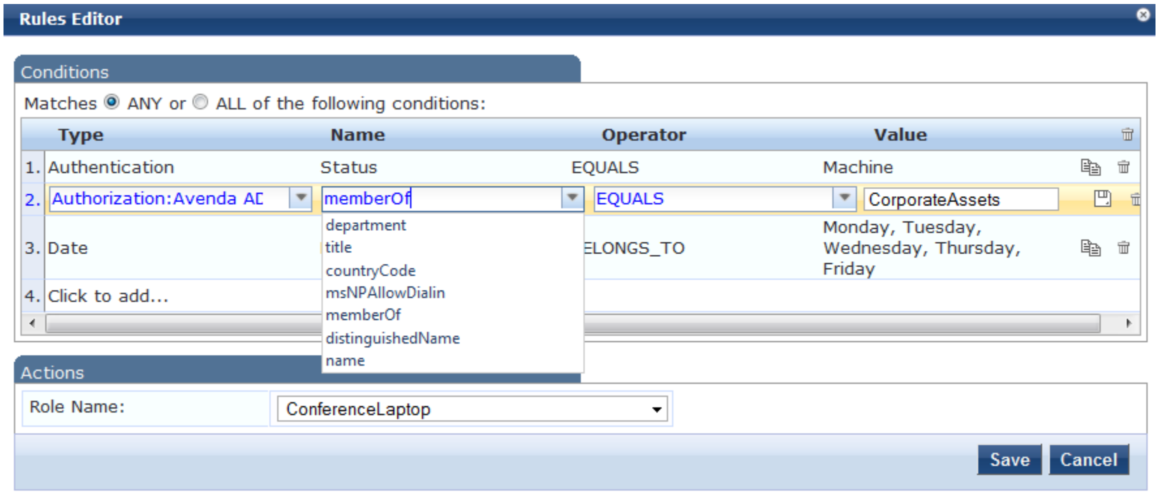
	Conditions	Role Name
1.	(Authorization:[Admin User Repository]:Role_Name EQUALS ADMIN) OR (Authorization:[Admin User Repository]:Role_Name EQUALS SYSADMIN)	[Contractor]
2.	(Authentication:Status EQUALS Machine) OR (Authorization:[Admin User Repository]:Role_Name EQUALS ADMIN)	[Contractor]

To add a mapping rule:

1. Click **Add Rule**.

   The **Rules Editor** page opens.

Figure 223: *Rules Editor Page*



Matches ● ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Status	EQUALS	Machine
2.	Authorization:Avenda AD	memberOf	EQUALS	CorporateAssets
3.	Date		ELONGS_TO	Monday, Tuesday, Wednesday, Thursday, Friday
4.	Click to add...			

Role Name: ConferenceLaptop

2. Specify the **Role Mappings Page > Rules Editor** page parameters as described in the following table.

Table 124: *Rules Editor Page Parameters*

Parameter	Action/Description
Type	The Rules Editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries, depending on context. (Refer to Namespaces on page 875.) In the role mapping context, Policy Manager allows attributes from following namespaces: ● Application ● Application:ClearPass ● Application:SSO ● 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 Configuring Authentication Sources on page 190). 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. For more information about operators, seeOperators on page 886.
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.

NOTE

The operator values that display for each type and name are based on the data type specified for the authentication source (from the **Configuration** > **Authentication** > **Sources** page). If, for example, you modify the *UserDN Data* type on the authentication sources page to be an integer rather than a string, then the list of operator values here will populate with values that are specific to integers.

Modifying a Role-Mapping Policy

After you save your role-mapping configuration, it is displayed in the **Mapping Rules** list.

To modify a role-mapping policy:

1. Select the rule you wish to modify.
2. Then you can move the rule up or down in the list, edit the rule, or remove the rule.
3. Click **Save**.

Chapter 6
Posture

This chapter provides the following information:

- Posture Architecture and Flow
- Creating a New Posture Policy
- Configuring Posture Policy Agents and Hosts
- Configuring Posture Policy Plug-ins
- Configuring Posture Policy Rules
- Configuring Posture for Services
- Configuring Audit Servers
- Unified Agent System Tray Status Icons

Posture Architecture and Flow

This section provides the following information:

- Posture Policy
- Audit Servers
- Assessing Client Consistency
- Application Token
- System Token

Policy Manager supports two types of posture checking: posture policies 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.

NOTE

A service can also be configured without any posture policy.

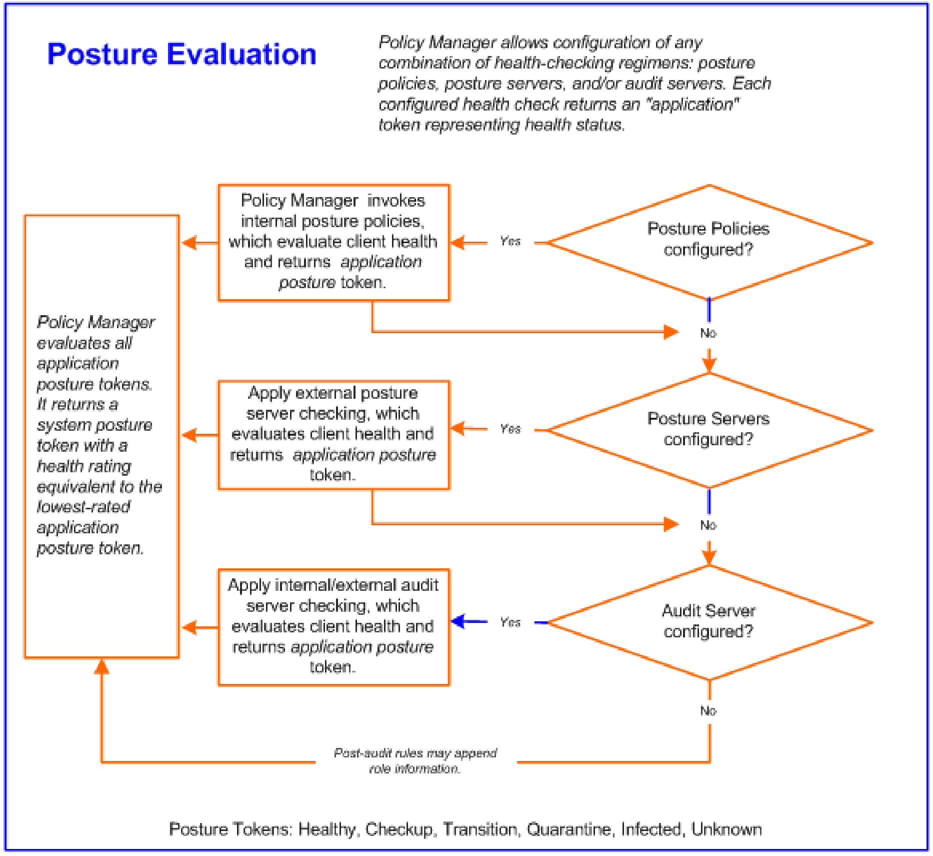
Audit Servers

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:

- **NMAP audit server**: Primarily used to derive roles from post-audit rules.
- **NESSUS audit server**: Primarily used for vulnerability scans (and, optionally, post-audit rules).

Figure 224: *Posture Evaluation Process*


Posture Evaluation
Policy Manager allows configuration of any combination of health-checking regimens: posture policies, posture servers, and/or audit servers. Each configured health check returns an "application" token representing health status.
Policy Manager invokes internal posture policies, which evaluate client health and returns application posture token.
Yes
Posture Policies configured?
No
Policy Manager evaluates all application posture tokens. It returns a system posture token with a health rating equivalent to the lowest-rated application posture token.
Apply external posture server checking, which evaluates client health and returns application posture token.
Yes
Posture Servers configured?
No
Apply internal/external audit server checking, which evaluates client health and returns application posture token.
Yes
Audit Server configured?
No
Post-audit rules may append role information.
Posture Tokens: Healthy, Checkup, Transition, Quarantine, Infected, Unknown

Assessing Client Consistency

ClearPass 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 software components
- Peer-to-Peer (P2P) application checks
- Services to be running or not running
- Processes to be running or not running

Application Token

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.

System Token

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.

Unified Agent System Tray Status Icons

This section provides the following information:

- About the Unified Agent
- Unified Agent System Tray Icons
- OnGuard-Only System Tray Icons

About the Unified Agent

ClearPass Onguard agent is integrated with Aruba VIA (Virtual Internet Adapter) to support both VIA functionality and Onguard agent system health status collection. Thus, the integrated product is the called the *Unified Agent*.

NAP (Network Access Protection) is a framework to collect system health status on Microsoft clients.

ClearPass supports health status collection for both NAP and OnGuard.

The Unified Agent System Tray icons display the following states of the Unified Agent status:

- OnGuard health status
- Trusted or untrusted network status
- VPN connectivity status
- Error conditions

Unified Agent System Tray Icons

Table 125 describes that icons that indicate the possible states for the Unified Agent.

Table 125: *Unified Agent System Tray Icons*

OnGuard Status	Network Type	VPN Status	Icon
Healthy	Trusted	Connected	🟢
Healthy	Trusted	Disconnected	🟢
Unhealthy	Trusted	Connected	🔴
Unhealthy	Trusted	Disconnected	🔴

Table 125: *Unified Agent System Tray Icons (Continued)*

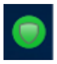
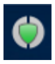
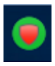
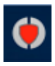
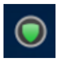
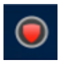
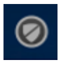
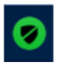
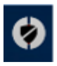
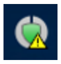
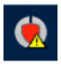
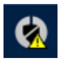
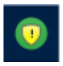
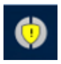
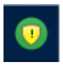
OnGuard Status	Network Type	VPN Status	Icon
Healthy	Untrusted	Connected	
Healthy	Untrusted	Disconnected	
Unhealthy	Untrusted	Connected	
Unhealthy	Untrusted	Disconnected	
Healthy	N/A	Error	
Unhealthy	N/A	Error	
Logged Out: No Health Status	N/A	Error	
Error	Trusted	Connected	
Error	Trusted	Disconnected	
Error	Untrusted	Connected	
Error	Untrusted	Disconnected	
Error	No Profile	N/A	
Error	N/A	Error	
Healthy	No Profile	N/A	
Unhealthy	No Profile	N/A	

Table 125: *Unified Agent System Tray Icons (Continued)*

OnGuard Status	Network Type	VPN Status	Icon
Logged Out: No Health Status	No Profile	N/A	🟡
Logged Out: No Health Status	Trusted	Connected	🟡
Logged Out: No Health Status	Untrusted	Disconnected	⊘

OnGuard-Only System Tray Icons

Table 126 describes that icons that indicate the possible states for OnGuard-only.

Table 126: *OnGuard-Only System Tray Icons*

OnGuard Status	Network Type	VPN Status	Icon
Healthy	N/A	N/A	🟢
Unhealthy	N/A	N/A	🔴
Logged Out: No Health Status	N/A	N/A	⊘
Error	N/A	N/A	🟡

Creating a New Posture Policy

This chapter provides the following information:

- About ClearPass Posture Policies
- Creating a New Posture Policy

About ClearPass Posture Policies

ClearPass Policy Manager evaluates the health of the clients that request access using posture policies and an audit server.

All these methods return posture tokens (for example, Healthy and Quarantine) for used by Policy Manager as input into an enforcement policy. You can associate one or more posture methods with a single service.

ClearPass Policy Manager forwards all or part of the posture data received from the client to a posture server. Nmap (Network Mapper) or Nessus audit servers provide posture checking for unmanageable devices, such as devices lacking adequate posture agents or supplicants. For more information on audit servers, see Configuring Audit Servers on page 338.

Creating a New Posture Policy

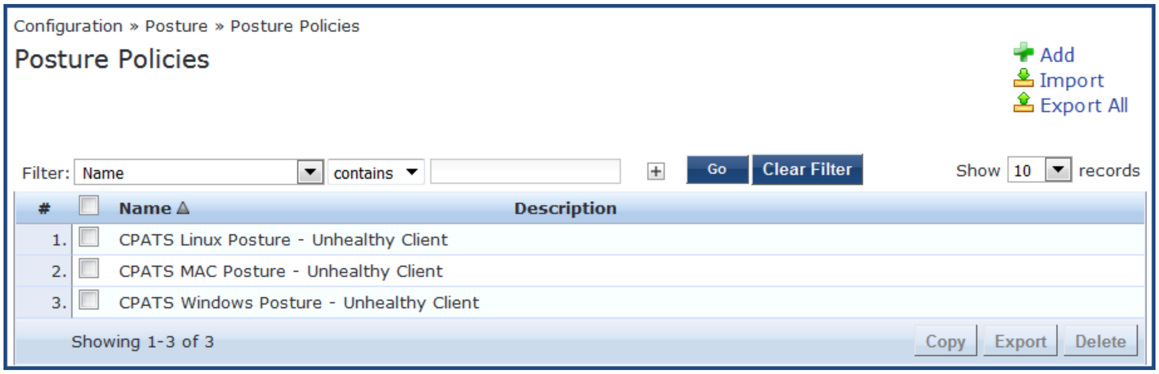
From the **Posture Policies** page, you can create a new policy or edit an existing policy.

To create a new posture policy:

1. Navigate to **Configuration > Posture > Posture Policies.**

   The **Posture Policies** page displays a list of all existing posture policies.

Figure 225: *Posture Policies Page*



Configuration » Posture » Posture Policies

Posture Policies

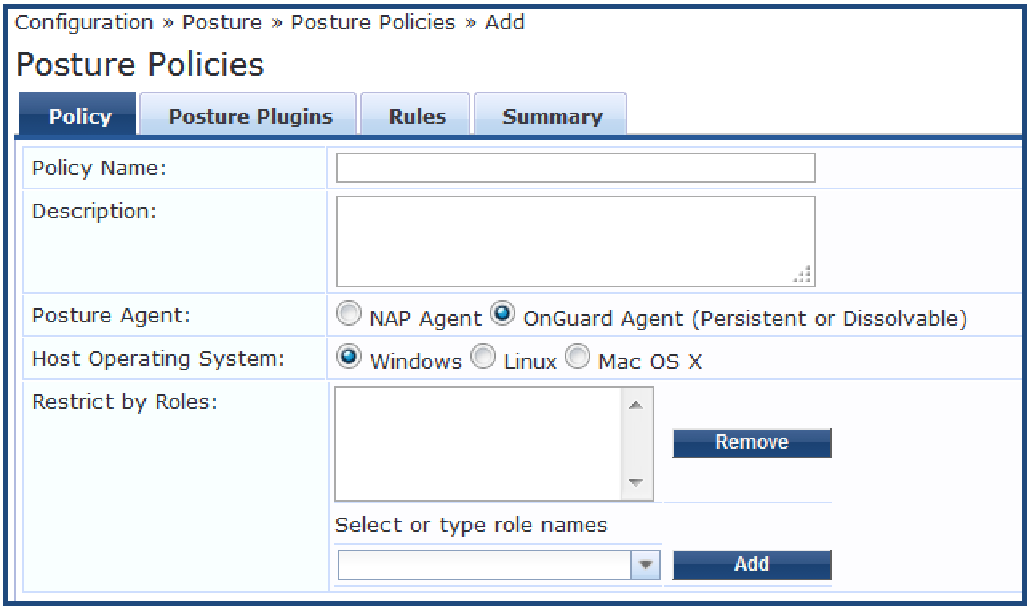
#	□	Name	Description
1.	□	CPATS Linux Posture - Unhealthy Client	
2.	□	CPATS MAC Posture - Unhealthy Client	
3.	□	CPATS Windows Posture - Unhealthy Client	

Showing 1-3 of 3

2. Click the **Add** link.

   The **Add Posture Policies** configuration dialog opens.

Figure 226: *Add Posture Policies Configuration Dialog*



Configuration » Posture » Posture Policies » Add

Posture Policies

Policy Name:	
Description:	
Posture Agent:	○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable)
Host Operating System:	● Windows ○ Linux ○ Mac OS X
Restrict by Roles:	Select or type role names

3. Configure the information in the **Add Posture Policies** page as described in Configuring Posture Policy Agents and Hosts on page 269.

   - For information on configuring the posture policy plug-ins, see Configuring Posture Policy Plug-ins on page 272.
   - For information on configuring posture policy rules, see Configuring Posture Policy Rules on page 335.

Configuring Posture Policy Agents and Hosts

This section provides the following information:

- Introduction
- NAP Agent Posture Plug-ins
- OnGuard Agent Posture Plug-ins

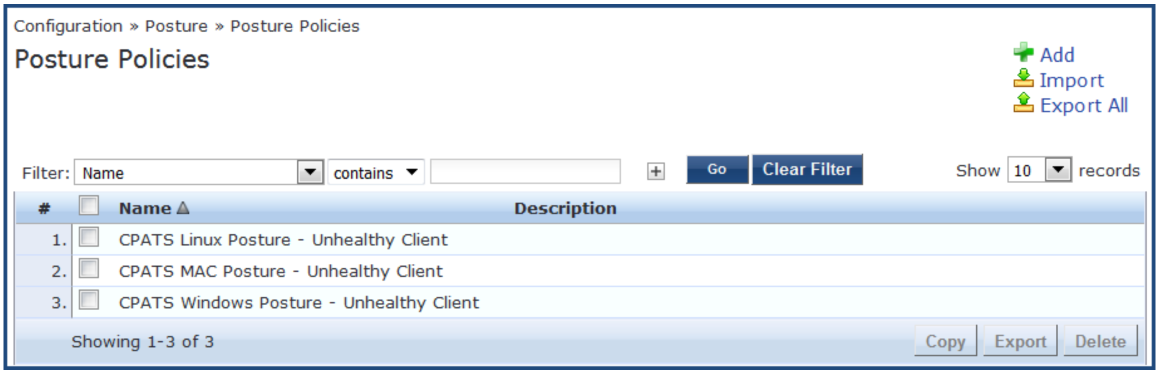
Introduction

To configure posture policy agents and hosts:

1. Navigate to **Configuration > Posture > Posture Policies.**

   The **Posture Policies** page displays a list of all existing posture policies.

Figure 227: *Posture Policies Page*



Configuration » Posture » Posture Policies

Posture Policies

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

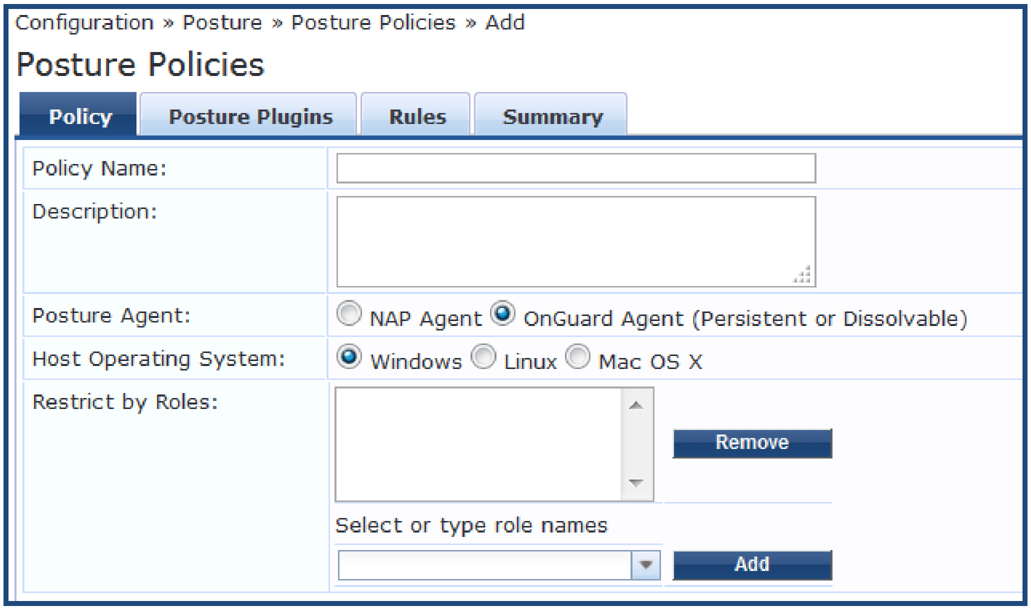
#	□	Name ▲	Description
1.	□	CPATS Linux Posture - Unhealthy Client	
2.	□	CPATS MAC Posture - Unhealthy Client	
3.	□	CPATS Windows Posture - Unhealthy Client	

Showing 1-3 of 3

2. Click the **Add** link.

   The **Add Posture Policies** page opens.

Figure 228: *Add Posture Policies Page*



Configuration » Posture » Posture Policies » Add

Posture Policies

Policy Name:

Description:

Posture Agent: ○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable)

Host Operating System: ● Windows ○ Linux ○ Mac OS X

Restrict by Roles:

Select or type role names

3. Use the **Posture Policies** > **Policy** dialog to configure the policy name and description, select a posture agent and host operating system, and specify role restrictions.

   Specify the **Add Posture Policy** parameters as described in the following table:

Table 127: *Add Posture Policy Parameters*

Parameter	Action/Description
Policy Name	1. Enter the name assigned to the policy by the ClearPass Policy Manager administrator.
Description	2. Specify the description that provides additional information about the posture policy.
Posture Agent	3. Select the posture agent type. For detailed information on these agents, see NAP Agent Posture Plug-ins on page 270 and OnGuard Agent Posture Plug-ins on page 270.
Host Operating System	4. Specify whether the host is using a Windows, Linux, or MAC OS X operating system.
Restrict by Roles	5. Apply the posture policy to the selected roles.

NAP Agent Posture Plug-ins

When you select **NAP Agent** as the Posture agent, you can configure the posture plug-ins as described in Table 128:

Table 128: *NAP Agent: Windows OS Posture Plug-ins Support*

Plug-in	Description	Windows Support
Windows System Health Validator	The Windows System Health Validator permits or denies client computers to connect to your network. The Windows System Health Validator also restricts client access to computers that have a service pack less than service pack *x*.	• Windows 10: Yes • Windows 8: Yes • Windows 7: Yes • Windows Vista: Yes • Windows XP Svc Pack 3: Yes • Windows Server 2008, 2008R2: Yes • Windows Server 2012, 2012R2: Yes
Windows Security Health Validator	The Windows Security Health Validator permits or denies 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. **NOTE:** If you configure the Windows Security Health Validator posture plug-in for Windows XP, spyware protection is disabled.	• Windows 10: Yes • Windows 8: Yes • Windows 7: Yes • Windows Vista: Yes • Windows XP Svc Pack 3: Yes • Windows Server 2008, 2008R2: No • Windows Server 2012, 2012R2: No

OnGuard Agent Posture Plug-ins

Select **OnGuard Agent (Persistent or Dissolvable)** as the **Posture Agent** 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 support for 802.1X natively, but does not have a built-in health agent. Macintosh OS X is an example of this type of environment.

When you select the **Posture Agent: OnGuard Agent (Persistent or Dissolvable)**, you can configure the posture plug-ins for:

- Windows (see Table 129)
- Macintosh OS X (see Table 130)
- Linux (see Table 131)

Table 129: *OnGuard Agent Validator Posture Plug-in Windows OS Support*

Plug-in	Description	Windows Support
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, Installed Applications, and File Check.	● Windows 10: Yes ● Windows 8: Yes ● Windows 7: Yes ● Windows Vista: Yes ● Windows 2003: Yes ● Windows XP Svc Pack 3: Yes ● Windows Server 2008, 2008R2: Yes **NOTE:** Configuration for Windows Server 2008 applies also to Windows Server 2008R2. ● Windows Server 2012, 2012R2: Yes **NOTE:** Configuration for Windows Server 2012 applies also to Windows Server 2012R2.
Windows System Health Validator	The Windows System Health Validator allows you to configure client computers that can connect to your 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 10: Yes ● Windows 8: Yes ● Windows 7: Yes ● Windows Vista: Yes ● Windows 2003: Yes ● Windows XP Svc Pack 3: Yes ● Windows Server 2008, 2008R2: Yes ● Windows Server 2012, 2012R2: Yes
Windows Security Health Validator	The configurable parameter categories for this validator allow you to configure parameters that permit or deny client computers access to your network, subject to checks of the client's system for Firewall, Virus Protection, Spyware Protection, Automatic Updates, and Security Updates. **NOTE:** If you configure the posture plug-in for Windows XP, spyware protection is disabled.	● Windows 10: Yes ● Windows 8: Yes ● Windows 7: Yes ● Windows Vista: Yes ● Windows 2003: No ● Windows XP Svc Pack 3: Yes ● Windows Server 2008, 2008R2: No ● Windows Server 2012, 2012R2: No

Table 130: *OnGuard Agent (Persistent or Dissolvable) Posture Plug-ins for Mac OS X*

Plug-in	Description
ClearPass Macintosh 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 ■ File Check

Table 131: *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

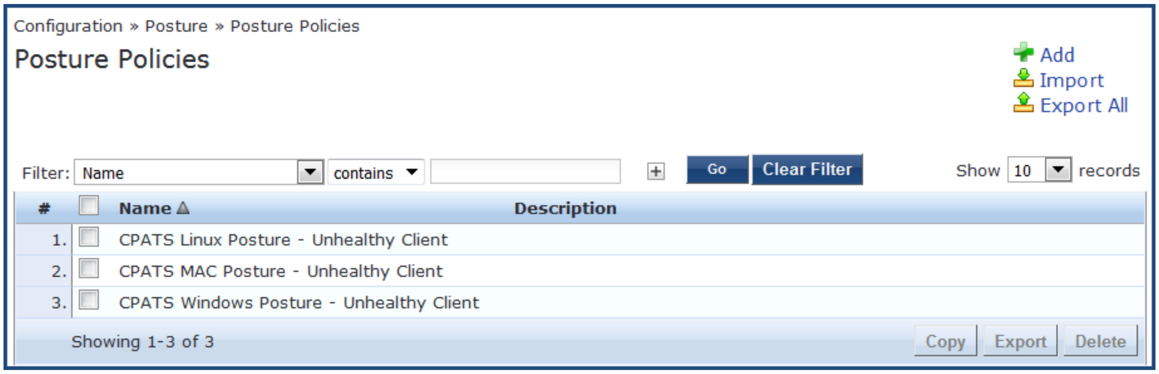
The **Posture Plugins** dialog of the **Posture Policies** page allows you to configure plug-ins for the posture policy. The plug-ins available on this tab vary, depending upon whether the policy is using a Network Access Protection (NAP) agent or the OnGuard Agent (Persistent or Dissolvable) plug-in.

To configure posture policy plug-ins:

1. Navigate to **Configuration > Posture > Posture Policies**.

   The **Posture Policies** page appears.

Figure 229: *Posture Policies Page*



Configuration » Posture » Posture Policies

Posture Policies

Filter: Name contains

Show 10 records

#	□	Name	Description
1.	□	CPATS Linux Posture - Unhealthy Client	
2.	□	CPATS MAC Posture - Unhealthy Client	
3.	□	CPATS Windows Posture - Unhealthy Client	

Showing 1-3 of 3

2. Click **Add**.

   The **Add Posture Policies** page appears.

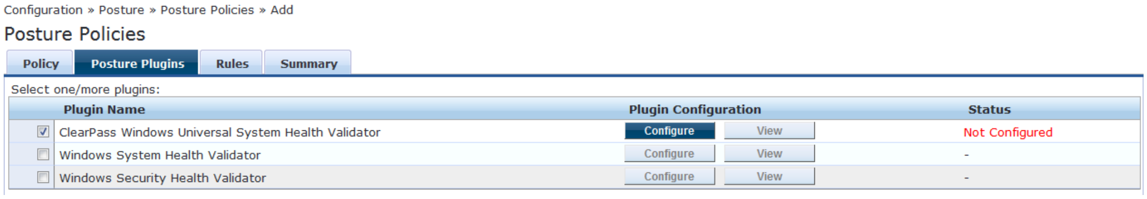
3. In the **Policy** tab, specify the following:

- Policy Name
- Description
- Posture Agent
- Host Operating System

4. Select the **Posture Plugins** tab .

   The **Add Posture Plugins** page appears.

Figure 230: *Add Posture Plugins Page*



Configuration » Posture » Posture Policies » Add

Posture Policies

Select one/more plugins:

	Plugin Name	Plugin Configuration		Status
☑	ClearPass Windows Universal System Health Validator	Configure	View	Not Configured
□	Windows System Health Validator	Configure	View	-
□	Windows Security Health Validator	Configure	View	-

You can configure the following posture plug-ins in the **Posture Policies** page:

- ClearPass Windows Universal System Health Validator > OnGuard Agent on page 273
- Windows System Health Validator: NAP Agent on page 332
- Windows System Health Validator: OnGuard Agent on page 311
- Windows Security Health Validator: NAP Agent on page 333

5. Select the check box of the plug-in you wish to configure.
6. To view the configuration page for the selected plug-in, click **Configure**.

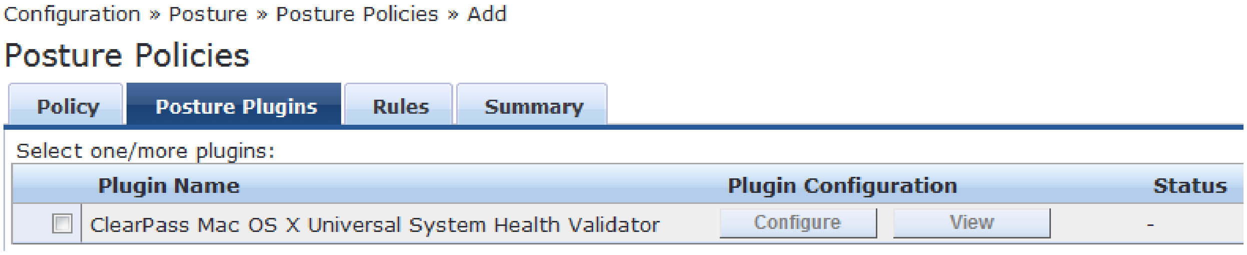
Configuring OnGuard Agent Plugins

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 273
  - Windows System Health Validator: OnGuard Agent on page 311
  - Windows Security Health Validator: OnGuard Agent on page 312
- For Linux: ClearPass Linux Universal System Health Validator Plugin on page 313
- For Mac OS X: ClearPass Macintosh OS X Universal System Health Validator: OnGuard Agent on page 316

The following figure displays the **Posture Policies - Posture Plugins** tab:

Figure 231: *OnGuard Agent Plugin Options for Mac OS X*



Configuration » Posture » Posture Policies » Add

Posture Policies

Select one/more plugins:

	Plugin Name	Plugin Configuration		Status
□	ClearPass Mac OS X Universal System Health Validator	Configure	View	-

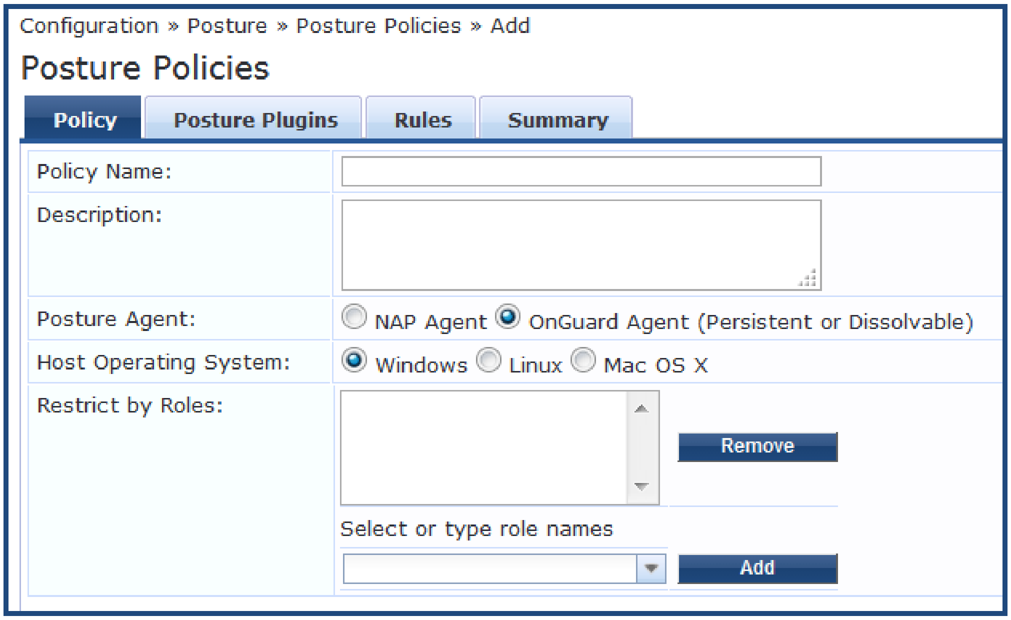
ClearPass Windows Universal System Health Validator > OnGuard Agent

To configure the ClearPass Windows Universal Health System Health Validator (OnGuard Agent):

1. Navigate to **Configuration** > **Posture** > **Posture Policies**, then click **Add**.

The **Add Posture Policies** dialog opens.

Figure 232: *Adding a Posture Policy*



Configuration » Posture » Posture Policies » Add

Posture Policies

Policy | Posture Plugins | Rules | Summary

Policy Name:	
Description:	
Posture Agent:	○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable)
Host Operating System:	● Windows ○ Linux ○ Mac OS X
Restrict by Roles:	Remove Select or type role names Add

a. Enter the name and a description of the posture policy.

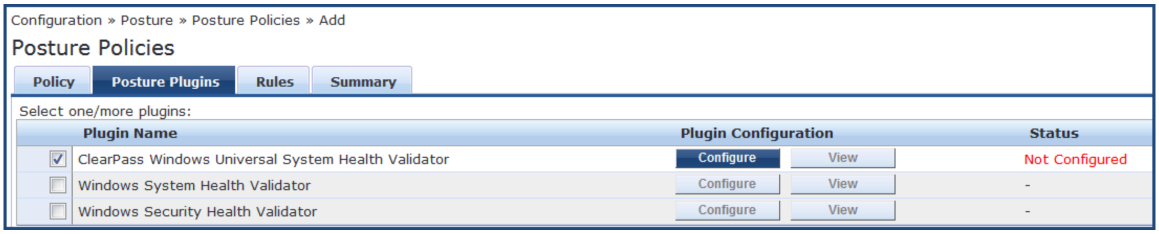
b. **Posture Agent**: Choose **OnGuard Agent (Persistent or Dissolvable)**.

c. **Host Operating System: Windows** is selected by default.

d. Click **Next**.

The **Posture Plugins** dialog opens.

Figure 233: *Selecting the Windows Posture Plugin*



Configuration » Posture » Posture Policies » Add

Posture Policies

Policy | Posture Plugins | Rules | Summary

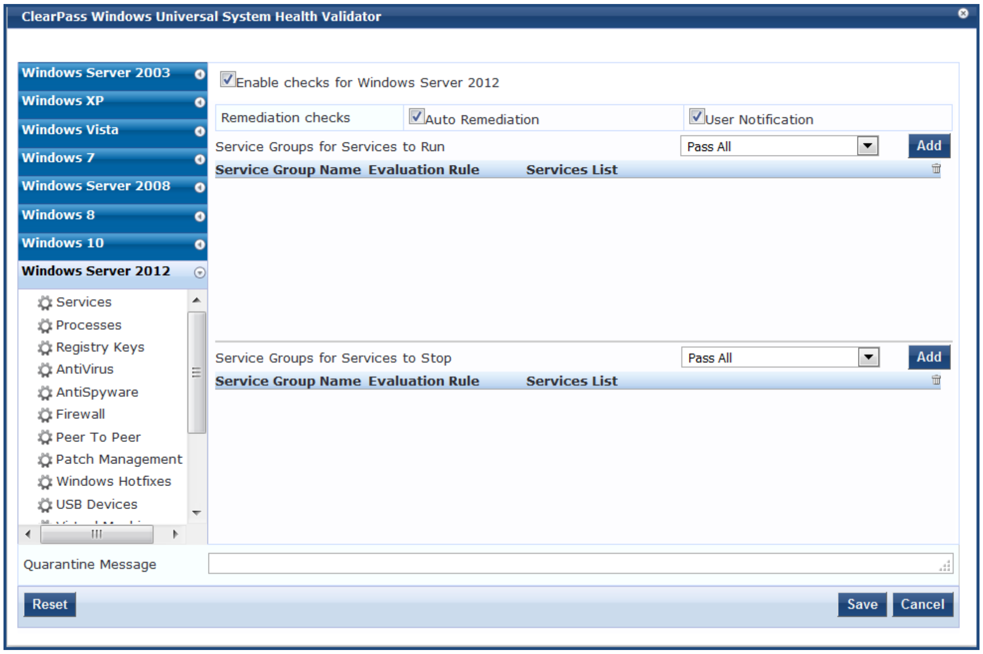
Select one/more plugins:

	Plugin Name	Plugin Configuration		Status
☑	ClearPass Windows Universal System Health Validator	Configure	View	Not Configured
□	Windows System Health Validator	Configure	View	-
□	Windows Security Health Validator	Configure	View	-

2. In the **Posture Plugins** page, click the check box for **ClearPass Windows Universal System Health Validator**.
3. Click **Configure**.

   The **ClearPass Windows Universal System Health Validator** page opens.
4. Select the desired version of Windows.
5. To enable checks for the selected version, click the **Enable checks for Windows Server** check box.

Figure 234: *ClearPass Windows Universal System Health Validator Page*



☑ Enable checks for Windows Server 2012

Remediation checks ☑ Auto Remediation ☑ User Notification

Service Groups for Services to Run: Pass All

Service Group Name	Evaluation Rule	Services List

Service Groups for Services to Stop: Pass All

Service Group Name	Evaluation Rule	Services List

Quarantine Message

The following list of configuration pages for the selected version of Windows appears (see Figure 234):

- Services on page 275
- Processes on page 280
- Registry Keys on page 283
- AntiVirus on page 286
- AntiSpyware on page 287
- Firewall on page 289
- Peer To Peer on page 290
- Patch Management on page 291
- Windows Hotfixes on page 295
- USB Devices on page 300
- Virtual Machines on page 300
- Network Connections on page 301
- Disk Encryption on page 303
- Installed Applications on page 304
- File Check on page 307

6. When finished, click **Save**.

Services

The **Service** feature allows network admins to determine how the overall health status of the Services health class is determined—whether by using an AND condition (for example, *Group1 AND Group2*) or an OR condition (for example, *Group1 OR Group2*).

Regarding services, for example, admins can run checks such as *Service1 AND Service2 OR Service3 AND Service4*. You can also use the **Services** page to verify the group of services to be present or absent and specify the service groups and services to run on a client.

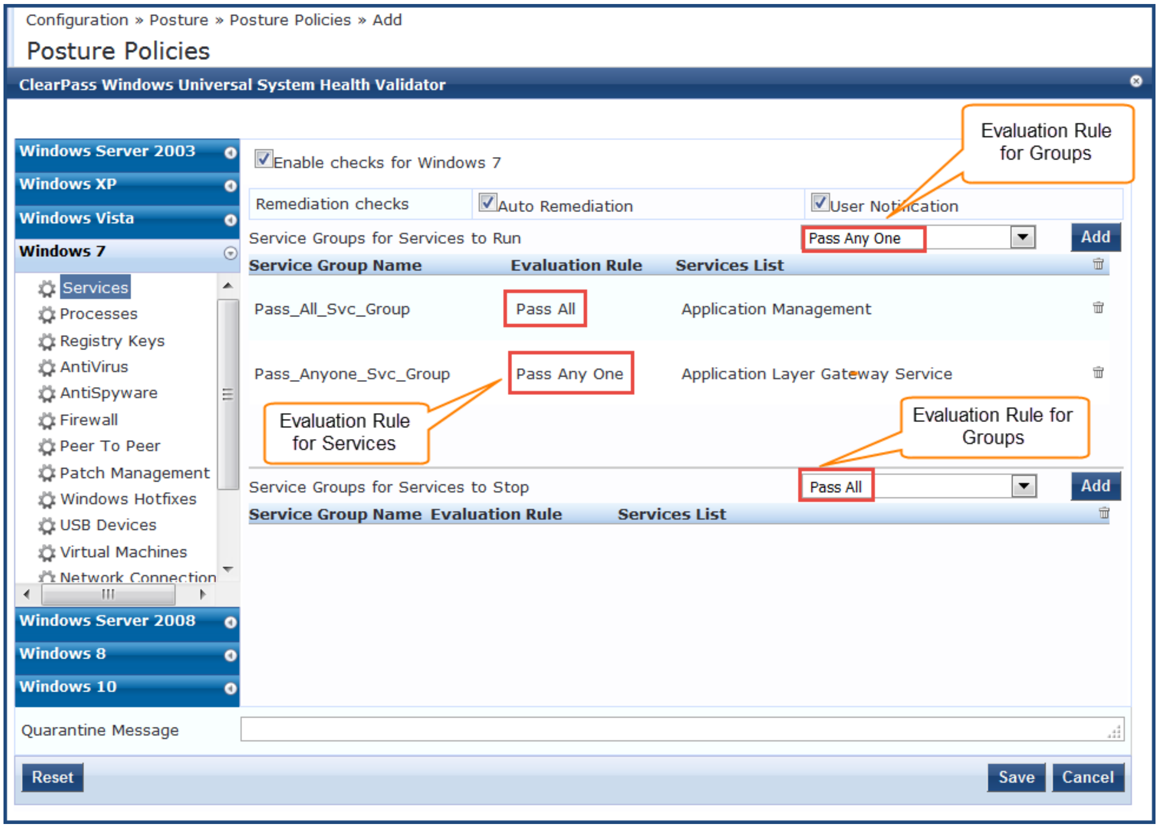
To define Windows Service Groups, specify the evaluation rules, and add or remove specific Windows services on the endpoint:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**, then click **Add**.
2. From the **Add Posture Policies** page, select the **Posture Plugins** tab.
3. Select the **ClearPass Windows Universal System Health Validator**, then click **Configure**.
4. Select the Windows operating system, then check the **Enable checks for *Windows_OS***.
5. Select **Services**.

   The **Services** health class configuration page opens:

   Figure 235 displays an example of the **ClearPass Widows Universal System Health Validator** > **Services** configuration page and highlights examples of the evaluation rule for groups and the evaluation rule for services:

Figure 235: *Specifying Service Groups to Run*



☑ Enable checks for Windows 7

Remediation checks ☑ Auto Remediation ☑ User Notification

Service Groups for Services to Run: Pass Any One

Service Group Name	Evaluation Rule	Services List
Pass_All_Svc_Group	Pass All	Application Management
Pass_Anyone_Svc_Group	Pass Any One	Application Layer Gateway Service

Service Groups for Services to Stop: Pass All

Service Group Name	Evaluation Rule	Services List

Quarantine Message

Evaluation Rule for Groups

Evaluation Rule for Services

Evaluation Rule for Groups

6. Specify the **ClearPass Widows Universal System Health Validator** > **Services** configuration parameters as described in the following table:

Table 132: *Services Configuration Parameters*

Parameter	Action/Description
Auto Remediation	Enable to allow auto-remediation for service checks. Enabling this option automatically stops or starts services based on the entries in **Service to Run** and **Services to Stop** configuration. Auto-remediation for the **Services** health class is enabled by default.
User Notification	When enabled, a remediation message that includes the groups of services to be present or absent is displayed to the end user.

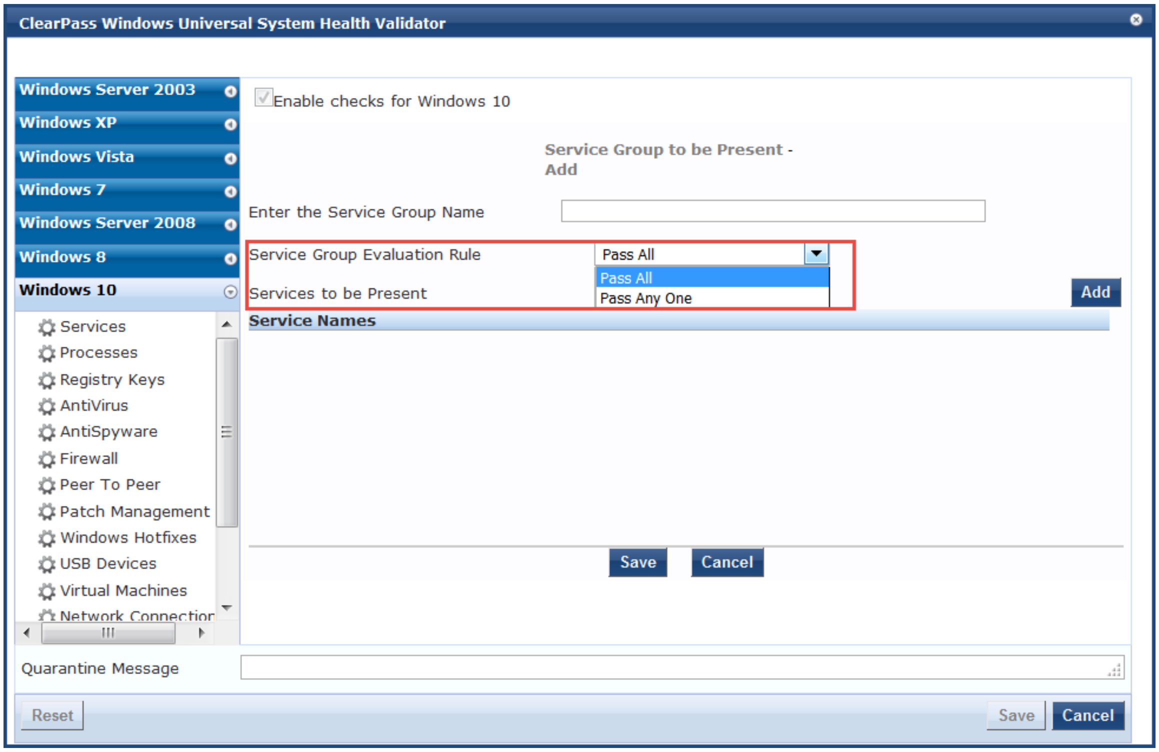
Defining the Service Group to Be Present

You can configure the name of the service group and specify the evaluation rule for the service group.

1. To configure the **Service Groups for Services to Run**, click **Add.**

   The **Add Service Group to Be Present** dialog opens.

Figure 236: *Specifying the Service Group Evaluation Rule*



☑ Enable checks for Windows 10

Enter the Service Group Name

Service Group Evaluation Rule: Pass All

Services to be Present

2. Specify the **Add Service Group to Be Present** parameters as described in the following table:

Table 133: *Add Service Group to Be Present Parameters*

Parameter	Action/Description
Enter the Service Group Name	1. Enter the name of the Service Group.
Service Group Evaluation Rule	2. Select the appropriate Service Group Evaluation Rule: • **Pass All**: Select this evaluation rule if you want the **Services** health class to be deemed as *healthy* only if all the configured service groups are present. **Pass All** is the equivalent of an **AND** condition. • **Pass Any One**: Select this evaluation rule if you want the **Services Check** health class to be deemed as *healthy* even if any one of the configured service groups are present. **Pass Any One** is the equivalent of an **OR** condition.

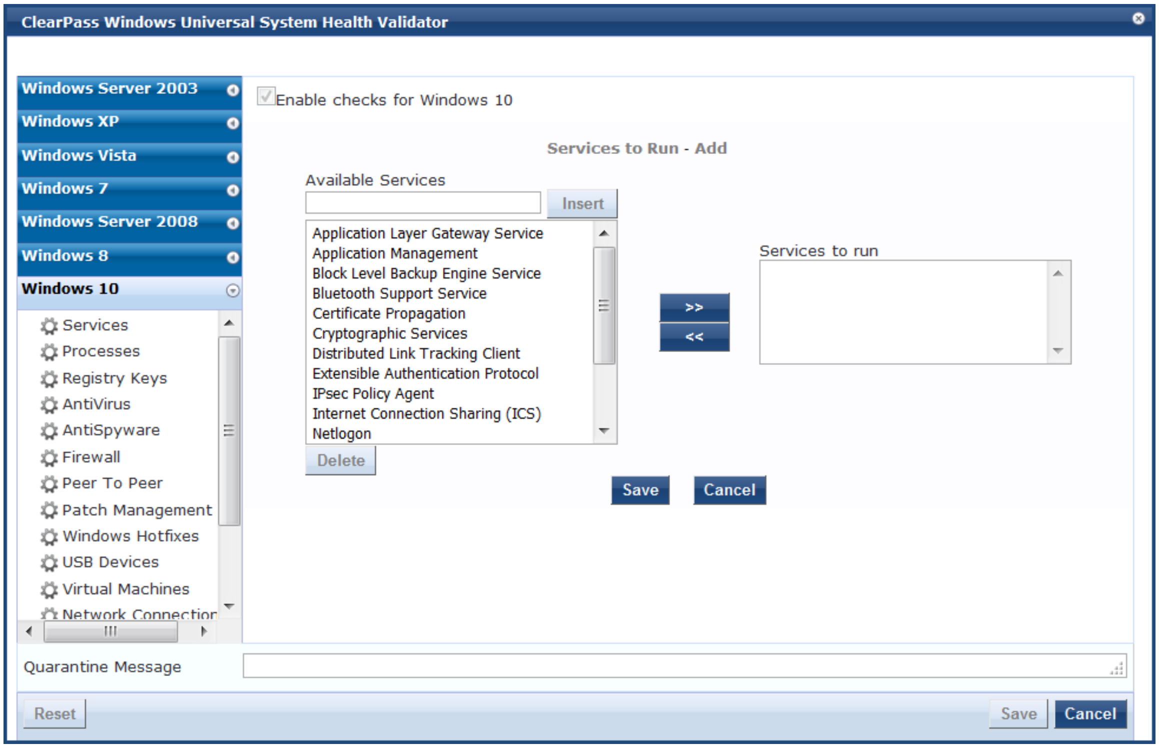
Specifying the Services to Be Present

To specify the services to be present:

1. Click the **Services to Be Present** > **Add** button.

   The **Add Services to Run** dialog opens.

Figure 237: *Specifying the Services to Run*



ClearPass Windows Universal System Health Validator

☑ Enable checks for Windows 10

Services to Run - Add

Available Services

Application Layer Gateway Service
Application Management
Block Level Backup Engine Service
Bluetooth Support Service
Certificate Propagation
Cryptographic Services
Distributed Link Tracking Client
Extensible Authentication Protocol
IPsec Policy Agent
Internet Connection Sharing (ICS)
Netlogon

Services to run

Quarantine Message

2. Select one or more of the desired services from the **Available Services** list.
3. To move the desired services to the **Services to Run** box,click **>>**, then click **Save**.
4. You can also add a service to the list of available services. To do so, enter the service name in the Insert text box, then click **Insert**.

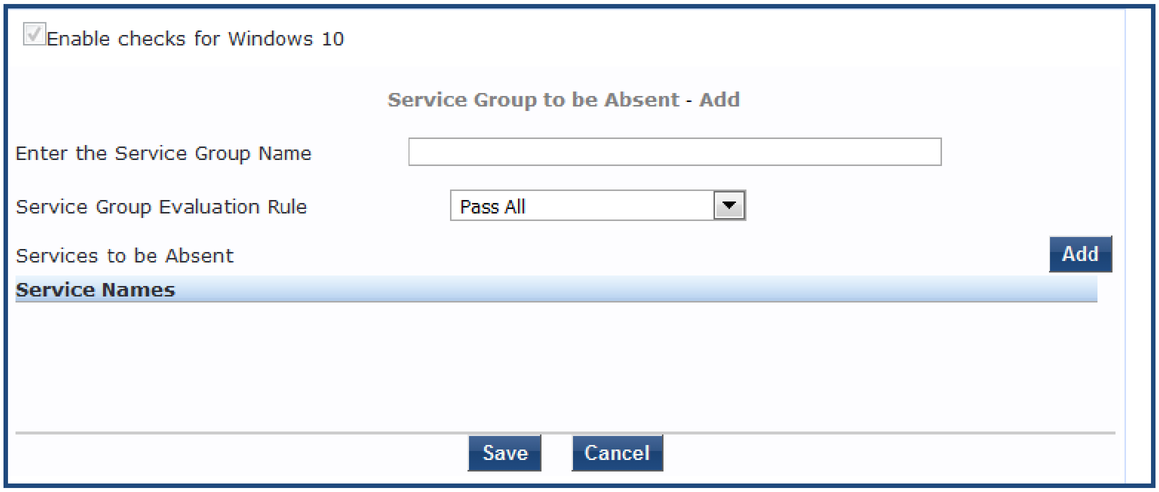
Defining the Service Group to Be Absent

You can configure the name of the service group and specify the evaluation rule for the service group.

1. To configure the **Service Groups for Services to Be Absent**, click **Add.**

   The **Add Service Group to Be Absent** dialog opens.

Figure 238: *Add Services to Be Absent Dialog*



☑ Enable checks for Windows 10

Service Group to be Absent - Add

Enter the Service Group Name

Service Group Evaluation Rule: Pass All

Services to be Absent

Service Names

2. Specify the Service Groups to Be Absent parameters as described in the following table:

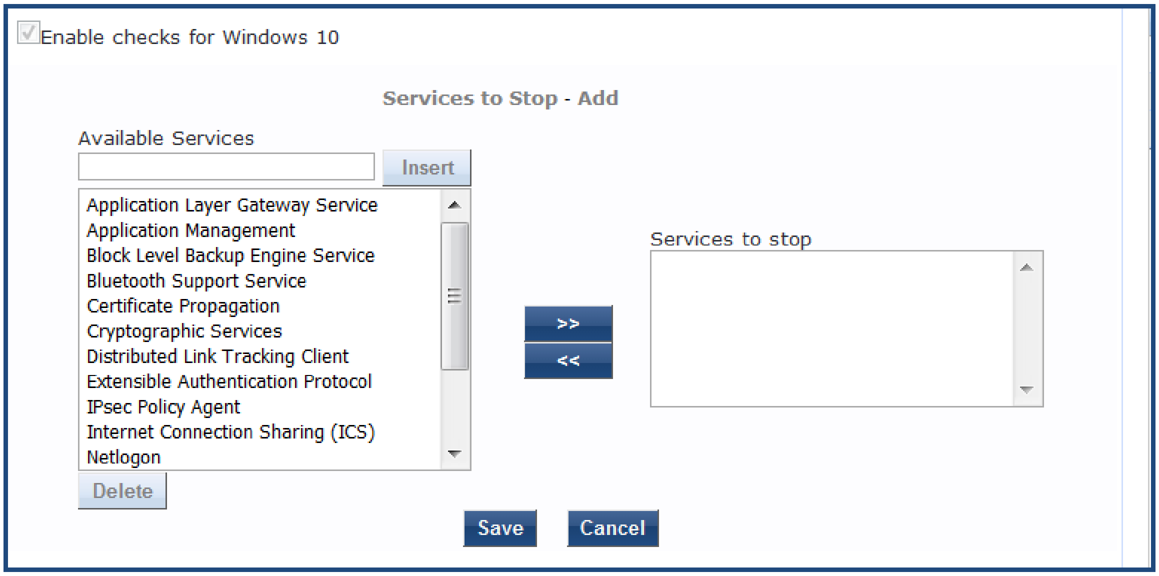
Table 134: *Add Service Group to Be Absent Parameters*

Parameter	Action/Description
Enter the Service Group Name	1. Enter the name of the Service Group.
Service Group Evaluation Rule	2. Select the appropriate Service Group Evaluation Rule: ● **Pass All**: Select this evaluation rule if you want all service groups to be stopped. **Pass All** is the equivalent of an **AND** condition. ● **Pass Any One**: Select this evaluation rule if you want any one of the service groups to be stopped. **Pass Any One** is the equivalent of an **OR** condition.

3. Click **Add**.

   The **Add Services to Stop** dialog opens.

Figure 239: *Specifying the Services to Stop*



☑ Enable checks for Windows 10

Services to Stop - Add

Available Services

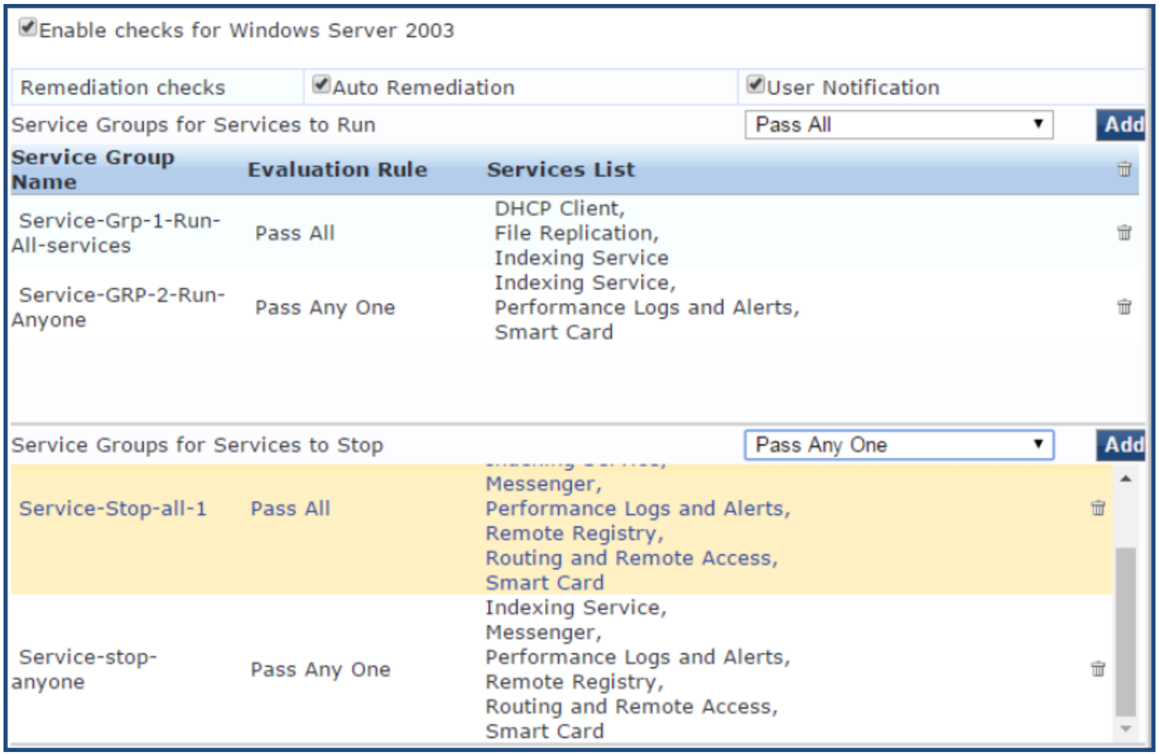
Application Layer Gateway Service
Application Management
Block Level Backup Engine Service
Bluetooth Support Service
Certificate Propagation
Cryptographic Services
Distributed Link Tracking Client
Extensible Authentication Protocol
IPsec Policy Agent
Internet Connection Sharing (ICS)
Netlogon

Services to stop

4. Select one or more of the desired services from the **Available Services** list.
5. To move the desired services to the **Services to Stop** box, select the desired services, then click **>>**.
   a. To remove services from the **Services to Stop box**, select the services to be removed, then click **<<**.
6. When finished configuring the services to stop, click **Save**.

   Figure 240 shows an example of services configured for Windows Server 2003.

Figure 240: *Example of Services Configured*



☑ Enable checks for Windows Server 2003

Remediation checks ☑ Auto Remediation ☑ User Notification

Service Groups for Services to Run: Pass All ▾ Add

Service Group Name	Evaluation Rule	Services List
Service-Grp-1-Run-All-services	Pass All	DHCP Client, File Replication, Indexing Service
Service-GRP-2-Run-Anyone	Pass Any One	Indexing Service, Performance Logs and Alerts, Smart Card

Service Groups for Services to Stop: Pass Any One ▾ Add

Service-Stop-all-1	Pass All	Messenger, Performance Logs and Alerts, Remote Registry, Routing and Remote Access, Smart Card
Service-stop-anyone	Pass Any One	Indexing Service, Messenger, Performance Logs and Alerts, Remote Registry, Routing and Remote Access, Smart Card

Processes

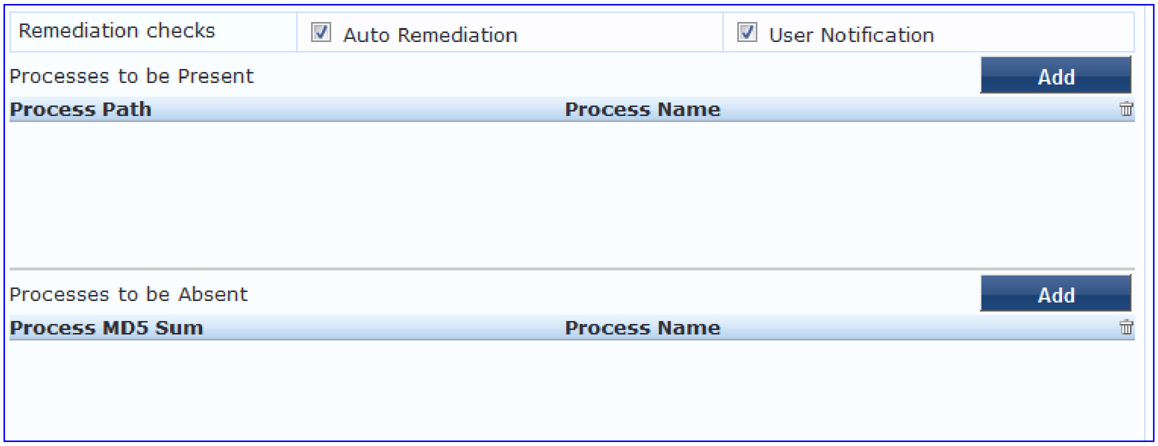
The **Processes** page provides a set of parameters to specify which processes to be explicitly present or absent on the system.

To configure Processes:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**, then click **Add**.
2. From the **Add Posture Policies** page, select the **Posture Plugins** tab.
3. Select the **ClearPass Windows Universal System Health Validator**, then click **Configure**.
4. Select the Windows operating system, then check the **Enable checks for *Windows_OS***.
5. Select **Processes**.

   The **Processes** health class configuration page opens:

Figure 241: *Processes Configuration Page*



Remediation checks ☑ Auto Remediation ☑ User Notification

Processes to be Present Add

Process Path	Process Name

Processes to be Absent Add

Process MD5 Sum	Process Name

6. Specify the **Processes** configuration parameters as described in the following table:

Table 135: *Processes Page Parameters*

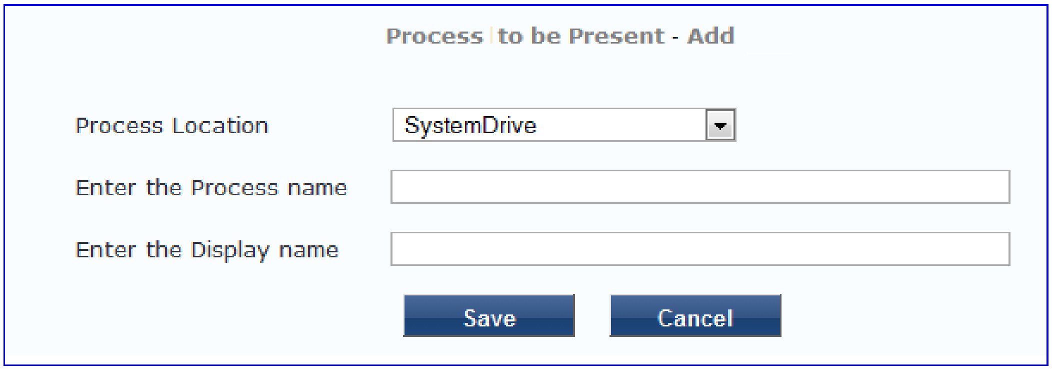
Parameter	Action/Description
Auto Remediation	1. Enable to allow auto-remediation for processes.
User Notification	2. Enable to allow user notifications in the event of process policy violations.

Processes to be Present Parameters

1. In the **Processes to be Present** section, click **Add.**

   The **Add Processes to be Present** page opens.

Figure 242: *Add Processes to be Present Page*



Process to be Present - Add

Process Location: SystemDrive

Enter the Process name:

Enter the Display name:

2. Specify the Processes to be Present parameters as described in the following table, then click **Save**:

Table 136: *Processes to be Present Page Parameters*

Parameter	Action/Description
Process Location	1. Choose from the following locations: ■ System Drive ■ Systemroot ■ Program Files ■ HOMEDRIVE ■ HOMEPATH ■ None
Enter the Process name	2. Specify the path name containing the process executable name.
Enter the Display name	3. Enter a user-friendly name for the process. This is displayed in end-user facing messages.

After you save the Processes parameters, the information appears in the **Processes to be Present** section.

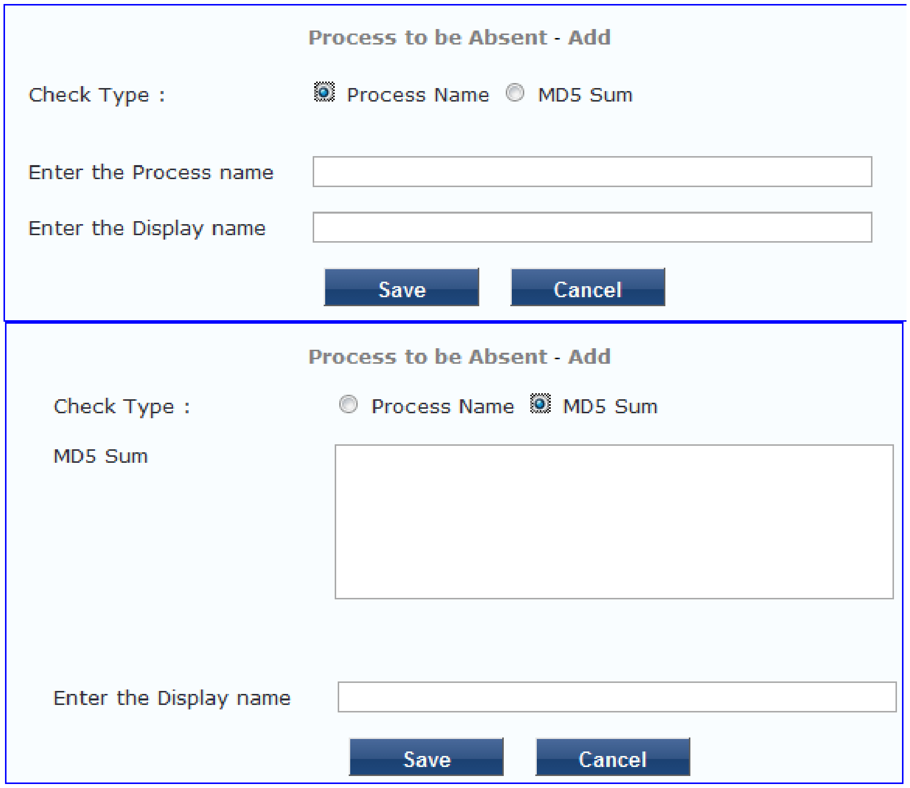
Processes to be Absent Parameters

1. In the **Processes to be Absent** section, click **Add.**

   The **Add Processes to be Absent** page opens.

Figure 243 shows the configuration parameters for when you select **Process Name** and when you select **MD5 Sum**.

Figure 243: *Process to be Absent Pages: Process Name and MD5 Sum*



Process to be Absent - Add

Check Type : ● Process Name ○ MD5 Sum

Enter the Process name

Enter the Display name

Process to be Absent - Add

Check Type : ○ Process Name ● MD5 Sum

MD5 Sum

Enter the Display name

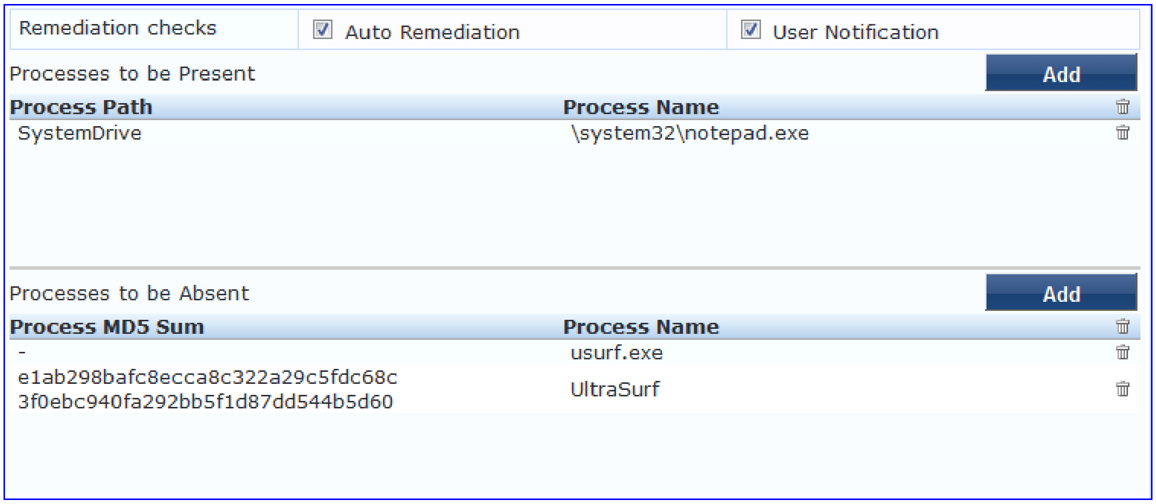
2. Specify the **Processes to be Absent** parameters as described in the following table, then click **Save**:

Table 137: *Processes to be Absent Page Parameters*

Parameter	Action/Description
Check Type	1. Select the type of process check to perform. The agent can look for the following: ▪ **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	2. Enter a user-friendly name for the process. This display name is displayed in end-user facing messages.

You return to the **Processes Configuration** page, which now shows the values for the processes that were configured:

Figure 244: *Processes Configured*



Remediation checks	☑ Auto Remediation	☑ User Notification

Processes to be Present

Process Path	Process Name
SystemDrive	\system32\notepad.exe

Processes to be Absent

Process MD5 Sum	Process Name
-	usurf.exe
e1ab298bafc8ecca8c322a29c5fdc68c 3f0ebc940fa292bb5f1d87dd544b5d60	UltraSurf

Registry Keys

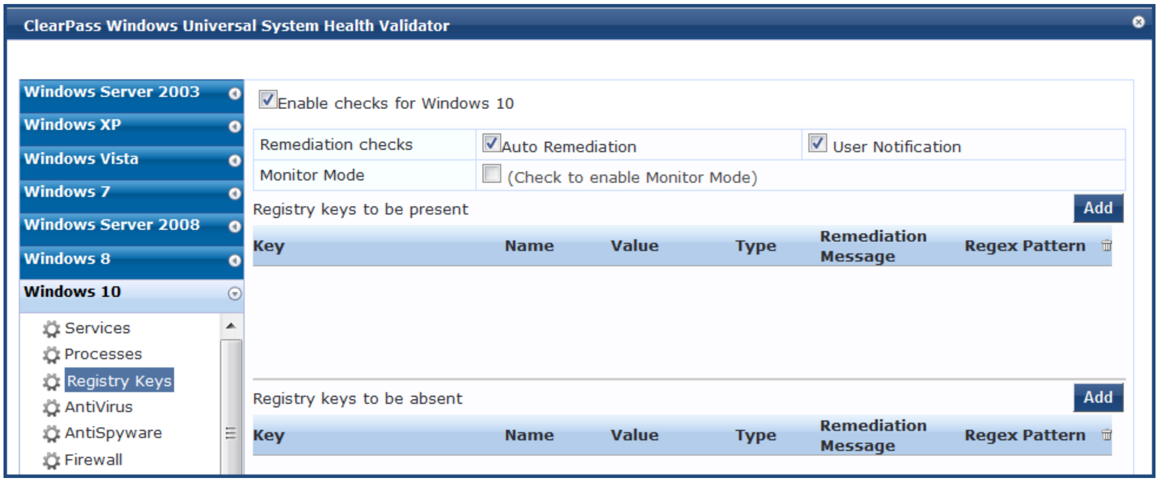
The **Registry Keys** page allows you to specify which registry keys are to be explicitly present or absent.

To define the registry keys:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**, then click **Add**.
2. From the **Add Posture Policies** page, select the **Posture Plugins** tab.
3. Select the **ClearPass Windows Universal System Health Validator**, then click **Configure**.
4. Select the Windows operating system, then check the **Enable checks for *Windows_OS***.
5. Select **Registry Keys**.

   The **Registry Keys** health class configuration page opens:

Figure 245: *Registry Keys Page (Overview)*



☑ Enable checks for Windows 10

Remediation checks	☑ Auto Remediation	☑ User Notification
Monitor Mode	☐ (Check to enable Monitor Mode)	

Registry keys to be present

Key	Name	Value	Type	Remediation Message	Regex Pattern

Registry keys to be absent

Key	Name	Value	Type	Remediation Message	Regex Pattern

6. Specify the **Registry Keys** page parameters as described in the following table:

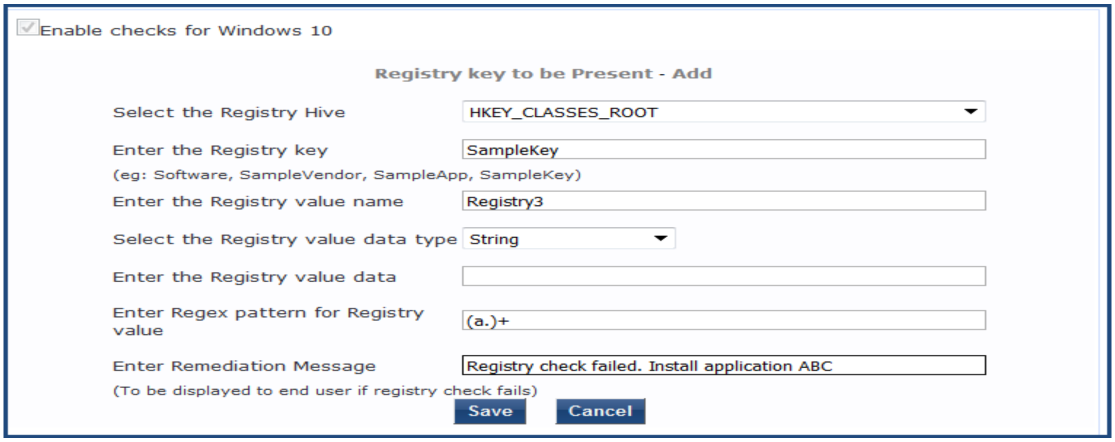
Table 138: *Registry Keys Page Parameters*

Parameter	Action/Description
Auto Remediation	1. 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	2. Enable user notifications for registry check policy violations.
Monitor Mode	3. 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	4. To specify a registry key to be added to the **Registry keys to be present** list, click **Add**. 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	5. To add a registry key to the **Registry keys to be absent** list, click **Add**. 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**.

6. To configure the **Registry key to be present**, click **Add**.

   The **Edit Registry Key to be Present** dialog opens.

Figure 246: *Edit Registry Keys to be Present Parameters*



☑ Enable checks for Windows 10

Registry key to be Present - Add

Select the Registry Hive	HKEY_CLASSES_ROOT
Enter the Registry key (eg: Software, SampleVendor, SampleApp, SampleKey)	SampleKey
Enter the Registry value name	Registry3
Select the Registry value data type	String
Enter the Registry value data	
Enter Regex pattern for Registry value	(a.)+
Enter Remediation Message (To be displayed to end user if registry check fails)	Registry check failed. Install application ABC

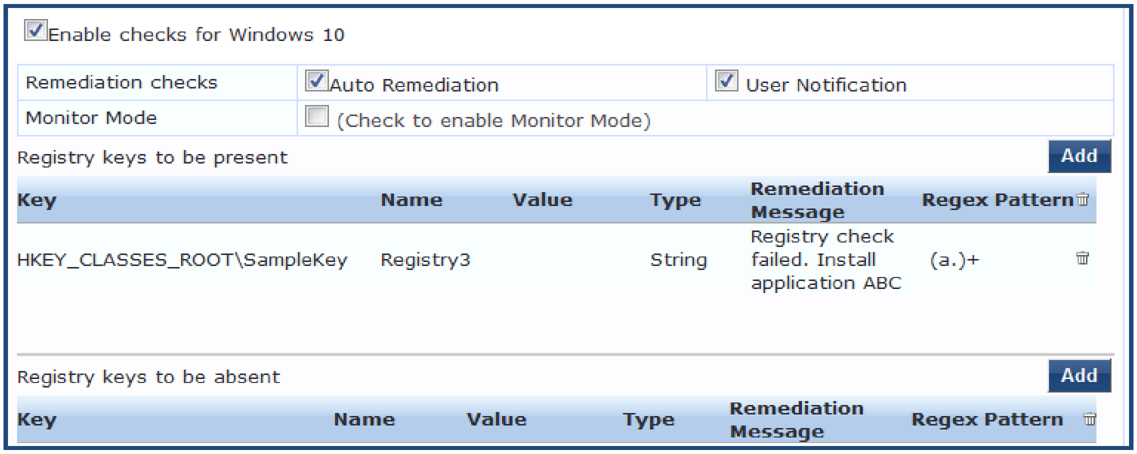
7. Specify the **Registry Key to be Present** parameters as described in Table 139, then click **Save**.

Table 139: *Registry Keys Page (Detail)*

Parameter	Action/Description
Select the Registry Hive	1. 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	2. Specify the registry key using the examples given in the GUI.
Enter the Registry value name	3. Specify the name of the registry value.
Select the Registry value data type	4. 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	5. Specify the registry value.
Enter Regex pattern for Registry value	6. Enter the Regular Expression (Regex) pattern for the Registry value. A regular expression is a pattern that the regular expression engine attempts to match in input text. A pattern consists of one or more character literals, operators, or constructs. **NOTE:** Perl regular expressions are supported.
Enter Remediation Message	7. Specify the custom remediation message to be displayed to end users if the registry check fails.

As shown in Figure 247, after you save the registry configuration settings, the remediation message and Regular Expression pattern appears in the **Registry** page.

Figure 247: *Registry Keys Added*



☑ Enable checks for Windows 10

Remediation checks	☑ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

Registry keys to be present

Key	Name	Value	Type	Remediation Message	Regex Pattern	🗑
HKEY_CLASSES_ROOT\SampleKey	Registry3		String	Registry check failed. Install application ABC	(a.)+	🗑

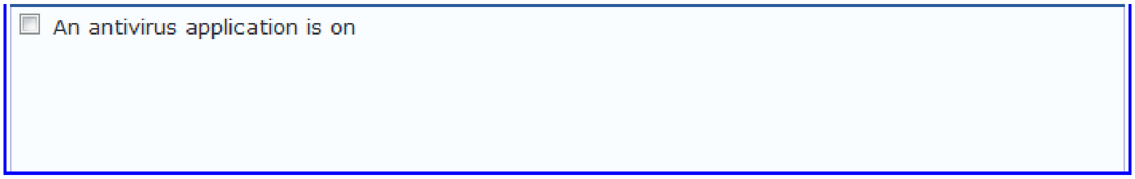
Registry keys to be absent

Key	Name	Value	Type	Remediation Message	Regex Pattern	🗑

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.

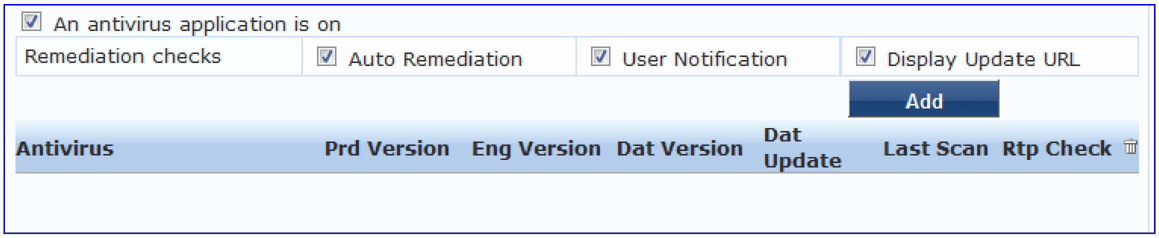
Figure 248: *Antivirus Page (Overview - Before)*



☐ An antivirus application is on

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

Figure 249: *Antivirus Page (Detail 1)*



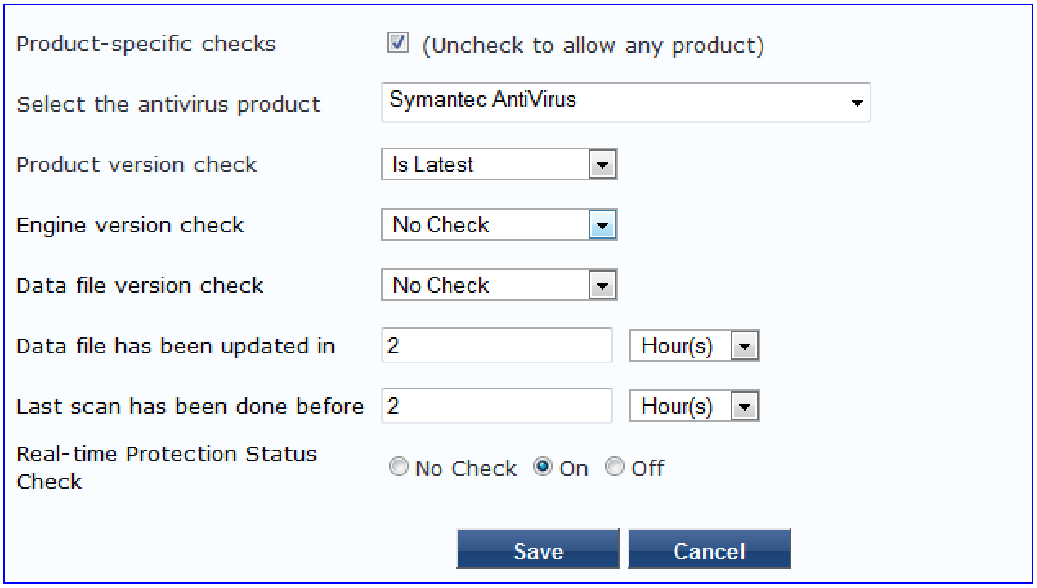
☑ An antivirus application is on

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

Antivirus	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	🗑

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

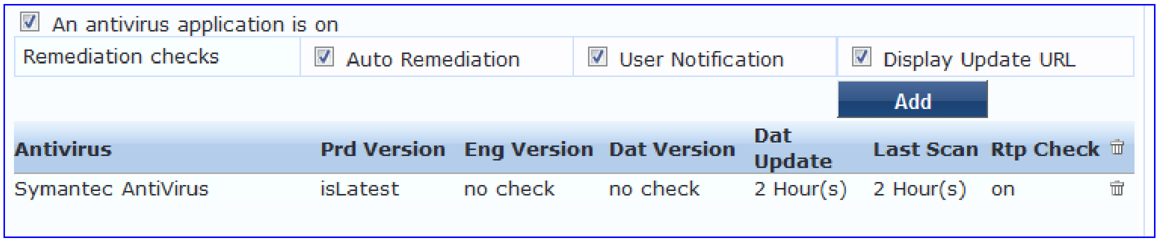
Figure 250: *Antivirus Page (Detail 2)*



Product-specific checks	☑ (Uncheck to allow any product)
Select the antivirus product	Symantec AntiVirus
Product version check	Is Latest
Engine version check	No Check
Data file version check	No Check
Data file has been updated in	2 Hour(s)
Last scan has been done before	2 Hour(s)
Real-time Protection Status Check	○ No Check ● On ○ Off

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

Figure 251: *Antivirus Page (Overview - After)*



☑ An antivirus application is on

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

Antivirus	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	🗑
Symantec AntiVirus	isLatest	no check	no check	2 Hour(s)	2 Hour(s)	on	🗑

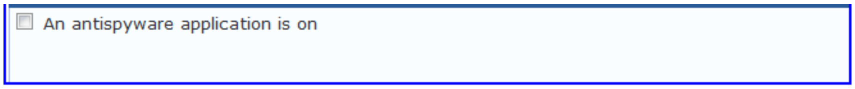
Table 140: *Antivirus Page*

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 - Engine version check - Datafile version check - Data file has been updated in - Last scan has been done before - Real-time Protection Status Check	Configure the specific settings for which to test against health data. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state on the UI. - Select the antivirus product - Select a vendor from the list. - Product version check - No Check, Is Latest (requires registration with ClearPass portal), At Least, In Last N Updates (requires registration with ClearPass Portal). - Engine version check - Same choices as product version check. - Data file version check - Same choices as product version check. - Data file has been updated in - Specify the interval in hours, days, weeks, or months. - Last scan has been done before - Specify the interval in hours, days, weeks, or months. - Real-time Protection Status Check ▪ No Check - 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.

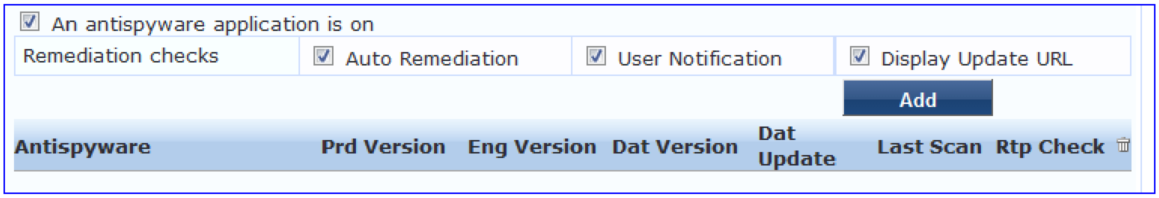
Figure 252: *AntiSpyware Page (Overview Before)*



☐ An antispyware application is on

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

Figure 253: *AntiSpyware Page (Detail 1)*



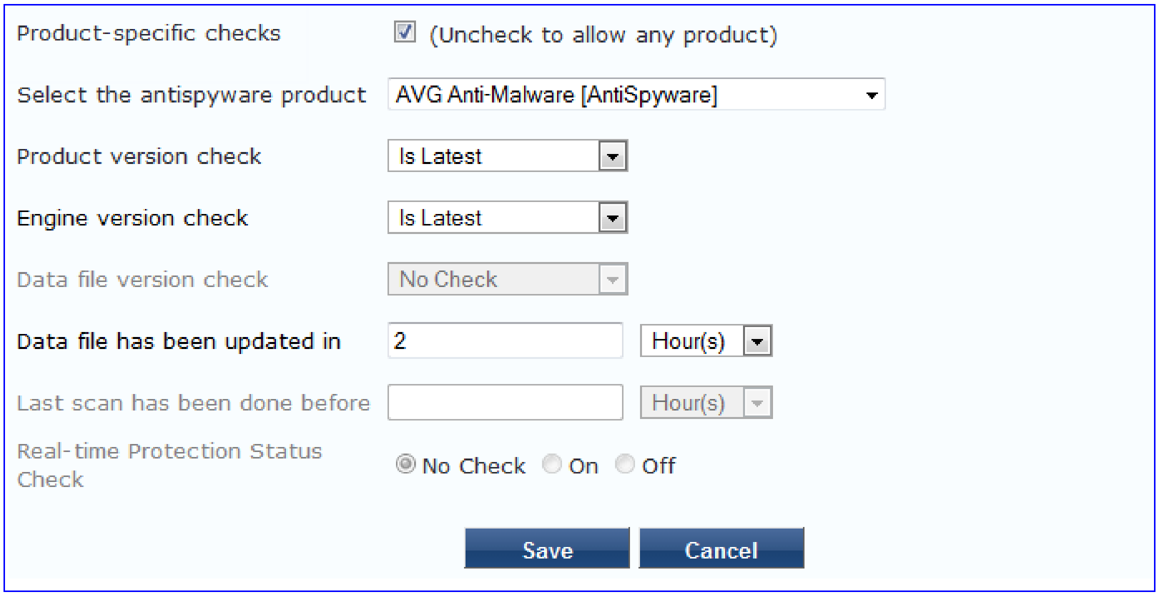
☑ An antispyware application is on

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

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	🗑

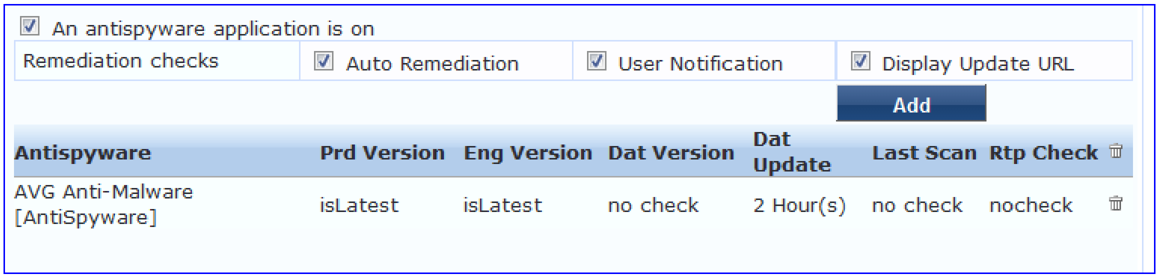
Click **Add** to specify product, and version check information.

Figure 254: *AntiSpyware Page (Detail 2)*



Product-specific checks	☑ (Uncheck to allow any product)
Select the antispyware product	AVG Anti-Malware [AntiSpyware]
Product version check	Is Latest
Engine version check	Is Latest
Data file version check	No Check
Data file has been updated in	2 Hour(s)
Last scan has been done before	Hour(s)
Real-time Protection Status Check	● No Check ○ On ○ Off

Figure 255: *AntiSpyware Page (Overview After)*



☑ An antispyware application is on

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

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	Rtp Check	🗑
AVG Anti-Malware [AntiSpyware]	isLatest	isLatest	no check	2 Hour(s)	no check	nocheck	🗑

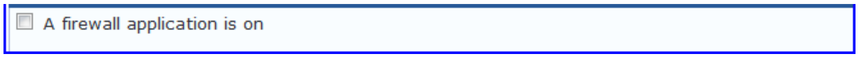
When you save your AntiSpyware configuration, it appears in the **AntiSpyware** page list.

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

Firewall

In the **Firewall** page, you can specify that a Firewall application must be on and specify information about the Firewall application.

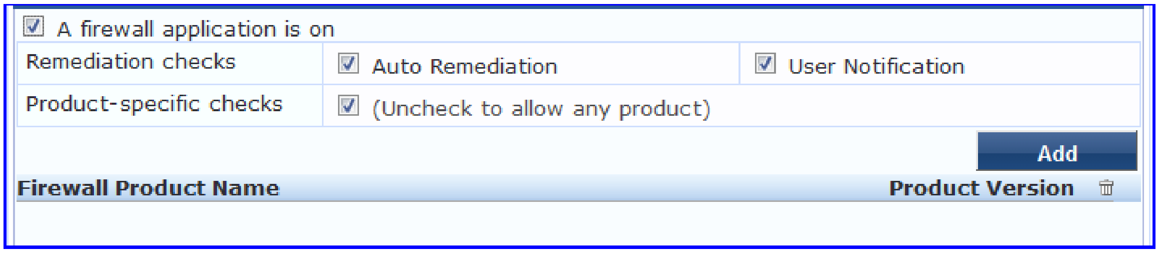
Figure 256: *Firewall Page (Overview Before)*



□ A firewall application is on

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

Figure 257: *Firewall Page (Detail 1)*



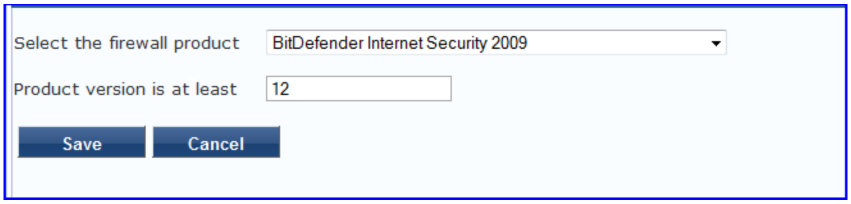
☑ A firewall application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☑ (Uncheck to allow any product)	

Firewall Product Name	Product Version	🗑

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

Figure 258: *Firewall Page (Detail 2)*

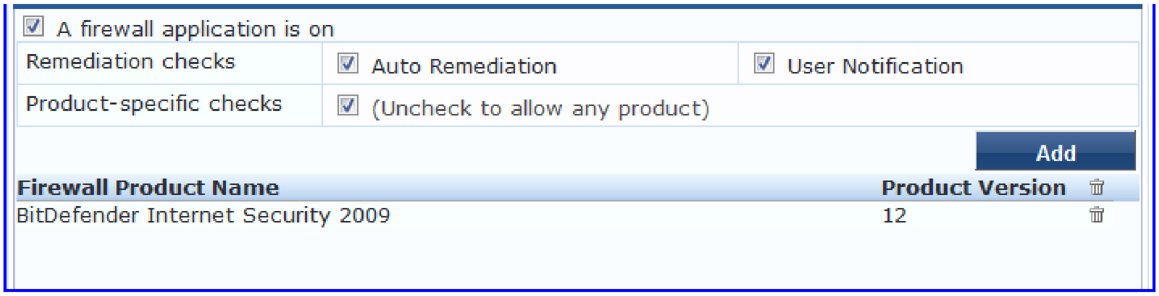


Select the firewall product: BitDefender Internet Security 2009

Product version is at least: 12

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

Figure 259: *Firewall Page (Overview After)*



☑ A firewall application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☑ (Uncheck to allow any product)	

Firewall Product Name	Product Version	🗑
BitDefender Internet Security 2009	12	🗑

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

Table 141: *Firewall Page Parameters*

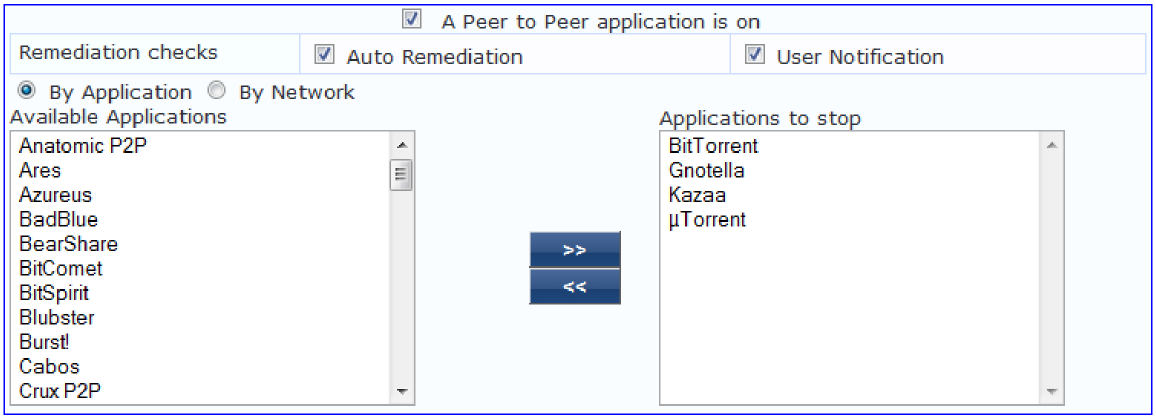
Interface	Parameter	Description
Firewall Page	- A Firewall Application is On - Auto Remediation - User Notification - Uncheck to allow any product	- Check the **Firewall Application is On** check box to enable testing of health data for configured firewall application(s). - Check the **Auto Remediation** 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 260: *Peer to Peer Page*



☑ A Peer to Peer application is on

Remediation checks ☑ Auto Remediation ☑ User Notification

● By Application ○ By Network

Available Applications

Anatomic P2P
Ares
Azureus
BadBlue
BearShare
BitComet
BitSpirit
Blubster
Burst!
Cabos
Crux P2P

Applications to stop

BitTorrent
Gnotella
Kazaa
µTorrent

The following table describes the **Peer to Peer** parameters:

Table 142: *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

The **Patch Management** page provides a way to specify that a patch management application must be on. You can also specify information about the patch management application, configure the Product Evaluation Rule, and configure patch management application checks.

To configure patch-management application(s):

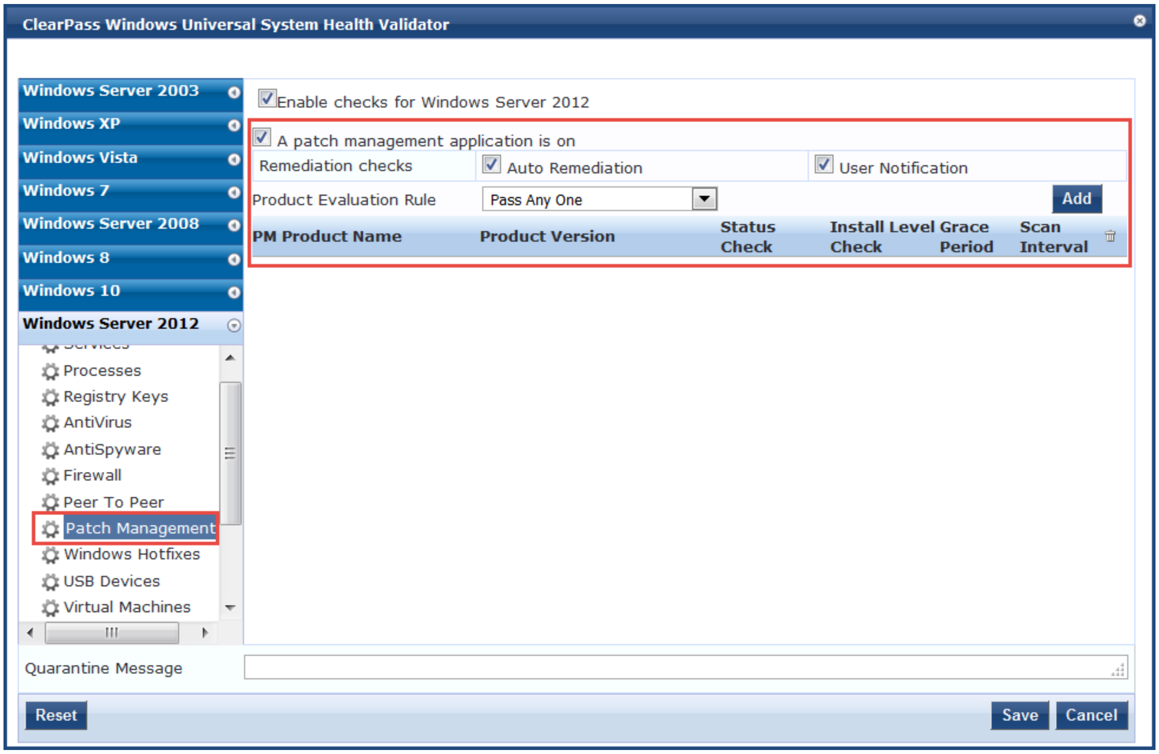
1. Navigate to **Configuration** > **Posture** > **Posture Policies**, then click **Add**.

   The **Add Posture Policies** dialog opens.
2. Select the **Posture Plugins** tab.
3. Click the check box for **ClearPass Windows Universal System Health Validator**.
4. Click **Configure**.

   The **ClearPass Windows Universal System Health Validator** page opens.
5. Select the desired version of Windows.
6. From the selected version of Windows list, select **Patch Management**.
7. To enable checks for the selected version, click the **Enable checks for Windows Server** check box.
8. Click the **A patch management application is on** check box.

   The Patch Management configuration dialog opens.

Figure 261: *ClearPass Windows Universal System Health Validator: Patch Management*



ClearPass Windows Universal System Health Validator

☑ Enable checks for Windows Server 2012

☑ A patch management application is on

Remediation checks ☑ Auto Remediation ☑ User Notification

Product Evaluation Rule: Pass Any One

PM Product Name	Product Version	Status Check	Install Level Check	Grace Period	Scan Interval

Quarantine Message

9. Specify the Patch Management parameters as described in the following table.

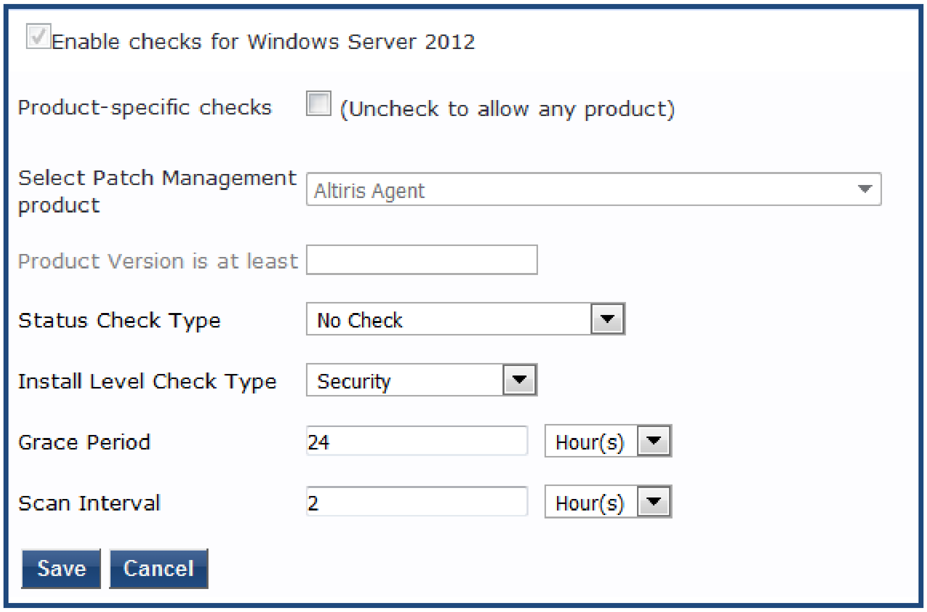
Table 143: *Patch Management Parameters*

Parameter	Action/Description
A patch management application is on	To enable testing of health data for configured Antivirus application(s), check the **A patch management application is on** check box. The Patch Management configuration dialog opens
Remediation Checks	
Auto Remediation	To enable auto-remediation of patch management status, check the **Auto Remediation** check box .
User Notification	To enable user notification of policy violation of patch management status, check the **User Notification** check box.
Product Evaluation Rule	
Product Evaluation Rule	Select the appropriate **Product Evaluation Rule**: ● **Pass All**: Select this product evaluation rule if you want the **Patch Management** health class to be deemed as *healthy* only if all the configured patch management products are present. **Pass All** is the equivalent of an **AND** condition. ● **Pass Any One**: Select this product evaluation rule if you want the **Patch Management** health class to be deemed as *healthy* if any one of the configured patch management products are present. **Pass Any One** is the equivalent of an **OR** condition. **Pass Any One** is the default.

10.To configure patch management application checks, click **Add**.

The **Patch Management Health Checks** configuration page opens:

Figure 262: *Configuration Page for the Patch Management Application*



☑ Enable checks for Windows Server 2012

Product-specific checks	☐ (Uncheck to allow any product)
Select Patch Management product	Altiris Agent
Product Version is at least	
Status Check Type	No Check
Install Level Check Type	Security
Grace Period	24 Hour(s)
Scan Interval	2 Hour(s)

11. Specify these parameters as described in the following table:

NOTE

All checks might not be available for some products. Where checks are not available, they are shown in a disabled state.

Table 144: *Patch Management Parameters*

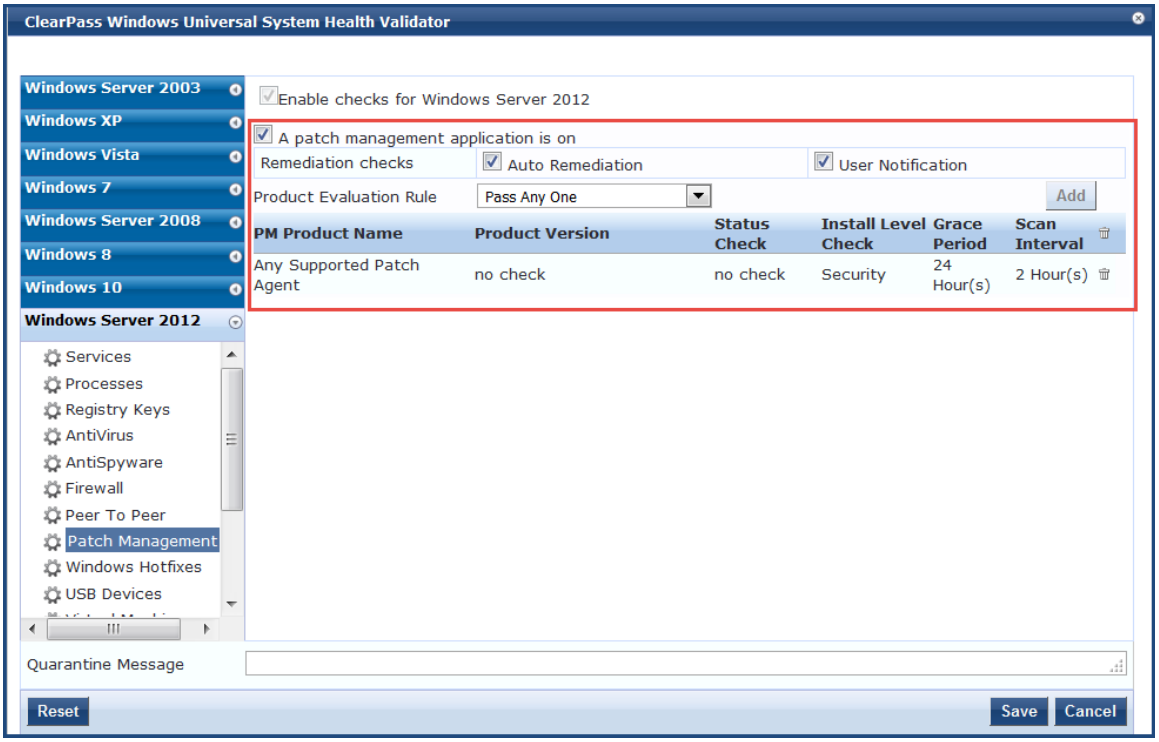
Parameter	Action/Description
Product-specific checks	To check whether any patch management application (any vendor) is running on the end host, clear the **Uncheck to allow any product** check box.
Select Patch Management Product	Select a patch management product vendor. This option is enabled *only* if the **Product-specific checks** check box is checked.
Product version is at least	Enter the minimally recommended product version number. This option is enabled *only* if the **Product-specific checks** check box is checked.
Status Check Type	Specify the **Status Check Type** to check whether the Patch Agent is enabled. The 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, the client is treated as unhealthy. If **Auto-remediation** is enabled, OnGuard Agent changes the Patch Agent Status on the client to the configured value. Select any of the following options: - **No Check**: ClearPass Policy Manager server ignores the Patch Agent Status value. This means it will not check the status of the Patch Agent application on the client.

Table 144: *Patch Management Parameters (Continued)*

Parameter	Action/Description
	■ **Enabled**: Patch Agent is turned on and it automatically updates 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 it notifies the user before downloading updates. ■ **Notify Before Install**: Patch Agent is turned on and it notifies the user before installing updates. **NOTE:** The values specific to the selected patch management product are displayed in the **Status Check Type** field. For example, all five values are displayed for Microsoft Windows Automatic Update. For Microsoft System Center Configuration Manager (SCCM), only **No Check**, **Disabled**, and **Notify Before Install** are displayed.
Install Level Check Type	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**: Checks for all missing patches and searches for all available patches. ■ **Selected on Server**: Checks 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**: Checks only for security updates. Some of the patch management 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 as follows: ■ **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, clients will be treated as *healthy* for three days even if some patches are missing. After three 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*. If you selected **No Check** from the **Install Level Check Type** field, **Grace Period** is disabled.
Scan Interval	Specify the **Scan Interval** by specifying the number of hours, days, weeks, or months. If you selected **No Check** from the **Install Level Check Type** field, **Scan Interval** is disabled.

When you save your patch management configuration, the configuration information is displayed on the **Patch Management** page:

Figure 263: *Patch Management Configuration Summary*



☑ Enable checks for Windows Server 2012

☑ A patch management application is on

Remediation checks ☑ Auto Remediation ☑ User Notification

Product Evaluation Rule: Pass Any One

PM Product Name	Product Version	Status Check	Install Level Check	Grace Period	Scan Interval
Any Supported Patch Agent	no check	no check	Security	24 Hour(s)	2 Hour(s)

Windows Hotfixes

There are two Hotfixes evaluation rules that can be applied:

- The **Windows Hotfixes Groups to be Present Evaluation Rule** specifies how to evaluate the health among multiple Hotfixes groups (see Table 145 for details).

  For example, if the status of *Group1* is [Hotfix1] AND [Hotfix 2], and the status of *Group2* is [Hotfix3] OR [Hotfix4], the overall health status of the two groups is calculated as follows:

  - **Pass All**: ([Hotfix1] AND [Hotfix2]) AND ([Hotfix3] OR [Hotfix4])
  - **Pass Any**: ([Hotfix1] AND [Hotfix2]) OR ([Hotfix3] OR [Hotfix4])

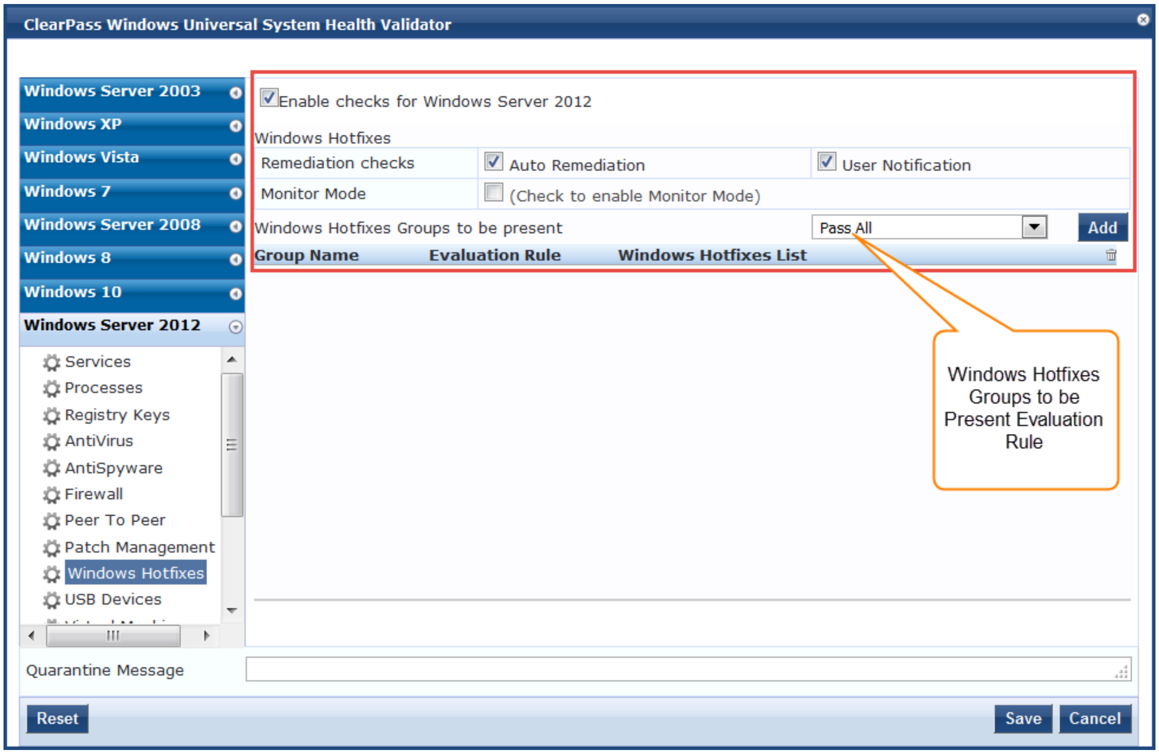
- The **Windows Hotfixes Group Evaluation Rule** specifies how to evaluate the health for a specific Hotfixes group (see Table 146 for details).

To define Windows Hotfixes Groups, specify the evaluation rules for multiple groups or a single group, and add or remove specific Windows hotfixes on the endpoint:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**, then click **Add**.
2. From the **Add Posture Policies** page, select the **Posture Plugins** tab.
3. Select the **ClearPass Windows Universal System Health Validator**, then click **Configure**.
4. Select the Windows operating system, then check the **Enable checks for *Windows_OS***.
5. Select **Windows Hotfixes**.

   The **Windows Hotfixes** health class configuration page opens:

Figure 264: *Windows Hotfixes Page*



☑ Enable checks for Windows Server 2012

Windows Hotfixes

Remediation checks	☑ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

Windows Hotfixes Groups to be present: Pass All

Group Name	Evaluation Rule	Windows Hotfixes List

Windows Hotfixes Groups to be Present Evaluation Rule

Quarantine Message

6. Specify the **Windows Hotfixes** parameters as described in the following table:

Table 145: *Windows Hotfixes Page Parameters*

Parameter	Action/Description
Auto Remediation	Enable to allow auto-remediation for hotfix checks. Enabling this automatically triggers updates of the specified hotfixes. Auto-remediation for the Windows Hotfixes health class is enabled by default.
User Notification	Enable to allow user notifications to check for hotfix policy violations.
Monitor Mode	Click to enable **Monitor Mode**.
Windows Hotfixes Groups to be Present Evaluation Rule	This evaluation rule specifies whether all groups should be healthy or any one group should be healthy. For example, if there are two Hotfixes Groups: • **Pass All**: Select this evaluation rule to calculate the two group's health status as *Group1* **AND** *Group2*. • **Pass Any One**: Select this evaluation rule to calculate the two group's health status as *Group1* **OR** *Group2*.

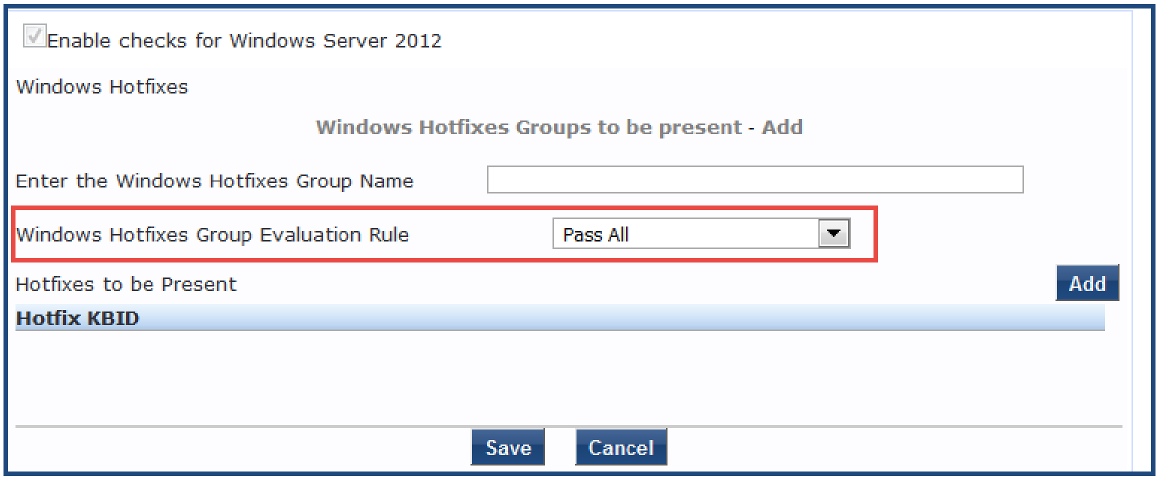
Configuring Windows Hotfixes Groups to Be Present

To configure the Windows Hotfixes Groups to be present:

1. From the **Windows Hotfixes** health class configuration page (see Figure 264), click **Add**.

   The following Hotfixes dialog opens:

Figure 265: *Defining the Hotfix Group*



☑ Enable checks for Windows Server 2012

Windows Hotfixes

Windows Hotfixes Groups to be present - Add

Enter the Windows Hotfixes Group Name

Windows Hotfixes Group Evaluation Rule: Pass All

Hotfixes to be Present

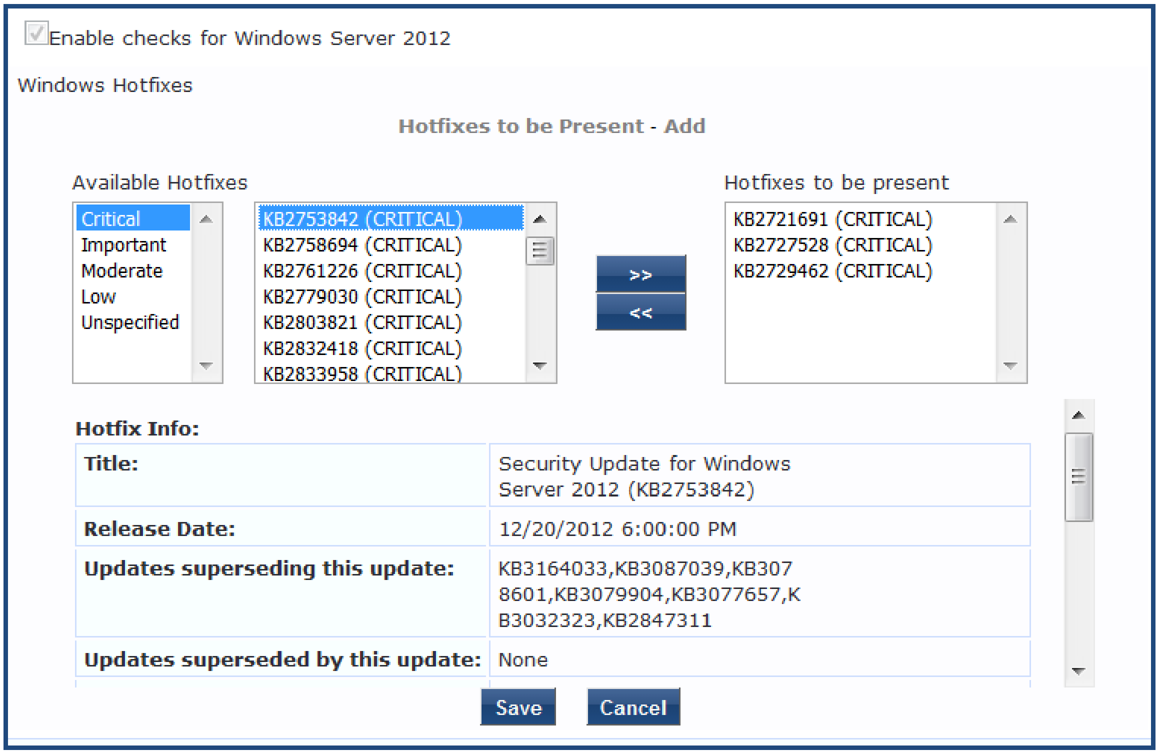
Hotfix KBID

2. Specify the Hotfixes Group parameters as described in the following table:

Table 146: *Specifying Hotfixes Group to Be Present Parameters*

Parameter	Action/Description
Enter the Windows Hotfixes Group Name	Enter the name of the Hotfixes Group.
Windows Hotfixes Group Evaluation Rule	This evaluation rule specifies how to evaluate the health of a specific Hotfixes Group. Select the appropriate Hotfix Group Evaluation Rule: ● **Pass All**: Select this evaluation rule if you want all hotfixes groups to be present. **Pass All** is the equivalent of an **AND** condition. ● **Pass Any One**: Select this evaluation rule if you want any one of the hotfixes groups to be present. **Pass Any One** is the equivalent of an **OR** condition.
Hotfixes to be Present	To add hotfixes to the Hotfixes Group, click **Add**. The dialog shown in Figure 266 opens.

Figure 266: *Specifying the Hotfixes to Be Present*



☑ Enable checks for Windows Server 2012

Windows Hotfixes

Hotfixes to be Present - Add

Available Hotfixes

- Critical
- Important
- Moderate
- Low
- Unspecified

- KB2753842 (CRITICAL)
- KB2758694 (CRITICAL)
- KB2761226 (CRITICAL)
- KB2779030 (CRITICAL)
- KB2803821 (CRITICAL)
- KB2832418 (CRITICAL)
- KB2833958 (CRITICAL)

Hotfixes to be present

- KB2721691 (CRITICAL)
- KB2727528 (CRITICAL)
- KB2729462 (CRITICAL)

Hotfix Info:

Title:	Security Update for Windows Server 2012 (KB2753842)
Release Date:	12/20/2012 6:00:00 PM
Updates superseding this update:	KB3164033,KB3087039,KB3078601,KB3079904,KB3077657,KB3032323,KB2847311
Updates superseded by this update:	None

3. From the first list, specify the criticality of the hotfixes:

- Critical
- Important
- Moderate
- Low
- Unspecified

   As shown in Figure 266, the list of hotfixes for the selected criticality are displayed.

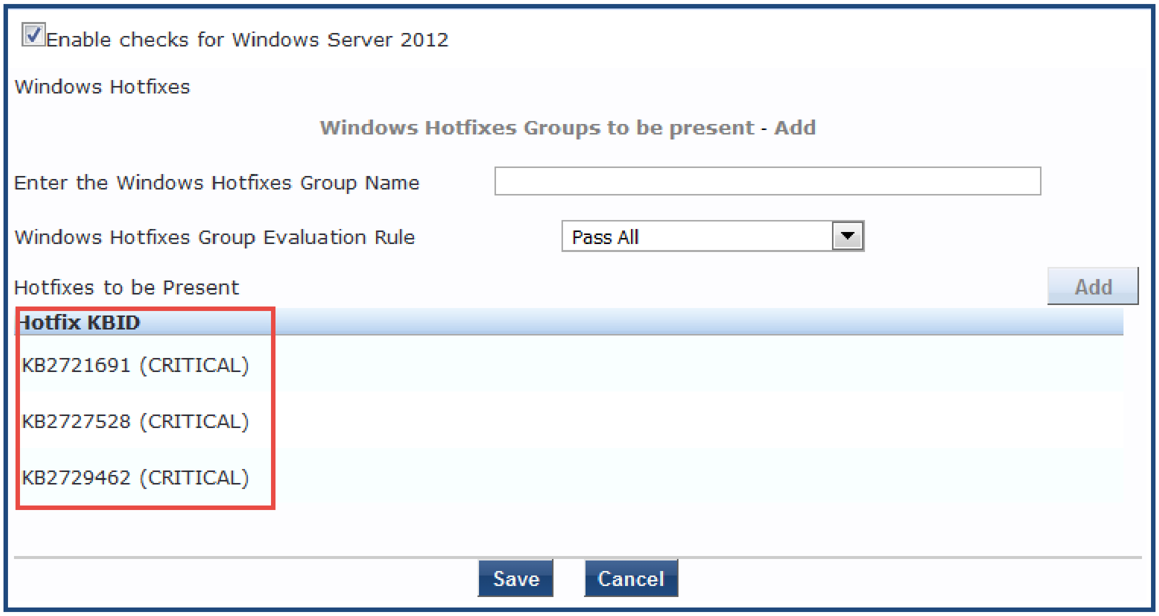
4. Select one or more of the desired hotfixes from the **Available Hotfixes** list.

   As shown in Figure 266, when you select a Hotfix from the list of available hotfixes, information about that hotfix is displayed.

5. To move hotfixes to the **Hotfixes to be present** box, select the desired hotfixes, then click **>>**.

   The selected hotfixes are moved to the **Hotfixes to be present** box.

Figure 267: *Windows Hotfixes Added*



☑ Enable checks for Windows Server 2012

Windows Hotfixes

Windows Hotfixes Groups to be present - Add

Enter the Windows Hotfixes Group Name

Windows Hotfixes Group Evaluation Rule: Pass All

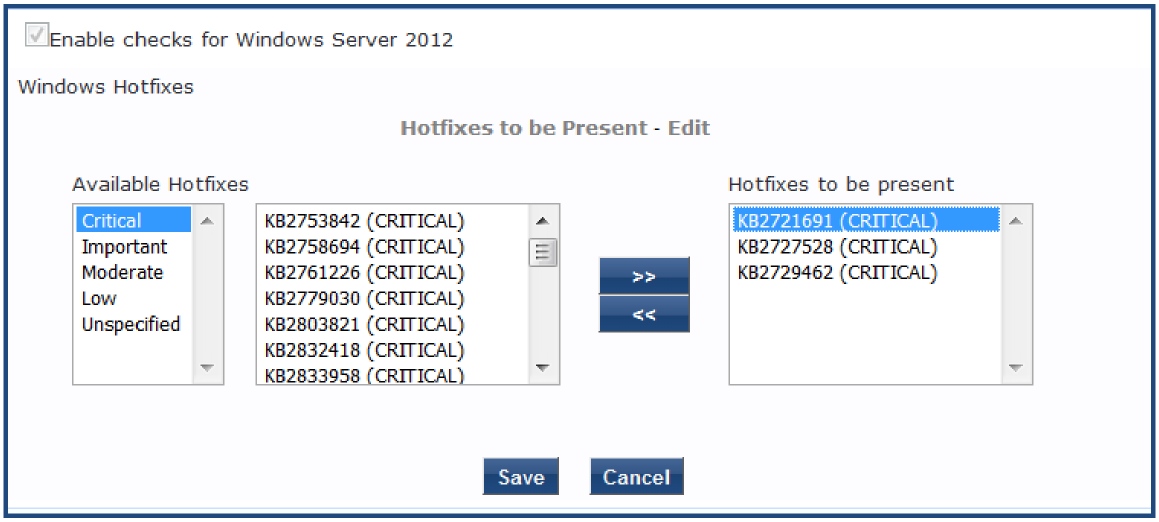
Hotfixes to be Present

Hotfix KBID
KB2721691 (CRITICAL)
KB2727528 (CRITICAL)
KB2729462 (CRITICAL)

6. To remove a hotfix from the **Hotfixes to be present** list, select the hotfix to be removed.

   The **Edit Hotfixes to be Present** dialog opens.

Figure 268: *Removing Hotfixes from the Hotfixes to Be Present List*



☑ Enable checks for Windows Server 2012

Windows Hotfixes

Hotfixes to be Present - Edit

Available Hotfixes

Critical
Important
Moderate
Low
Unspecified

KB2753842 (CRITICAL)
KB2758694 (CRITICAL)
KB2761226 (CRITICAL)
KB2779030 (CRITICAL)
KB2803821 (CRITICAL)
KB2832418 (CRITICAL)
KB2833958 (CRITICAL)

Hotfixes to be present

KB2721691 (CRITICAL)
KB2727528 (CRITICAL)
KB2729462 (CRITICAL)

7. From the Hotfixes to be present list, select the hotfix(es) you wish to remove and click **<<**.

   The selected hotfix is removed from the Hotfixes to be present list.

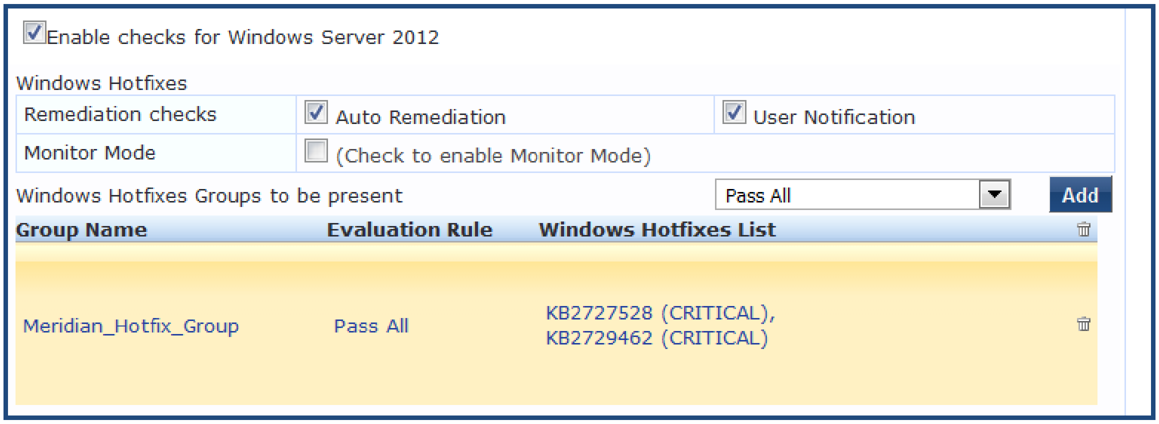
8. When finished, click **Save**.

   You return to the **Windows Hotfixes** dialog, where the **Hotfixes to be Present** > **Hotfix KBID** (Knowledge Base Article ID) list displays the updated list.

9. Click **Save**.

   The **Windows Hotfixes** page displays a summary of the Hotfixes Group configuration:

Figure 269: *Summary of Hotfixes Groups Configuration*



☑ Enable checks for Windows Server 2012

Windows Hotfixes

Remediation checks	☑ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

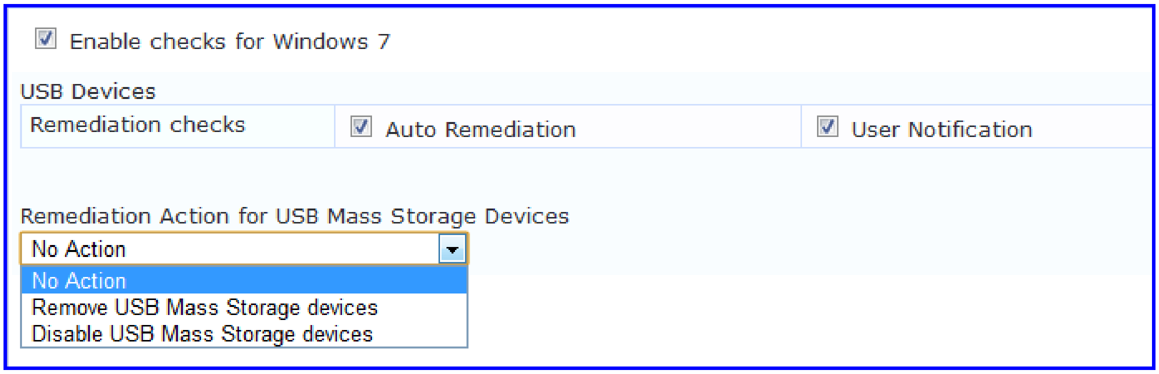
Windows Hotfixes Groups to be present: Pass All

Group Name	Evaluation Rule	Windows Hotfixes List
Meridian_Hotfix_Group	Pass All	KB2727528 (CRITICAL), KB2729462 (CRITICAL)

USB Devices

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

Figure 270: *USB Devices*



☑ Enable checks for Windows 7

USB Devices

Remediation checks	☑ Auto Remediation	☑ User Notification

Remediation Action for USB Mass Storage Devices: No Action

No Action
Remove USB Mass Storage devices
Disable USB Mass Storage devices

The following table describes the **USB Devices** parameters:

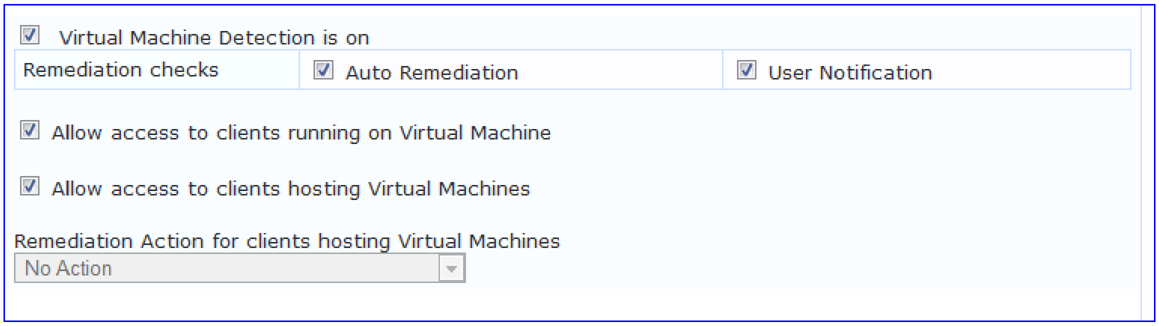
Table 147: *USB Devices*

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 271: *Virtual Machines*



☑ Virtual Machine Detection is on

Remediation checks ☑ Auto Remediation ☑ User Notification

☑ Allow access to clients running on Virtual Machine

☑ Allow access to clients hosting Virtual Machines

Remediation Action for clients hosting Virtual Machines

No Action

The following table describes the **Virtual Machines** parameters:

Table 148: *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

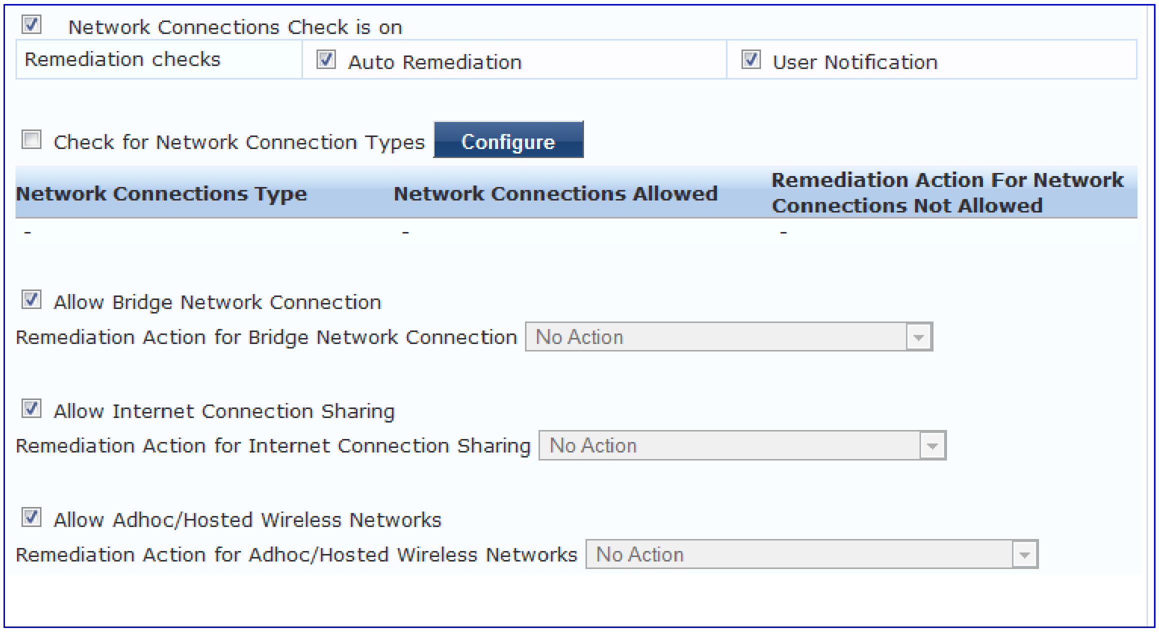
The **Network Connections** page provides configuration to control network connections based on connection type.

To configure Network Connections:

1. From the ClearPass Windows Universal System Health Validator page, enable checks for the selected version of Windows.
2. Select **Network Connections**.
3. Enable the **Network Connection Check is on** check box.

   The **Network Connections** configuration page appears.

Figure 272: *Network Connections Configuration Page*



☑ Network Connections Check is on

Remediation checks ☑ Auto Remediation ☑ User Notification

□ Check for Network Connection Types

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

☑ Allow Bridge Network Connection

Remediation Action for Bridge Network Connection: No Action

☑ Allow Internet Connection Sharing

Remediation Action for Internet Connection Sharing: No Action

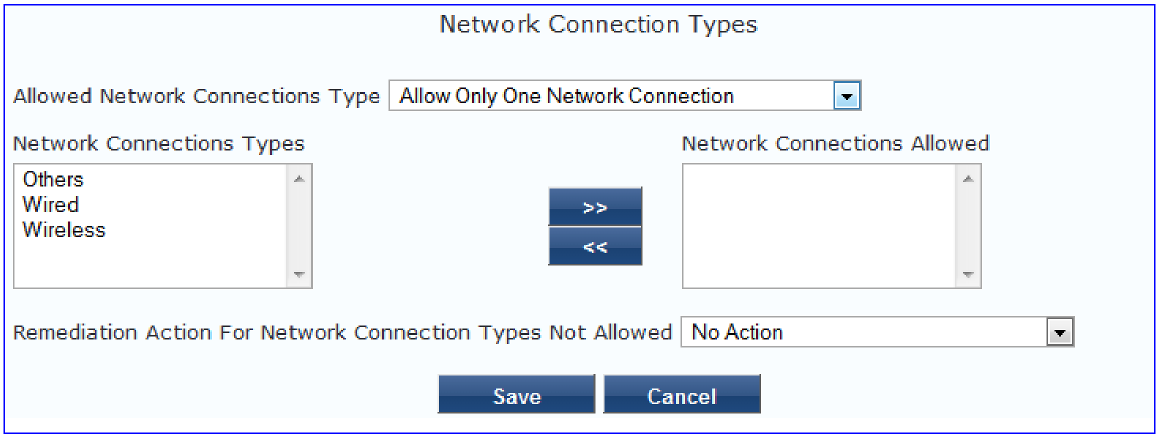
☑ Allow Adhoc/Hosted Wireless Networks

Remediation Action for Adhoc/Hosted Wireless Networks: No Action

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

   The **Network Connection Types** configuration page appears.

Figure 273: *Network Connection Types Configuration Page*



Network Connection Types

Allowed Network Connections Type: Allow Only One Network Connection

Network Connections Types: Others, Wired, Wireless

Network Connections Allowed:

Remediation Action For Network Connection Types Not Allowed: No Action

The following table describes the **Network Connection Types** configuration parameters:

Table 149: *Network Connection Type Configuration Parameters*

Parameter	Action/Description
Allow Network Connections Type	1. Select one of the following options: ▪ Allow Only One Network Connection ▪ Allow One Network Connection with VPN ▪ Allow Multiple Network Connections
Network Connection Types	2. To add or remove **Others**, **Wired**, and **Wireless** network connection types, click **>>** or **<<**.
Remediation Action for Network Connection Types Not Allowed	3. Specify one of the following ▪ No Action: Take no action. Do not eject or disable the attached devices. ▪ Disable Network Connections ▪ Disconnect Network Connections
	4. Click **Save**.

This returns you to the **Network Connections** configuration page. The following table describes the remaining fields on this page.:

Table 150: *Network Connections Configuration Parameters*

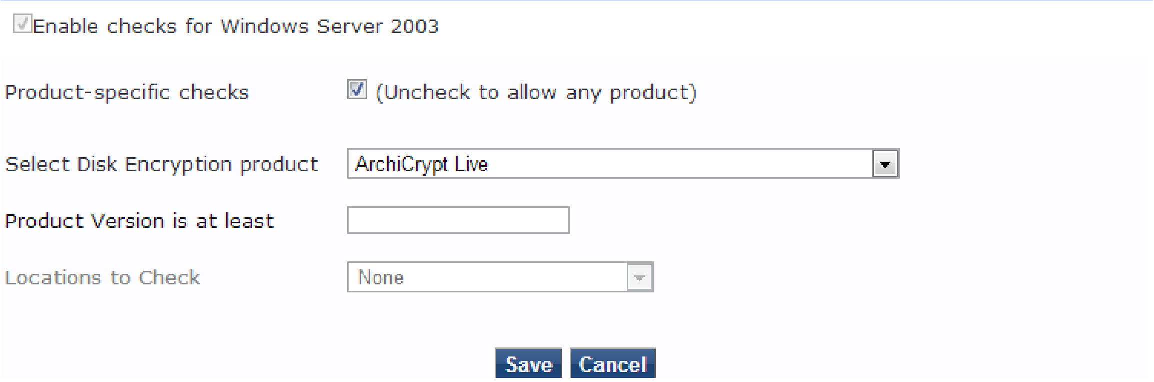
Parameter	Action/Description
Auto Remediation	1. Enable to allow auto-remediation for network connections.
User Notification	2. Enable to allow user notifications in the event of network connection policy violations.
Remediation Action for Bridge Network Connection	3. If **Allow Bridge Network Connection** 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	4. 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	5. If **Allow Adhoc/Hosted Wireless Networks** is disabled, then specify whether to take no action when an adhoc wireless networks exist 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 274: *Disk Encryption Configuration Page*



☑ Enable checks for Windows Server 2003

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

Select Disk Encryption product: ArchiCrypt Live

Product Version is at least:

Locations to Check: None

The following table describes the Disk Encryption parameters:

Table 151: *Disk Encryption Parameters*

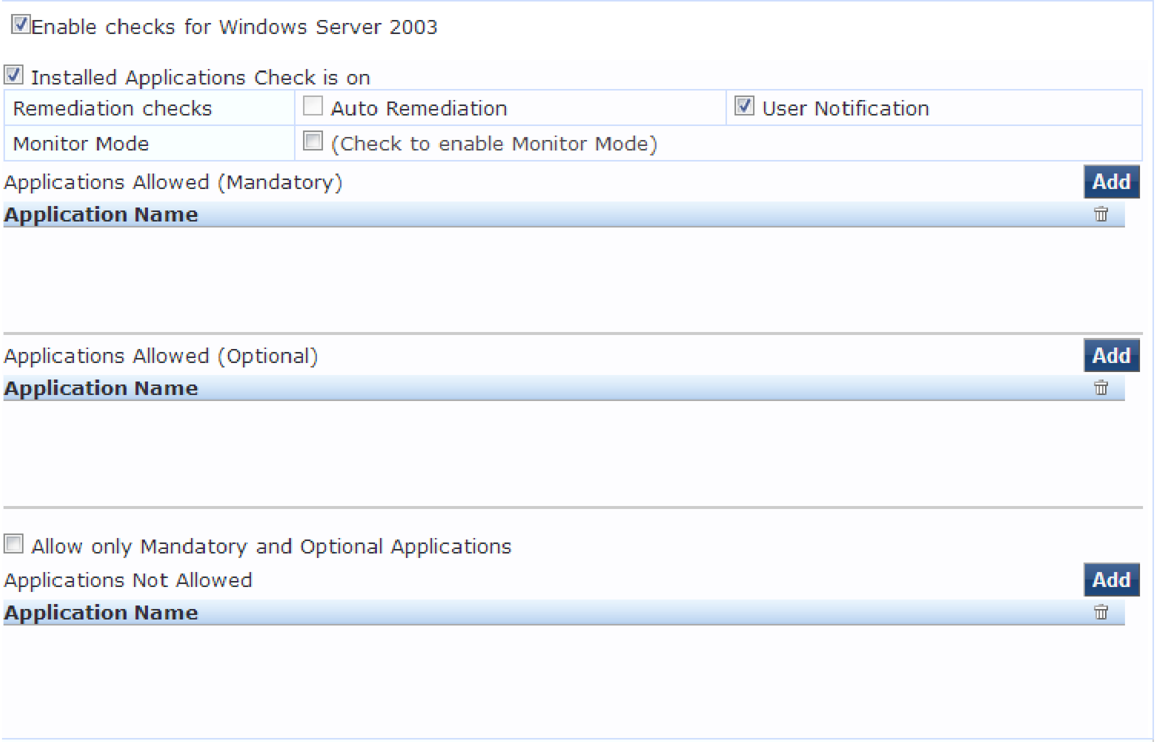
Parameter	Description
User Notification	Enable to allow user notifications for virtual machine policy violations.
Product-specific checks	Clear to allow disk encryption on any product. The Select Disk Encryption product and Product Version is at least fields are disabled after you clear the check box.
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 the Windows Installer. Examples of objects in this category are installed products, file specifications, and registration actions.

In the **Installed Applications Configuration** page (see Figure 275), you can turn on the installed applications check and specify information about which installed applications you want to monitor.

Figure 275: *Installed Applications for Windows Configuration Page*



☑ Enable checks for Windows Server 2003

☑ Installed Applications Check is on

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

Applications Allowed (Mandatory)

Application Name

Applications Allowed (Optional)

Application Name

□ Allow only Mandatory and Optional Applications

Applications Not Allowed

Application Name

The following table describes the **Installed Applications Configuration** page parameters:

Table 152: *Installed Applications for Windows Configuration Page Parameters*

Parameter	Action/Description
Remediation checks	**Auto-Remediation** for the Installed Applications health class is not supported.
User Notification	1. Enable sending a remediation message with a list of applications to install or uninstall to the user.
Monitor Mode	2. Enable **Monitor Mode** to treat all the installed applications as always healthy.

Table 152: *Installed Applications for Windows Configuration Page Parameters (Continued)*

Parameter	Action/Description
Applications Allowed (Mandatory)	3. Specify installed applications to be monitored on a mandatory basis. **NOTE:** Enter the application name as they are shown in Add/Remove Programs.
Applications Allowed (Optional)	4. Specify installed applications to be monitored on an optional basis. **NOTE:** Enter the application name as they are shown in Add/Remove Programs.
Allow only Mandatory and Optional Applications	5. Specify that only the mandatory and optional applications are monitored. **NOTE:** All applications that are not either mandatory or optional must be removed or uninstalled.

Enabling Regular Expressions for a Windows Application

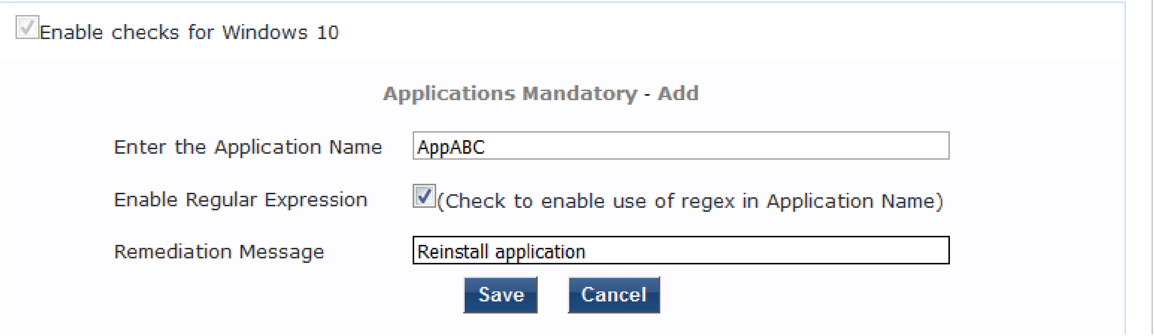
To enable regular expressions for an application:

1. From the **ClearPass Windows Universal System Health Validator** > **Configure** page (see Windows Universal System Health Validator on page 1), then select the desired version of Windows.
2. Select **Installed Applications**.
3. Click (enable) the **Installed Applications Check is on** check box.

   The Installed Applications dialog appears (see Figure 275).
4. From the desired **Applications Allowed** category, click **Add**.

   The **Add Mandatory Applications** dialog for the selected **Applications Allowed** category appears.

Figure 276: *Enabling Regular Expression*



☑Enable checks for Windows 10

Applications Mandatory - Add

Enter the Application Name: AppABC

Enable Regular Expression: ☑(Check to enable use of regex in Application Name)

Remediation Message: Reinstall application

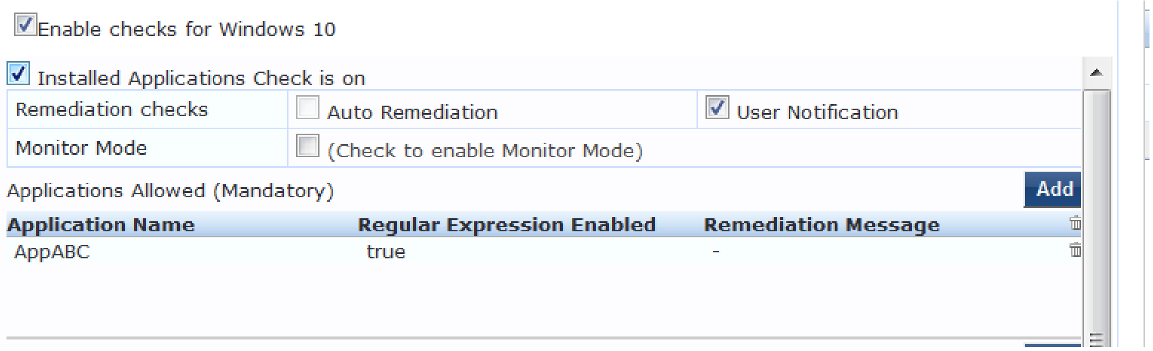
5. Configure the **Add Mandatory Applications** parameters as described in Table 153.

Table 153: *Mandatory Applications Parameters*

Parameter	Action/Description
Enter the Application Name	1. Enter the name of the application.
Enable Regular Expression	2. Check (enable) this check box to enable the use of regular expressions in the **Application Name**. When this field is enabled, ClearPass treats the **Application Name** as regular expression when comparing application names.
Remediation Message	3. Optionally, enter the remediation message that will be displayed to the user in the event of an error. **NOTE:** Remedition messages can include reasons for remediation, links to helpful URLs and helpdesk contact information.
	4. Click **Save**.

You return to the **Installed Applications** dialog, where **Regular Expression Enabled** is set to **true** for the specified application (see Figure 277).

Figure 277: *Regular Expression Enabled*



☑ Enable checks for Windows 10

☑ Installed Applications Check is on

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

Applications Allowed (Mandatory)

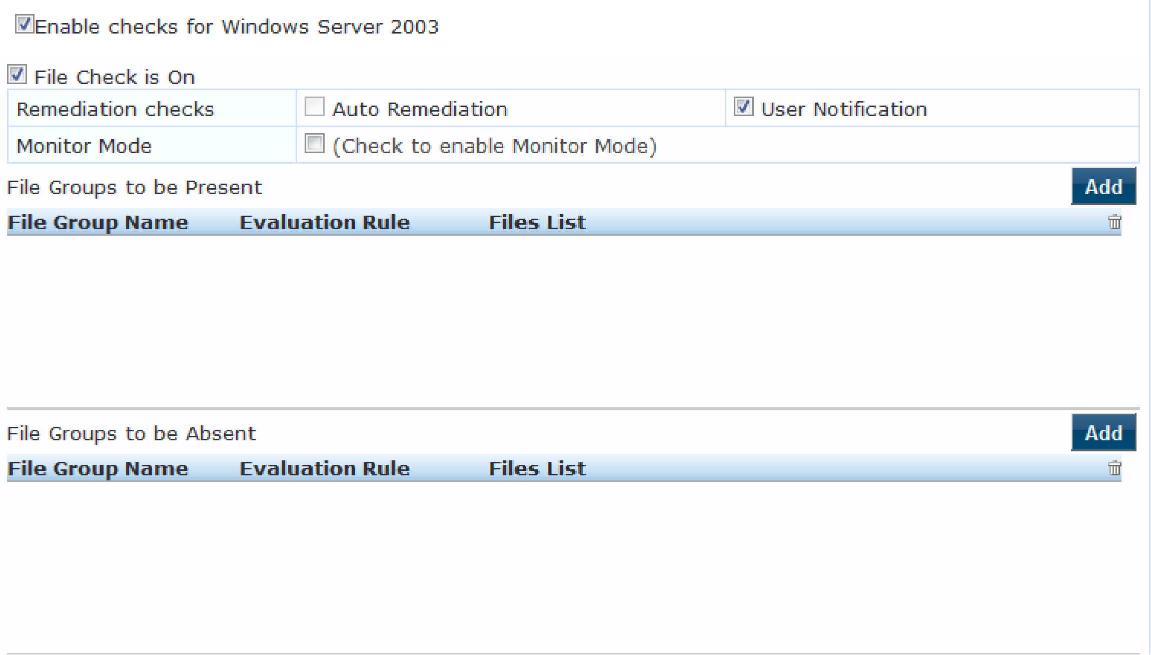
Application Name	Regular Expression Enabled	Remediation Message
AppABC	true	-

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 278: *Windows File Check Health Class Configuration*



☑ Enable checks for Windows Server 2003

☑ File Check is On

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

File Groups to be Present

File Group Name	Evaluation Rule	Files List

File Groups to be Absent

File Group Name	Evaluation Rule	Files List

The following table describes the **File Check Configuration** parameters:

Table 154: *File Check Configuration Parameters*

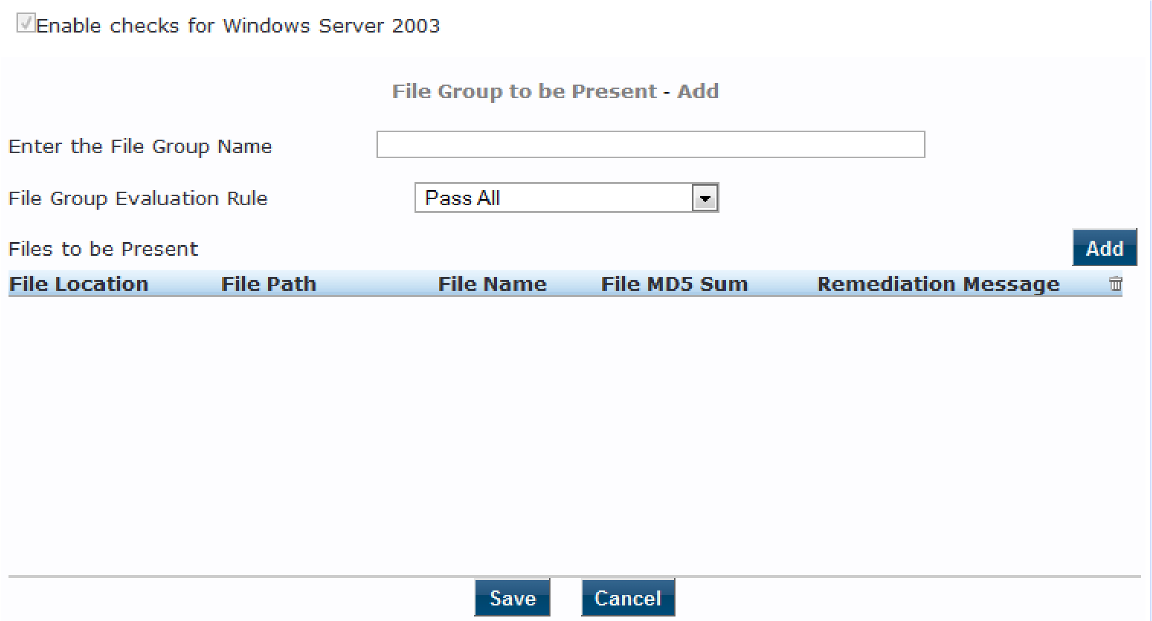
Parameter	Action/Description
Remediation checks	Auto-remediation for the **File Check** health class is not supported.
User Notification	1. When enabled, a remediation message that includes the groups of files to be present or absent is displayed to the end user.
Monitor Mode	2. To treat all the file check health classes as always healthy, enable **Monitor Mode**.
File Groups to be Present	3. To add the files to be present in the **File Check** health class, click **Add**.
File Groups to be Absent	4. To add the files to be absent in the **File Check** health class, click **Add**.

Defining the File Group to Be Present

1. To open the **File Group to be Present > Add** page, click **Add**:

   You can configure the name of the file group and specify the evaluation rule for the file group.

   The following figure displays the **File Group to Be Present > Add** dialog:



☑ Enable checks for Windows Server 2003

File Group to be Present - Add

Enter the File Group Name

File Group Evaluation Rule: Pass All

Files to be Present

File Location	File Path	File Name	File MD5 Sum	Remediation Message

The following table describes the **File Group to be Present > Add** parameters:

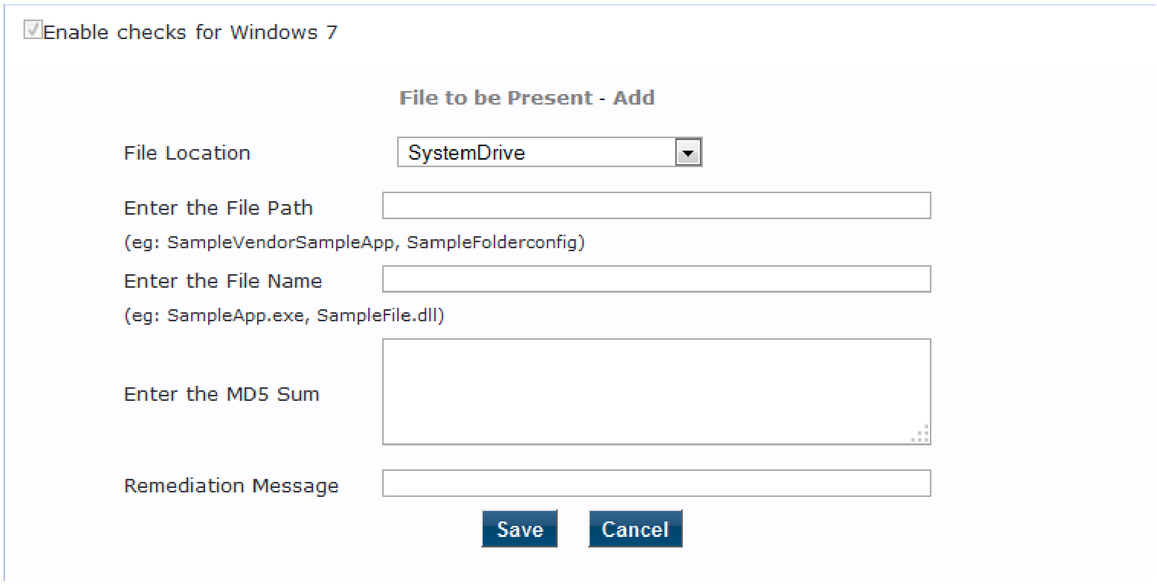
Table 155: *File Group to be Present - Add Parameters*

Parameter	Action/Description
Enter the File Group Name	1. Enter the name of the file group.
File Group Evaluation Rule	2. Select the appropriate 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 if any one of the configured file groups are present.

3. To configure the name of the file group and the evaluation rule for the file group, from **File Groups to be Present**, click **Add**.

   The following figure displays the **File to Be Present > Add** page:

Figure 279: *File to be Present > Add Dialog*



☑ Enable checks for Windows 7

File to be Present - Add

File Location	SystemDrive
Enter the File Path (eg: SampleVendorSampleApp, SampleFolderconfig)	
Enter the File Name (eg: SampleApp.exe, SampleFile.dll)	
Enter the MD5 Sum	
Remediation Message	

The following table describes the **File to be Present > Add** parameters:

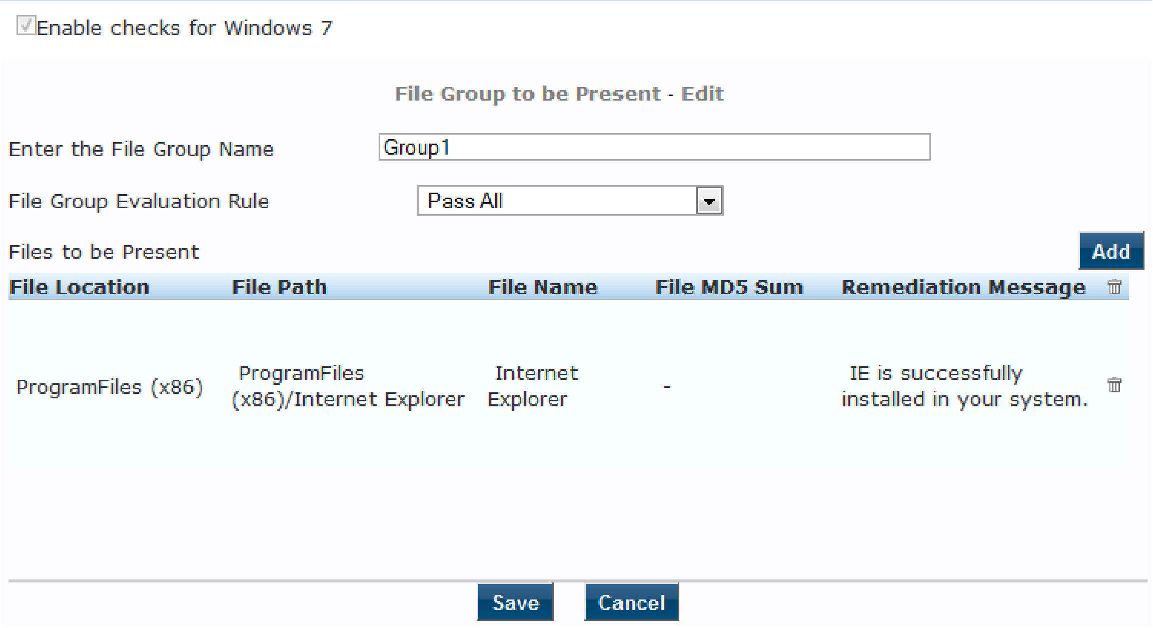
Table 156: *File to be Present > Add Parameters*

Parameter	Action/Description
File Location	1. Select any location of the file from the drop-down list: - SystemDrive - Systemroot - ProgramFiles - ProgramFiles (x86) - HOMEDRIVE - HOMEPATH - None
Enter the File Path	2. Enter the file path as described in the examples from the user interface.
Enter the File Name	3. Enter the name of the file.
Enter the MD5 Sum	Optionally, specify one or more (comma separated) MD5 checksums of the process executable file.
Remediation Message	4. Specify the custom remediation message to be displayed to end users if **File check** fails.

5. When finished, click **Save**.

   The parameters configured in the **File to be Present > Add** dialog are reflected in the **File Groups to be Present** page as illustrated in the following figure:

Figure 280: *File Group to be Present Parameters Displayed*



☑ Enable checks for Windows 7

File Group to be Present - Edit

Enter the File Group Name: Group1

File Group Evaluation Rule: Pass All

Files to be Present

File Location	File Path	File Name	File MD5 Sum	Remediation Message
ProgramFiles (x86)	ProgramFiles (x86)/Internet Explorer	Internet Explorer	-	IE is successfully installed in your system.

Windows System Health Validator: OnGuard Agent

This Windows System Health Validator checks for current Windows Service Packs. The OnGuard Agent also supports legacy Windows operating systems such as Windows Server 2003 and Windows Server 2012.

Use the check boxes to enable support of specific operating systems and to restrict access based on the Service Pack level.

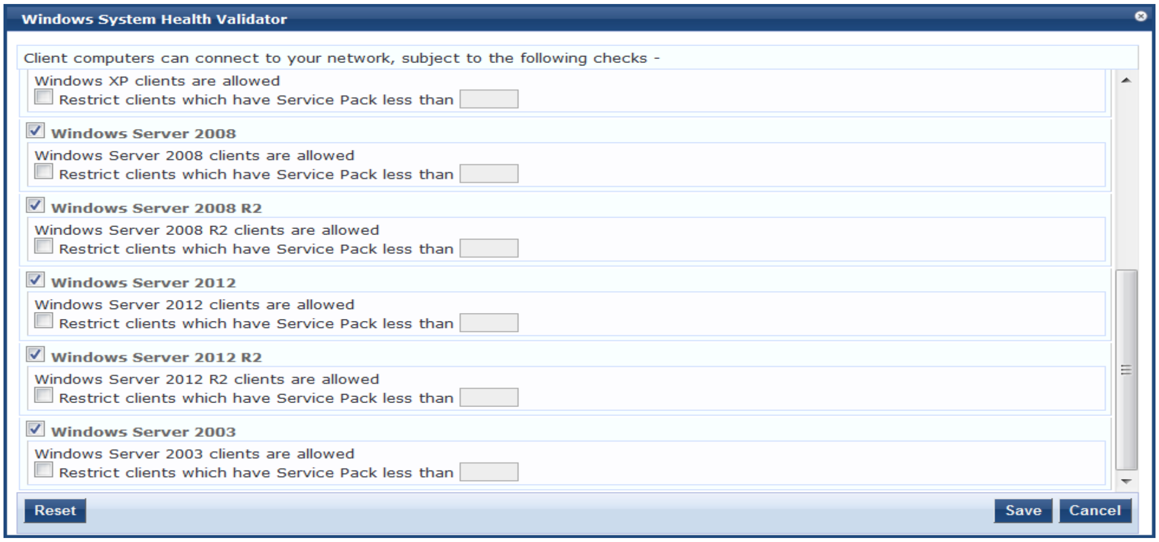
To configure the Windows System Health Validator:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**.
2. Click **Add**.

   The **Add Posture Policies** dialog opens.
3. Specify the following:
   a. Policy Name: Enter the name of the posture policy.
   b. Posture Agent: **Onguard Agent**
   c. Host Operating System: **Windows**
4. Click **Next**.
5. From the **Posture Plugins** tab, select **Windows System Health Validator**, then click the **Configure** button.

   The **Windows System Health Validator** page appears:

Figure 281: *OnGuard Agent: Windows System Health Validator*



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

Windows XP clients are allowed
□ Restrict clients which have Service Pack less than

☑ **Windows Server 2008**
Windows Server 2008 clients are allowed
□ Restrict clients which have Service Pack less than

☑ **Windows Server 2008 R2**
Windows Server 2008 R2 clients are allowed
□ Restrict clients which have Service Pack less than

☑ **Windows Server 2012**
Windows Server 2012 clients are allowed
□ Restrict clients which have Service Pack less than

☑ **Windows Server 2012 R2**
Windows Server 2012 R2 clients are allowed
□ Restrict clients which have Service Pack less than

☑ **Windows Server 2003**
Windows Server 2003 clients are allowed
□ Restrict clients which have Service Pack less than

6. To enable support of specific operating systems, click the corresponding check box.
7. Enter the minimum Service Pack level required on the client computer to connect to your network.
8. Click **Save**.

Windows Security Health Validator: OnGuard Agent

The Windows Security Health Validator checks for the presence of specific types of security applications. You can use the options to restrict access based on the absence of the selected security application types.

To configure the Windows Security Health Validator:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**.
2. Click **Add**.

   The Add Posture Policies dialog appears. Specify the following:

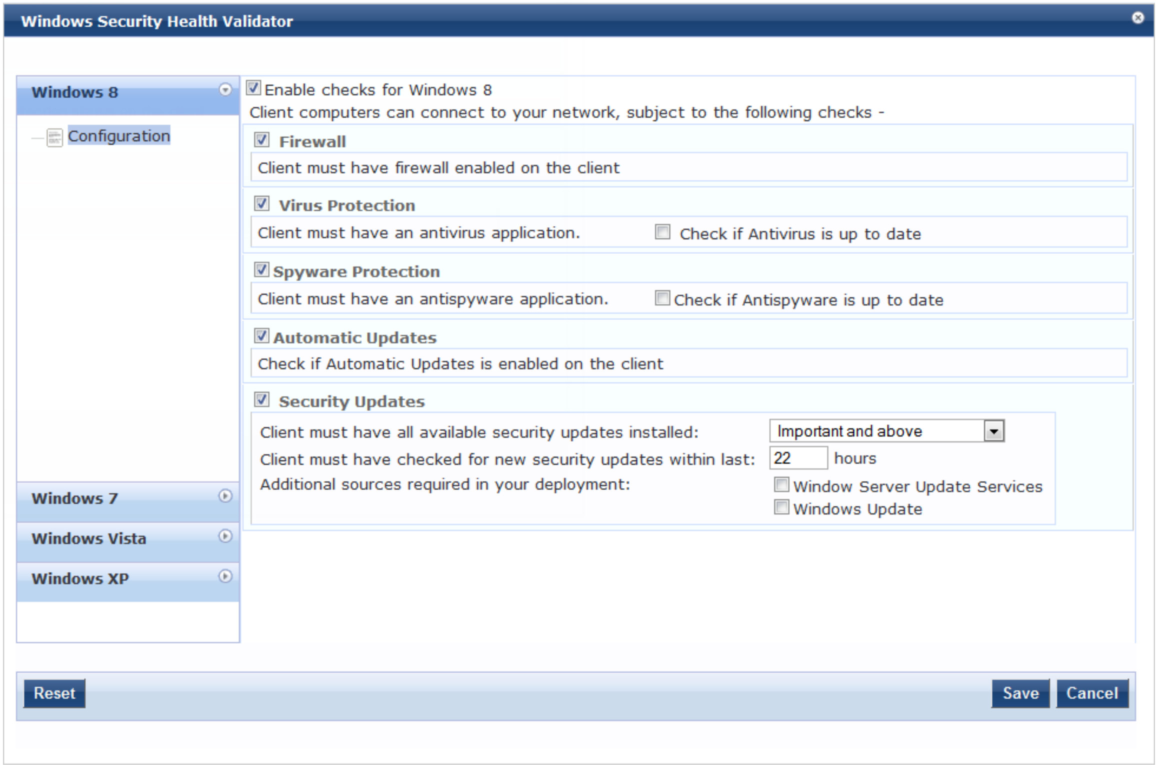
   a. **Policy Name**: Enter the name of the posture policy.

   b. **Posture Agent**: **Onguard Agent**

   c. **Host Operating System**: **Windows**
3. Click **Next**.
4. From the **Posture Plugins** tab, select **Windows Security Health Validator**, then click the **Configure** button.

The following screen appears:

Figure 282: *Onguard Agent: Windows Security Health Validator Page*



☑ Enable checks for Windows 8

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

☑ Firewall

Client must have firewall enabled on the client

☑ Virus Protection

Client must have an antivirus application. ☐ Check if Antivirus is up to date

☑ Spyware Protection

Client must have an antispyware application. ☐ Check if Antispyware is up to date

☑ Automatic Updates

Check if Automatic Updates is enabled on the client

☑ Security Updates

Client must have all available security updates installed: Important and above

Client must have checked for new security updates within last: 22 hours

Additional sources required in your deployment: ☐ Window Server Update Services ☐ Windows Update

5. To enable support of specific operating systems, click the corresponding check box.
6. Enter the minimum Service Pack level required on the client computer to connect to your network.
7. Click **Save**.

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.

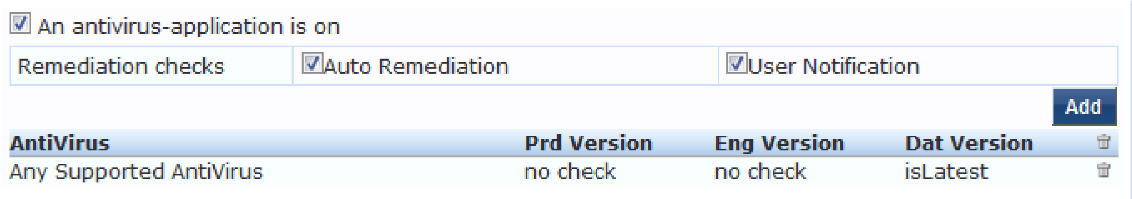
The OnGuard Dissolvable Agent version of the **ClearPass Linux Universal System Health Validator** plug-in supports the following health classes:

- Antivirus on page 314
- Services on page 315

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 283: *Antivirus Page*



☑ An antivirus-application is on

Remediation checks	☑Auto Remediation	☑User Notification

AntiVirus	Prd Version	Eng Version	Dat Version
Any Supported AntiVirus	no check	no check	isLatest

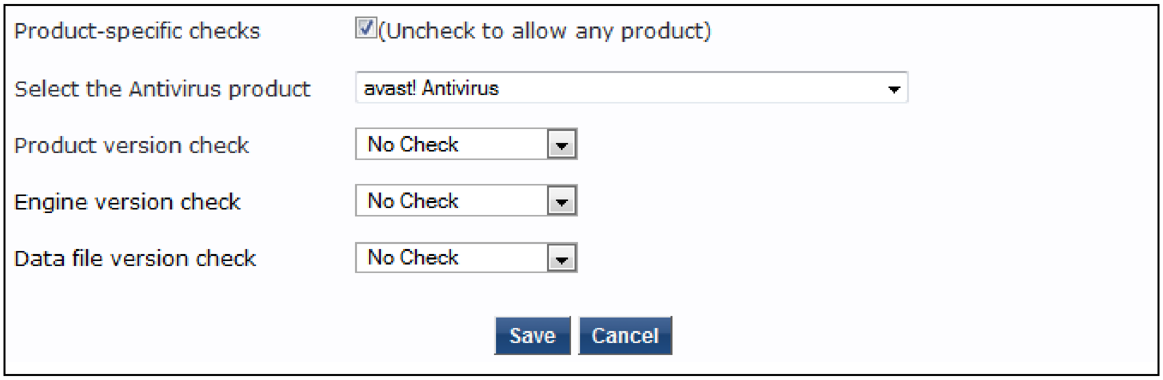
The following table describes the **Antivirus** parameters:

Table 157: *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 284: *Antivirus Product configuration Pop-up*



Product-specific checks	☑(Uncheck to allow any product)
Select the Antivirus product	avast! Antivirus
Product version check	No Check
Engine version check	No Check
Data file version check	No Check

The following table describes the **Antivirus Product configuration** parameters:

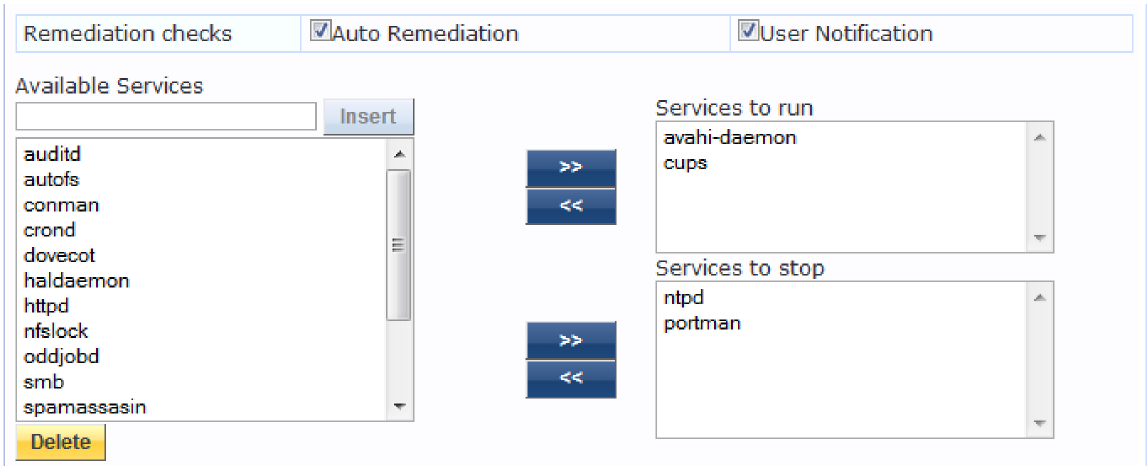
Table 158: *Antivirus Product configuration Parameters*

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 285: *Services Page*



Remediation checks ☑ Auto Remediation ☑ User Notification

Available Services

auditd
autofs
conman
crond
dovecot
haldaemon
httpd
nfslock
oddjobd
smb
spamassasin

Services to run

avahi-daemon
cups

Services to stop

ntpd
portman

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

Table 159: *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**.

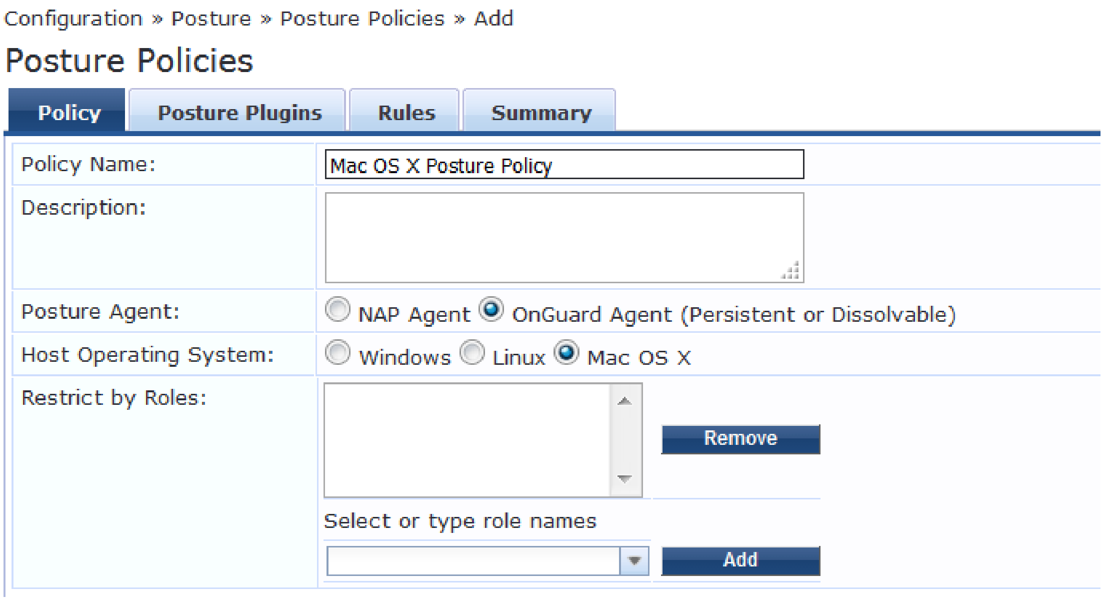
ClearPass Macintosh OS X Universal System Health Validator: OnGuard Agent

To configure the ClearPass Universal System Health Validator for Macintosh OS X:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**, then click **Add**.

   The **Add Posture Policies** dialog appears.

Figure 286: *Adding a Universal System Health Validator for a Mac OS X Posture Policy*



Configuration » Posture » Posture Policies » Add

Posture Policies

Policy Name: Mac OS X Posture Policy

Description:

Posture Agent: ○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable)

Host Operating System: ○ Windows ○ Linux ● Mac OS X

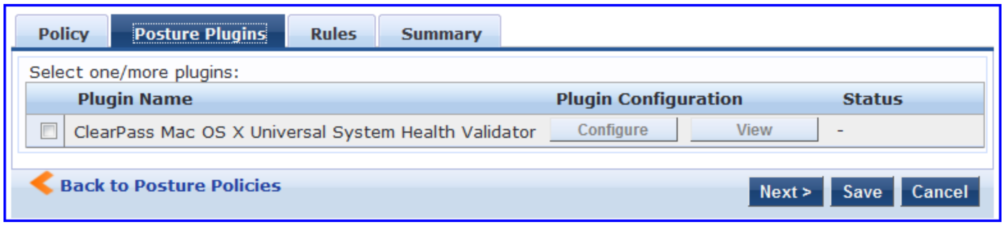
Restrict by Roles:

Select or type role names

2. Specify the following:
   a. **Policy Name/Description**: Enter the name and a description of the posture policy.
   b. **Posture Agent**: Select **OnGuard Agent.**
   c. **Host Operating System**: Select **Mac OS X.**
3. Click **Next**.

The **Posture Plugins** dialog appears.

Figure 287: *Selecting the Mac OS X Universal System Health Validator Posture Plug-in*



Select one/more plugins:

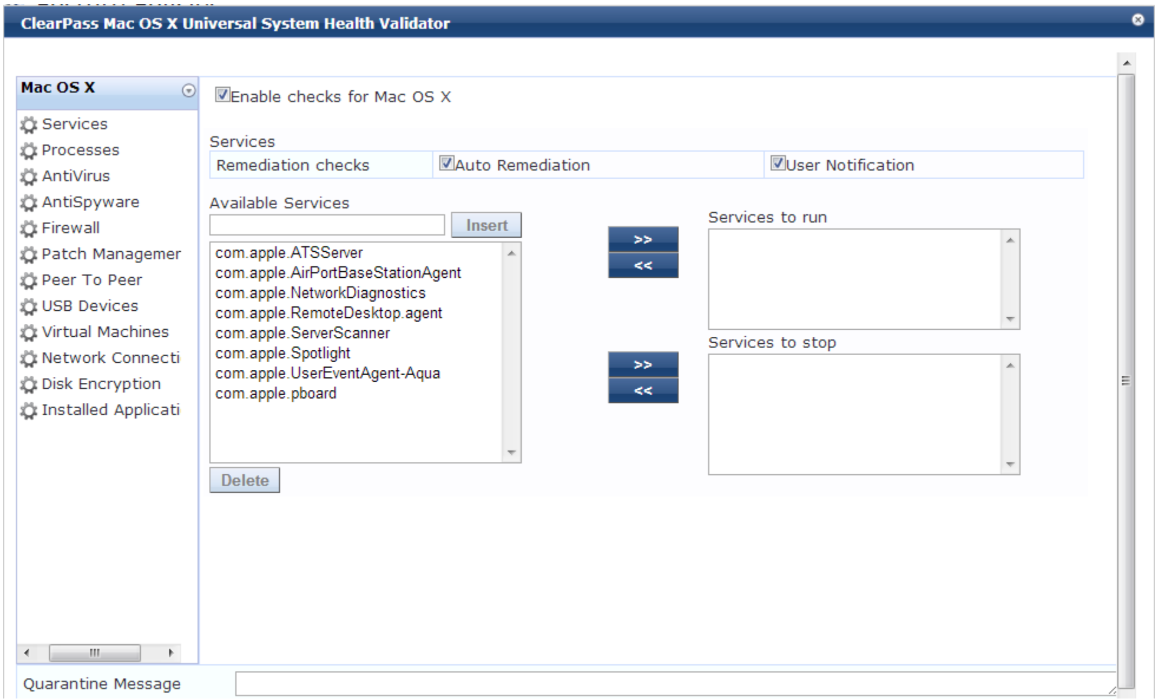
	Plugin Name	Plugin Configuration		Status
☐	ClearPass Mac OS X Universal System Health Validator	Configure	View	-

4. In the **Posture Plugins** page, click the check box for **ClearPass Mac OS X Universal System Health Validator**.
5. Click **Configure**.

   The **ClearPass Mac OS X Universal System Health Validator** configuration page is displayed.
6. To enable checks for Mac OS X, select the **Enable checks for Mac OS X** check box.

   The following configuration page appears:

Figure 288: *Configuration Page: Mac OS X Universal System Health Validator*



☑ Enable checks for Mac OS X

Services

Remediation checks ☑ Auto Remediation ☑ User Notification

Available Services

com.apple.ATSServer
com.apple.AirPortBaseStationAgent
com.apple.NetworkDiagnostics
com.apple.RemoteDesktop.agent
com.apple.ServerScanner
com.apple.Spotlight
com.apple.UserEventAgent-Aqua
com.apple.pboard

Services to run

Services to stop

Quarantine Message

Enabling these check boxes display a corresponding set of configuration pages that are described in the following sections.

- Services on page 318
- Processes on page 318
- Antivirus on page 319
- AntiSpyware on page 320
- Firewall on page 321
- Patch Management on page 321
- USB Devices on page 322
- Virtual Machine on page 323
- Network Connections on page 323

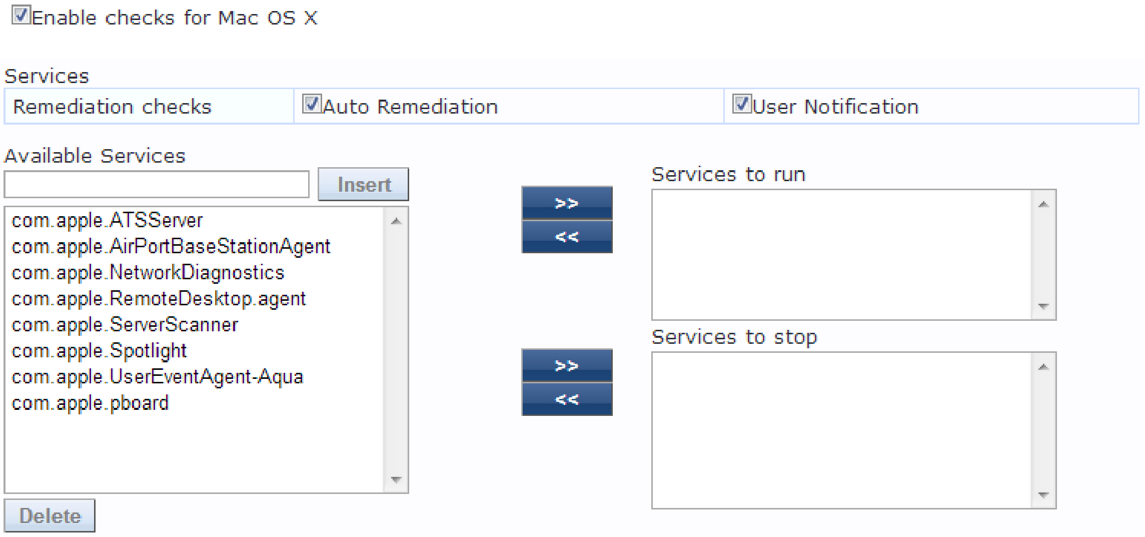
- Disk Encryption on page 324
- Installed Applications on page 325
- File Check on page 328

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 273 for description of the fields on this page.

The following figure displays the **Services** health class configuration page:

Figure 289: *Services Health Class Configuration Page*



☑Enable checks for Mac OS X

Services

Remediation checks	☑Auto Remediation	☑User Notification

Available Services

com.apple.ATSServer
com.apple.AirPortBaseStationAgent
com.apple.NetworkDiagnostics
com.apple.RemoteDesktop.agent
com.apple.ServerScanner
com.apple.Spotlight
com.apple.UserEventAgent-Aqua
com.apple.pboard

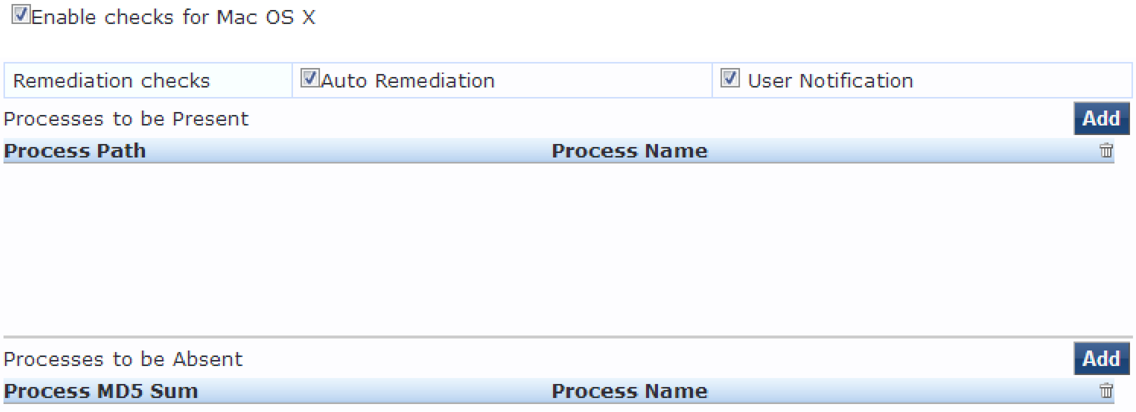
Services to run

Services to stop

Processes

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 290: *Processes Page*



☑Enable checks for Mac OS X

Remediation checks	☑Auto Remediation	☑ User Notification

Processes to be Present

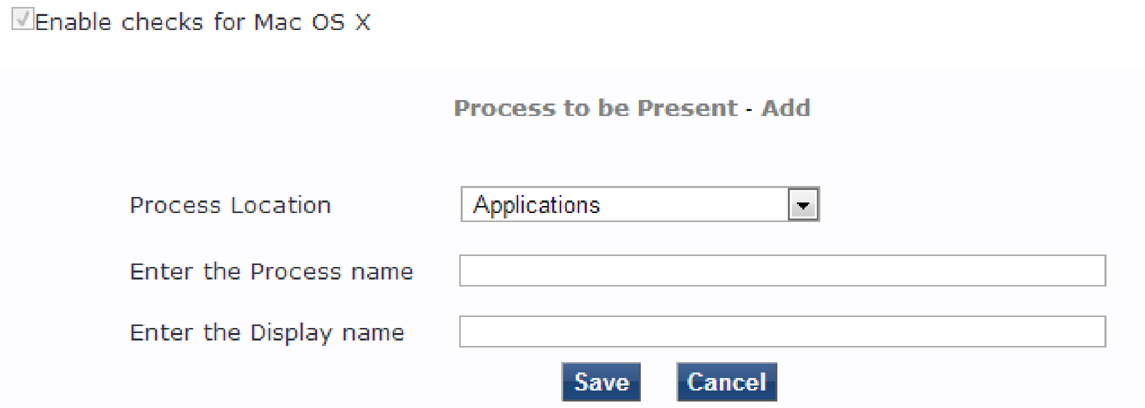
Process Path	Process Name

Processes to be Absent

Process MD5 Sum	Process Name

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 291: *Processes to be Present - Add Page*



☑ Enable checks for Mac OS X

Process to be Present - Add

Process Location: Applications

Enter the Process name:

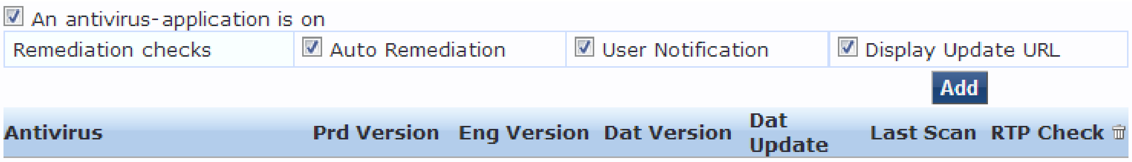
Enter the Display name:

Antivirus

In the **Antivirus** page, you can specify 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 292: *Antivirus Page (Detail 1)*



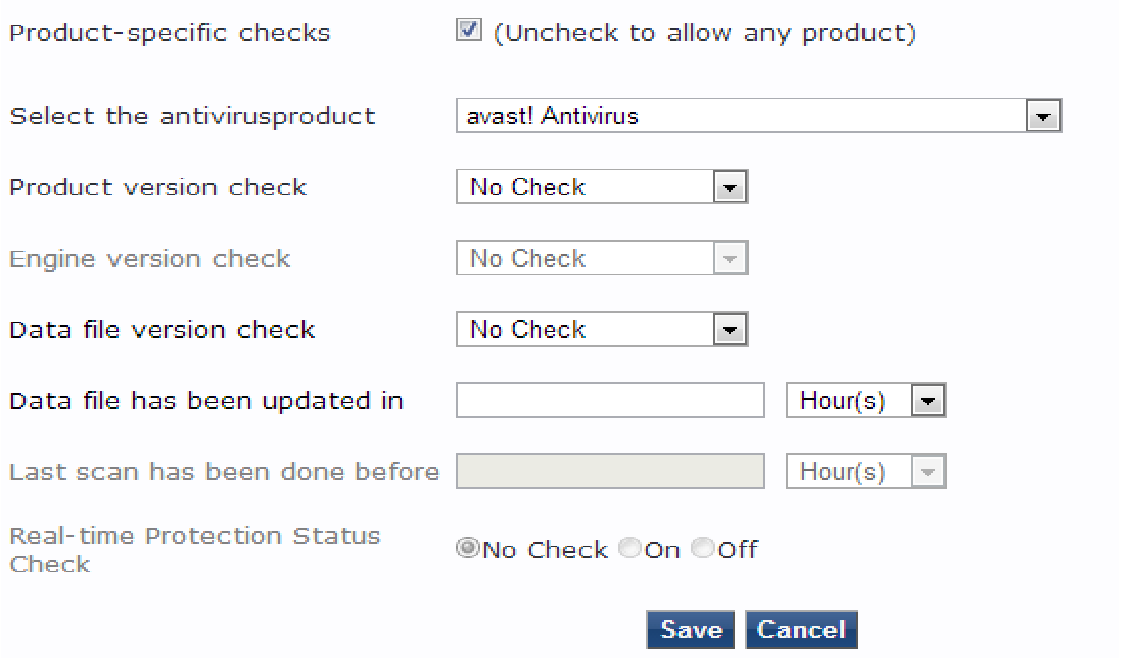
☑ An antivirus-application is on

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

Antivirus	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	RTP Check

Click **Add** to specify product and version check information in the antivirus configuration page.

Figure 293: *Antivirus Configuration Page (Detail 2)*



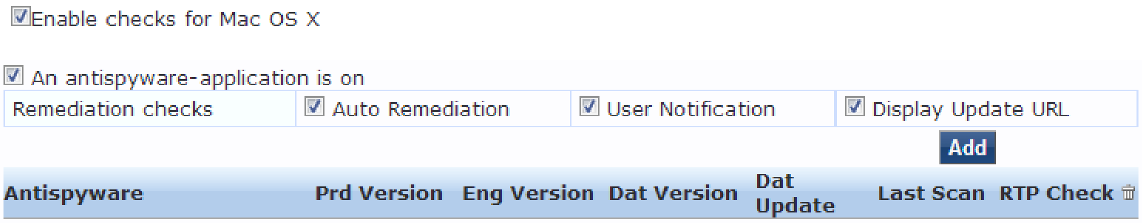
Product-specific checks	☑ (Uncheck to allow any product)
Select the antivirusproduct	avast! Antivirus
Product version check	No Check
Engine version check	No Check
Data file version check	No Check
Data file has been updated in	Hour(s)
Last scan has been done before	Hour(s)
Real-time Protection Status Check	● No Check ○ On ○ Off

When you save your antivirus configuration, it appears in the **Antivirus** page list. See ClearPass Windows Universal System Health Validator > OnGuard Agent on page 273 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 294: *Anti-Spyware Page*



☑ Enable checks for Mac OS X

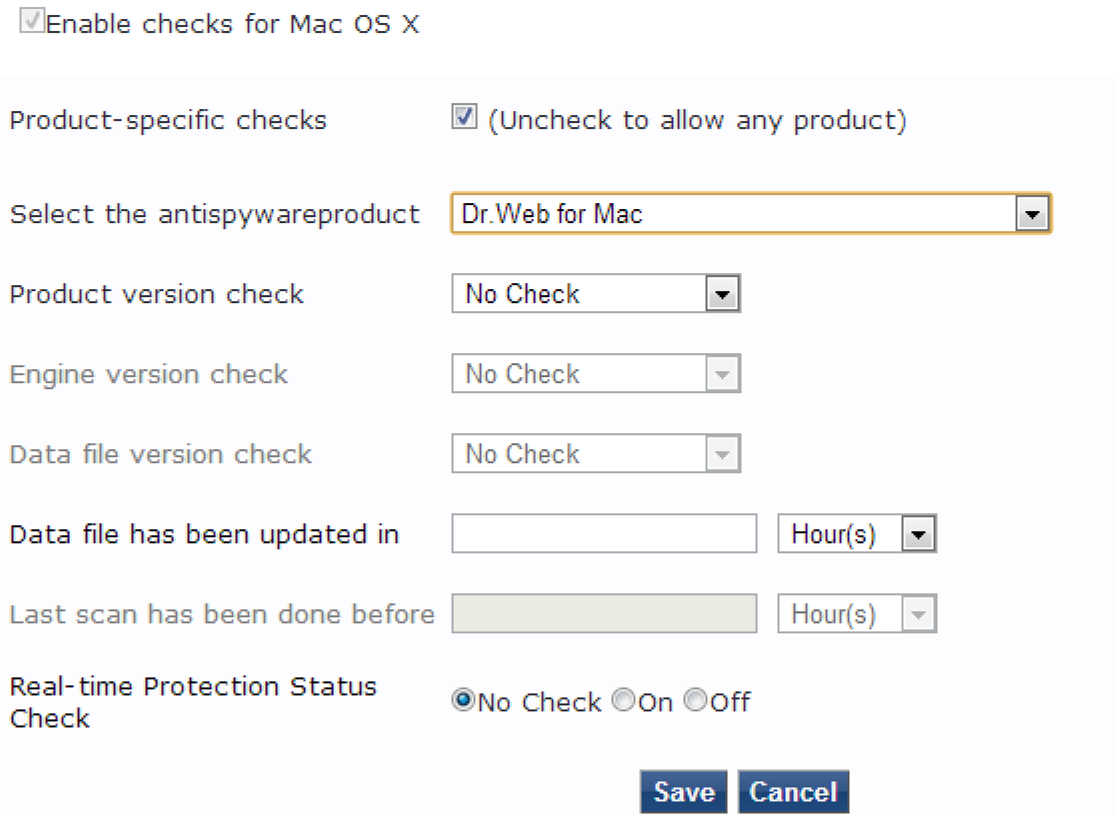
☑ An antispyware-application is on

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

Antispyware	Prd Version	Eng Version	Dat Version	Dat Update	Last Scan	RTP Check

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 295: *Anti-Spyware Add Page*



☑ Enable checks for Mac OS X

Product-specific checks	☑ (Uncheck to allow any product)
Select the antispywareproduct	Dr.Web for Mac
Product version check	No Check
Engine version check	No Check
Data file version check	No Check
Data file has been updated in	Hour(s)
Last scan has been done before	Hour(s)
Real-time Protection Status Check	● No Check ○ On ○ Off

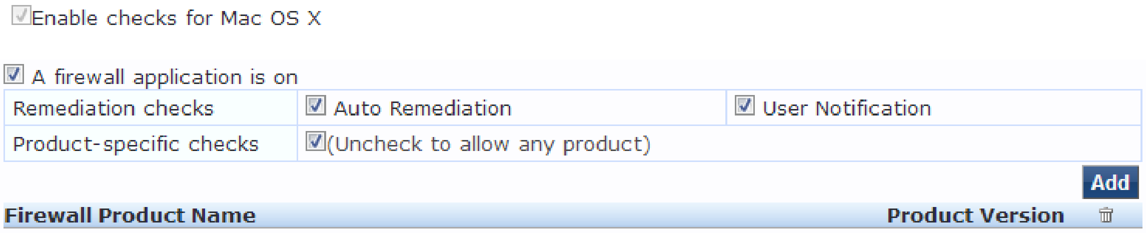
NOTE

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 296: *Firewall Page*



☑Enable checks for Mac OS X

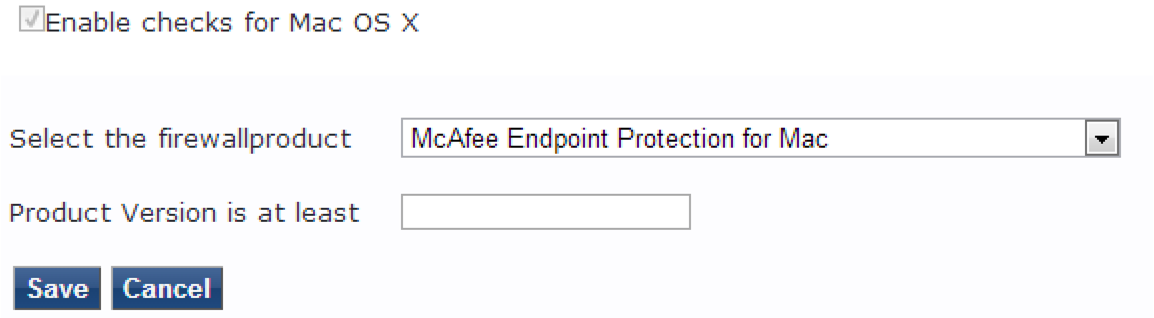
☑ A firewall application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☑(Uncheck to allow any product)	

Firewall Product Name	Product Version	

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 297: *Firewall Add Page*



☑Enable checks for Mac OS X

Select the firewallproduct: McAfee Endpoint Protection for Mac

Product Version is at least:

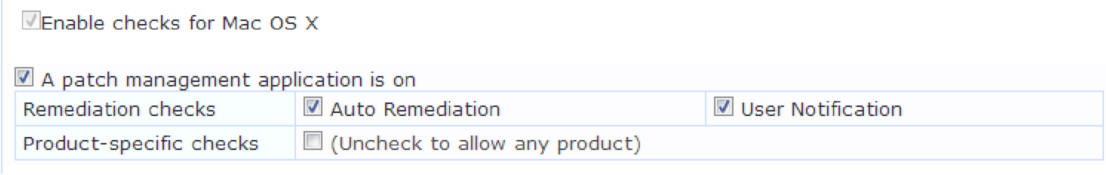
When enabled, the **Firewall** detail page appears. See ClearPass Windows Universal System Health Validator > OnGuard Agent on page 273 for firewall page and field descriptions.

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 298: *Patch Management Page*



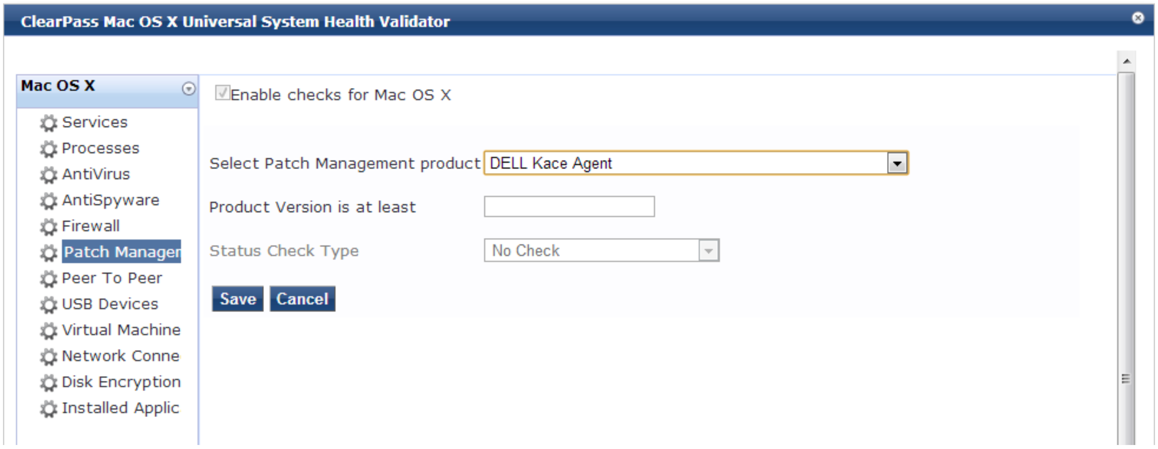
☑Enable checks for Mac OS X

☑ A patch management application is on

Remediation checks	☑ Auto Remediation	☑ User Notification
Product-specific checks	☐ (Uncheck to allow any product)	

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 299: *Patch Management - Add Page*



ClearPass Mac OS X Universal System Health Validator

☑ Enable checks for Mac OS X

Select Patch Management product: DELL Kace Agent

Product Version is at least:

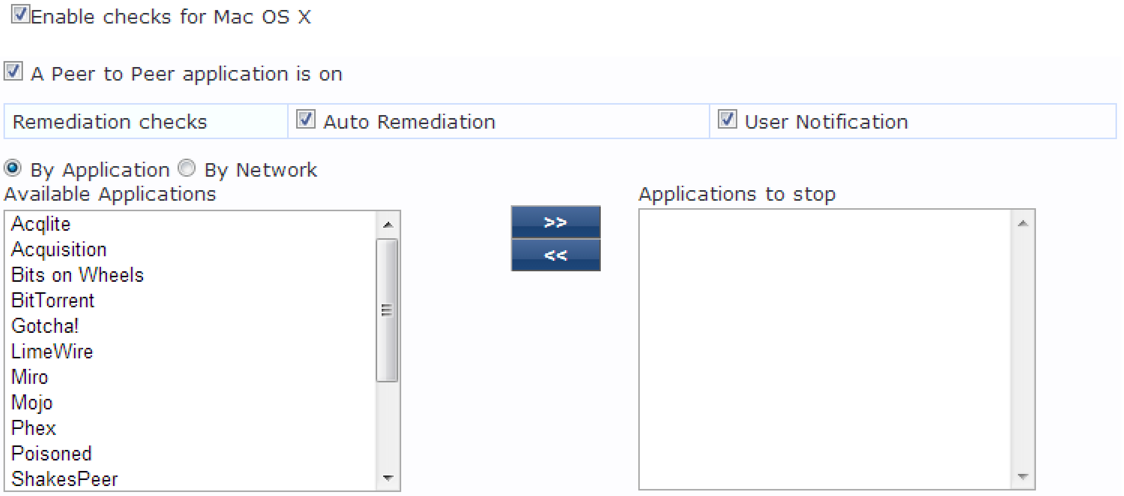
Status Check Type: No Check

Peer To Peer

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 300: *Peer To Peer Page*



☑ Enable checks for Mac OS X

☑ A Peer to Peer application is on

Remediation checks ☑ Auto Remediation ☑ User Notification

● By Application ○ By Network

Available Applications: Acqlite, Acquisition, Bits on Wheels, BitTorrent, Gotcha!, LimeWire, Miro, Mojo, Phex, Poisoned, ShakesPeer

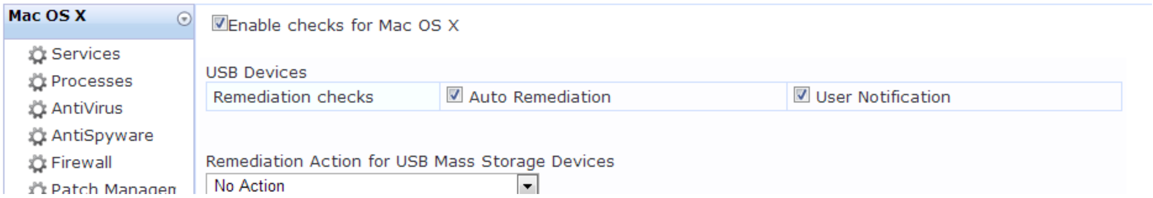
Applications to stop:

USB Devices

Use this page to configure 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 301: *USB Devices Page*



Mac OS X

- Services
- Processes
- AntiVirus
- AntiSpyware
- Firewall
- Patch Managen

☑Enable checks for Mac OS X

USB Devices

Remediation checks	☑ Auto Remediation	☑ User Notification

Remediation Action for USB Mass Storage Devices

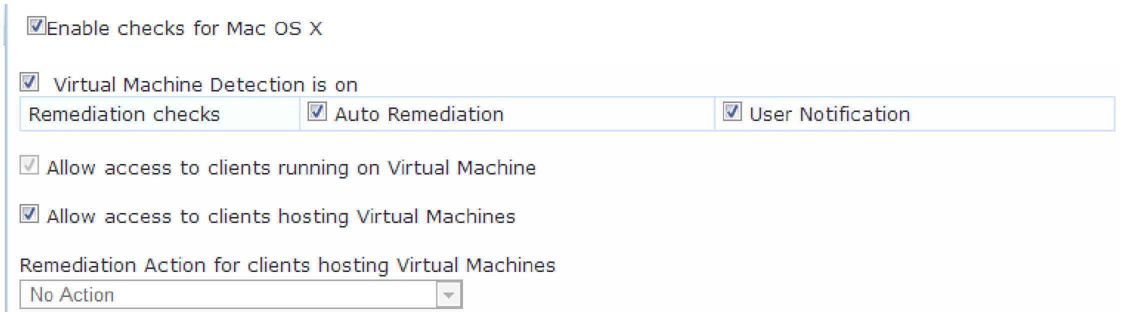
No Action

Virtual Machine

The **Virtual Machines** page provides configuration 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 302: *Virtual Machine Page*



☑Enable checks for Mac OS X

☑ Virtual Machine Detection is on

Remediation checks	☑ Auto Remediation	☑ User Notification

☑ Allow access to clients running on Virtual Machine

☑ Allow access to clients hosting Virtual Machines

Remediation Action for clients hosting Virtual Machines

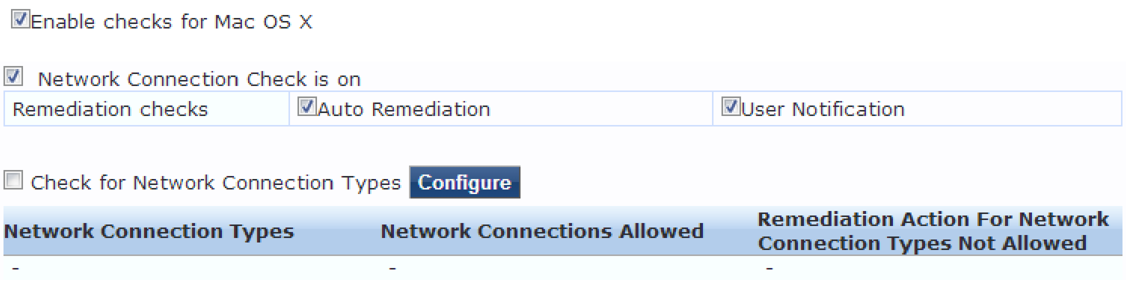
No Action

Network Connections

The **Network Connections** page provides configuration 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 303: *Network Connections Page*



☑Enable checks for Mac OS X

☑ Network Connection Check is on

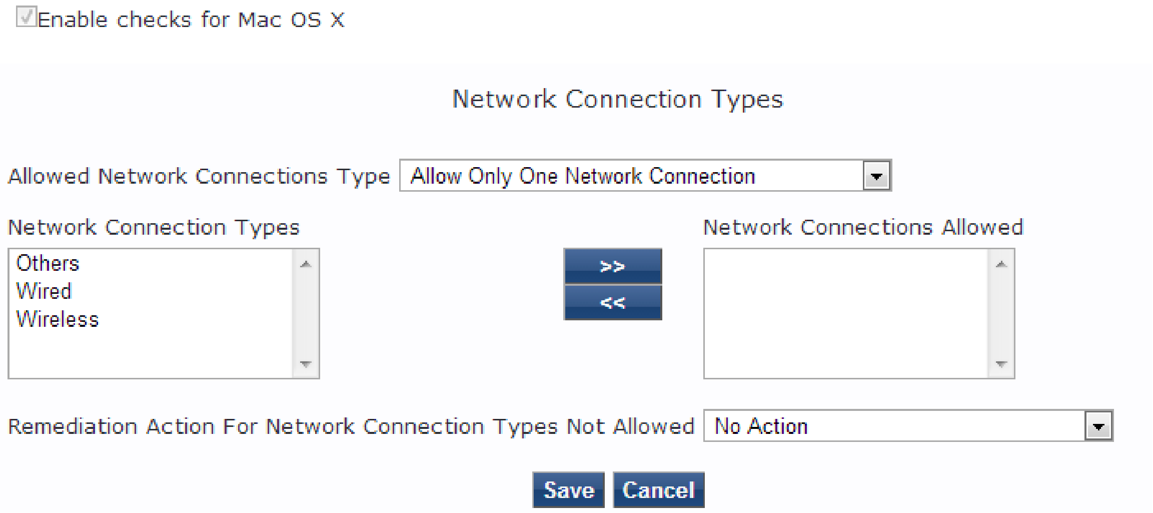
Remediation checks	☑Auto Remediation	☑User Notification

□ Check for Network Connection Types

Network Connection Types	Network Connections Allowed	Remediation Action For Network Connection Types Not Allowed
-	-	-

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 304: *Network Connections Configuration Page*



☑ Enable checks for Mac OS X

Network Connection Types

Allowed Network Connections Type: Allow Only One Network Connection

Network Connection Types: Others, Wired, Wireless

Network Connections Allowed:

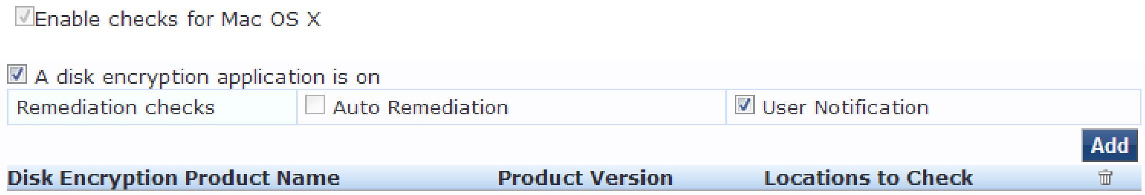
Remediation Action For Network Connection Types Not Allowed: No Action

Disk Encryption

Disk encryption is a technology that protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

The following figure displays the **Disk Encryption** page:

Figure 305: *Disk Encryption Page*



☑ Enable checks for Mac OS X

☑ A disk encryption application is on

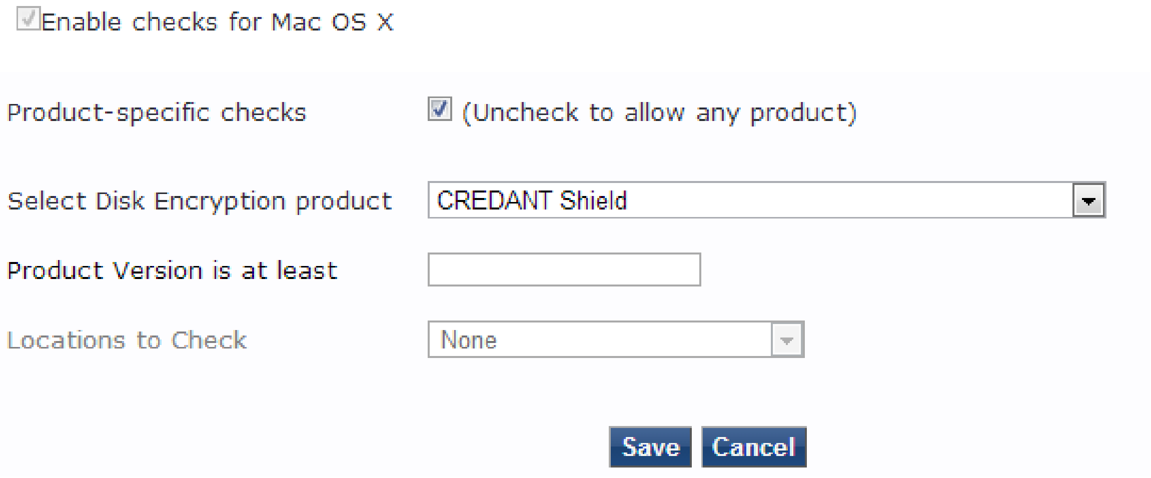
Remediation checks	□ Auto Remediation	☑ User Notification

Disk Encryption Product Name	Product Version	Locations to Check	🗑

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 306: *Disk Encryption Add Page*



☑ Enable checks for Mac OS X

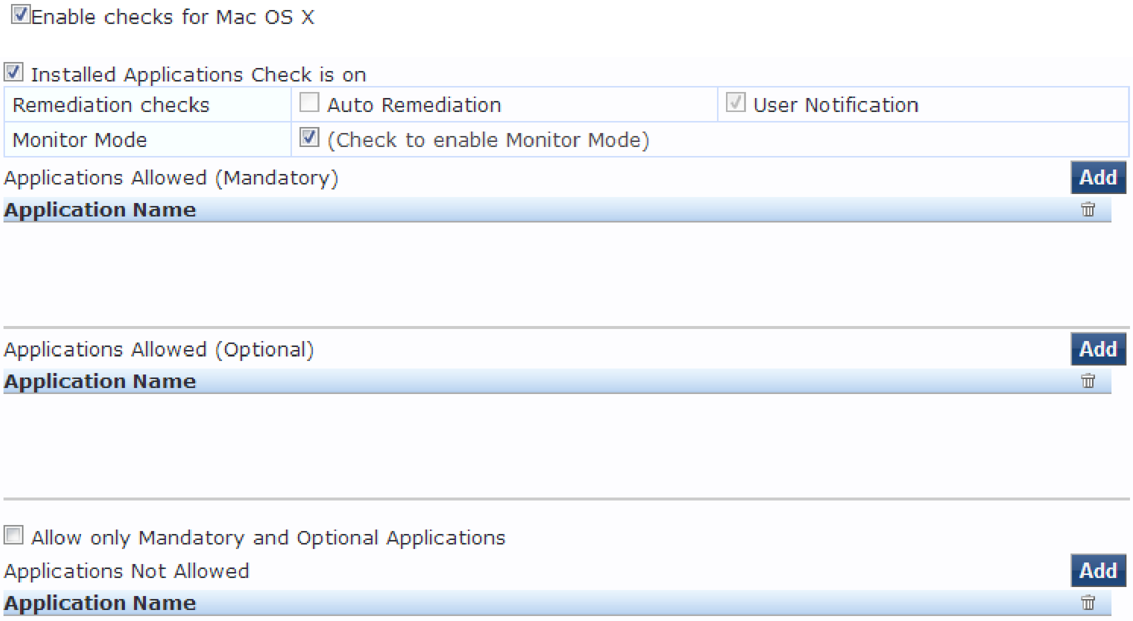
Product-specific checks	☑ (Uncheck to allow any product)
Select Disk Encryption product	CREDANT Shield
Product Version is at least	
Locations to Check	None

Installed Applications

The **Installed Applications** category groups classes that represent software-related objects.

From the **Installed Applications** page, you can specify information about which installed applications you want to monitor.

Figure 307: *Installed Applications Page for Macinstosh OS X*



☑ Enable checks for Mac OS X

☑ Installed Applications Check is on

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	☑ (Check to enable Monitor Mode)	

Applications Allowed (Mandatory)

Application Name

Applications Allowed (Optional)

Application Name

□ Allow only Mandatory and Optional Applications

Applications Not Allowed

Application Name

The following table describes the **Installed Applications for Mac OSX Configuration** page parameters:

Table 160: *Installed Applications for Mac OS X Configuration Page Parameters*

Parameter	Action/Description
Remediation checks	**Auto-Remediation** for the Installed Applications health class is not supported.
User Notification	1. Enable sending a remediation message with a list of applications to install or uninstall to the user.
Monitor Mode	2. Enable **Monitor Mode** to treat all the installed applications as always healthy.
Applications Allowed (Mandatory)	3. Specify installed applications to be monitored on a mandatory basis. **NOTE:** Enter the application names as they are shown in Add/Remove Programs.
Applications Allowed (Optional)	4. Specify installed applications to be monitored on an optional basis. **NOTE:** Enter the application name as they are shown in Add/Remove Programs.
Allow only Mandatory and Optional Applications	5. Specify that only the mandatory and optional applications are monitored. **NOTE:** All applications that are not either mandatory or optional must be removed or uninstalled.

Enabling Regular Expressions for a Mac OS X Application

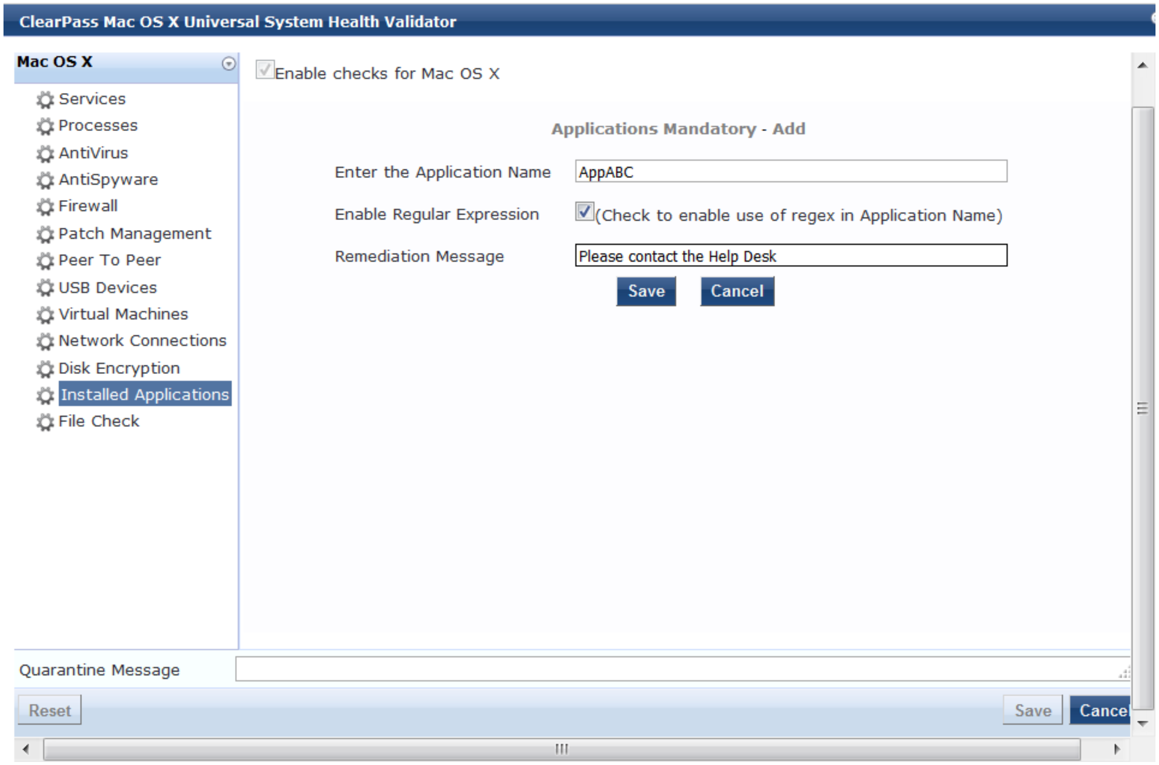
To enable regular expressions for an application:

1. From the **ClearPass Windows Universal System Health Validator** > **Configure** page (see ClearPass Macintosh OS X Universal System Health Validator: OnGuard Agent on page 316), select **Installed Applications**.
2. Click (enable) the **Installed Applications Check is on** check box.

   The Installed Applications dialog appears (see above).
3. From the desired **Applications Allowed** category, click **Add**.

   The Mandatory Applications dialog appears for the selected **Applications Allowed** category (see Figure 308).

Figure 308: *Enabling Regular Expression*



☑ Enable checks for Mac OS X

Applications Mandatory - Add

Enter the Application Name: AppABC

Enable Regular Expression: ☑ (Check to enable use of regex in Application Name)

Remediation Message: Please contact the Help Desk

Save Cancel

Quarantine Message

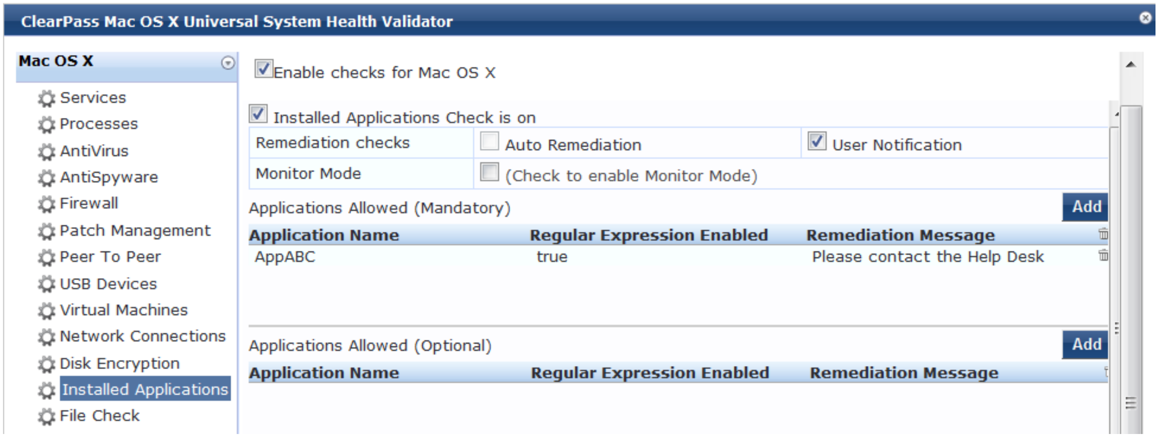
4. Configure the **Add Mandatory Applications** parameters as described in Table 161.

Table 161: *Add Mandatory Applications Parameters*

Parameter	Action/Description
Enter the Application Name	1. Enter the name of the application.
Enable Regular Expression	2. Check (enable) this check box to enable the use of regular expressions in the **Application Name**. When this field is enabled, ClearPass treats the **Application Name** as regular expression when comparing application names.
Remediation Message	3. Optionally, enter the remediation message that will be displayed to the user in the event of an error. **NOTE:** Remedition messages can include reasons for remediation, links to helpful URLs and helpdesk contact information.
	4. Click **Save**.

You return to the **Installed Applications** dialog, where **Regular Expression Enabled** is set to **true** for the specified application (see Figure 309).

Figure 309: *Regular Expression Enabled*



☑ Enable checks for Mac OS X

☑ Installed Applications Check is on

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

Applications Allowed (Mandatory)

Application Name	Regular Expression Enabled	Remediation Message
AppABC	true	Please contact the Help Desk

Applications Allowed (Optional)

Application Name	Regular Expression Enabled	Remediation Message

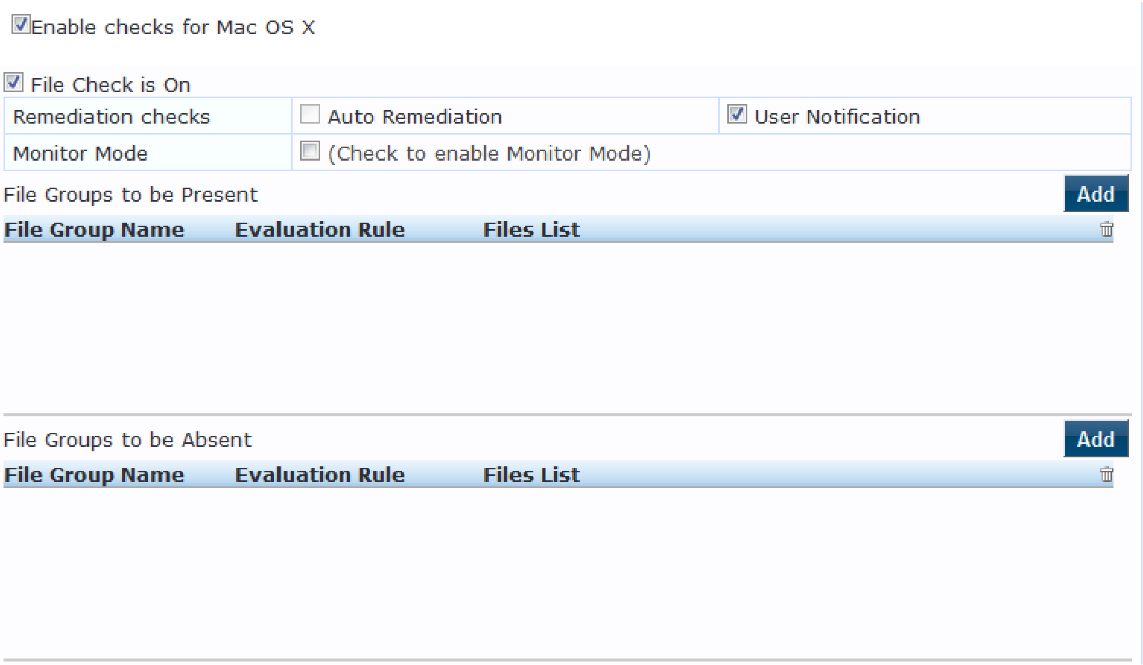
File Check

From the **File Check** page, you can turn on the file check feature and specify information about which the files you want to check.

Use the **File Check** page to verify the group of files to be present or absent.

The following figure is an example of the **File Check** health class configuration dialog:

Figure 310: *Mac OS X File Check Health Class Configuration*



☑ Enable checks for Mac OS X

☑ File Check is On

Remediation checks	□ Auto Remediation	☑ User Notification
Monitor Mode	□ (Check to enable Monitor Mode)	

File Groups to be Present

File Group Name	Evaluation Rule	Files List

File Groups to be Absent

File Group Name	Evaluation Rule	Files List

The following table describes the **File Check Configuration** parameters:

Table 162: *File Check Configuration Parameters*

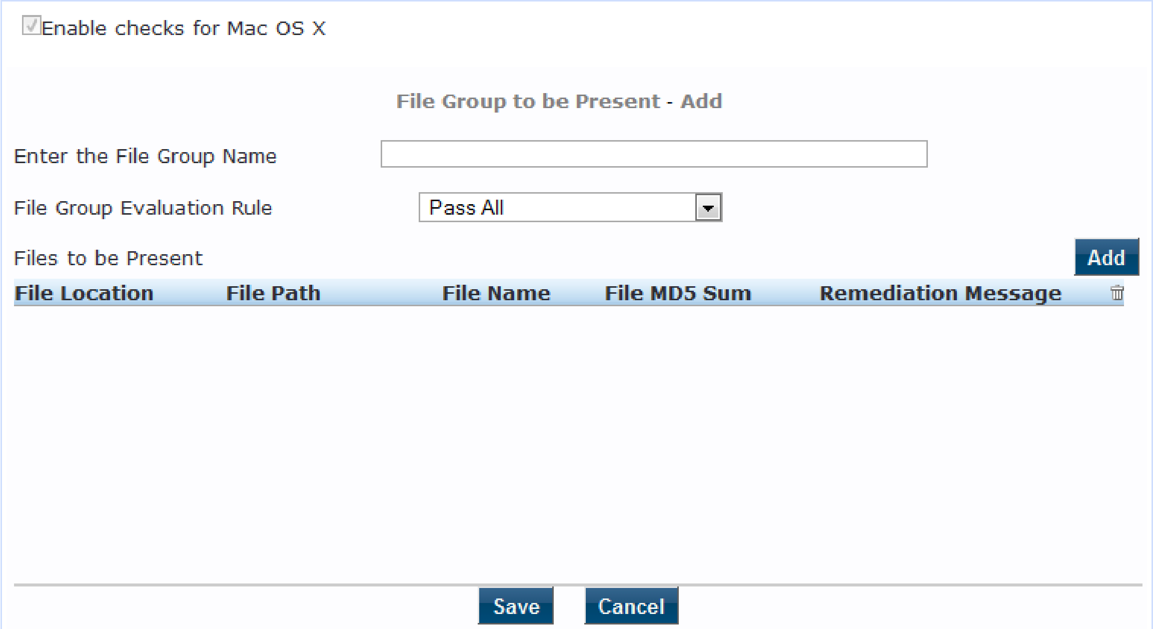
Parameter	Action/Description
Remediation checks	Auto-remediation for the **File Check** health class is not supported.
User Notification	1. When enabled, a remediation message that includes the groups of files to be present or absent is displayed to the end user.
Monitor Mode	2. To treat all the file check health classes as always healthy, enable **Monitor Mode**.
File Groups to be Present	3. To add the files to be present in the **File Check** health class, click **Add**.
File Groups to be Absent	4. To add the files to be absent in the **File Check** health class, click **Add**.

1. To open the **File Group to be Present > Add** page, click **Add**:

   You can configure the name of the file group and specify the evaluation rule for the file group.

   The following figure displays the **File Group to Be Present > Add** dialog:

Figure 311: *MacOSX File Group to Be Present > Add Dialog*



☑ Enable checks for Mac OS X

File Group to be Present - Add

Enter the File Group Name

File Group Evaluation Rule: Pass All

Files to be Present

File Location	File Path	File Name	File MD5 Sum	Remediation Message

The following table describes the **File Group to Be Present > Add** parameters:

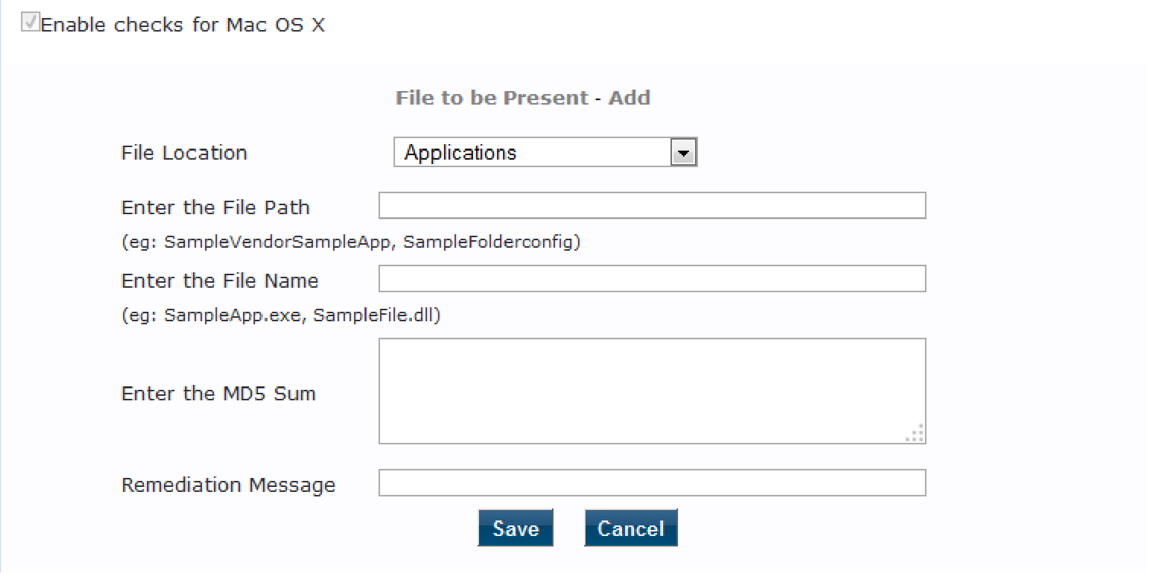
Table 163: *File Group to Be Present > Add Parameters*

Parameter	Action/Description
Enter the File Group Name	1. Enter the name of the file group.
File Group Evaluation Rule	2. Select the appropriate 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 if any one of the configured file groups are present.

3. To configure the name of the file group and the evaluation rule for the file group, from **File Groups to be Present**, click **Add**.

   The following figure displays the **File to Be Present > Add** page:

Figure 312: *File to be Present > Add Dialog*



☑ Enable checks for Mac OS X

File to be Present - Add

File Location: Applications

Enter the File Path:

(eg: SampleVendorSampleApp, SampleFolderconfig)

Enter the File Name:

(eg: SampleApp.exe, SampleFile.dll)

Enter the MD5 Sum:

Remediation Message:

The following table describes the **File to Be Present > Add** parameters:

Table 164: *File to Be Present > Add Parameters*

Parameter	Action/Description
File Location	1. Select any location of the file from the drop-down list: ● Applications ● UserBin ● UserLocalBin ● UserSBin ● None
Enter the File Path	2. Enter the file path as described in the examples from the GUI.
Enter the File Name	3. Enter the name of the file.

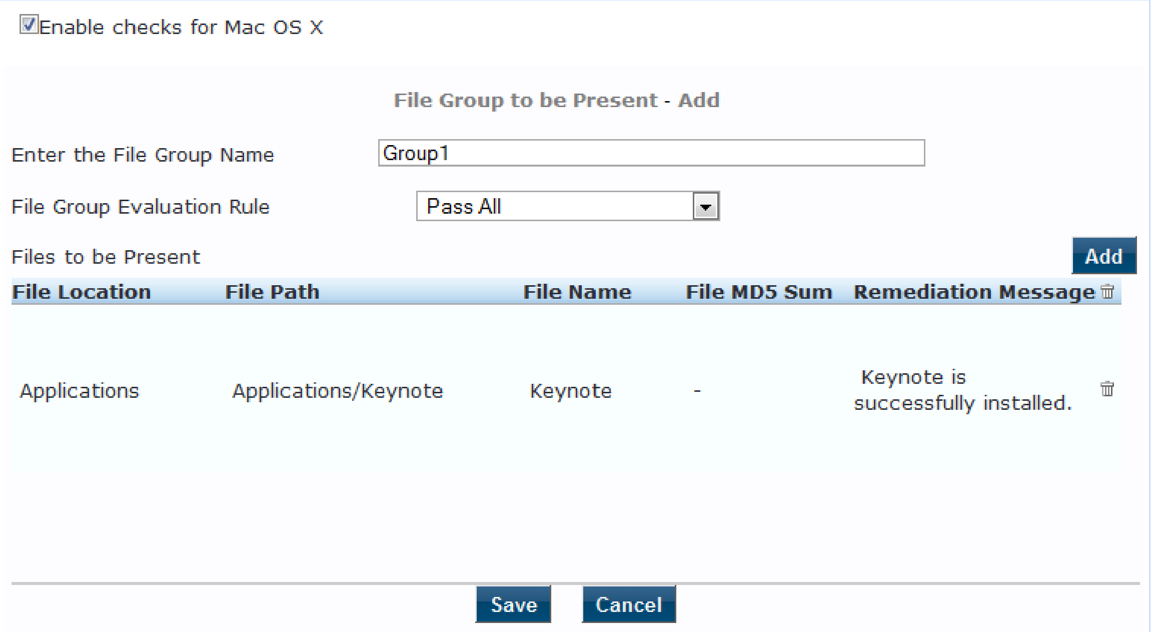
Table 164: *File to Be Present > Add Parameters (Continued)*

Parameter	Action/Description
Enter the MD5 Sum	Optionally, you can specify one or more (comma separated) MD5 checksums of the process executable file.
Remediation Message	4. Specify the custom remediation message to be displayed to end users if **File check** fails.

5. When finished, click **Save**.

   The parameters configured in the **File to Be Present > Add** dialog are reflected in the **File Groups to be Present** dialog as illustrated in the following figure:

Figure 313: *File Group to Be Present Parameters Displayed*



☑ Enable checks for Mac OS X

File Group to be Present - Add

Enter the File Group Name: Group1

File Group Evaluation Rule: Pass All

Files to be Present

File Location	File Path	File Name	File MD5 Sum	Remediation Message
Applications	Applications/Keynote	Keynote	-	Keynote is successfully installed.

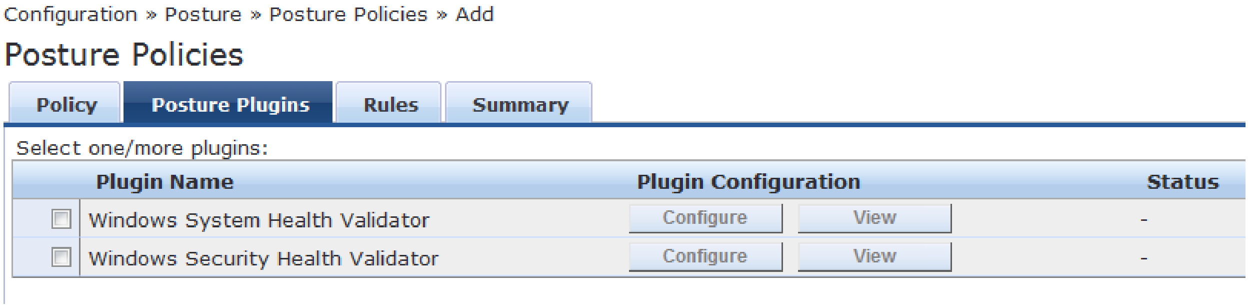
Configuring NAP Agent Plugins

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 332
- Windows Security Health Validator: NAP Agent on page 333

The following figure displays the **NAP Agent - Posture Plugins** tab:

Figure 314: *NAP Agent - Posture Plugins Options*



Configuration » Posture » Posture Policies » Add

Posture Policies

Select one/more plugins:

	Plugin Name	Plugin Configuration		Status
☐	Windows System Health Validator	Configure	View	-
☐	Windows Security Health Validator	Configure	View	-

Windows System Health Validator: NAP Agent

The Windows System Health Validator NAP (Network Access Protection) Agent checks for the level of Windows Service Packs.

To configure the minimum service pack level required, perform the following steps:

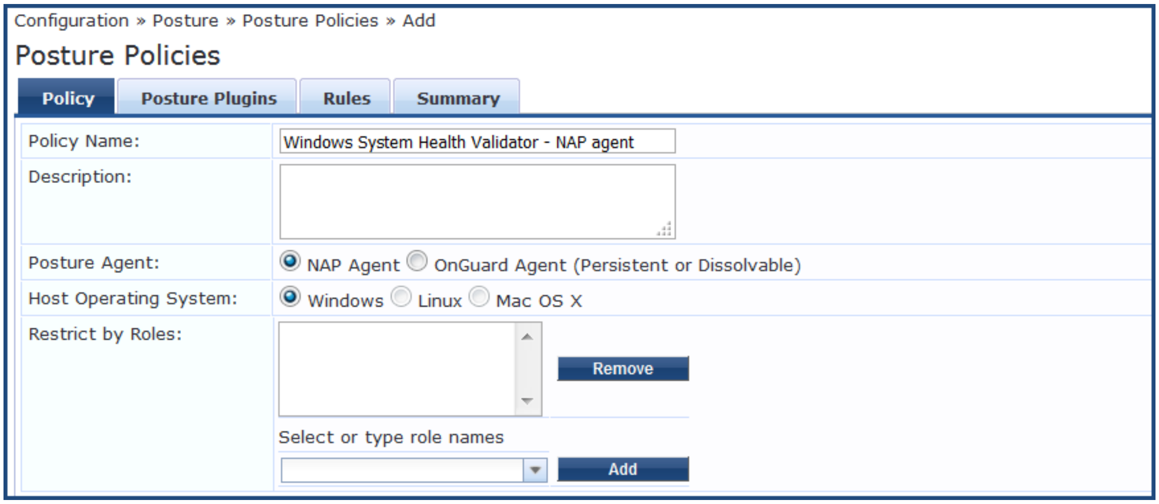
1. Navigate to **Configuration** > **Posture** > **Posture Policies**.

   The **Posture Policies** page appears.

2. Click **Add**.

   The **Add Posture Policies** > **Policy** dialog opens.

Figure 315: *Adding a Windows NAP Agent Posture Policy*



Policy Name: Windows System Health Validator - NAP agent

Description:

Posture Agent: ● NAP Agent ○ OnGuard Agent (Persistent or Dissolvable)

Host Operating System: ● Windows ○ Linux ○ Mac OS X

Restrict by Roles:

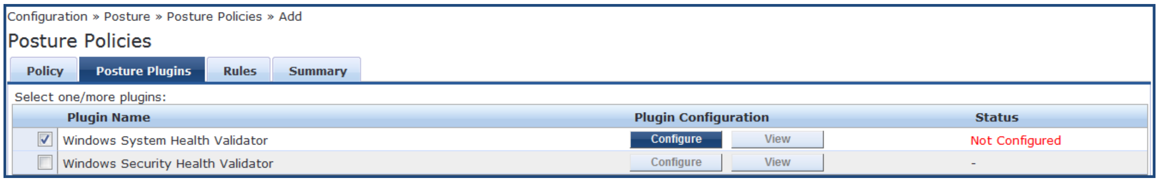
Select or type role names

3. Specify the following:
   a. **Policy Name/Description**: Enter the name and description of the posture policy.
   b. **Posture Agent**: Select **NAP Agent.**
   c. **Host Operating System**: Select **Windows.**

4. Click **Next**.

   The **Posture Policies** > **Posture Plugins** page opens.

Figure 316: *Posture Plugins for Windows Health Validators*



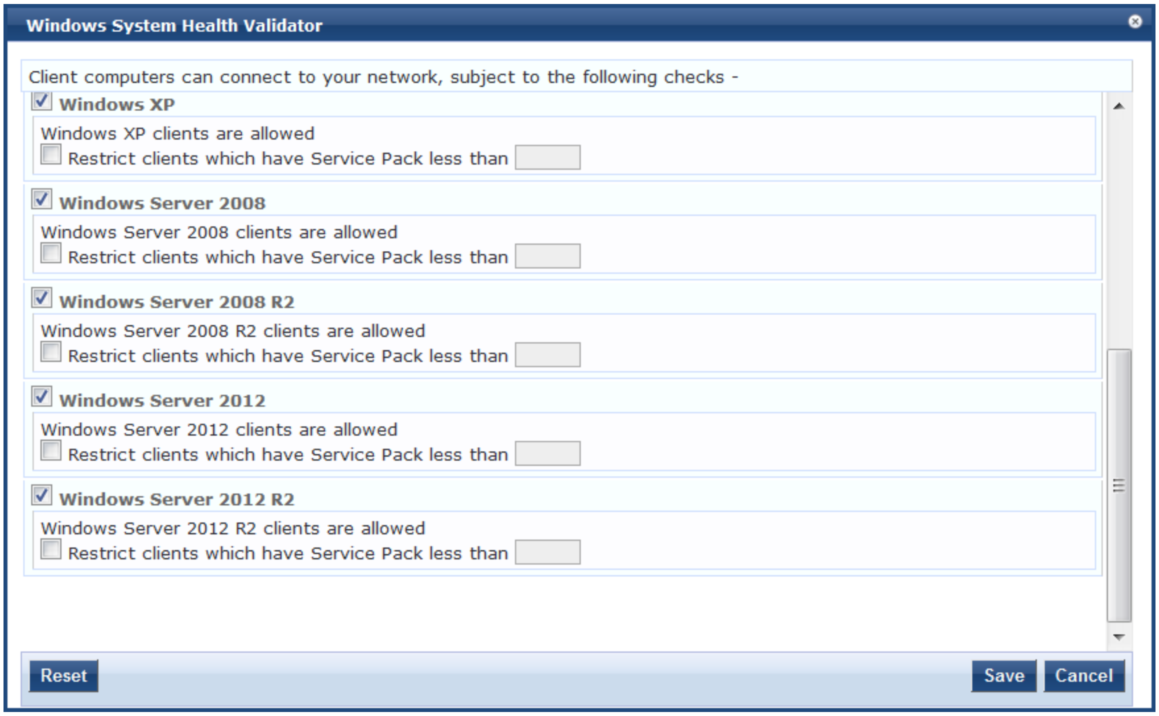
Select one/more plugins:

	Plugin Name	Plugin Configuration		Status
☑	Windows System Health Validator	Configure	View	Not Configured
□	Windows Security Health Validator	Configure	View	-

5. From the **Posture Plugins** tab, select **Windows System Health Validator**, then click the **Configure** button.

   The **Windows System Health Validator** page appears:

Figure 317: *Onguard NAP Agent: Windows System Health Validator*



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

☑ Windows XP

Windows XP clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows Server 2008

Windows Server 2008 clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows Server 2008 R2

Windows Server 2008 R2 clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows Server 2012

Windows Server 2012 clients are allowed

□ Restrict clients which have Service Pack less than

☑ Windows Server 2012 R2

Windows Server 2012 R2 clients are allowed

□ Restrict clients which have Service Pack less than

6. To enable support of specific Windows operating systems, click the corresponding check boxes.
7. Enable the **Restrict clients...** check box and specify the minimum Service Pack level required on the client computer to connect to your network.
8. Click **Save**.

   You return to the Posture Plugins page where the status of the plug-in is now set to **Configured**.

Windows Security Health Validator: NAP Agent

The Windows Security Health Validator: NAP (Network Access Protection) Agent checks for the presence of specific types of security applications. You can use the check boxes to restrict access based on the absence of the selected security application types.

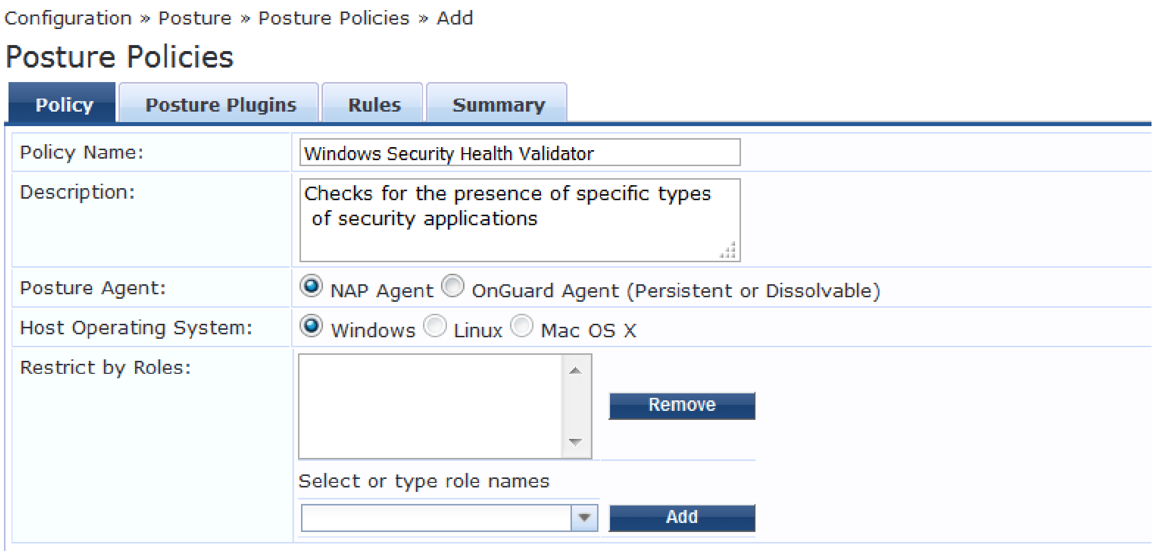
To configure the minimum service pack level required, perform the following steps:

1. Navigate to **Configuration** > **Posture** > **Posture Policies**.

   The Posture Policies page appears.
2. Click **Add**.

   The Add Posture Policies dialog appears.

Figure 318: *Adding Windows Security Health Validator: NAP Agent Posture Policy*



Configuration » Posture » Posture Policies » Add

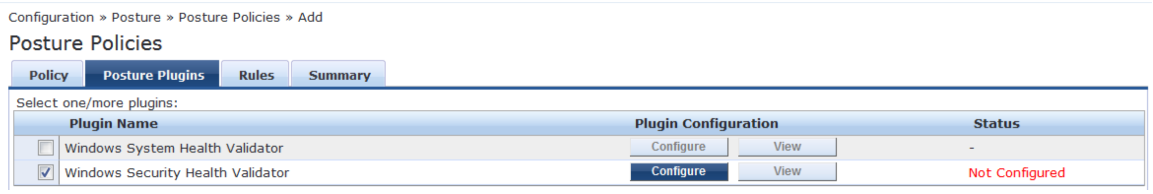
Posture Policies

Policy Name:	Windows Security Health Validator
Description:	Checks for the presence of specific types of security applications
Posture Agent:	● NAP Agent ○ OnGuard Agent (Persistent or Dissolvable)
Host Operating System:	● Windows ○ Linux ○ Mac OS X
Restrict by Roles:	Select or type role names

3. Specify the following:
   a. **Policy Name**: Enter the name of the posture policy.
   b. **Posture Agent**: Select **NAP Agent**.
   c. **Host Operating System**: Select **Windows**.
4. Click **Next**.

   The **Posture Policies** > **Posture Plugins** page appears.

Figure 319: *Selecting Posture Plugins for Windows Security Health Validator: NAP Agent*



Configuration » Posture » Posture Policies » Add

Posture Policies

Select one/more plugins:

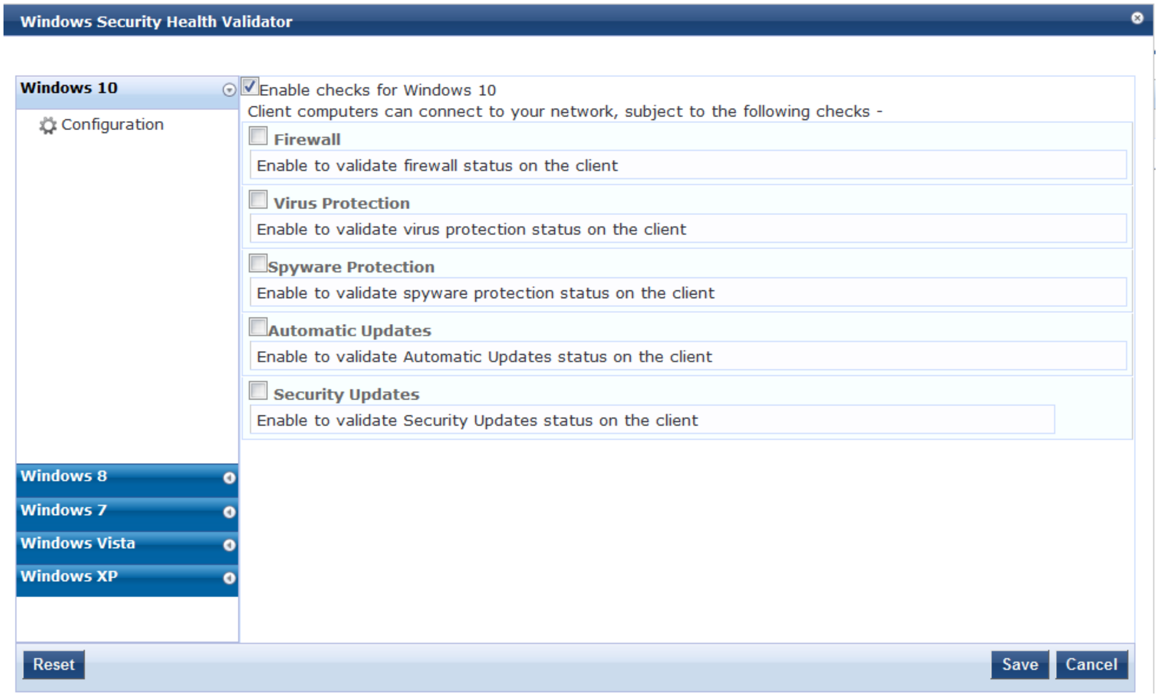
	Plugin Name	Plugin Configuration		Status
□	Windows System Health Validator	Configure	View	-
☑	Windows Security Health Validator	Configure	View	Not Configured

5. From the **Posture Plugins** page, select **Windows Security Health Validator**, then click **Configure**.

   The **Windows System Health Validator** page appears:.
6. Click the **Enable checks for Windows 10** check box.

   The Windows Security Health Validator configuration page appears as shown in Figure 320.

Figure 320: *Windows Security Health Validator*



Windows Security Health Validator

Windows 10

Configuration

☑ Enable checks for Windows 10

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

☐ **Firewall**

Enable to validate firewall status on the client

☐ **Virus Protection**

Enable to validate virus protection status on the client

☐ **Spyware Protection**

Enable to validate spyware protection status on the client

☐ **Automatic Updates**

Enable to validate Automatic Updates status on the client

☐ **Security Updates**

Enable to validate Security Updates status on the client

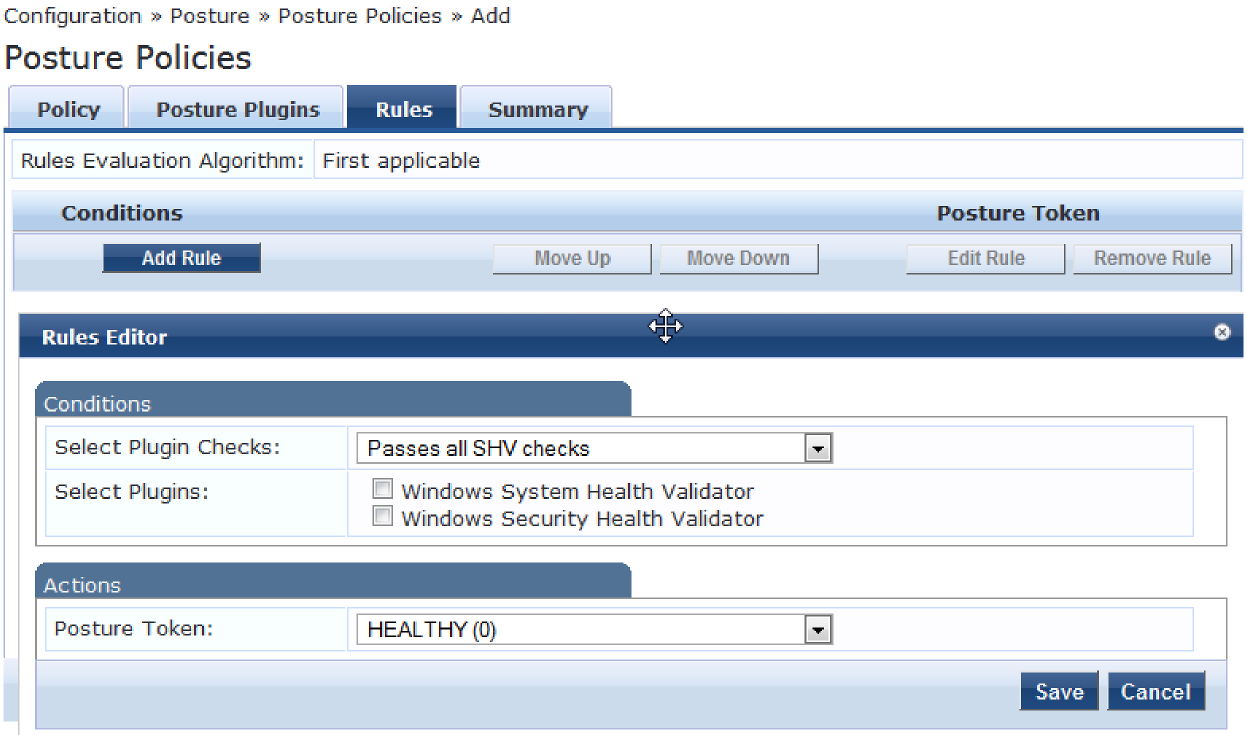
7. To enable support of specific operating systems, click the corresponding check boxes.
8. Click **Save**.

   You return to the **Posture Plugins** page where the status of the Windows Security Health Validator plug-in is now **Configured**.

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 321: *Posture Policy Rules Tab and Rules Editor*



Configuration » Posture » Posture Policies » Add

Posture Policies

Rules Evaluation Algorithm: First applicable

Rules Editor

Conditions

Select Plugin Checks: Passes all SHV checks

Select Plugins:

□ Windows System Health Validator

□ Windows Security Health Validator

Actions

Posture Token: HEALTHY (0)

The following table describes the **Rules Editor** configuration parameters:

Table 165: *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

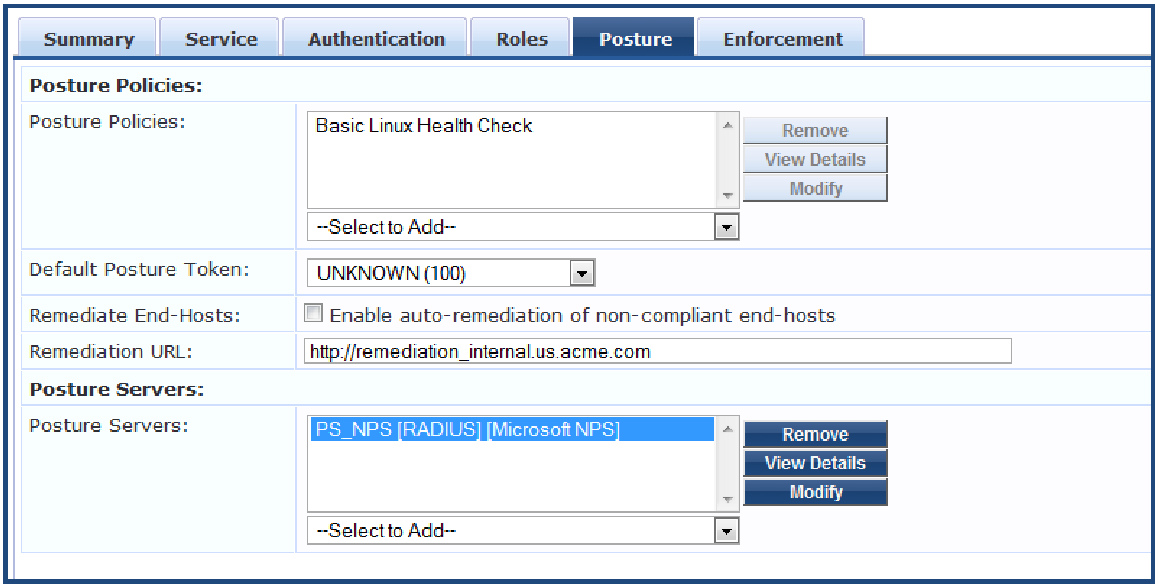
- Aruba hosted captive portal that performs posture checks through a dissolvable agent

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 322: *Posture Features at the Service Level*



Posture Policies:

Posture Policies: Basic Linux Health Check

--Select to Add--

Default Posture Token: UNKNOWN (100)

Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts

Remediation URL: http://remediation_internal.us.acme.com

Posture Servers:

Posture Servers: PS_NPS [RADIUS] [Microsoft NPS]

--Select to Add--

You can configure the following components of a posture:

Table 166: *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 269. • To edit the selected posture policy, click **Modify**. For more information, see Configuring Posture Policy Agents and Hosts on page 269.
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 166: *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 Adding and Modifying Posture Servers. ● To edit the selected posture server, click **Modify**. For more information, see Adding and Modifying Posture Servers.
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 Audit Servers

The ClearPass Policy Manager server contains default Nessus (v2.X through v6.x) and Nmap (Network Mapping) servers. For enterprises with existing audit server infrastructure, or with external audit servers, Policy Manager supports these servers externally.

For more information, see:

- Default Audit Servers on page 339
- Custom Audit Servers on page 342
- Post-Audit Rules on page 351

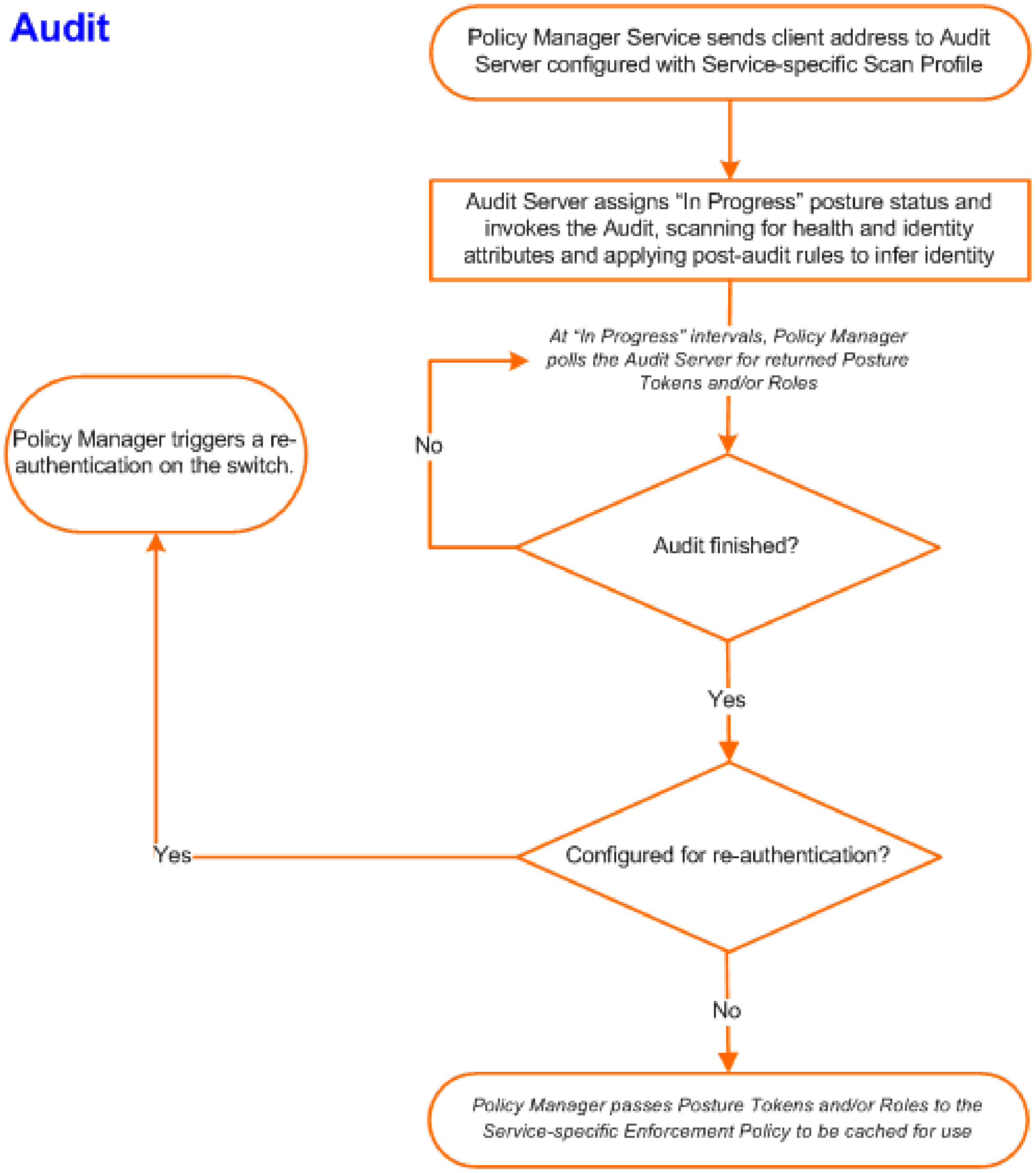
Audit Service Flow Control

Audit servers evaluate posture, role, or both for unmanaged or unmanageable clients. One example is clients that lack an adequate posture agent or an 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 below.

Figure 323: *Flow of Policy Manager Auditing Control*


Audit
Policy Manager Service sends client address to Audit Server configured with Service-specific Scan Profile
Audit Server assigns "In Progress" posture status and invokes the Audit, scanning for health and identity attributes and applying post-audit rules to infer identity
At "In Progress" intervals, Policy Manager polls the Audit Server for returned Posture Tokens and/or Roles
No
Audit finished?
Yes
Configured for re-authentication?
Yes
Policy Manager triggers a re-authentication on the switch.
No
Policy Manager passes Posture Tokens and/or Roles to the Service-specific Enforcement Policy to be cached for use

Default Audit Servers

When you configure an audit as part of a Policy Manager service, you can select the default Nessus (Nessus Server) or the Nmap Audit configuration.

Adding Auditing to a Service

To configure an audit server for a new service:

1. Navigate to **Configuration > Services**.

   The **Services** page opens.

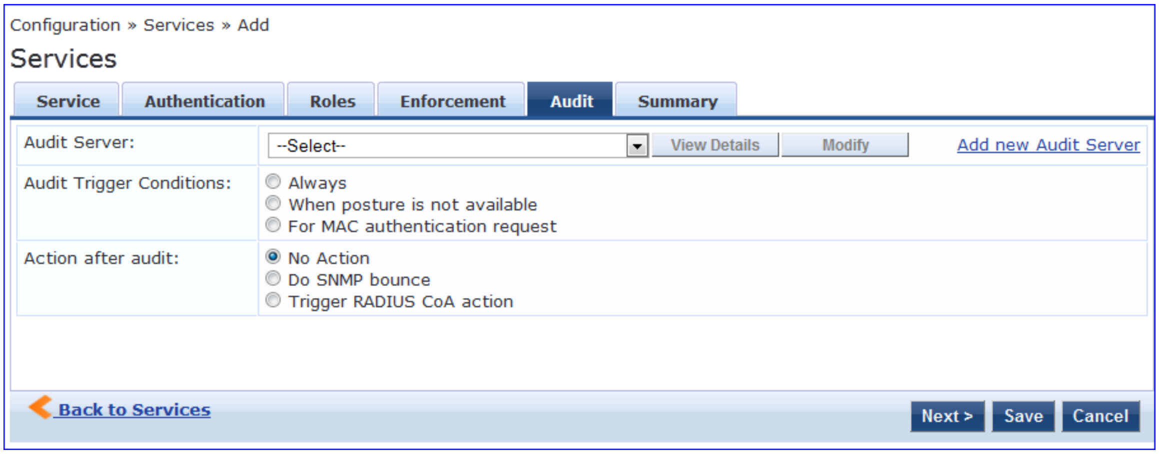
2. Select the **Add** link in the top-right corner.

   The **Add Services** dialog opens.

3. To display the **Audit** tab, select the **More Options** > **Audit End-Hosts** check box.
4. In the **Add Services** dialog, select the **Audit** tab.

The **Add Services** > **Audit** dialog opens.

Figure 324: *Add Services > Audit Dialog*



Configuration » Services » Add

Services

Audit Server: --Select--

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

Action after audit:
● No Action
○ Do SNMP bounce
○ Trigger RADIUS CoA action

5. Complete the fields in the **Add Services** > **Audit** tab as described in Table 167, then click **Save**.

Table 167: *Add Services > Audit Dialog Parameters*

Parameter	Action/Description
Audit Server	Select a server profile from the list: - **Nessus Server**: Performs vulnerability scanning and returns a Healthy/Quarantine result. - **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. You can click the **View Details** button to view the **Policy Manager Entity Details** dialog with the summary of audit server details. To view the **Summary** tab with audit server details, click the **Modify** button. 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's DHCP snooping service examines the DHCP request and response packets to derive the IP address of the end-host. For this to work, you need to use this service, Policy Manager must be configured as a DHCP “IP Helper” on your router/switch in addition to your main DHCP server. Refer to your switch documentation for “IP Helper” configuration. To audit devices that have a **static IP address** assigned, it is recommended that you create a static binding between the MAC address and IP address of the endpoint in your DHCP server. Refer to your DHCP server documentation for configuring 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:** 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:** 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 an 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.

Table 167: *Add Services > Audit Dialog Parameters (Continued)*

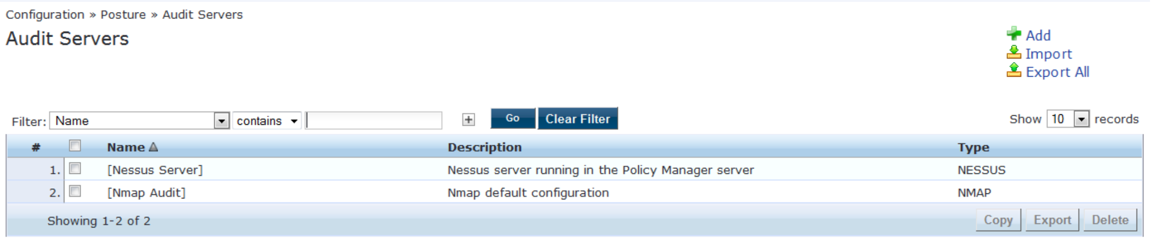
Parameter	Action/Description
	If the audit server already has the posture token and attributes associated with this client in its cache, it returns the token and the attributes to Policy Manager. ● **Trigger RADIUS CoA action:** This option sends a RADIUS CoA command to the network device.

Modifying Default Audit Servers

To reconfigure default Policy Manager audit servers:

1. Navigate to **Configuration > Posture > Audit Servers**.

Figure 325: *Audit Servers Page*



Configuration » Posture » Audit Servers

Audit Servers

Add
Import
Export All

Filter: Name contains Go Clear Filter Show 10 records

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

Showing 1-2 of 2

Copy Export Delete

2. Select an audit server from the list of available servers.

   The **Edit Audit Servers** page opens.
3. 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, the **Primary Server** and **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 346 for more information.

     The default Policy Manager Nessus audit server ships with approximately 1,000 of the most commonly used Nessus plugins.

Rules Tab

In the **Rules** tab, you can create post-audit rules for determining roles based on identity attributes discovered by the audit. For more information on creating post-audit rules, see Post-Audit Rules on page 351.

Custom Audit Servers

This section provides the following information:

- Adding a Nessus Audit Server on page 342
- Required Configuration Updates for External Nessus Servers
- Adding an Nmap Audit Server on page 349

For enterprises with existing audit server infrastructure or preferring custom audit servers, Policy Manager supports Nessus (v2.x through v6.x) and Nmap scans using the NMAP plug-in on external Nessus servers.

Adding a Nessus Audit Server

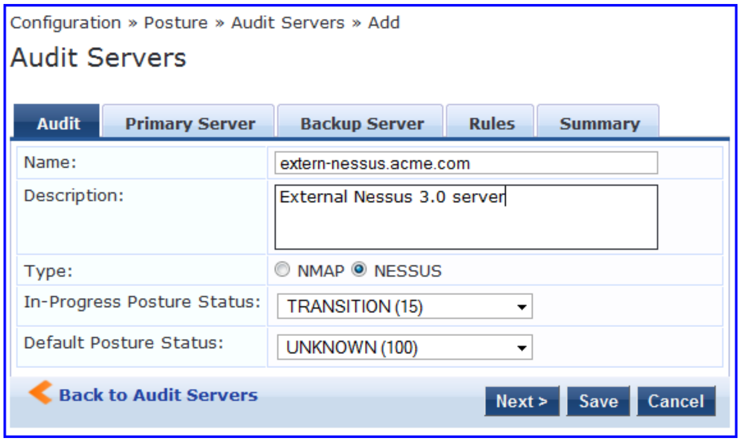
ClearPass uses the Nessus audit server interface primarily to perform vulnerability scanning. It returns a result of *Healthy* or *Quarantine*.

To add a Nessus audit server:

1. Navigate to **Configuration > Posture > Audit Servers**, then click **Add**.

   The **Add Audit Servers** dialog opens to the **Audit** tab.

Figure 326: *Add Nessus Audit Server > Audit Tab*



Configuration » Posture » Audit Servers » Add

Audit Servers

Name:	extern-nessus.acme.com
Description:	External Nessus 3.0 server
Type:	○ NMAP ● NESSUS
In-Progress Posture Status:	TRANSITION (15)
Default Posture Status:	UNKNOWN (100)

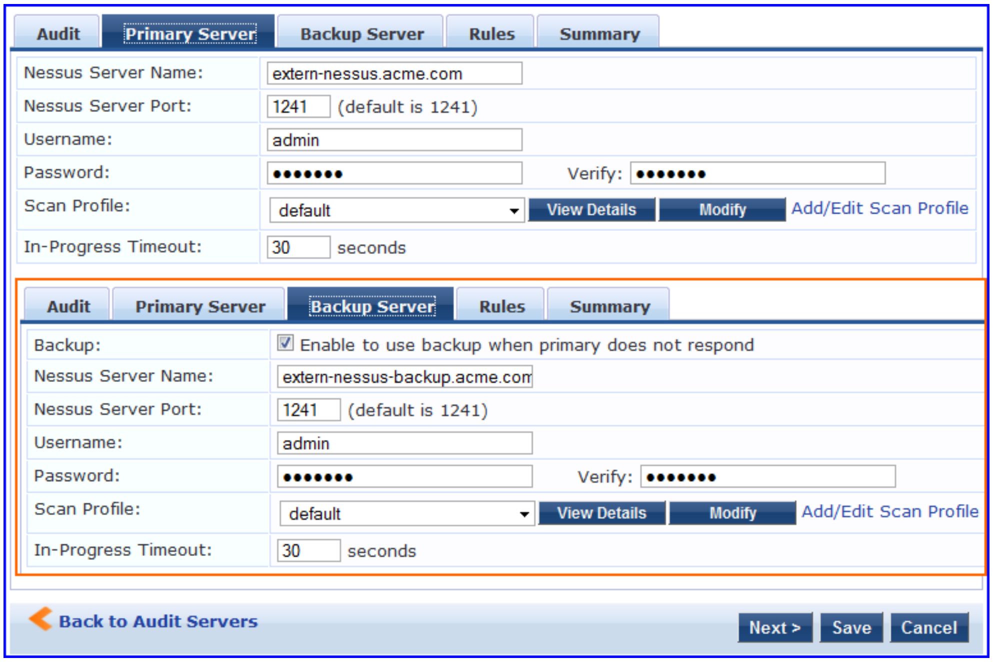
2. Specify the **Nessus Audit Server** > **Audit** tab parameters as described in Table 168.

Table 168: *Add Nessus Audit Server > Audit Tab Parameters*

Parameter	Action/Description
Name	Specify the name of the audit server.
Description	Optionally (and recommended), enter the description that provides additional information about the audit server.
Type	Specify the type of audit server: **Nmap** (Network Mapper) or **Nessus**.
In-Progress Posture Status	Specify the posture status during audit.
Default Posture Status	Specify the posture status if evaluation does not return a condition/action match.

The **Primary Server** and **Backup Server** tabs specify connection information for the Nessus audit server.

Figure 327: *Add Nessus Audit Server > Primary and Backup Server Tabs*



Nessus Server Name: extern-nessus.acme.com

Nessus Server Port: 1241 (default is 1241)

Username: admin

Password: ••••••• Verify: •••••••

Scan Profile: default

In-Progress Timeout: 30 seconds

Backup: ☑ Enable to use backup when primary does not respond

Nessus Server Name: extern-nessus-backup.acme.com

Nessus Server Port: 1241 (default is 1241)

Username: admin

Password: ••••••• Verify: •••••••

Scan Profile: default

In-Progress Timeout: 30 seconds

3. Specify the **Nessus Audit Server** > **Primary Server** tab and **Backup Server** tab parameters as described in Table 169.

Table 169: *Nessus Audit Server > Primary and Backup Server Tabs Parameters*

Parameter	Action/Description
Backup	On the **Backup Server** dialog: For the backup server to be invoked on primary server failover, check the **Enable to use backup when primary does not respond** check box.
Nessus Server Name	Enter the name of the Nessus server.
Nessus Server Port	Specify the Nessus Server port. The default is **1241**.
Username	Enter the username for the primary and backup Nessus servers.
Password	Enter the password for the primary and backup Nessus servers.
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 346.
In-Progress Timeout	Specify the duration (in seconds) before polling for Nmap results. The default is **30** seconds.

4. Configure the audit server Rules.

   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 351.

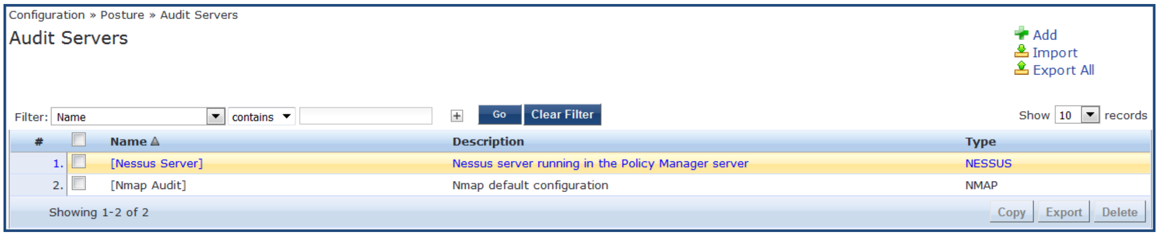
Modifying a Nessus Audit Server

To modify an existing Nessus audit server:

1. Navigate to **Configuration > Posture > Audit Server**.

   The **Audit Servers** dialog opens.

Figure 328: *Selecting a Nessus Audit Server*



Configuration » Posture » Audit Servers

Audit Servers

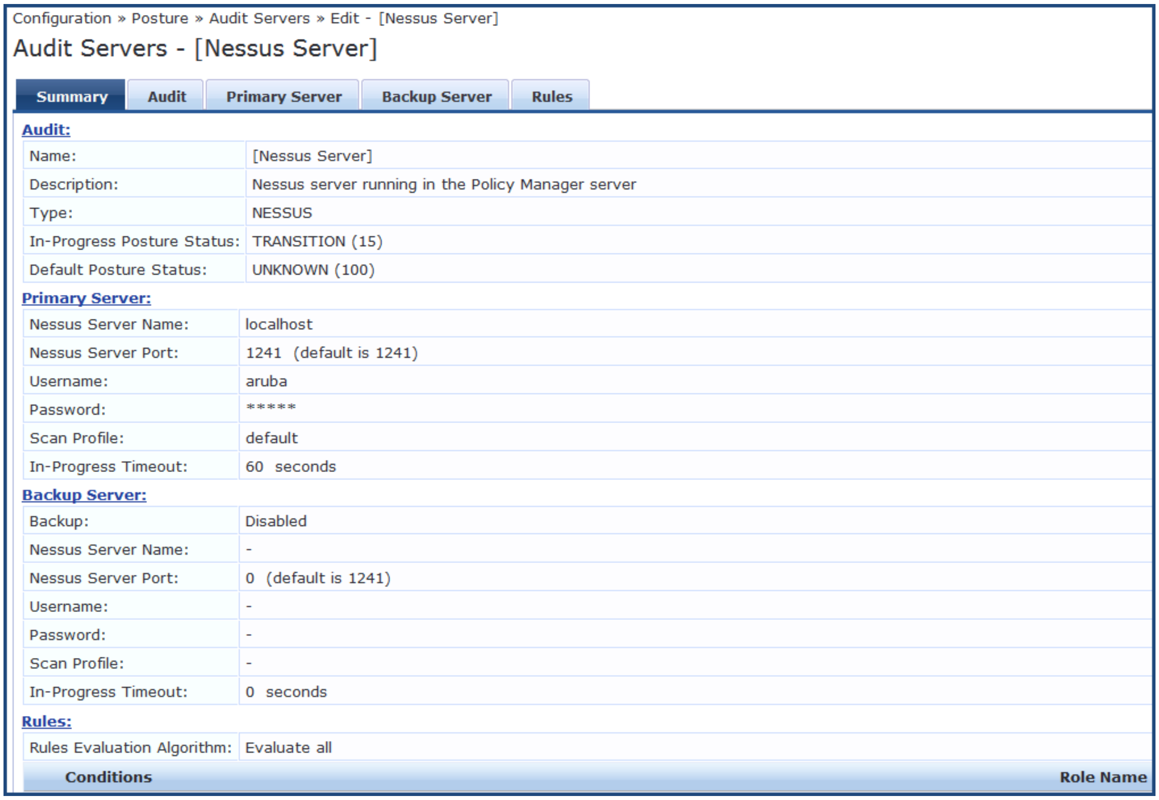
#		Name	Description	Type
1.	□	[Nessus Server]	Nessus server running in the Policy Manager server	NESSUS
2.	□	[Nmap Audit]	Nmap default configuration	NMAP

Showing 1-2 of 2

2. Select the Nessus audit server you wish to modify.

   The **Edit Nessus Server** dialog opens to the **Summary** tab, which displays the configuration settings for the selected Nessus server.

Figure 329: *Edit Nessus Server > Summary Page*



Configuration » Posture » Audit Servers » Edit - [Nessus Server]

Audit Servers - [Nessus Server]

Audit:

Name:	[Nessus Server]
Description:	Nessus server running in the Policy Manager server
Type:	NESSUS
In-Progress Posture Status:	TRANSITION (15)
Default Posture Status:	UNKNOWN (100)

Primary Server:

Nessus Server Name:	localhost
Nessus Server Port:	1241 (default is 1241)
Username:	aruba
Password:	*****
Scan Profile:	default
In-Progress Timeout:	60 seconds

Backup Server:

Backup:	Disabled
Nessus Server Name:	-
Nessus Server Port:	0 (default is 1241)
Username:	-
Password:	-
Scan Profile:	-
In-Progress Timeout:	0 seconds

Rules:

Rules Evaluation Algorithm:	Evaluate all

Conditions	Role Name

3. Make any necessary configuration changes, then click **Save**.

Required Configuration Updates for External Nessus Servers

To properly support Nessus server configuration on ClearPass servers, you must make the following configuration settings on the external Nessus server:

1. On the external Nessus server, set the value for the **disable_ntp** parameter to **no**.

   For example, on a CENTOS/RHEL server running Nessus, you would enter the following command:

```
centos# /opt/nessus/sbin/nessuscli fix --set disable_ntp=no
```

2. Restart the Nessus service.

   For example:

   ```
   centos# service nessusd restart
   ```

3. If the external Nessus server has Transport Layer Security (TLS) enabled, add the Nessus CA Certificate to the ClearPass Certificate Trust List (see Certificate Trust List on page 659).

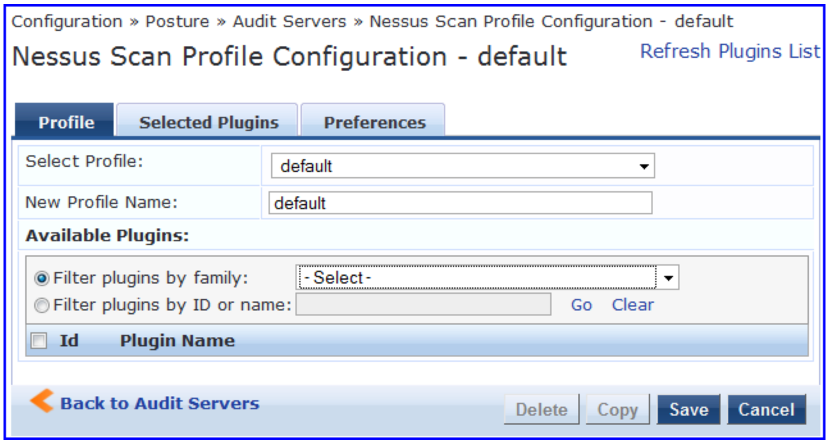
   You can download the Nessus CA certificate from:

   ```
   https://<nessus_server_name>:8834/getcert
   ```

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 330: *Nessus Scan Profile Configuration Page*



Configuration » Posture » Audit Servers » Nessus Scan Profile Configuration - default

Nessus Scan Profile Configuration - default

Select Profile: default

New Profile Name: default

Available Plugins:

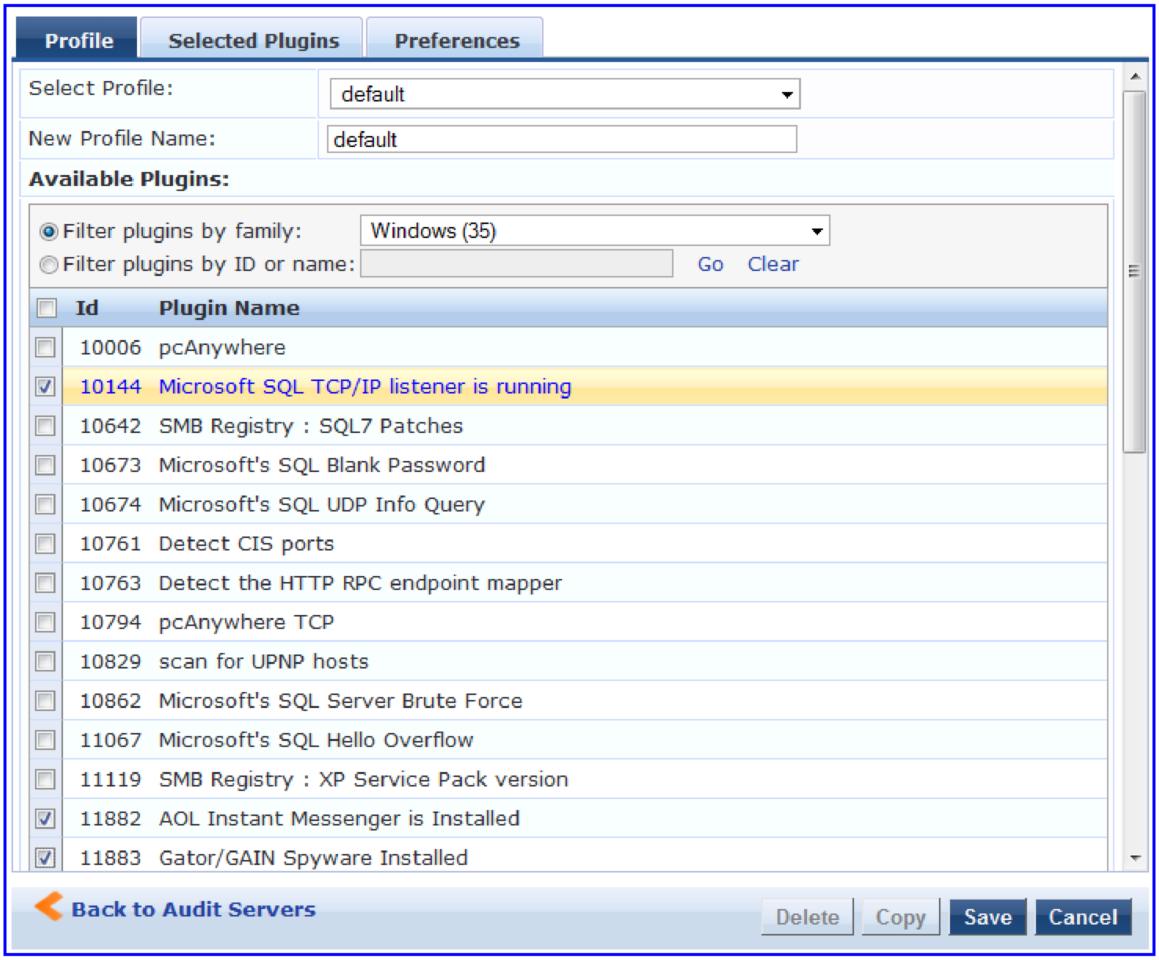
● Filter plugins by family: - Select -

○ Filter plugins by ID or name:

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

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

Figure 331: *Nessus Scan Profile Configuration - Profile Tab*



Select Profile: default

New Profile Name: default

Available Plugins:

● Filter plugins by family: Windows (35)

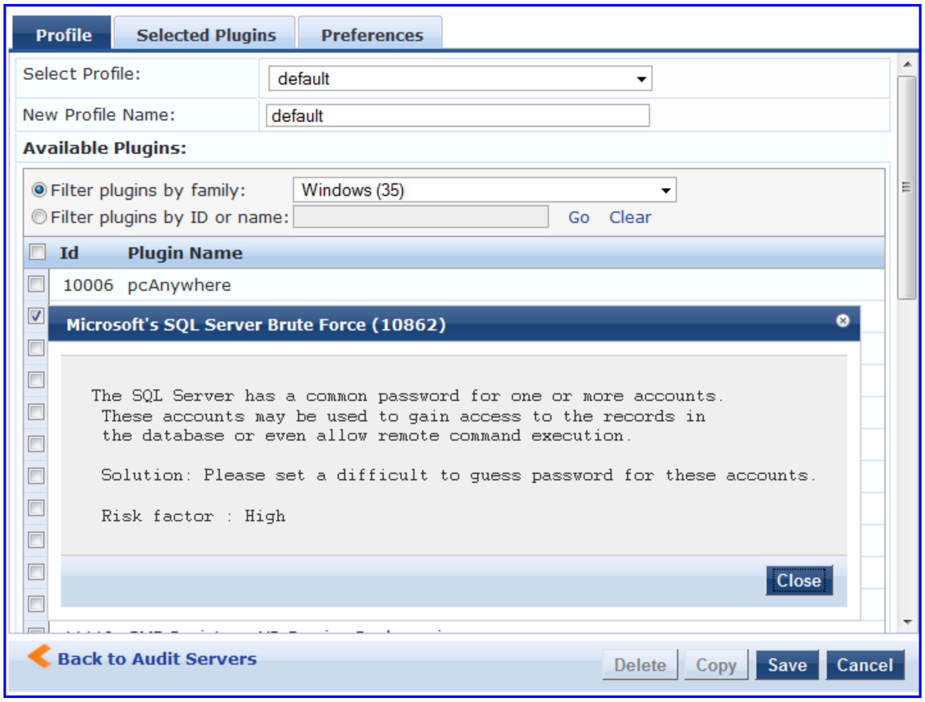
○ Filter plugins by ID or name:

□	Id	Plugin Name
□	10006	pcAnywhere
☑	10144	Microsoft SQL TCP/IP listener is running
□	10642	SMB Registry : SQL7 Patches
□	10673	Microsoft's SQL Blank Password
□	10674	Microsoft's SQL UDP Info Query
□	10761	Detect CIS ports
□	10763	Detect the HTTP RPC endpoint mapper
□	10794	pcAnywhere TCP
□	10829	scan for UPNP hosts
□	10862	Microsoft's SQL Server Brute Force
□	11067	Microsoft's SQL Hello Overflow
□	11119	SMB Registry : XP Service Pack version
☑	11882	AOL Instant Messenger is Installed
☑	11883	Gator/GAIN Spyware Installed

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

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

Figure 332: *Nessus Scan Profile Configuration Profile Tab - Plugin Synopsis*



Select Profile: default

New Profile Name: default

Available Plugins:

● Filter plugins by family: Windows (35)

○ Filter plugins by ID or name: Go Clear

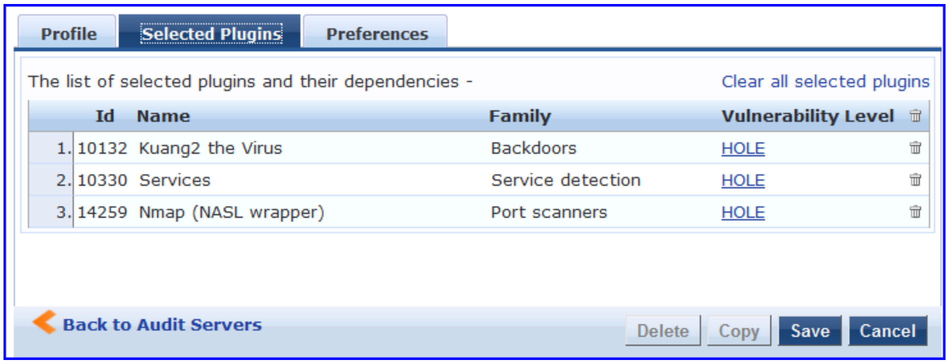
□	Id	Plugin Name
□	10006	pcAnywhere

☑ **Microsoft's SQL Server Brute Force (10862)**

```
 The SQL Server has a common password for one or more accounts.
  These accounts may be used to gain access to the records in
  the database or even allow remote command execution.

  Solution: Please set a difficult to guess password for these accounts.

  Risk factor : High
```

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

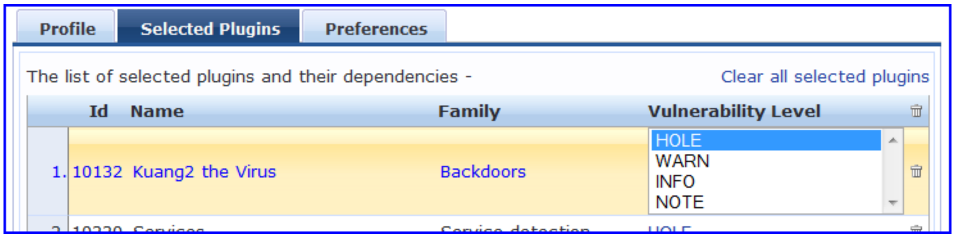
Figure 333: *Nessus Scan Profile Configuration - Selected Plugins Tab*



The list of selected plugins and their dependencies -

	Id	Name	Family	Vulnerability Level
1.	10132	Kuang2 the Virus	Backdoors	HOLE
2.	10330	Services	Service detection	HOLE
3.	14259	Nmap (NASL wrapper)	Port scanners	HOLE

Figure 334: *Nessus Scan Profile Configuration Selected Plugins Tab - Vulnerability Level*



The list of selected plugins and their dependencies -

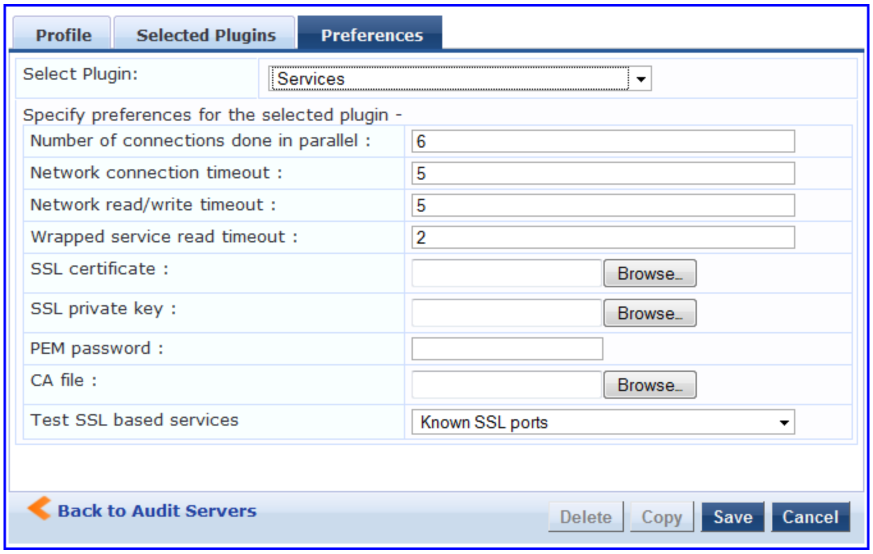
	Id	Name	Family	Vulnerability Level
1.	10132	Kuang2 the Virus	Backdoors	HOLE WARN INFO NOTE

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 335: *Nessus Scan Profile Configuration - Preferences Tab*



Select Plugin:	Services

Specify preferences for the selected plugin -

Number of connections done in parallel :	6
Network connection timeout :	5
Network read/write timeout :	5
Wrapped service read timeout :	2
SSL certificate :	
SSL private key :	
PEM password :	
CA file :	
Test SSL based services	Known SSL ports

After saving the profile, plugin, and preference information for your new (or modified) plugin, you can go to the **Primary/Backup Servers** tabs and select it from the **Scan Profile** drop-down list.

Adding an Nmap Audit Server

To create an Nmap (Network Mapping) audit server:

1. Navigate to the **Configuration** > **Posture** > **Audit Servers** page, then click **Add**.
2. From the **Audit** tab, select the **NMAP** radio button in the **Type** field.

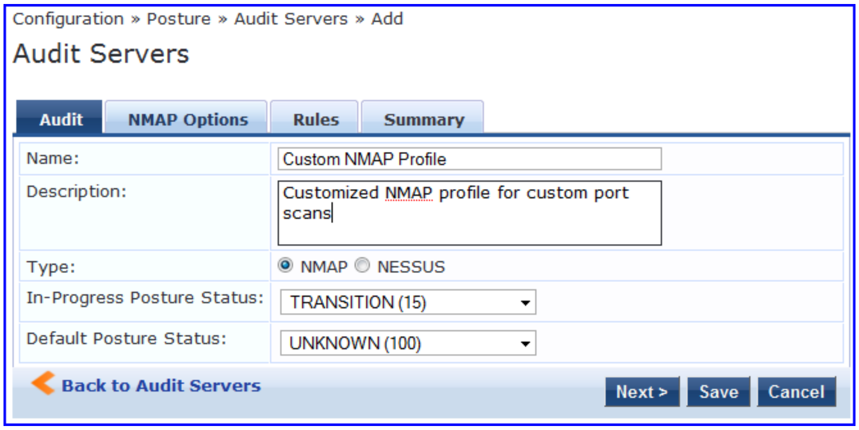
   Policy Manager uses the Nmap audit server interface exclusively for network port scans.

   - The Health evaluation always returns a status of **Healthy**.
   - The port scan gathers attributes that allow determination of role(s) through post-audit rules.

Audit Tab

You can use the **Audit** tab to identify the server and define configuration details. Figure 336 shows an example of the **Audit** tab:

Figure 336: *NMAP Audit Server > Audit Tab*



Name:	Custom NMAP Profile
Description:	Customized NMAP profile for custom port scans
Type:	● NMAP ○ NESSUS
In-Progress Posture Status:	TRANSITION (15)
Default Posture Status:	UNKNOWN (100)

The following table describes the parameters configured in the **Audit** tab:

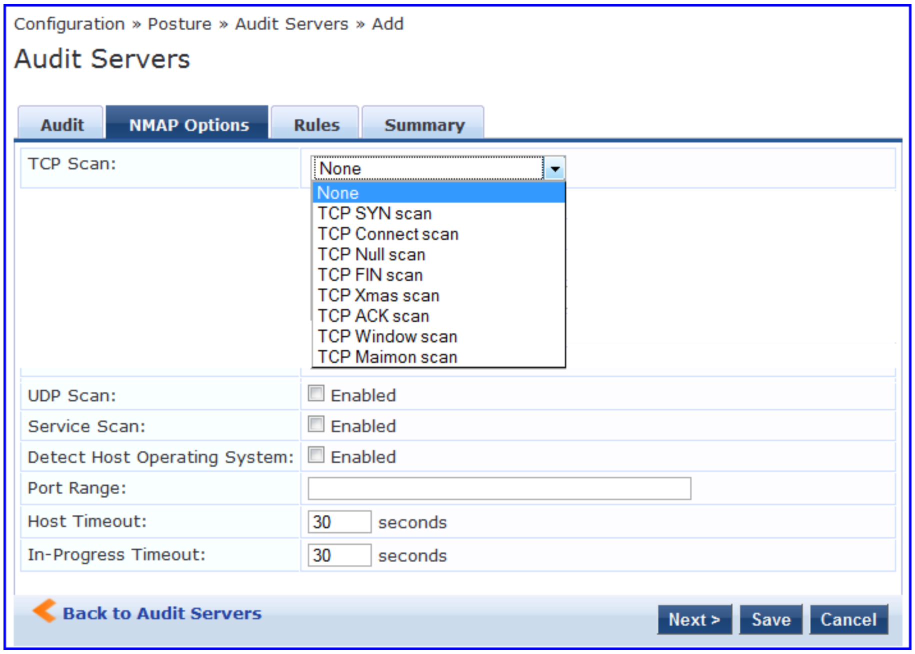
Table 170: *Audit Tab Parameters*

Parameter	Action/Description
Name	Enter the name of the NMAP audit server.
Description	Optionally (and recommended), enter the description of the Nmap audit server.
Type	Select **NMAP**.
In-Progress Posture Status	Specify the posture status during audit.
Default Posture Status	Select the posture status if evaluation does not return a condition/action match.

NMAP Options Tab

You can use the **NMAP Options** tab to specify the type of scan configuration.

Figure 337: *Nmap Server > NMAP Options Tab*



Configuration » Posture » Audit Servers » Add

Audit Servers

TCP Scan: None

UDP Scan: □ Enabled

Service Scan: □ Enabled

Detect Host Operating System: □ Enabled

Port Range:

Host Timeout: 30 seconds

In-Progress Timeout: 30 seconds

Table 171: *NMAP Options Tab*

Parameter	Action/Description
TCP Scan	Specify the type of TCP scan: ● TCP SYN scan ● TCP Connect scan ● TCP Null Scan ● TCP FIN scan ● TCP Xmas scan ● TCP ACK scan ● TCP Window scan ● TCP Maimon scan Refer to Nmap documentation for more information on the TCP scan options. Nmap option: **scanflags**.
UDP Scan	To enable UDP (User Datagram Protocol) scanning, check the **UDP Scan** check box. Nmap option: **sU**.
Service Scan	To enable Service scanning, check the **Service Scan** check box. Nmap option: **sV**.
Detect Host Operating System	To enable host OS detection, check the **Detect Host Operating System** check box. NMAP option: **A**.
Port Range	Specify the range of ports to scan. NMAP option: **p**.
Host Timeout	Specify the time in seconds for the target host to timeout. Nmap option: **host-timeout**
In-Progress Timeout	Specify the duration (in seconds) before polling for Nmap results.

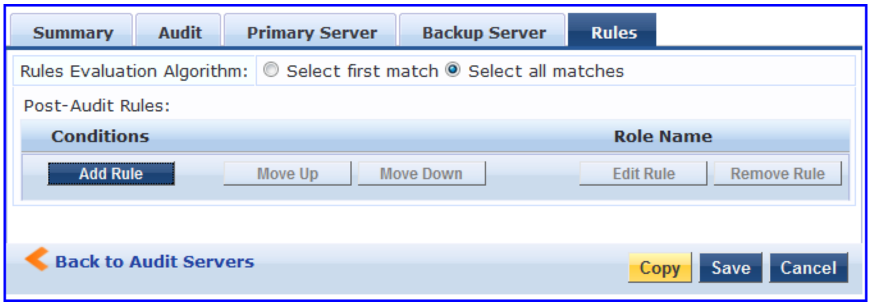
Rules Tab

The **Rules** tab specifies rules for post-audit evaluation of the request to assign a role. For details, refer to Post-Audit Rules on page 351.

Post-Audit Rules

The **Audit Servers** > **Rules** dialog specifies rules for post-audit evaluation of the request to assign a role.

Figure 338: *All Audit Server Configurations > Rules Dialog*



Rules Evaluation Algorithm: ○ Select first match ● Select all matches

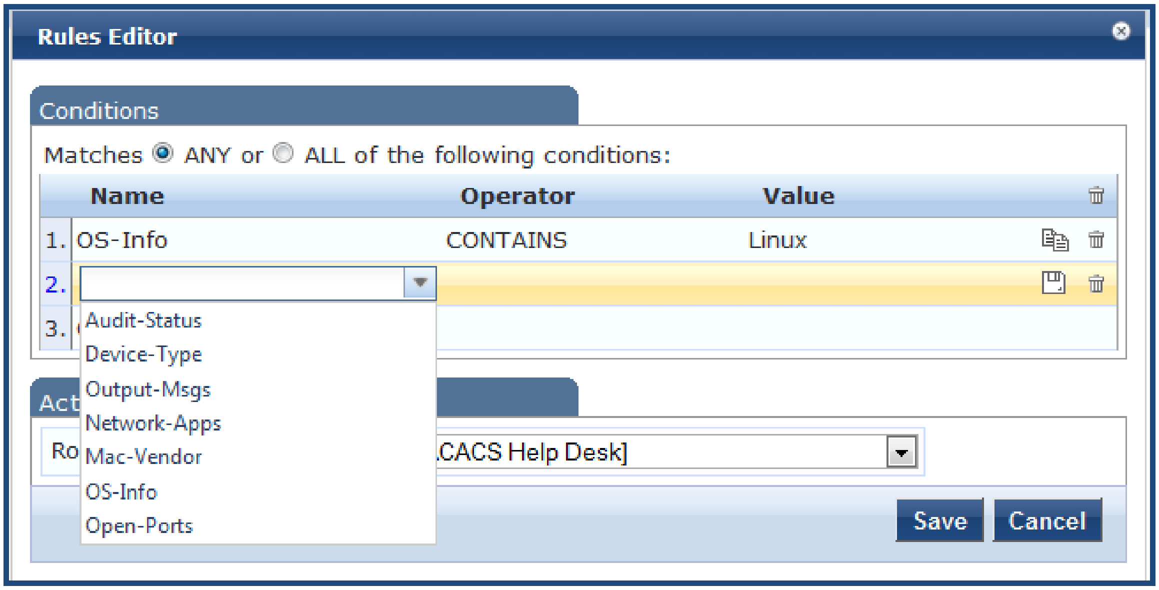
Post-Audit Rules:

Conditions	Role Name

Table 172: *All Audit Server Configurations > Rules Dialog Parameters*

Parameter	Action/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	When you add a rule, the Rules Editor opens. See below for details.
Move Up/Down	Reorder the rules as necessary.
Edit Rule	Opens the selected rule in Edit mode.
Remove Rule	Removes the selected rule.

Figure 339: *All Audit Server Configurations > Rules Editor*



Matches ● ANY or ○ ALL of the following conditions:

	Name	Operator	Value
1.	OS-Info	CONTAINS	Linux
2.			
3.			

Table 173: *All Audit Server Configurations > Rules Editor Parameters*

Parameter	Description
Conditions	The **Conditions** list includes five dictionaries: - Audit-Status - Device-Type - Output-Msgs - MAC-Vendor - Network-Apps - Open-Ports - OS-Info For more information, refer to Namespaces on page 875.
Actions	The **Actions** list includes the names of the roles configured in Policy Manager.
Save	To commit a Condition/Action pairing, click **Save**.

Chapter 7
Configuring Enforcement

This chapter describes the following topics:

- Configuring Enforcement Policies on page 355
- Configuring Enforcement Profiles on page 357

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).

For a general overview of network access enforcement policies, see Enforcement Architecture and Flow on page 1.

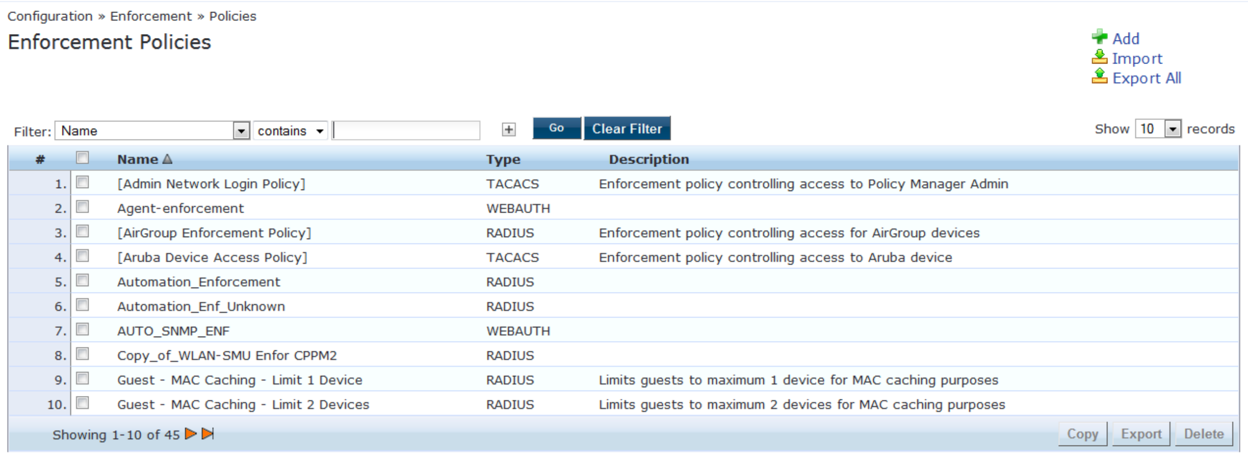
Configuring Enforcement Policies

One and only one enforcement policy can be associated with each service. Enforcement policies can be added in one of two ways:

- From **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 340: *Enforcement Policies Page*



Configuration » Enforcement » Policies

Enforcement Policies

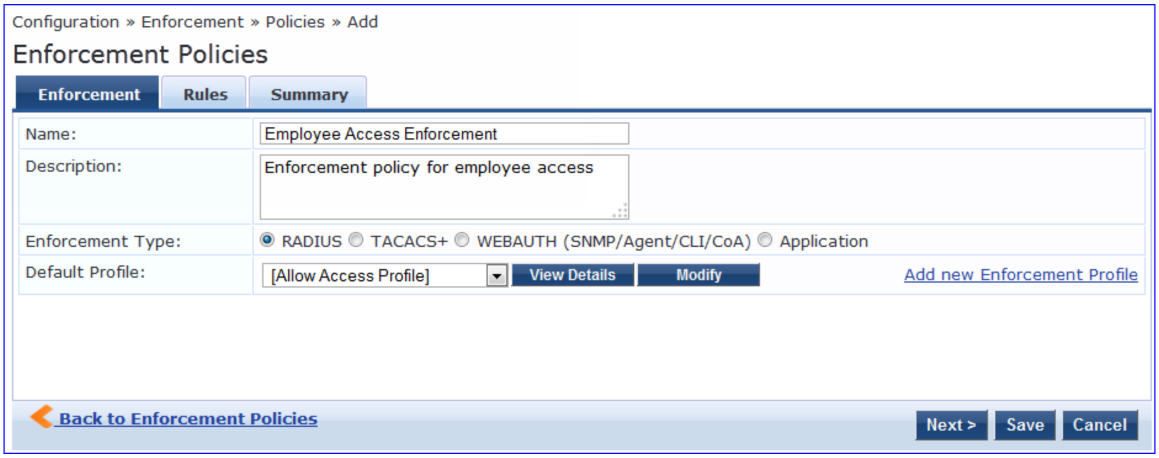
#	□	Name	Type	Description
1.	□	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin
2.	□	Agent-enforcement	WEBAUTH	
3.	□	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
4.	□	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device
5.	□	Automation_Enforcement	RADIUS	
6.	□	Automation_Enf_Unknown	RADIUS	
7.	□	AUTO_SNMP_ENF	WEBAUTH	
8.	□	Copy_of_WLAN-SMU Enfor CPPM2	RADIUS	
9.	□	Guest - MAC Caching - Limit 1 Device	RADIUS	Limits guests to maximum 1 device for MAC caching purposes
10.	□	Guest - MAC Caching - Limit 2 Devices	RADIUS	Limits guests to maximum 2 devices for MAC caching purposes

Showing 1-10 of 45

1. To add a new enforcement policy, click **Add**.

   The **Add Enforcement Policy** page opens to the **Enforcement** tab:

Figure 341: *Add Enforcement Policy > Enforcement Tab*



Configuration » Enforcement » Policies » Add

Enforcement Policies

Name: Employee Access Enforcement

Description: Enforcement policy for employee access

Enforcement Type: ● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application

Default Profile: [Allow Access Profile]

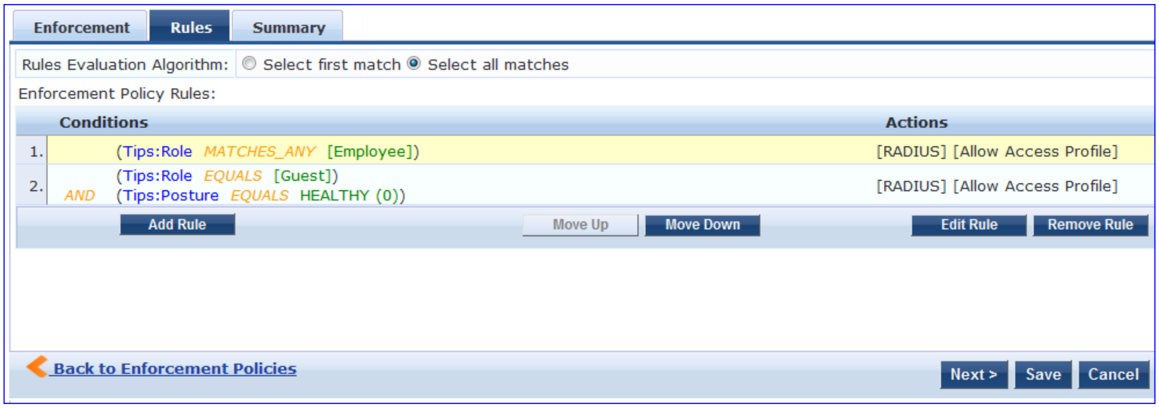
2. Specify the **Add Enforcement Policy** > **Enforcement** parameters as described in the following table:

Table 174: *Add Enforcement Policy > Enforcement Tab Parameters*

Parameter	Action/Description
Name	Enter the name of this enforcement policy.
Description	Enter a useful description of this enforcement policy (recommended).
Enforcement Type	Select one of the following enforcement types: ● RADIUS ● TACACS+ ● WebAuth (SNMP/CLI)/CoA ● Application ● Event Based on this selection, the **Default Profile** drop-down lists the associated enforcement profiles. **NOTE:** Web-based Authentication or WebAuth (HTTPS) is the mechanism used by authentications performed via a browser, and authentications performed via Aruba OnGuard. Both SNMP- and CLI- (SSH/Telnet) based enforcement profiles can be sent to the network device based on the type of device and the use case.
Default Profile	An enforcement policy applies conditions (roles, health, and time attributes) against specific values associated with those attributes to determine the enforcement profile. If none of the rules matches, Policy Manager applies the default profile. To add a new profile, click **Add New Enforcement Profile**.

3. In the **Rules** tab, click **New Rule** to display the **Rules Editor**:

Figure 342: *Add Enforcement Policy > Rules Editor*



Rules Evaluation Algorithm: ○ Select first match ● Select all matches

Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role MATCHES_ANY [Employee])	[RADIUS] [Allow Access Profile]
2.	(Tips:Role EQUALS [Guest]) AND (Tips:Posture EQUALS HEALTHY (0))	[RADIUS] [Allow Access Profile]

4. Specify the **Add Enforcement Policy** > **Rules** tab parameters as described in the following table:

Table 175: *Add Enforcement Policy: Rules Editor*

Field	Action/Description
Add Rule	Click this button to bring up the Rules Editor.
Move Up/Down	To reorder the rules in the enforcement policy, select an enforcement policy rule, then click **Move Up** or **Move Down**.
Remove Rule	To delete a rule, select the rule, then click **Remove Rule**.

Table 176: *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. You can enter role names fetched from the authorization source freeform in the Value field. To commit the rule, click **Save**.
Enforcement Profiles	If the rule conditions match, attributes from the selected enforcement profiles are sent to the 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 357 for a list of the default profiles.

Configuring Enforcement Profiles

This section includes the following information:

- Adding an Enforcement Profile
- Modifying an Existing Enforcement Profile

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 specific enforcement profiles, see:

- Agent Enforcement Profile on page 360
- Agent Script Enforcement Profile on page 363
- Aruba Downloadable Role Enforcement Profile on page 367
- Aruba RADIUS Enforcement Profile on page 376
- Cisco Downloadable ACL Enforcement Profile on page 379
- Cisco Web Authentication Enforcement Profile on page 381
- ClearPass Entity Update Enforcement Profile on page 383
- CLI-Based Enforcement Profile on page 384
- Filter ID Based Enforcement Profile on page 386
- Generic Application Enforcement Profile on page 388
- HTTP Based Enforcement Profile on page 390
- RADIUS Based Enforcement Profile on page 391
- RADIUS Change of Authorization (CoA) Profile on page 393
- Session Restrictions Enforcement Profile on page 397
- SNMP-Based Enforcement Profile on page 402
- TACACS+ Based Enforcement Profile on page 403
- VLAN Enforcement Profile on page 406

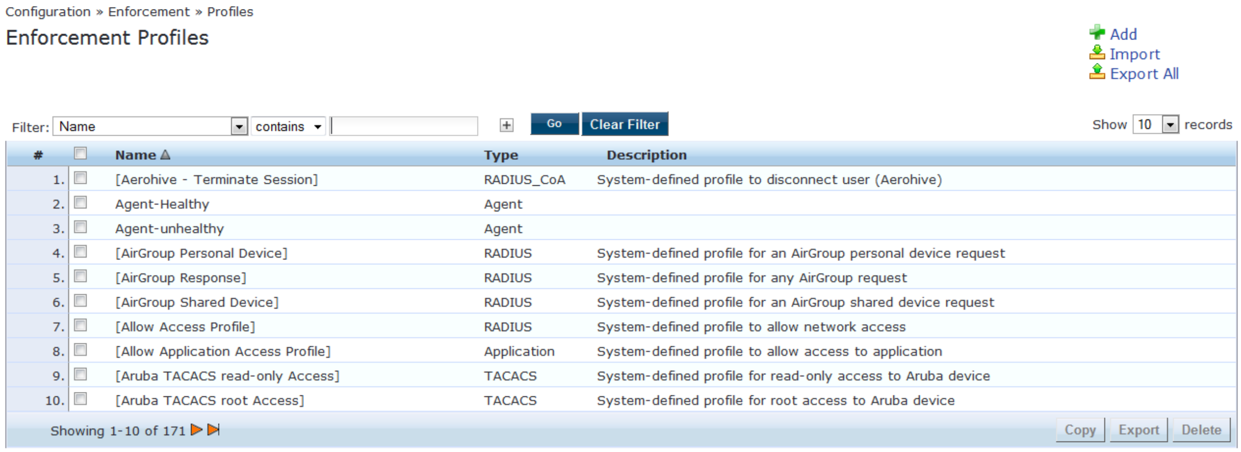
Adding an Enforcement Profile

To add an enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.

   The **Enforcement Profiles** page opens:

Figure 343: *Enforcement Profiles Page*



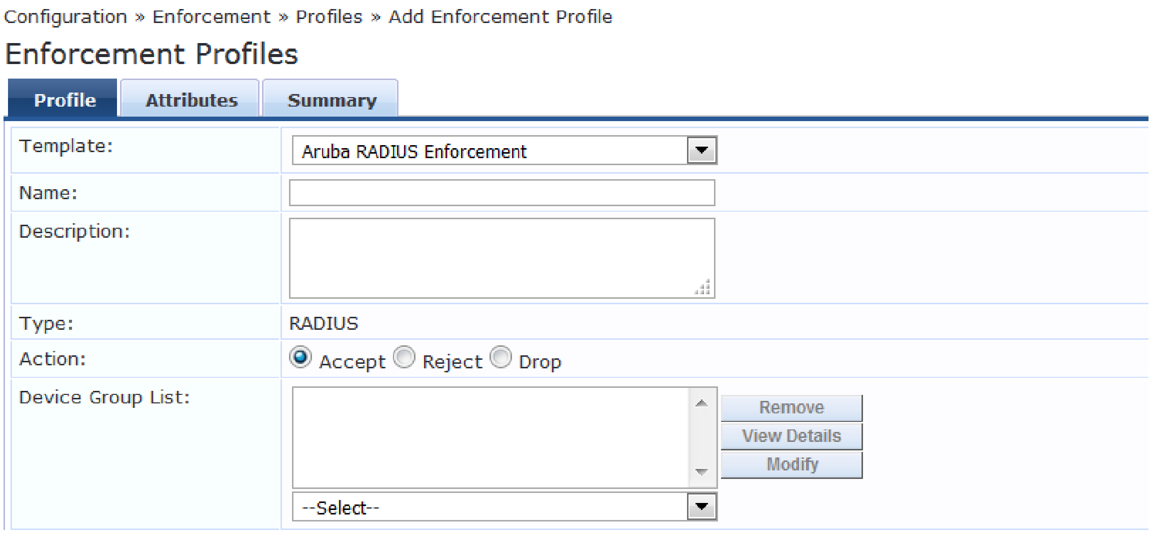
#	☐	Name	Type	Description
1.	☐	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	☐	Agent-Healthy	Agent	
3.	☐	Agent-unhealthy	Agent	
4.	☐	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
5.	☐	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
6.	☐	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
7.	☐	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
8.	☐	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
9.	☐	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
10.	☐	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device

Showing 1-10 of 171

2. Click **Add** at the top-right corner.

   The **Add Enforcement Profile** dialog opens.

Figure 344: *Add Enforcement Profile Dialog*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template: Aruba RADIUS Enforcement

Name:

Description:

Type: RADIUS

Action: ● Accept ○ Reject ○ Drop

Device Group List: --Select--

The following table describes the default set of enforcement profiles included with Policy Manager:

Table 177: *Default Enforcement Profiles*

Enforcement Profile	Available for These Enforcement Types
[Aerohive - Terminate Session]	RADIUS_CoA
[AirGroup Personal Device]	RADIUS
[AirGroup Response]	RADIUS
[AirGroup Shared Device]	RADIUS
[Allow Access Profile]	RADIUS
[Allow Application Access Profile]	Application
[Aruba TACACS read-only Access]	TACACS
[Aruba TACACS root Access]	TACACS
[Aruba Terminate Session]	RADIUS_CoA
[Cisco - Bounce-Host-Port]	RADIUS_CoA
[Cisco - Disable Host-Port]	RADIUS_CoA
[Cisco - Reauthenticate-Session]	RADIUS_CoA
[Cisco - Terminate-Session]	RADIUS_CoA
[Deny Access Profile]	RADIUS
[Deny Application Access Profile]	Application

Table 177: *Default Enforcement Profiles (Continued)*

Enforcement Profile	Available for These Enforcement Types
[Drop Access Profile]	RADIUS
[Handle AirGroup Time Sharing]	HTTP
[HP - Terminate Session]	RADIUS_CoA
[Juniper Terminate Session]	RADIUS_CoA
[Motorola - Terminate Session]	RADIUS_CoA
[Operator Login - Admin Users]	Application
[Operator Login - Local Users]	Application
[TACACS API Admin]	TACACS
[TACACS Deny Profile]	TACACS
[TACACS Help Desk]	TACACS
[TACACS Network Admin]	TACACS
[TACACS Read-only Admin]	TACACS
[TACACS Receptionist]	TACACS
[TACACS Super Admin]	TACACS
[Trapeze - Terminate Session]	RADIUS_CoA
[Update Endpoint Known]	Post-Authentication

Modifying an Existing Enforcement Profile

To modify an existing enforcement profile:

1. Navigate to the **Configuration > Enforcement > Profiles** page.
2. Click the name of the profile in the **Enforcement Profile** list that you wish to modify.

   The **Edit Enforcement Profile** dialog for the selected profile opens. The parameters vary according to which profile is selected.
3. Make the necessary changes in the **Profile** and **Attributes** dialogs, then click **Save**.

Agent Enforcement Profile

To configure profile and attribute parameters for an Agent Enforcement profile:

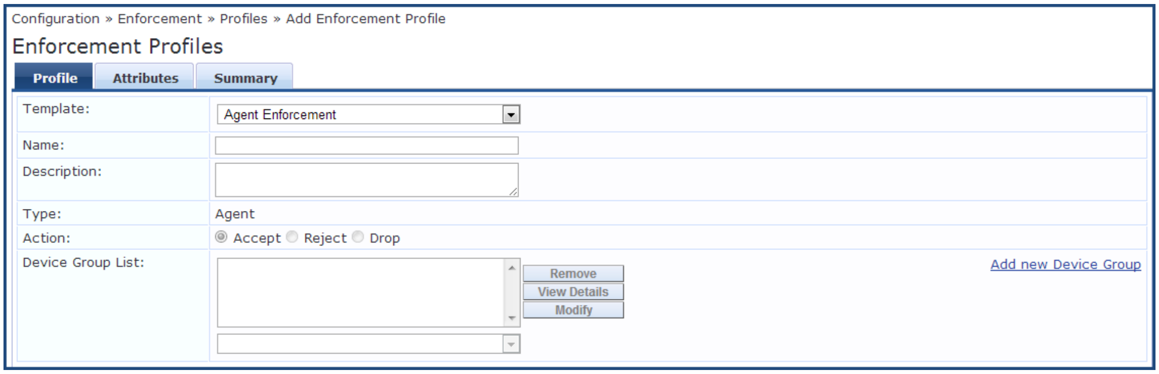
1. Navigate to **Configuration** > **Enforcement** > **Profiles**.

   The **Enforcement Profiles** page opens.
2. Click **Add**.

   The **Add Enforcement Profiles** > **Profile** tab opens.
3. From the **Template** drop-down, select **Agent Enforcement**.

The following figure displays the **Agent Enforcement > Profile** dialog:

Figure 345: *Agent Enforcement > Profile Tab*


Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	Agent Enforcement
Name:	
Description:	
Type:	Agent
Action:	● Accept ○ Reject ○ Drop
Device Group List:	

4. Specify the **Add Agent Enforcement > Profile** parameters as described in the following table:

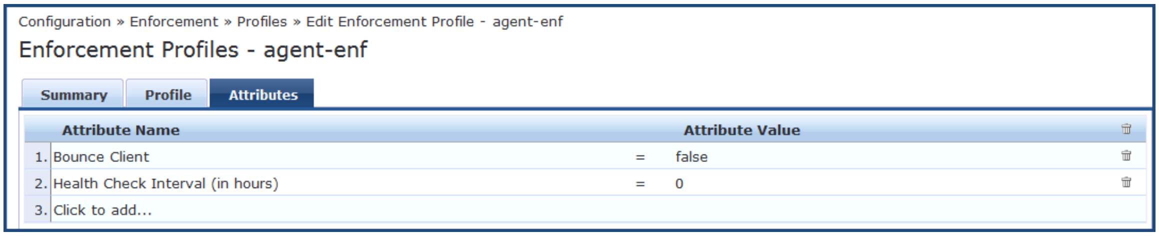
Table 178: *Add Agent Enforcement > Profile Parameters*

Parameter	Action/Description
Template	Select the template from the drop-down list. In this context, select **Agent Enforcement**.
Name	Enter the name of the enforcement profile.
Description	Optionally, enter a description of the enforcement profile (recommended).
Type	This field is populated automatically with type **Agent**.
Action	By default, this field is disabled. It is enabled only when **RADIUS** type is selected.
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 **Configuration > Network > Device Groups** page. After you add one or more device groups, you can select a group and take one of the following actions: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Attributes Configuration

Use the **Attributes** tab to configure the attribute name and attribute value for each attribute you add.

Figure 346: *Agent Enforcement > Attributes Dialog*


Configuration » Enforcement » Profiles » Edit Enforcement Profile - agent-enf

Enforcement Profiles - agent-enf

	Attribute Name		Attribute Value
1.	Bounce Client	=	false
2.	Health Check Interval (in hours)	=	0
3.	Click to add...		

Specify the **Agent Enforcement > Attributes** parameters as described in the following table:

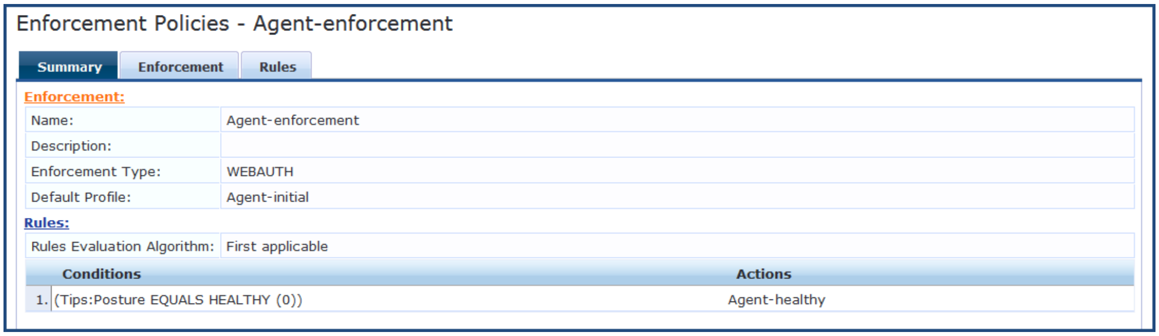
Table 179: *Agent Enforcement > Attributes Tab Parameters*

Attribute	Action/Description
Attribute Name	Select one of the following attribute names: ● **Bounce Client:** To bounce the network interface, set the value to **True**. ● **Message:** Enter the message that needs to be notified on the endpoint. ● **Session Timeout (in seconds)**: Configure the agent session timeout interval to periodically evaluate the endpoint's health. OnGuard Agent performs health checks after the specified session timeout interval and updates the health status of the endpoint in Policy Cache. You can specify the session timeout interval from **60** to **600** seconds. The default value is **0**. Note that setting the lower value for the session timeout interval results in numerous authentication requests in the **Access Tracker** page. ● **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** to **1000** hours. **NOTE:** The value of the **Policy result cache timeout** parameter (**Administration** > **Server Manager** > **Server Configuration** > **Cluster-Wide Parameters** > **General** tab) must be greater than the highest value of all the **Health Check Interval (in hours)** values. Note the following information when you set the **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. ● **Enable to hide Retry button**: To hide the **Retry** button in the OnGuard Agent, set the value to **True**. ● **Enable to hide Logout button**: To hide the **Logout** button in the OnGuard Agent, set the value to **True**. ● **Enable to hide Quit option**: To hide all Quit options in the OnGuard Agent, set the value to **True**. ● **Bounce Delay (in seconds)**: When **Bounce Delay** is configured, the network interface is bounced after the specified delay.
Attribute Value	The value set depends on the selected **Attribute Name**.

Summary Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs.

Figure 347: *Agent Enforcement > Summary Tab*



Enforcement Policies - Agent-enforcement

Enforcement:

Name:	Agent-enforcement
Description:	
Enforcement Type:	WEBAUTH
Default Profile:	Agent-initial

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Posture EQUALS HEALTHY (0))	Agent-healthy

Agent Script Enforcement Profile

This section provides the following information:

- Introduction
- Configuring the Agent Script Enforcement Profile
- Configuring Agent Script Enforcement Attributes
- Viewing the Configuration Summary

Introduction

Agent Script Enforcement profiles allow execution of custom scripts on endpoint devices as part of agent enforcement. All the details of custom script configuration, such as the path of the custom script, the command to be executed, execution level, and so on, are configured in the Agent Script Enforcement profile.

You can select multiple Agent Script Enforcement Profiles in a rule in an enforcement profile. OnGuard Agent executes them one after another.

The Agent Script Enforcement profile is currently supported only with the OnGuard Agent for Windows.

OnGuard Agent applies the Agent Script Enforcement profile (that is, it executes a custom script) after first applying Agent Enforcement profiles (that is, after **Agent Bounce** is executed, if configured).

While applying an Agent Script Enforcement profile, OnGuard Agent does not check to see if a script is already running. It is possible for OnGuard Agent to launch the script multiple times if a previously launched script is still running. This can occur if OnGuard Agent performs multiple health checks (either manually triggered or caused by a change in health status). The script should exit after performing its task.

Mandatory Attributes

The following attributes are mandatory when configuring Agent Script Enforcement:

- Path of the Script
- Command to Execute
- Execution Level

Optional Attributes

The following attributes are optional when configuring Agent Script Enforcement:

- SHA256 Checksum
- Wait Time (Seconds) Before Executing Script
- Pass Health Evaluation Results to Script
- Success Message
- Failure Message
- Download URL

Configuring the Agent Script Enforcement Profile

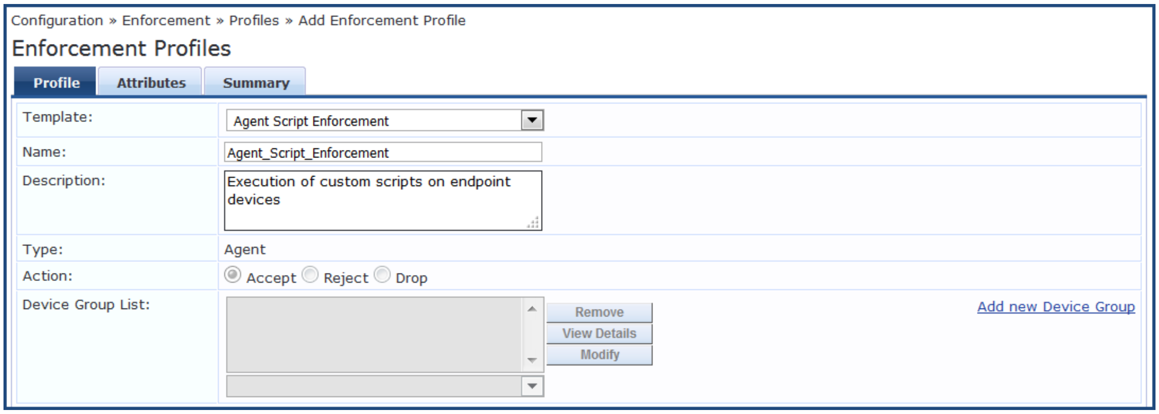
To configure an Agent Script Enforcement profile:

1. Navigate to **Configuration** > **Enforcement** > **Profiles**.

   The **Enforcement Profiles** page opens.
2. Click **Add**.

   The **Add Enforcement Profiles** dialog opens to the **Profile** tab.

Figure 348: *Agent Script Enforcement > Profile Dialog*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template: Agent Script Enforcement

Name: Agent_Script_Enforcement

Description: Execution of custom scripts on endpoint devices

Type: Agent

Action: ● Accept ○ Reject ○ Drop

Device Group List:

3. Specify the **Add Agent Script Enforcement > Profile** parameters as described in the following table:

Table 180: *Add Agent Script Enforcement > Profile Parameters*

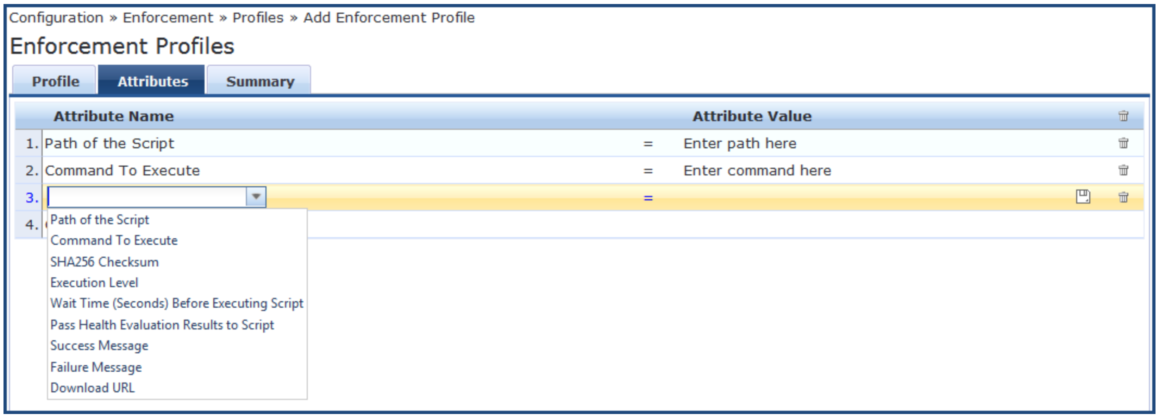
Parameter	Action/Description
Template	Select the **Agent Script Enforcement** template.
Name	Enter the name of the enforcement profile.
Description	Optionally, enter a description of the enforcement profile (recommended).
Type	This field is populated automatically with type **Agent**.
Action	This parameter is disabled because it is not applicable to the Agent Script Enforcement Profile.
Device Group List	This parameter is disabled because it is not applicable to the Agent Script Enforcement Profile.
Add new Device Group	This parameter is disabled because it is not applicable to the Agent Script Enforcement Profile.

Configuring Agent Script Enforcement Attributes

Use the **Attributes** tab to configure the attribute name and attribute value for each attribute you add.

The following figure displays the **Agent Enforcement > Attributes** dialog:

Figure 349: *Agent Script Enforcement > Attributes Dialog*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Attribute Name		Attribute Value
1.	Path of the Script	=	Enter path here
2.	Command To Execute	=	Enter command here
3.		=	
4.			

Specify the **Agent Script Enforcement > Attributes** parameters as described in the following table:

Table 181: *Agent Script Enforcement > Attributes Parameters*

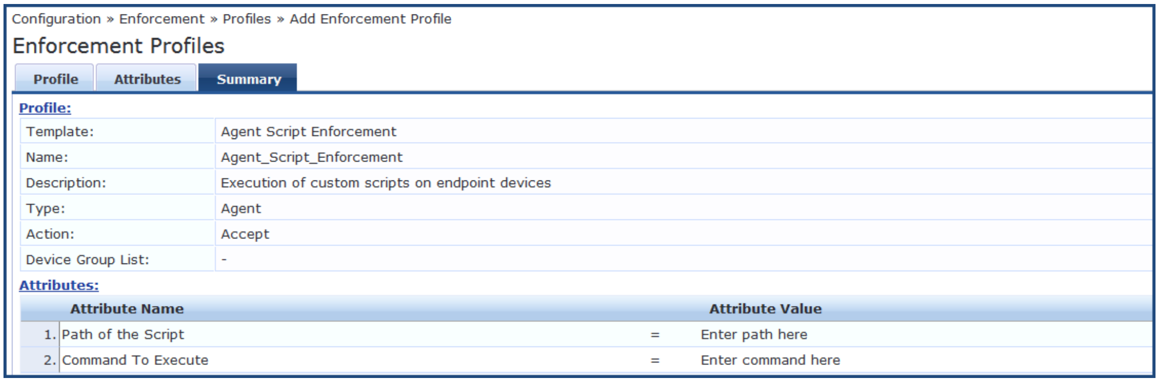
Attribute	Action/Description
Attribute Name	Select one of the following attribute names: ● **Path of the Script:** Complete the path of the script/program, including the filename. This attribute checks for the existence of a file on an endpoint device and also verifies the SHA256 Checksum. ● **Command to Execute:** Specify the complete command that OnGuard Agent should execute. You can use the command to launch scripts or pass command line arguments. For example, to launch VBScript (InstallHotfixes.vbs) and pass **All** as an argument, you would enter the following: `cscript /nologo C:\Test\InstallHotfixes.vbs All` If it is not required to pass arguments, set the value of this attribute to the same value specified for **Path of the Script**. ● **SHA256 Checksum**: Specify the SHA256 checksum of the script/program. This attribute accepts comma-separated multiple SHA256 checksums to allow execution of different versions of same script/program. ● **Execution Level**: The attribute values are: **User** and **System**. ■ To launch the script/program as the current logged-on user, select **User**. ■ To launch the script/program as the system user with admin rights, select **System**. ● **Wait Time (Seconds) Before Executing Script**: Specify the time (in seconds) after which OnGuard Agent should launch the script/program. ■ When **Wait Time Before Executing Script** is configured, the OnGuard Agent does not process events such as Interface Up/Interface Down and health changes during the wait time. ● **Pass Health Evaluation Results to Script**: Check the check box (which sets the value to **true**) to enable OnGuard Agent to pass health evaluation results to the script/program as an argument. The default is **false**. ■ When the **Pass Health Evaluation Results to Script** attribute is set to **true**, OnGuard Agent passes health evaluation results to the script in a URL Encoded JSON format. ■ URL Encode replaces double quotes, spaces, and Unicode characters with their ASCII value in %XX format. For example, spaces are replaced by %20 and double quotes are replaced by %22. ● **Success Message**: Enter the message to be shown to the end user when the script/program is launched successfully. ● **Failure Message**: Enter the message to be shown to the end user when execution of the script/program fails. ● **Download URL**: If the script/program configured in the **Path of the Script** attribute is not present on the client machine, enter the URL of the remote server from which OnGuard Agent can download the script/program. ■ OnGuard Agent supports downloading scripts only from HTTP and HTTPS URLs. For HTTPS URLs, OnGuard skips server certificate verification. ■ Also, OnGuard Agent does not support downloading files from URLs that require credentials.
Attribute Value	The **Attribute Value** set depends on the selected **Attribute Name**.

Viewing the Configuration Summary

The **Summary** page summarizes the parameters configured in the **Profile** and **Attribute** tabs.

The following figure displays the **Agent Script Enforcement** > **Summary** page:

Figure 350: *Agent Script Enforcement > Summary Dialog*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile:

Template:	Agent Script Enforcement
Name:	Agent_Script_Enforcement
Description:	Execution of custom scripts on endpoint devices
Type:	Agent
Action:	Accept
Device Group List:	-

Attributes:

	Attribute Name		Attribute Value
1.	Path of the Script	=	Enter path here
2.	Command To Execute	=	Enter command here

Aruba Downloadable Role Enforcement Profile

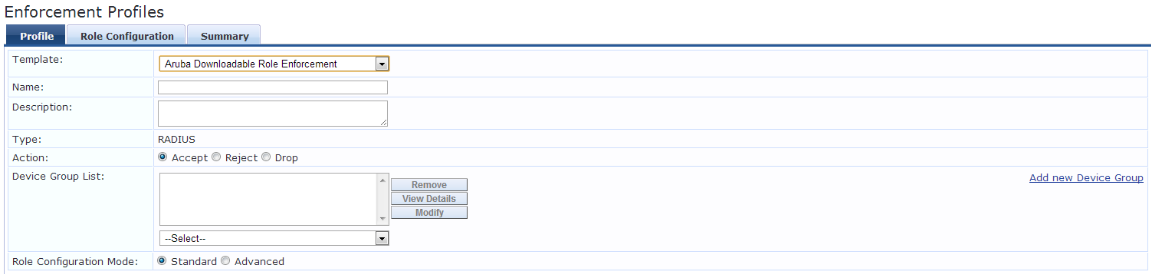
This section describes the following **Aruba Downloadable Role Enforcement** profile features:

- Profile Configuration on page 367
- Role Configuration on page 368
- Adding a Stateless Access Control List on page 374
- Adding a Session Access Control List on page 374
- Adding an Ethernet/MAC Access Control List on page 375
- Summary Information on page 376

Profile Configuration

Use the **Profile** tab to configure the template, type of the profile, and the device group list.

Figure 351: *Aruba Downloadable Role Enforcement > Profile Tab*



Enforcement Profiles

Template:	Aruba Downloadable Role Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--
Role Configuration Mode:	● Standard ○ Advanced

Specify the **Aruba Downloadable Role Enforcement** > **Profile** parameters as described in the following table:

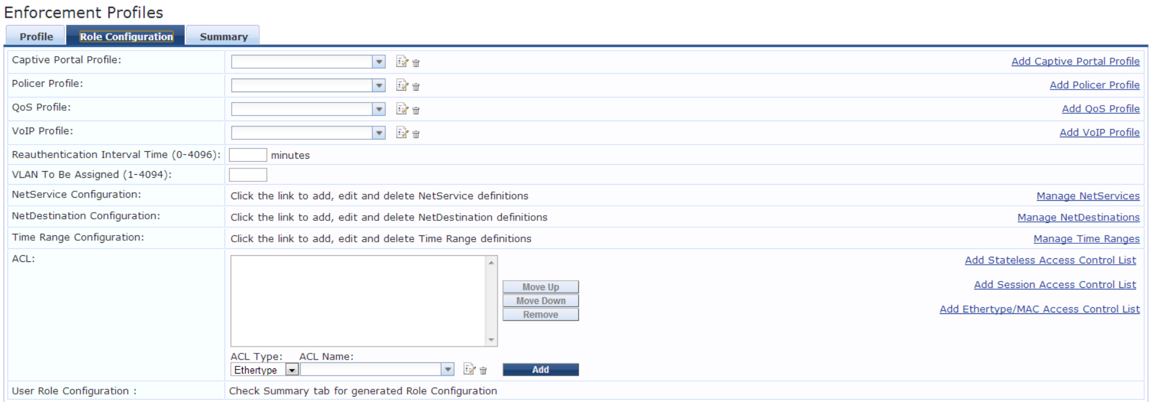
Table 182: *Aruba Downloadable Role Enforcement > Profile Parameters*

Parameter	Action/Description
Template	Select the **Aruba Downloadable Role Enforcement** template.
Name	Enter the name of the profile. .
Description	Enter a description of the profile.
Type	This field is automatically populated with: **RADIUS**.
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 **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Role Configuration

The fields on the **Role Configuration** tab require you to select a link to launch a new page where you set role configuration attributes.

Figure 352: *Aruba Downloadable Role Enforcement Role > Configuration Tab*



Enforcement Profiles

Captive Portal Profile:

Policer Profile:

QoS Profile:

VoIP Profile:

Reauthentication Interval Time (0-4096): minutes

VLAN To Be Assigned (1-4094):

NetService Configuration: Click the link to add, edit and delete NetService definitions

NetDestination Configuration: Click the link to add, edit and delete NetDestination definitions

Time Range Configuration: Click the link to add, edit and delete Time Range definitions

ACL:

ACL Type: Ethertype ACL Name:

User Role Configuration : Check Summary tab for generated Role Configuration

The following table describes the **Role Configuration** > **Attributes** parameters:

Table 183: *Role Configuration > Attributes Parameters*

Parameters	Action/Configuration
Captive Portal Profile	Select the captive portal profile from the drop-down list if already configured. Click the **Add Captive Portal Profile** link to add a new captive portal profile. For more information, see Captive Portal Profile on page 370.
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 370.
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 371.
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 372.
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. For more information, see NetService Configuration.
NetDestination Configuration	Select the **Manage NetDestinations** link to add, edit, and delete the NetDestinations definitions. For more information, see NetDestination Configuration.
Time Range Configuration	Select the **Manage Time Ranges** link to add, edit, and delete time range definitions. For more information, see Time Range Configuration.
NAT Pool Configuration	Select the **Manage NAT Pool** link to add, edit and delete NAT Pool definitions. For morfe information, see NAT Pool Configuration.

Table 183: *Role Configuration > Attributes Parameters (Continued)*

Parameters	Action/Configuration
ACL Type	Select from the following ACL types: - Ethertype - MAC - Session - Stateless
ACL Name	Click the name of the ACL type. - To move the **ACL Name** to the **ACL** field, click **Add**. - To modify the order of the names in the ACL list, click **Move Up**, **Move Down**. - To delete an ACL from the list, click **Remove**.
User Role Configuration	Check the **Summary** tab for generated role configuration.

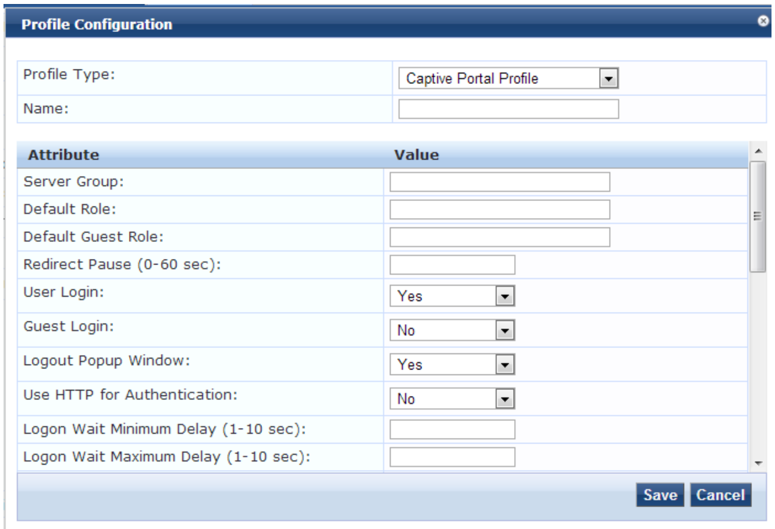
Captive Portal Profile

To define the Captive Portal Profile:

1. Click the **Add Captive Portal Profile** link.

   The **Add Captive Portal Profile** dialog opens:

Figure 353: *Add Captive Portal Profile Dialog*



Profile Configuration

Profile Type:	Captive Portal Profile
Name:	

Attribute	Value
Server Group:	
Default Role:	
Default Guest Role:	
Redirect Pause (0-60 sec):	
User Login:	Yes
Guest Login:	No
Logout Popup Window:	Yes
Use HTTP for Authentication:	No
Logon Wait Minimum Delay (1-10 sec):	
Logon Wait Maximum Delay (1-10 sec):	

2. Enter a name of the profile and configure the required attributes.

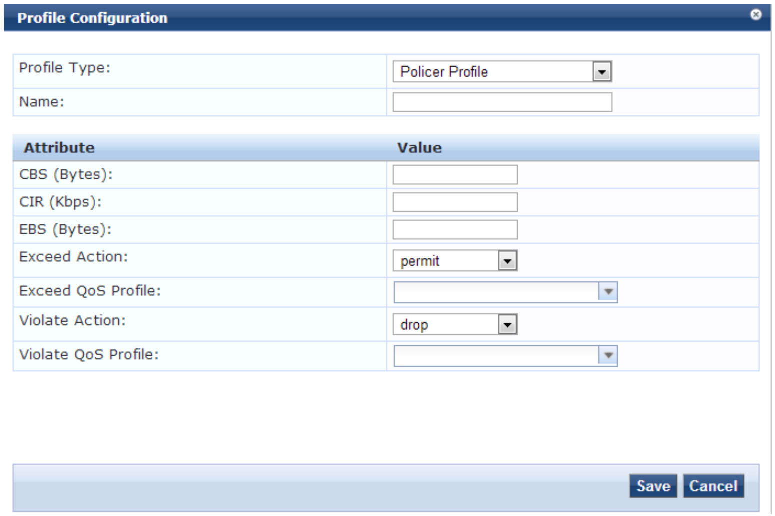
Policer Profile

To define a Policer Profile:

1. Click the **Add Policer Profile** link.

   The **Add Policer Profile** dialog opens:

Figure 354: *Add Policer Profile Dialog*



Profile Type:	Policer Profile
Name:	

Attribute	Value
CBS (Bytes):	
CIR (Kbps):	
EBS (Bytes):	
Exceed Action:	permit
Exceed QoS Profile:	
Violate Action:	drop
Violate QoS Profile:	

2. Enter a name of the profile and configure the required attributes.

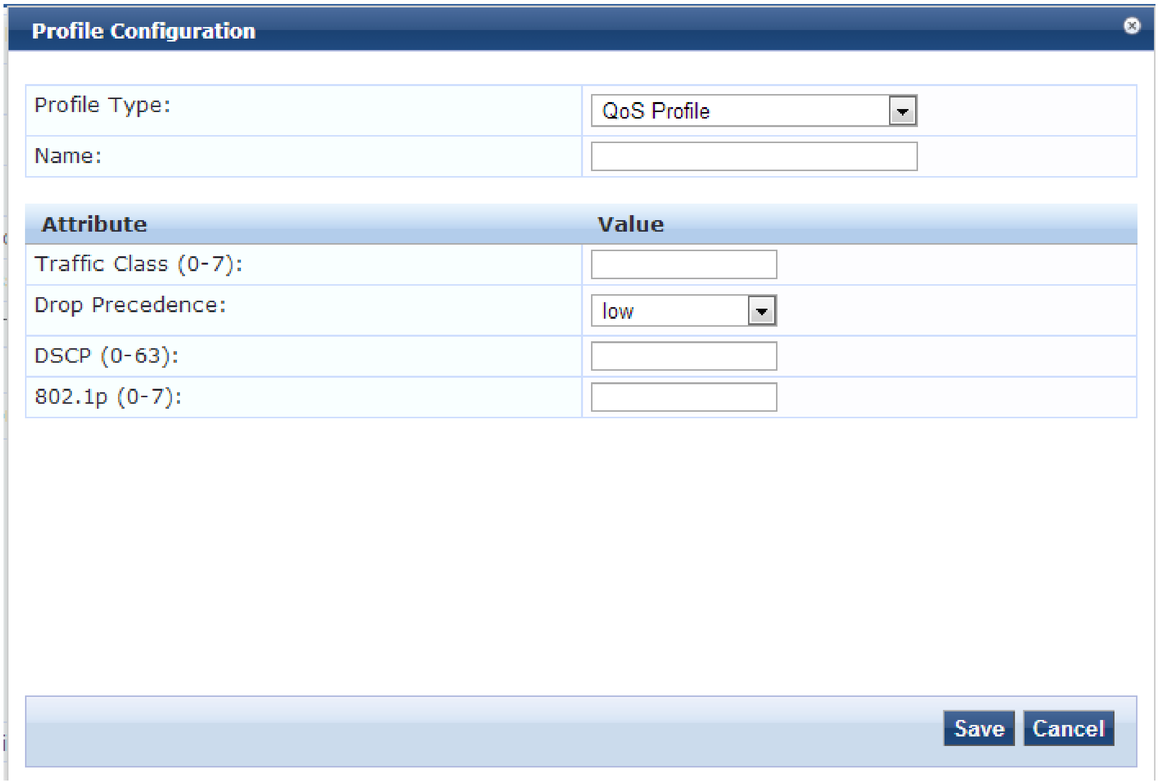
QoS Profile

To define a QoS Profile:

1. Click the **Add QoS Profile** link.

   The **Add QoS Profile** opens:

Figure 355: *Add QosProfle Dialog*



Profile Type:	QoS Profile
Name:	

Attribute	Value
Traffic Class (0-7):	
Drop Precedence:	low
DSCP (0-63):	
802.1p (0-7):	

2. Enter a name of the profile and configure the required attributes.

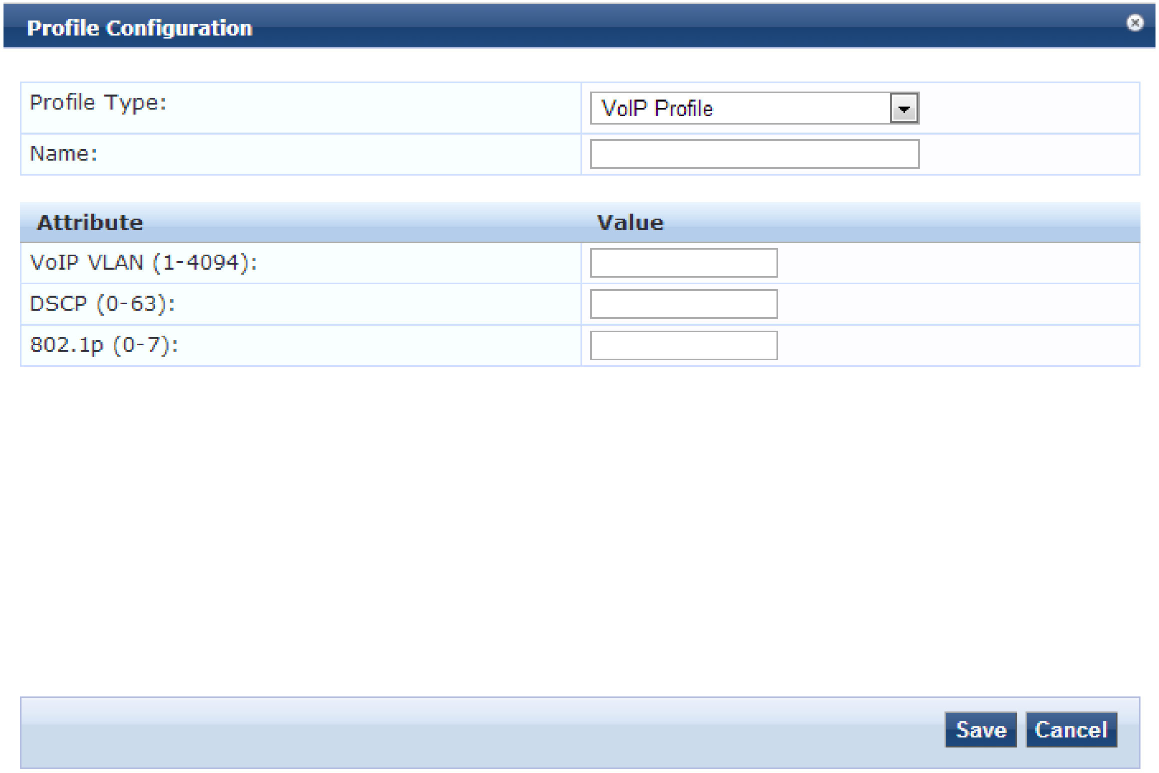
VoIP Profile

To define a VoIP Profile:

1. Click the **Add VoIP Profile** link.

   The **Add VoIP Profile** dialog opens:

Figure 356: *Add VoIP Profile Dialog*



Profile Type:	VoIP Profile
Name:	

Attribute	Value
VoIP VLAN (1-4094):	
DSCP (0-63):	
802.1p (0-7):	

2. Enter a name for the profile and configure the required attributes.

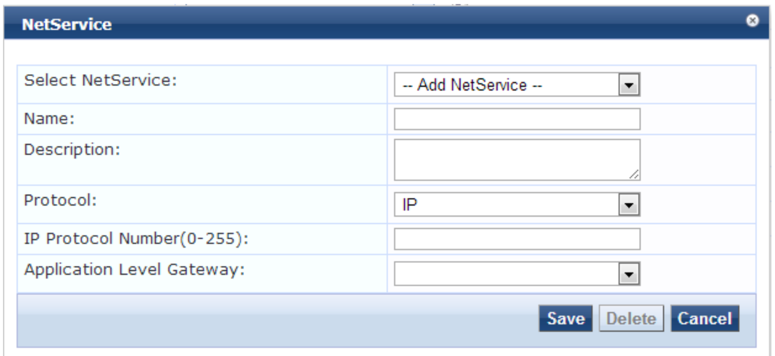
NetService Configuration

To define a NetService Configuration profile:

1. Click the **Manage NetServices** link.

   The **NetService** dialog opens:

Figure 357: *NetService Dialog*



Select NetService:	-- Add NetService --
Name:	
Description:	
Protocol:	IP
IP Protocol Number(0-255):	
Application Level Gateway:	

2. Enter a name for the profile and configure the required attributes.

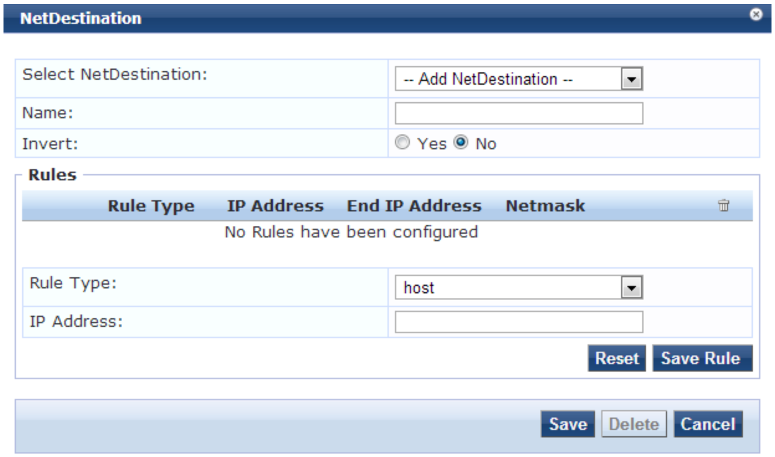
NetDestination Configuration

To define a NetDestination Configuration profile:

1. Click the **Manage NetDestinations** link.

   The **NetDestinations** dialog opens:

Figure 358: *NetDestinations Dialog*



NetDestination

Select NetDestination:	-- Add NetDestination --
Name:	
Invert:	○ Yes ● No

Rules

Rule Type	IP Address	End IP Address	Netmask

No Rules have been configured

Rule Type:	host
IP Address:	

2. Enter a name for the profile and configure the required attributes.

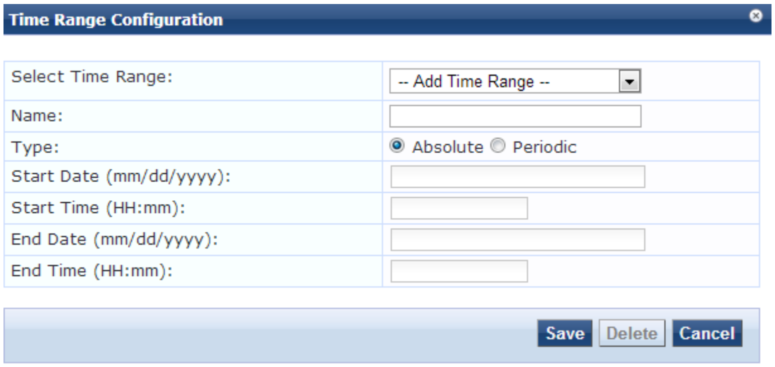
Time Range Configuration

To define a Time Range Configuration profile:

1. Click the **Manage Time Ranges** link.

   The **Time Range Configuration** dialog opens:

Figure 359: *Time Range Configuration Dialog*



Time Range Configuration

Select Time Range:	-- Add Time Range --
Name:	
Type:	● Absolute ○ Periodic
Start Date (mm/dd/yyyy):	
Start Time (HH:mm):	
End Date (mm/dd/yyyy):	
End Time (HH:mm):	

2. Enter a name for the profile and configure the required attributes.

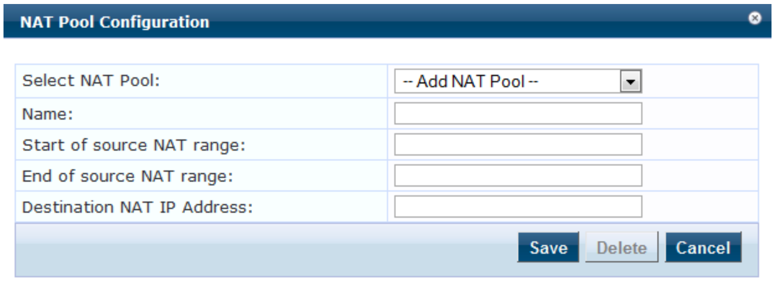
NAT Pool Configuration

To define a NAT (Network Address Translation) Pool Configuration profile:

1. Click the **Manage NAT Pool Configuration** link.

   The **NAT Pool Configuration** dialog opens:

Figure 360: *NAT Pool Configuration Dialog*



NAT Pool Configuration

Select NAT Pool:	-- Add NAT Pool --
Name:	
Start of source NAT range:	
End of source NAT range:	
Destination NAT IP Address:	

2. Enter a name for the profile and configure the required attributes.

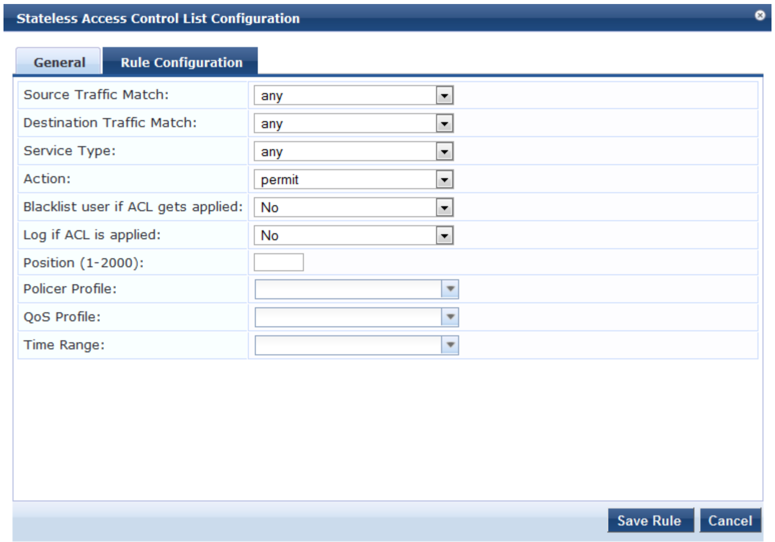
Adding a Stateless Access Control List

To add a Stateless Access Control List:

1. Click the **Add Stateless Access Control List** link.

   The **Stateless Access Control List Configuration** dialog opens:

Figure 361: *Stateless Access Control List Configuration Dialog*



Stateless Access Control List Configuration

Source Traffic Match:	any
Destination Traffic Match:	any
Service Type:	any
Action:	permit
Blacklist user if ACL gets applied:	No
Log if ACL is applied:	No
Position (1-2000):	
Policer Profile:	
QoS Profile:	
Time Range:	

2. Enter a name for the Stateless ACL.
3. On the **General** tab, click the **Add Rule** link.

   The **Rule Configuration** dialog opens.
4. Enter the required attributes in the **Rule Configuration** dialog.
5. Click **Save Rule**.

Adding a Session Access Control List

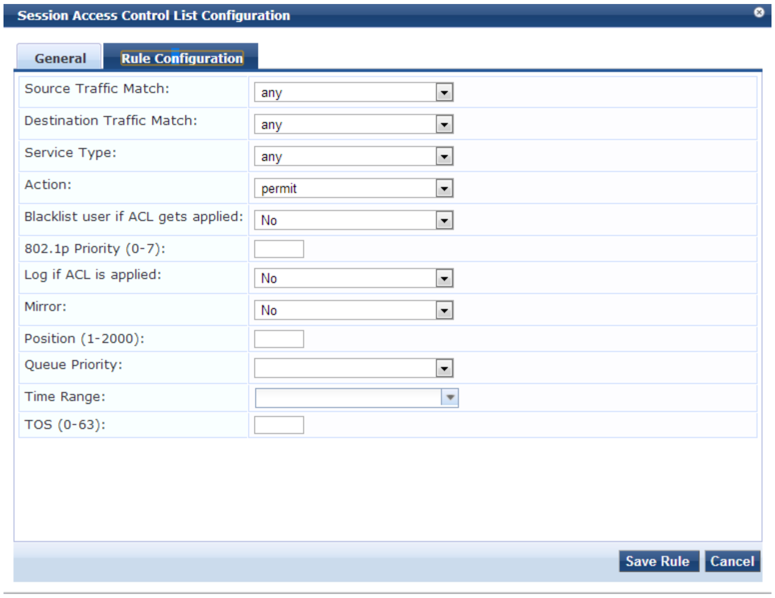
To add a Session Access Control List:

1. Click the **Add Session Access Control List** link.

   The **Session Access Control List Configuration** dialog opens.
2. Enter a name for the Session ACL.
3. On the **General** tab, click the **Add Rule** link.

   The **Rule Configuration** dialog opens.

Figure 362: *Session Access Control List Rule Configuration Dialog*



Session Access Control List Configuration

Source Traffic Match:	any
Destination Traffic Match:	any
Service Type:	any
Action:	permit
Blacklist user if ACL gets applied:	No
802.1p Priority (0-7):	
Log if ACL is applied:	No
Mirror:	No
Position (1-2000):	
Queue Priority:	
Time Range:	
TOS (0-63):	

You can view different fields depending on the **Action** type you choose. For example, if you select the **dual-nat** action type, you can view the **Dual NAT Pool** field additionally to specify the action.

4. Enter the required attributes in the **Rule Configuration** dialog.
5. Click **Save Rule**.

Adding an Ethernet/MAC Access Control List

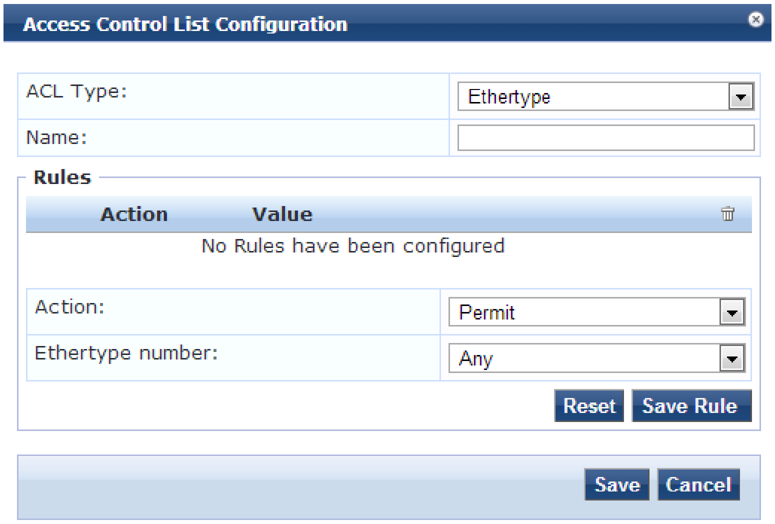
To add an Ethernet/MAC Access Control List:

1. Click the **Add Ethernet/MAC Access Control List** link.

   The **Session Access Control List Configuration** dialog opens.

   The ACL Type is set to **Ethertype**.

Figure 363: *Ethernet/MAC Access Control List Configuration Dialog*



Access Control List Configuration

ACL Type:	Ethertype
Name:	

Rules

Action	Value
No Rules have been configured	

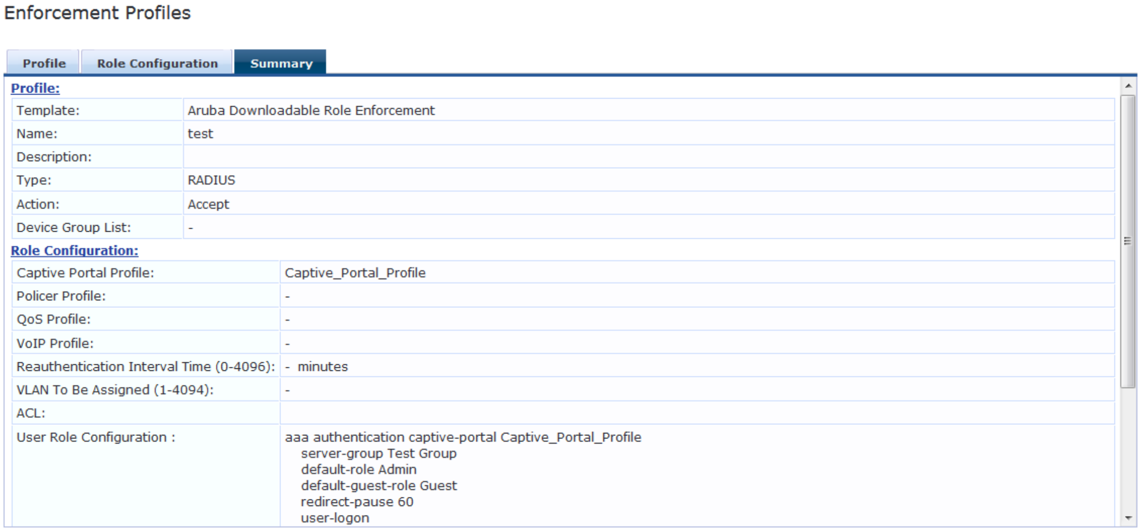
Action:	Permit
Ethertype number:	Any

2. Enter a name for the Ethernet/MAC Access Control List.
3. Enter the required attributes in the **Rules** section of the page and click **Reset**, then click **Save Rule**.
4. When finished, click **Save**.

Summary Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Role Configuration** tabs.

Figure 364: *Aruba Downloadable Role Enforcement > Summary Tab*



Enforcement Profiles

Profile:

Template:	Aruba Downloadable Role Enforcement
Name:	test
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Role Configuration:

Captive Portal Profile:	Captive_Portal_Profile
Policer Profile:	-
QoS Profile:	-
VoIP Profile:	-
Reauthentication Interval Time (0-4096):	- minutes
VLAN To Be Assigned (1-4094):	-
ACL:	
User Role Configuration :	aaa authentication captive-portal Captive_Portal_Profile server-group Test Group default-role Admin default-guest-role Guest redirect-pause 60 user-logon

Aruba RADIUS Enforcement Profile

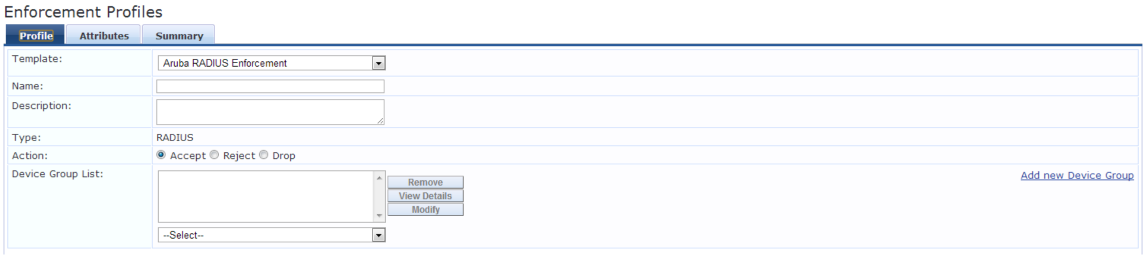
This section describes the following Aruba RADIUS Enforcement profile features:

- Profile Configuration on page 376
- Attributes Configuration on page 377
- Summary Information on page 378

Profile Configuration

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 365: *Aruba RADIUS Enforcement > Profile Tab*



Enforcement Profiles

Template:	Aruba RADIUS Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

The following table describes the **Aruba RADIUS Enforcement** > **Profile** tab parameters:

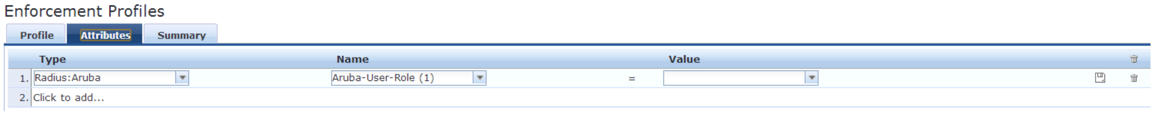
Table 184: *Aruba RADIUS Enforcement > Profile Parameters*

Parameter	Action/Description
Template	Select Aruba RADIUS Enforcement.
Name	Enter the name of the profile. The name is displayed on the **Configuration** > **Enforcement** > **Profiles** page.
Description	Enter a description that provides additional information about the profile. This description is displayed in 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 **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
Add New Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 459.

Attributes Configuration

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 366: *Aruba RADIUS Enforcement > Attributes Dialog*



Enforcement Profiles

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role (1)	=	
2.	Click to add...			

The following table describes the **Aruba RADIUS Enforcement** > **Attributes** parameters:

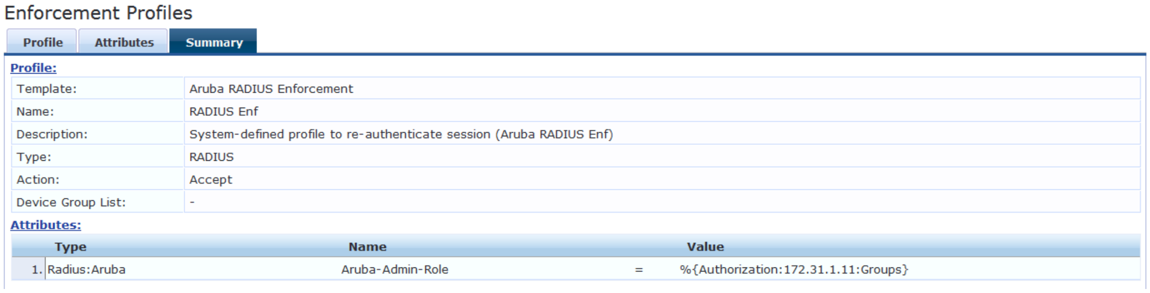
Table 185: *Aruba RADIUS Enforcement > Attributes Parameters*

Attribute	Action/Description
Type	Select one of the following attribute types: - Radius:Aruba - Radius:IETF - Radius:Cisco - Radius: Hewlett-Packared-Enterprise - Radius: Lucent-Alcatel-Enterprise - Radius:Microsoft - Radius:Avenda For more information, see RADIUS Namespaces on page 884.
Name	Select the appropriate **Name** attribute. The options provided for the **Name** attribute depend on the **Type** attribute selected.
Value	Specify the appropriate **Value** attribute. The options provided for the **Value** attribute depend on the **Type** and **Name** attributes selected.

Summary Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab.

Figure 367: *Aruba RADIUS Enforcement > Summary Tab*



Profile:

Template:	Aruba RADIUS Enforcement
Name:	RADIUS Enf
Description:	System-defined profile to re-authenticate session (Aruba RADIUS Enf)
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-Admin-Role	=	%{Authorization:172.31.1.11:Groups}

Cisco Downloadable ACL Enforcement Profile

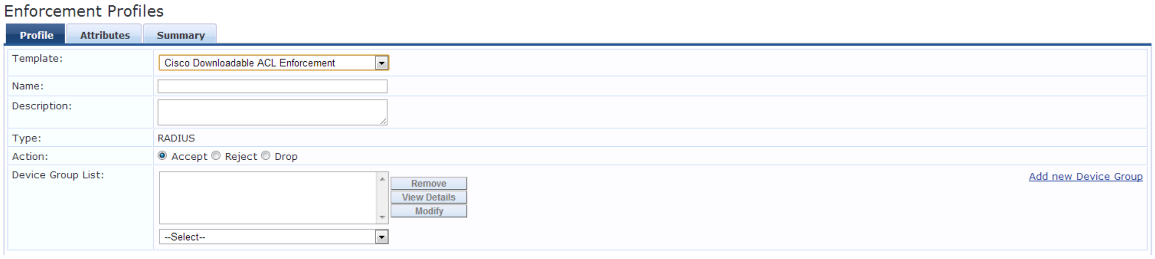
Use this page to configure the Cisco Downloadable ACL Enforcement profile.

Profile Configuration

Use the **Profile** tab to configure the Cisco Downloadable ACL Enforcement profile.

The following figure displays the **Cisco Downloadable ACL Enforcement** > **Profile** dialog:

Figure 368: *Cisco Downloadable ACL Enforcement > Profile Dialog*



Enforcement Profiles

Template: Cisco Downloadable ACL Enforcement

Name:

Description:

Type: RADIUS

Action: ● Accept ○ Reject ○ Drop

Device Group List: --Select--

Specify the **Cisco Downloadable ACL Enforcement** > **Profile** parameters as described in the following table:

Table 186: *Cisco Downloadable ACL Enforcement > Profile Parameters*

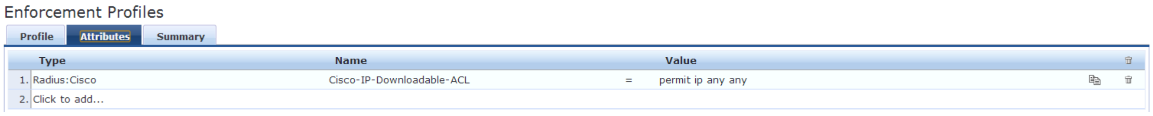
Parameter	Action/Description
Template	Select the **Cisco Downloadable ACL Enforcement** template.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	The field is populated automatically with Type: **RADIUS**.
Action	To define the action to take on the request, click **Accept**, **Reject**, or **Drop**.
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 **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Attributes Configuration

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** dialog:

Figure 369: *Cisco Downloadable ACL Enforcement > Attributes Dialog*



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

Specify the **Cisco Downloadable ACL Enforcement > Attributes** parameters as described in the following table:

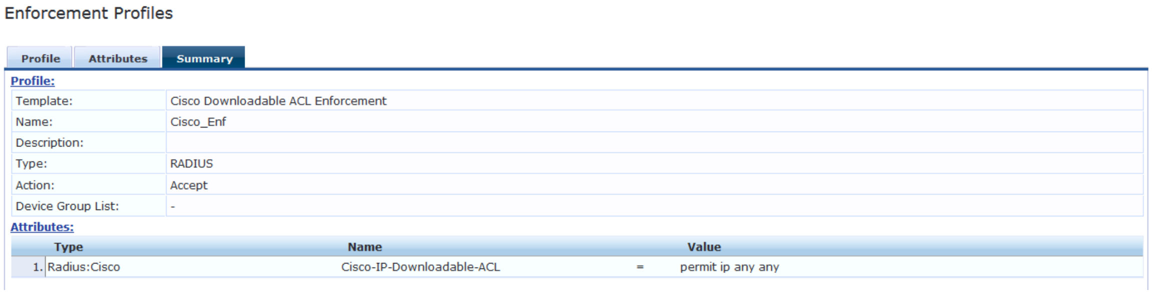
Table 187: *Cisco Downloadable ACL Enforcement > Attributes Parameters*

Parameter	Action/Description
Type	Select one of the following attribute types: ■ Radius:IETF ■ Radius:Cisco ■ Radius: Hewlett-Packared-Enterprise ■ Radius: Alcatel-Lucent-Enterprise ■ Radius:Microsoft ■ Radius:Avenda ■ Radius:Aruba For more information, see RADIUS Namespaces on page 884.
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 Information

The **Summary** tab summarizes the parameters configured in the Cisco Downloadable ACL Enforcement profile.

Figure 370: *Cisco Downloadable ACL Enforcement > Summary Tab*



Profile:

Template:	Cisco Downloadable ACL Enforcement
Name:	Cisco_Enf
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Cisco	Cisco-IP-Downloadable-ACL	=	permit ip any any

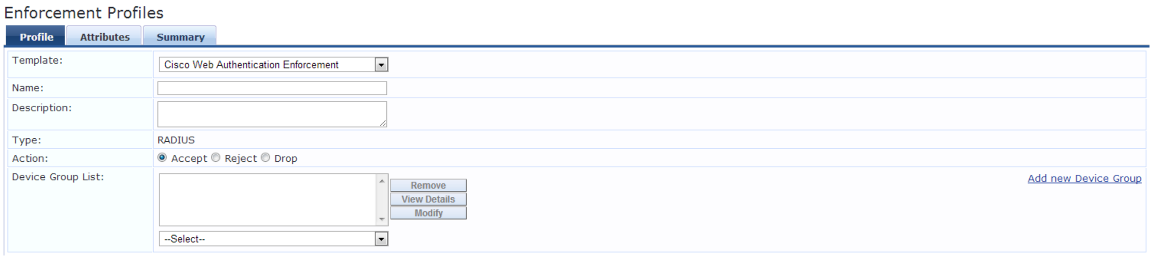
Cisco Web Authentication Enforcement Profile

Use this page to configure profile and attribute parameters for the **Cisco Web Authentication Enforcement** profile.

Profile Configuration

Use the **Profile** tab to configure the template, type of the profile, and device group list.

Figure 371: *Cisco Web Authentication Enforcement > Profile Tab*



Template: Cisco Web Authentication Enforcement
Name:
Description:
Type: RADIUS
Action: ● Accept ○ Reject ○ Drop
Device Group List: --Select--

Specify the **Cisco Web Authentication Enforcement > Profile** tab parameters as described in the following table:

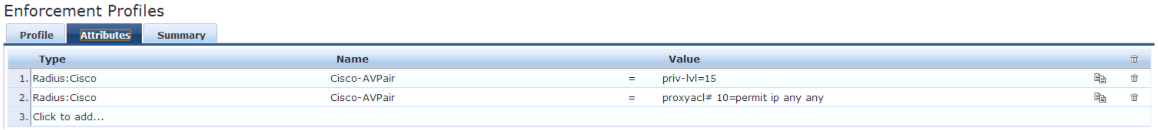
Table 188: *Cisco Web Authentication Enforcement > Profile Tab Parameters*

Parameter	Action/Description
Template	Select the **Cisco Web Authentication Enforcement** template.
Name	Enter the name of the profile.
Description	Enter a description that provides additional information about the profile (recommended).
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 **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 459.

Attributes Configuration

Use the **Attributes** tab to configure the attribute name and attribute value. The following figure displays the **Cisco Web Authentication Enforcement > Profile** tab:

Figure 372: *Cisco Web Authentication Enforcement > Attributes Tab*



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

The following table describes the **Cisco Web Authentication Enforcement > Attributes** parameters:

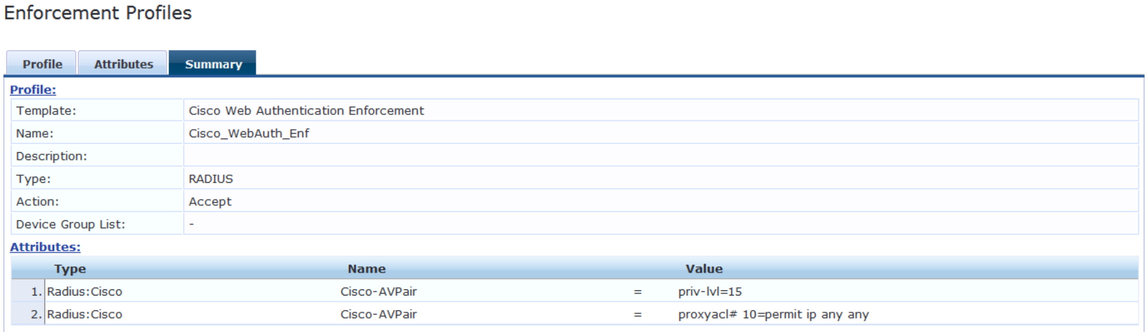
Table 189: *Cisco Web Authentication Enforcement > Attributes Parameters*

Parameter	Description
Type	Select one of the following attribute types: ● Radius:Aruba ● Radius:IETF ● Radius:Cisco ● Radius: Hewlett-Packared-Enterprise ● Radius: Lucent-Alcatel-Enterprise ● Radius:Microsoft ● Radius:Avenda For more information, see RADIUS Namespaces on page 884.
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 Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attribute** tabs.

Figure 373: *Cisco Web Authentication Enforcement > Summary Tab*



Profile:

Template:	Cisco Web Authentication Enforcement
Name:	Cisco_WebAuth_Enf
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

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

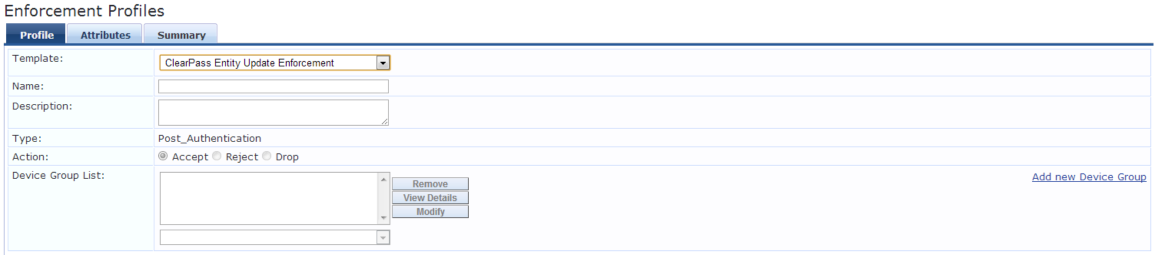
ClearPass Entity Update Enforcement Profile

Use this page to configure profile and attribute parameters for the **ClearPass Entity Update Enforcement** profile.

Profile Configuration

Use the **Profile** tab to configure the template, type of the profile, and device group list.

Figure 374: *ClearPass Entity Update Enforcement > Profile Tab*



Enforcement Profiles

Template:	ClearPass Entity Update Enforcement
Name:	
Description:	
Type:	Post_Authentication
Action:	● Accept ○ Reject ○ Drop
Device Group List:	

Specify the **ClearPass Entity Update Enforcement > Profile** parameters as described in the following table:

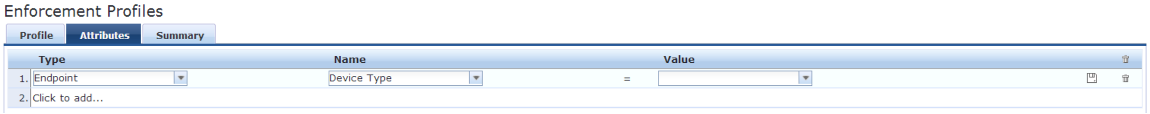
Table 190: *ClearPass Entity Update Enforcement > Profile Parameters*

Parameter	Acvtion/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 **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
Add new Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 459.

Attributes Configuration

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 375: *ClearPass Entity Update Enforcement Attributes tab*



	Type	Name		Value
1.	Endpoint	Device Type	=	
2.	Click to add...			

Specify the **ClearPass Entity Update Enforcement > Attributes** parameters as described in the following table:

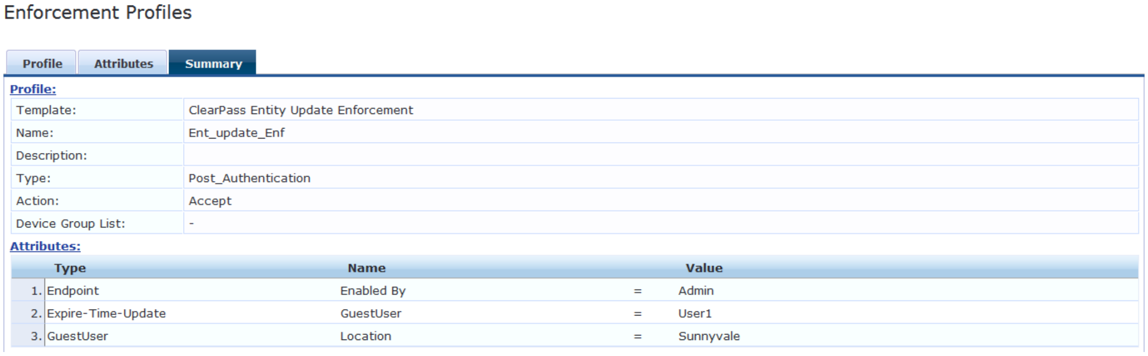
Table 191: *ClearPass Entity Update Enforcement > Attributes Parameters*

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 Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab.

Figure 376: *ClearPass Entity Update Enforcement > Summary Tab*



Profile:

Template:	ClearPass Entity Update Enforcement
Name:	Ent_update_Enf
Description:	
Type:	Post_Authentication
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	Enabled By	=	Admin
2.	Expire-Time-Update	GuestUser	=	User1
3.	GuestUser	Location	=	Sunnyvale

CLI-Based Enforcement Profile

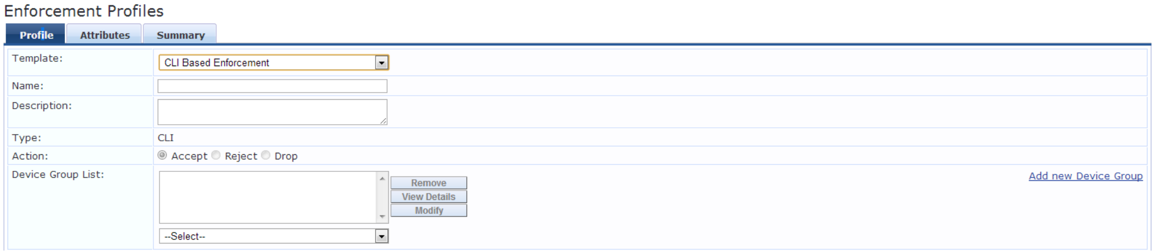
Use this page to configure profile and attribute parameters for the **CLI-Based Enforcement** profile. The **CLI-Based Enforcement** profile contains the following tabs:

- Profile Configuration on page 385
- Attributes Configuration on page 385
- Summary Information on page 386

Profile Configuration

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 377: *CLI-Based Enforcement > Profile Tab*



Enforcement Profiles

Profile | Attributes | Summary

Template:	CLI Based Enforcement
Name:	
Description:	
Type:	CLI
Action:	● Accept ○ Reject ○ Drop
Device Group List:	Remove View Details Modify --Select-- Add new Device Group

Specify the **CLI-Based Enforcement > Profile** tab parameters as described in the following table:

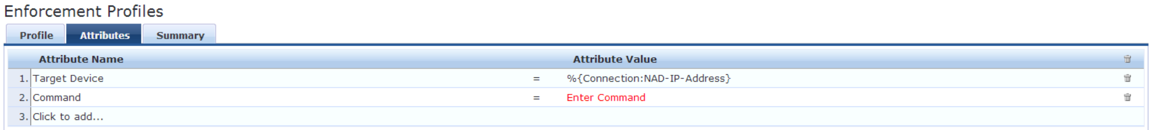
Table 192: *CLI Based Enforcement > Profile Parameters*

Parameter	Action/Description
Template	Select the **CLI Based Enforcement** template.
Name	Enter the name of the profile.
Description	Enter a description that provides additional information about the profile.
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 459.

Attributes Configuration

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile.

Figure 378: *CLI Based Enforcement > Attributes Tab*



Enforcement Profiles

Profile | Attributes | Summary

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

Specify the **CLI Based Enforcement > Attributes** parameters as described in the following table:

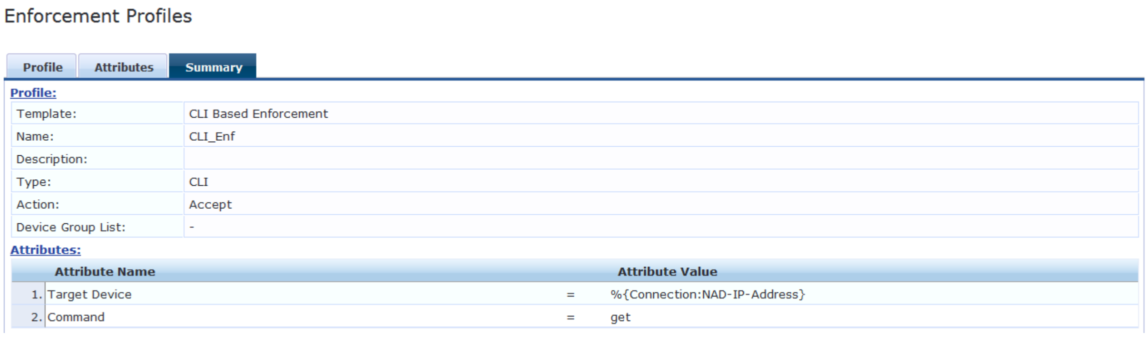
Table 193: *CLI Based Enforcement > Attributes Parameters*

Attribute	Action/Parameter
Attribute Name	Select **Command** or **Target Device**.
Attribute Value	Specify the appropriate **Attribute Value**. The options provided for the **Attribute Value** depend on the selected **Attribute Name**.

Summary Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab. The following figure displays the **CLI-Based Enforcement > Summary** tab:

Figure 379: *CLI-Based Enforcement > Summary Tab*



Profile:

Template:	CLI Based Enforcement
Name:	CLI_Enf
Description:	
Type:	CLI
Action:	Accept
Device Group List:	-

Attributes:

	Attribute Name		Attribute Value
1.	Target Device	=	%{Connection:NAD-IP-Address}
2.	Command	=	get

Filter ID Based Enforcement Profile

This section provides the following information:

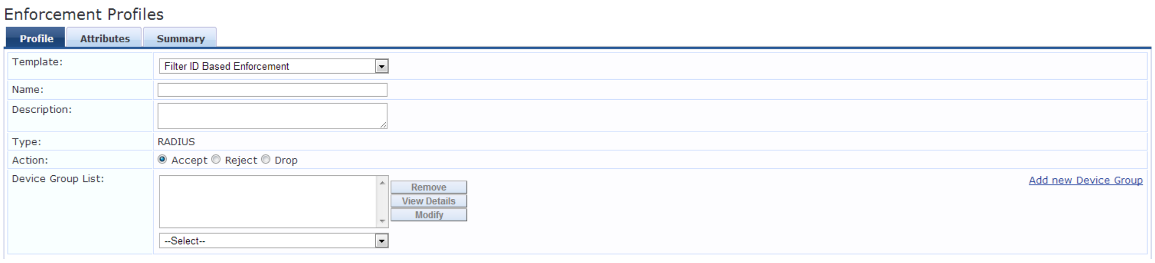
- Profile Configuration on page 386
- Attributes Configuration on page 387

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 Configuration

The following figure displays the **Filter ID Based Enforcement > Profile** dialog:

Figure 380: *Filter ID Based Enforcement Profile Dialog*



Template:	Filter ID Based Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Specify the **Filter ID Based Enforcement Profile** parameters as described in the following table:

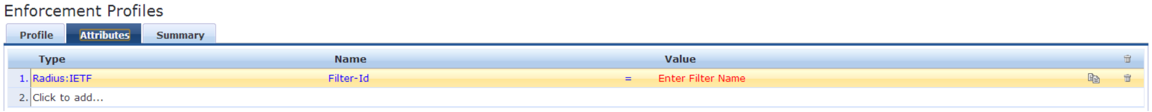
Table 194: *Filter ID Based Enforcement > Profile Parameters*

Parameter	Action/Description
Template	Select the **Filter ID Based Enforcement** template.
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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Attributes Configuration

The following figure displays the **Filter ID Based Enforcement Profile > Attributes** dialog:

Figure 381: *Filter ID Based Enforcement Profile > Attributes Dialog*



Enforcement Profiles

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

Specify the **Filter ID Based Enforcement > Attributes** parameters as described in the following table:

Table 195: *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: Hewlett-Packared-Enterprise - Radius: Lucent-Alcatel-Enterprise - Radius:Microsoft - Radius:Avenda For more information, see RADIUS Namespaces on page 884.
Name	Select the desired **Name** attribute. The options displayed for the **Name** attribute depend on the attribute that was selected.
Value	Specify the appropriate **Value**. The options displayed for the **Value** attribute depend on the **Type** attribute and **Name** attribute that were selected.

Generic Application Enforcement Profile

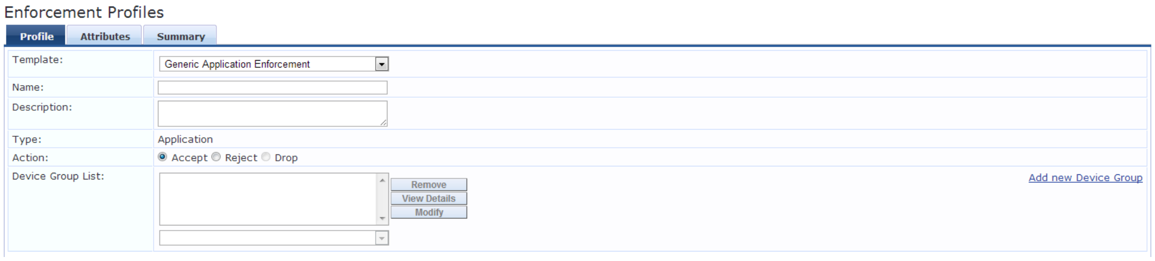
Use this page to configure profile and attribute parameters for the **Generic Application Enforcement** profile. The **Generic Application Enforcement** profile contains the following tabs:

- Profile Configuration on page 388
- Attributes Configuration on page 389
- Summary Information on page 390

Profile Configuration

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 382: *Generic Application Enforcement > Profile Tab*



Template: Generic Application Enforcement

Name:

Description:

Type: Application

Action: ● Accept ○ Reject ○ Drop

Device Group List:

Specify the **Generic Application Enforcement > Profile** parameters as described in the following table:

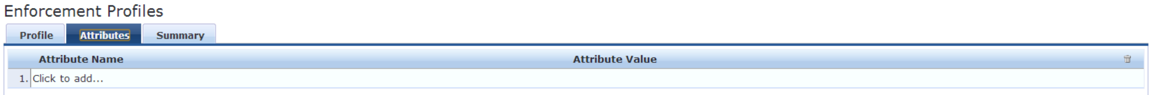
Table 196: *Generic Application Enforcement > Profile Tab Parameters*

Parameter	Action/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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
Add New Device Group	Click this link to add a new device group, For more information, see Adding and Modifying Device Groups on page 459.

Attributes Configuration

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 383: *Generic Application Enforcement > Attributes Tab*


Enforcement Profiles

	Attribute Name	Attribute Value
1.	Click to add...	

Specify the **Generic Application Enforcement > Attributes** parameters as described in the following table:

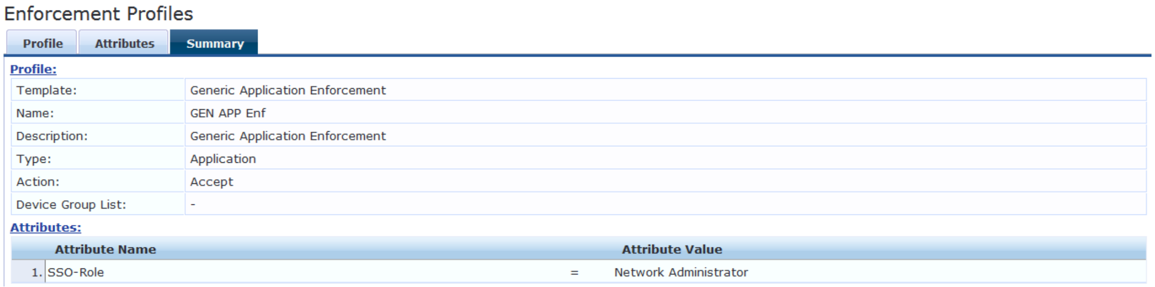
Table 197: *Generic Application Enforcement > Attributes Parameters*

Parameter	Action/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 Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab.

Figure 384: *Generic Application Enforcement > Summary Tab*



Profile:

Template:	Generic Application Enforcement
Name:	GEN APP Enf
Description:	Generic Application Enforcement
Type:	Application
Action:	Accept
Device Group List:	-

Attributes:

	Attribute Name		Attribute Value
1.	SSO-Role	=	Network Administrator

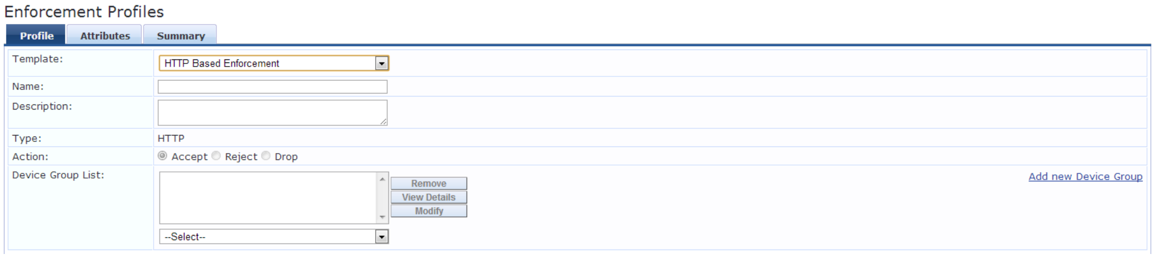
HTTP Based Enforcement Profile

Use this page to configure the HTTP based Enforcement Profile.

Profile Configuration

The following figure displays the **HTTP Based Enforcement > Profile** dialog:

Figure 385: *HTTP Based Enforcement Profile Dialog*



Template:	HTTP Based Enforcement
Name:	
Description:	
Type:	HTTP
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Specify the **HTTP Based Enforcement > Profile** parameters as described in the following table:

Table 198: *HTTP Based Enforcement Profile Parameters*

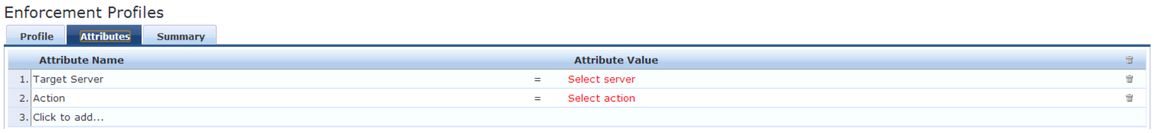
Parameter	Action/Description
Template	Select the **HTTP Based Enforcement** template.
Name	Enter the name of the profile. The name is displayed in the **Name** column on the **Configuration > Enforcement > Profiles** page.
Description	Enter a description of the profile. The description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	This field is populated automatically with **HTTP**.

Table 198: *HTTP Based Enforcement Profile Parameters (Continued)*

Parameter	Action/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 **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Attributes Configuration

Figure 386: *HTTP Based Enforcement Attributes Dialog*



Enforcement Profiles

	Attribute Name		Attribute Value
1.	Target Server	=	Select server
2.	Action	=	Select action
3.	Click to add...		

Table 199: *HTTP Based Enforcement Attributes Parameters*

Parameter	Action/Description
Attribute Name	Select the attribute name: **Target Server** or **Action**.
Attribute Value	Specify the appropriate value. The options displayed for the **Attribute Value** depend on the Attribute Name that was selected.

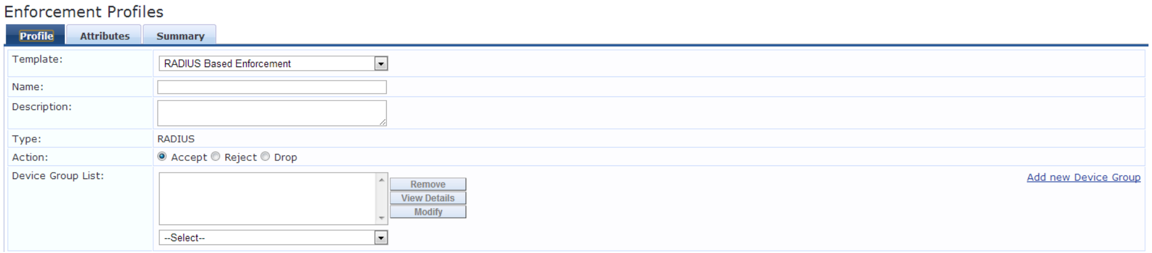
RADIUS Based Enforcement Profile

Use this page to configure profile and attribute parameters for the RADIUS based enforcement profiles.

Profile Configuration

The following figure displays the **RADIUS Based Enforcement Profile** tab:

Figure 387: *RADIUS Based Enforcement > Profile Tab*



Enforcement Profiles

Template:	RADIUS Based Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Specify the **RADIUS Based Enforcement Profile** parameters as described in the following table:

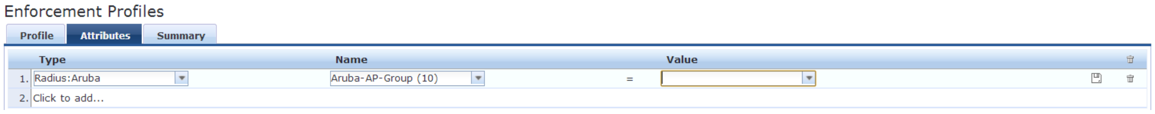
Table 200: *RADIUS Based Enforcement Profile Parameters*

Parameter	Action/Description
Template	Select the **RADIUS Based Enforcement** template.
Name	Enter the name of the profile.
Description	Enter a description of the profile.
Type	**RADIUS**. This field is populated automatically.
Action	Enabled. Click **Accept**, **Reject**, or **Drop**.
Device Group List	Select a Device Group from the drop-down list. All configured device groups are listed in the **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459

Attributes Tab

The following figure displays the **RADIUS Based Enforcement > Attributes** dialog:

Figure 388: *RADIUS Based Enforcement Attributes Dialog*



Enforcement Profiles

	Type	Name		Value
1.	Radius:Aruba	Aruba-AP-Group (10)	=	
2.	Click to add...			

Specify the **RADIUS Based Enforcement > Attributes** parameters as described in the following table:

Table 201: *RADIUS Based Enforcement > Attributes Parameters*

Parameter	Description
Type	Select one of the following attribute types: - Radius:Aruba - Radius:IETF - Radius:Cisco - Radius: Hewlett-Packared-Enterprise - Radius: Lucent-Alcatel-Enterprise - Radius:Microsoft - Radius:Avenda For more information, see RADIUS Namespaces on page 884.
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.

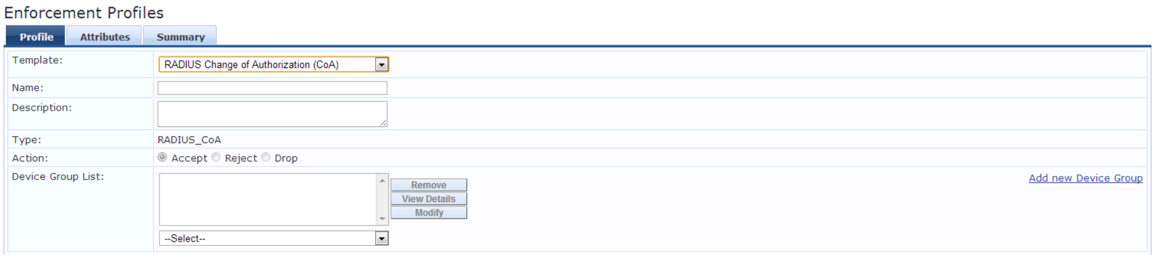
RADIUS Change of Authorization (CoA) Profile

Use this page to configure the RADIUS Change of Authorization (CoA) enforcement profile.

Profile Configuration

The following figure displays the **RADIUS Change of Authorization (CoA)** > **Profile** tab:

Figure 389: *RADIUS Change of Authorization (CoA) > Profile Tab*



Enforcement Profiles

Template:	RADIUS Change of Authorization (CoA)
Name:	
Description:	
Type:	RADIUS_CoA
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Specify the **RADIUS Change of Authorization (CoA) > Profile** tab parameters as described in the following table:

Table 202: *RADIUS Change of Authorization (CoA) Profile Parameters*

Parameter	Action/Description
Template	Select the **RADIUS Change of Authorization (CoA)** template.
Name	Enter the name of this enforcement profile.
Type	**RADIUS_CoA** is automatically populated.

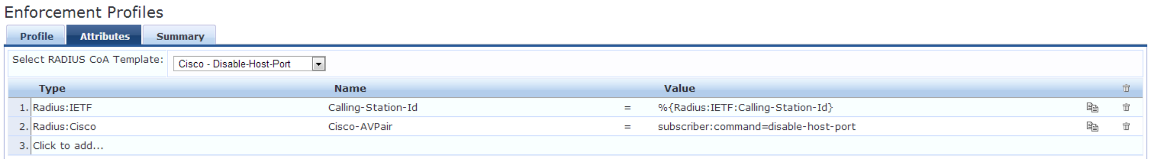
Table 202: *RADIUS Change of Authorization (CoA) Profile Parameters (Continued)*

Parameter	Action/Description
Action	Disabled.
Device Group List	Optionally, select a Device Group from the drop-down list. 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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Attributes Configuration

The following figure displays the **RADIUS Change of Authorization (CoA)** > **Attributes** tab:

Figure 390: *RADIUS Change of Authorization (CoA) > Attributes Dialog*



Enforcement Profiles

Select RADIUS CoA Template: Cisco - Disable-Host-Port

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:Cisco	Cisco-AVPair	=	subscriber:command=disable-host-port
3.	Click to add...			

The following table describes the **RADIUS Change of Authorization (CoA)** > **Attributes** parameters:

Table 203: *RADIUS Change of Authorization (CoA) Attributes Parameters*

Parameter	Action/Description
Select RADIUS CoA Template	Select one of the following RADIUS CoA templates: ● Aruba - Change-User-Role ● Aruba - Change-VPN-User-Role ● Cisco - Bounce-Host-Port ● Cisco-Disable-Host-Port ● Cisco - Reauthenticate-Session ● Hewlett-Packard-Enterprise - Change-VLAN ● Hewlett-Packard-Enterprise - Generic-CoA ● Hewlett-Packard-Enterprise - Port-Bounce-Host-HP ● IETF- Generic-CoA-IETF ● IETF - Terminate-Session-IETF
Type	Select one of the following attribute types: ■ Radius:IETF ■ Radius:Cisco ■ Radius: Hewlett-Packared-Enterprise ■ Radius: Alcatel-Lucent-Enterprise ■ Radius:Microsoft ■ Radius:Avenda ■ Radius:Aruba
Name	The options displayed for the **Name** attribute depend on the **Template** and **Type** attributes that were selected.
Value	The content for the **Value** attribute depends on the **Template**, **Type**, and **Name** attributes that were selected.

Session Notification Enforcement Profile

Use this page to configure the **Session Notification Enforcement** profile.

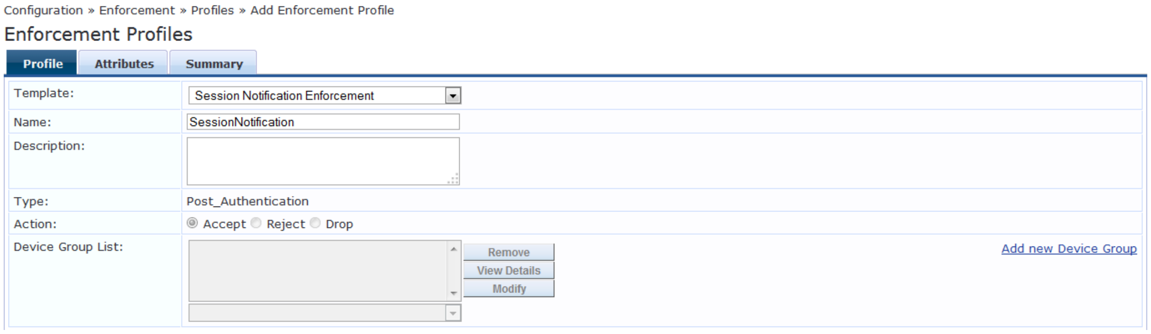
You can send notification of a change in IP address to any external context server (such as a firewall) by configuring that server as a generic HTTP server and adding the appropriate generic HTTP context server actions.

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.

Profile Configuration

The following figure displays the **Session Notification Enforcement** > **Profile** tab:

Figure 391: *Session Notification Enforcement > Profile Configuration Dialog*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template: Session Notification Enforcement

Name: SessionNotification

Description:

Type: Post_Authentication

Action: ● Accept ○ Reject ○ Drop

Device Group List:

The following table describes the **Session Notification Enforcement** > **Profile** parameters:

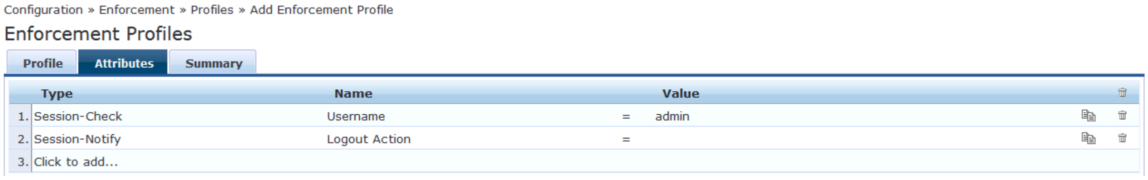
Table 204: *Session Notification Enforcement Profile Tab Parameters*

Parameter	Action/Description
Template	Select **Session Notification Enforcement**.
Name	Enter the name of the profile.
Description	Enter a description of the profile (recommended).
Type	The field is populated automatically with: **Post_Authentication**.
Action	Disabled.
Device Group List	Select a device group from the drop-down list. 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. See Adding and Modifying Device Groups on page 459for more information.

Attributes Configuration

The following figure displays the **Session Notification Enforcement** > **Attributes** dialog:

Figure 392: *Session Notification Enforcement > Attributes Configuration Dialog*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Type	Name		Value
1.	Session-Check	Username	=	admin
2.	Session-Notify	Logout Action	=	
3.	Click to add...			

Specify the **Session Notification Enforcement** > **Attributes** parameters as described in the following table:

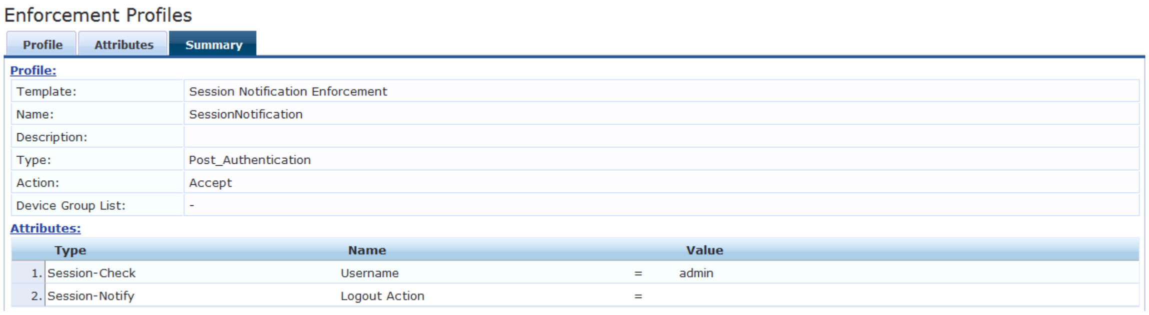
Table 205: *Session Notification Enforcement > Attributes Parameters*

Parameter	Action/Description
Type	Select one of the following **Type** attributes: • Session-Check • Session-Notify Palo Alto integration is extended to Guest MAC Caching use cases. Configure the Session-Check attributes as follows: • **Session-Check::Username = %{Endpoint:Username}** **NOTE:** Post authentication sends the Guest username instead of the MAC address in the user ID updates. • **Session-Notify**: The **Name** options are: ▪ Login Action ▪ Logout Action ▪ Server IP ▪ Server Type **Server Type** options: ▪ Generic HTTP ▪ Palo Alto Networks Panorama ▪ Palo Alto Networks Firewall **Server IP** options: a choice of IP address/hostnames for the corresponding type of server as **Value**. The **Target Server** attribute must be specified before you can use the **Server IP** option. Once the server IP address is selected, you can select **Login Action** or **Logout Action**. 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.
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 Information

This **Summary** tab summarizes the parameters configured for Session Notification Enforcement.

Figure 393: *Session Notification Enforcement > Summary Tab*



Profile:

Template:	Session Notification Enforcement
Name:	SessionNotification
Description:	
Type:	Post_Authentication
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Session-Check	Username	=	admin
2.	Session-Notify	Logout Action	=	

Session Restrictions Enforcement Profile

ClearPass uses Keep-Alive messages to issue CoA (Change of Authorization) for a Session Restrictions Enforcement Profile if OnGuard Agent is disconnected (see below, Examples of Session-Check Enforcement

Profile Configurations). For related information, see OnGuard Global Agent Settings on page 682.

Profile Configuration

To configure Profile and Attribute parameters for a Session Restrictions Enforcement profile:

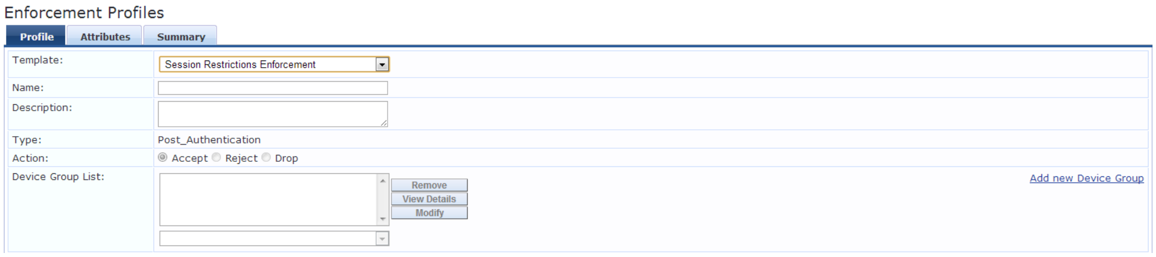
1. Navigate to **Configuration** > **Enforcement** > **Profiles**.

   The **Enforcement Profiles** page opens.
2. Click **Add**.

   The **Add Enforcement Profiles** > **Profile** tab opens.
3. From the **Template** drop-down, select **Session Restrictions Enforcement**.

   The **Add Session Restrictions Enforcement > Profile** dialog opens:

Figure 394: *Add Session Restrictions Enforcement > Profile Tab*



Template: Session Restrictions Enforcement

Name:

Description:

Type: Post_Authentication

Action: ● Accept ○ Reject ○ Drop

Device Group List:

4. Specify the **Session Restrictions Enforcement > Profile** parameters as described in the following table:

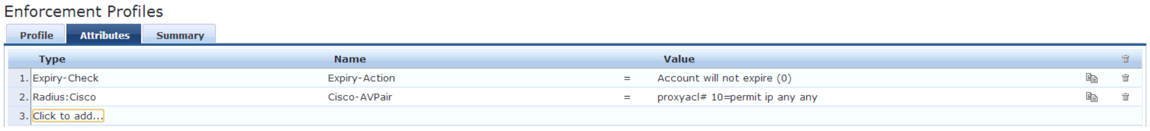
Table 206: *Session Restrictions Enforcement Profile Parameters*

Parameter	Action/Description
Template	Select **Session Restrictions Enforcement**.
Name	Enter the name of the enforcement profile.
Description	Optionally, enter a description of the enforcement profile (recommended).
Type	**Post_Authentication**. The **Type** field is populated automatically when you select the **Session Restrictions Enforcement** template.
Action	By default, this field is disabled. It is enabled only when **RADIUS** type is selected.
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 **Configuration > Network > Device Groups** page. After you add one or more device groups, select a group and take one of the following actions: ● To delete the selected device group list entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Attributes Configuration

The following figure displays the **Session Restrictions Enforcement > Attributes** tab:

Figure 395: *Session Restrictions Enforcement Profile > Attributes Dialog*



	Type	Name		Value
1.	Expiry-Check	Expiry-Action	=	Account will not expire (0)
2.	Radius:Cisco	Cisco-AVPair	=	proxyacl# 10=permit ip any any
3.	Click to add...			

1. Specify the **Session Restrictions Enforcement > Attributes** parameters as described in Table 207:

Table 207: *Session Restrictions Enforcement Attributes Parameters*

Parameter	Description
Type	Select from the following attribute types: ● Bandwidth-Check ● Expiry-Check ● Post-Auth-Check ● Session-Check
Name	The options displayed for the **Name** attribute depend on the **Type** attribute that was selected. ● **Type: Bandwidth-Check** ■ **Allowed-Limit**: Defines the total bandwidth limit to be allowed per user or endpoint. ■ **Check-Type**: Defines the period/interval for bandwidth-based checks. Applicable only with **Allowed-Limit**. ■ **Limit-Units**: Defines the metric for bandwidth-based checks (KB, MB, GB, TB). Applicable only with **Allowed-Limit**. ■ **Start-Date**: Defines the start date for bandwidth-based checks. Applicable only with **Allowed-Limit**. ■ **Start-Time**: Defines the start time for bandwidth-based checks. Applicable only with **Allowed-Limit**. ■ **Stop-Date**: Defines the stop date for bandwidth-based checks. Applicable only with **Allowed-Limit**. ■ **Stop-Time**: Defines the stop time for bandwidth-based checks. Applicable only with **Allowed-Limit**. For configuration examples, see the next section, Examples of Bandwidth-Check Enforcement Profile Configurations. ● **Type: Expiry-Check** ■ Expiry-Action ● **Type: Post-Auth-Check** ■ Action ● **Type: Session-Check** ■ **Active-Session-Count**: Defines the number of active sessions to be allowed per user or endpoint. ■ **Agent-Connection**: Set the value to **Down** to have ClearPass check to see if the OnGuard Agent is down. ■ **Allowed-Duration**: Defines the total session duration to be allowed per user or endpoint. ■ **Check-Type**: Defines the period or interval for duration-based checks. Applicable only with **Allowed-Duration**. ■ **Duration-Units**: Defines the metric for duration-based checks. Applicable only with **Allowed-Duration**. ■ **Start-Date**: Defines the start date for duration-based checks. Applicable only with **Allowed-Duration**. ■ **Start-Time**: Defines the start time for duration-based checks. Applicable only with **Allowed-Duration**. ■ **Stop-Date**: Defines the stop date for duration-based checks. Applicable only with **Allowed-Duration**. ■ **Stop-Time**: Defines the stop time for duration-based checks. Applicable only with **Allowed Duration**.

Table 207: *Session Restrictions Enforcement Attributes Parameters (Continued)*

Parameter	Description
	■ **Username**: Defines the username for which session restrictions are enabled. Used when the client MAC address is to be defined as a username. For configuration examples, see the section below, Examples of Session-Check Enforcement Profile Configurations.
Value	The options displayed for the **Value** attribute depend on the **Type** and **Name** attributes that were selected.

Examples of Bandwidth-Check Enforcement Profile Configurations

The following are typical examples of **Session Restriction** > **Bandwidth-Check** enforcement profile configurations:

1. **Allowed-Limit**: Users/Endpoints will be disconnected after exceeding the 50 MB daily limit:
   - Bandwidth-Check > Allowed-Limit = 50
   - Bandwidth-Check > Limit-Units = MB
   - Bandwidth-Check > Check-Type = Daily
   - Post-Auth-Check > Action = Disconnect
2. **Allowed-Limit**: Users/Endpoints will be disconnected after exceeding 1 GB total bandwidth consumption. Also, users are allowed access to the network only during the defined period (between 9:00 a.m. and 6:00 p.m.).
   - Bandwidth-Check > Allowed-Limit = 1
   - Bandwidth-Check > Limit-Units = GB
   - Bandwidth-Check > Check-Type = Total
   - Bandwidth-Check > Start-Time = 09:00:00
   - Bandwidth-Check > Stop-Time = 18:00:00
   - Post-Auth-Check > Action = Disconnect

Examples of Session-Check Enforcement Profile Configurations

The following are typical examples of **Session Restriction** > **Session-Check** enforcement profile configurations:

1. **Active Session Count**: The Users/Endpoints active session count is set to **5**. Users/Endpoints connecting after the session count reaches **5** are disconnected:
   - Session-Check > Active-Session-Count = 5
   - Post-Auth-Check > Action = Disconnect
2. **Agent-Connection**: You can disconnect a session if OnGuard Agent is down:
   - Session-Check > Agent-Connection = Down
   - Post-Auth-Check > Action = Disconnect
3. **Session Duration**: The User/Endpoint is allowed access for 60 minutes daily. Users/Endpoints that exceed this session duration limit are disconnected:
   - Session-Check > Allowed-Duration = 60
   - Session-Check > Duration-Units = Minutes
   - Session-Check > Check-Type = Daily

- Post-Auth-Check > Action = Disconnect

4. **Session Duration**: The User/Endpoint is allowed access to the network daily for three hours in a specified time period (between 9:00 a.m. and 5:00 p.m.)
   - Session-Check > Allowed-Duration = 3
   - Session-Check >Duration-Units = Hours
   - Session-Check > Check-Type = Daily
   - Session-Check > Start-Time = 09:00:00
   - Session-Check Stop-Time = 17:00:00
   - Post-Auth-Check > Action = Disconnect

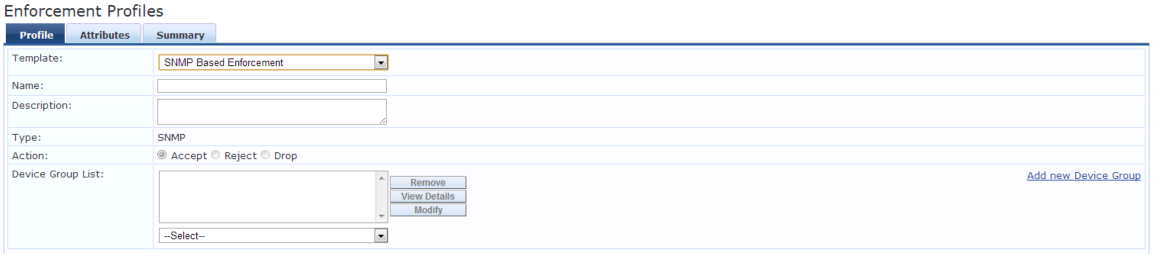
SNMP-Based Enforcement Profile

Use this page to configure the SNMP-Based Enforcement profile.

Profile Configuration

The following figure displays the **SNMP Based Enforcement** > **Profile** dialog:

Figure 396: *SNMP Based Enforcement > Profile Dialog*



Template:	SNMP Based Enforcement
Name:	
Description:	
Type:	SNMP
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Specify the **SNMP Based Enforcement** > **Profile** parameters as described in the following table:

Table 208: *SNMP Based Enforcement > Profile Tab Parameters*

Parameter	Description
Template	Select the **SNMP Based Enforcement** template.
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 (recommended). The description is displayed in the **Description** column on the **Configuration > Enforcement > Profiles** page.
Type	**SNMP**. The field is populated automatically.

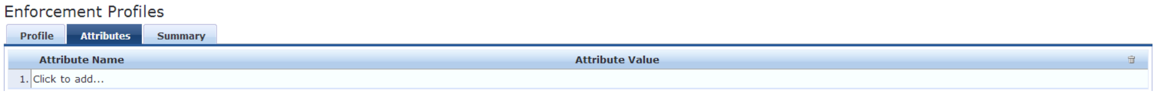
Table 208: *SNMP Based Enforcement > Profile Tab Parameters (Continued)*

Parameter	Description
Action	Disabled.
Device Group List	Select a Device Group from the drop-down list. All configured device groups are listed in the **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: - To delete the selected Device Group List entry, click **Remove**. - To see the device group parameters, click **View Details**. - To change the parameters of the selected device group, click **Modify**.
Add New Device Group	To add a new a device group, click the **Add New Device Group** link. See Adding and Modifying Device Groups on page 459.

Attributes Configuration

The following figure displays the **SNMP Based Enforcement** > **Attributes** dialog:

Figure 397: *SNMP Based Enforcement > Attributes Dialog*



Specify the **SNMP Based Enforcement** > **Attributes** parameters as described in the following table:

Table 209: *SNMP Based Enforcement Attributes Parameters*

Parameter	Action/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** depends on the **Attribute Name** that was selected.

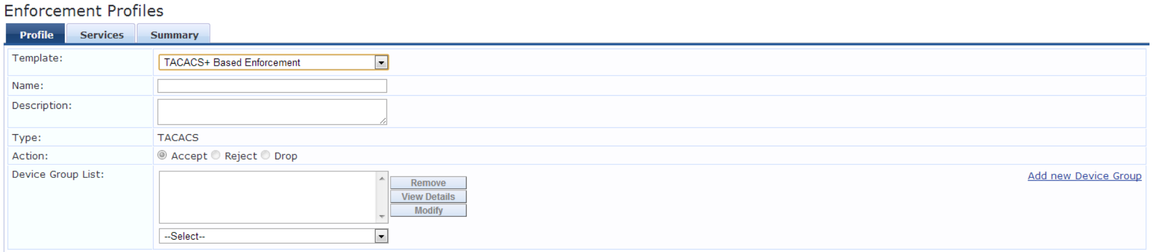
TACACS+ Based Enforcement Profile

Use this page to configure the TACACS+ Based Enforcement profile.

Profile Configuration

The following figure displays the **TACACS+ Based Enforcement** > **Profile** tab:

Figure 398: *TACACS+ Based Enforcement Profile Dialog*



Template: TACACS+ Based Enforcement

Name:

Description:

Type: TACACS

Action: ● Accept ○ Reject ○ Drop

Device Group List: --Select--

Specify the **TACACS+ Based Enforcement Profile** > **Profile** parameters as described in the following table:

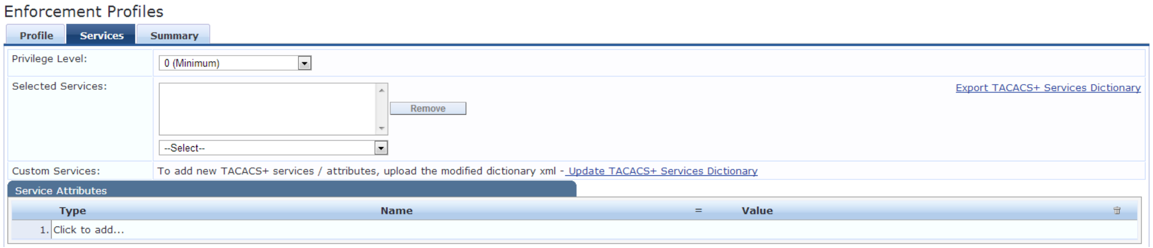
Table 210: *TACACS+ Based Enforcement > Profile Parameters*

Parameter	Action/Description
Template	Select the **TACACS+ Based Enforcement** template.
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 (recommended). 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. All configured device groups are listed in the **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: - To delete the selected Device Group List entry, click **Remove**. - To see the device group parameters, click **View Details**. - To change the parameters of the selected device group, click **Modify**.
Add New Device Group	To add a new a device group, click the **Add New Device Group** link. See Adding and Modifying Device Groups on page 459.

Services Configuration

The following figure displays the **TACACS+ Based Enforcement** > **Services** dialog:

Figure 399: *TACACS+ Based Enforcement > Services Dialog*



Enforcement Profiles

Privilege Level: 0 (Minimum)

Selected Services: --Select--

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary xml - Update TACACS+ Services Dictionary

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

Specify the **TACACS+ Based Enforcement Profile** > **Service** parameters as described in the following table:

Table 211: *TACACS+ Based Enforcement > Services Parameters*

Parameter	Action/Description
Privilege Level	Select a level between **0** and **15**, with **0** being the mininum privilege level and **15** being the highest.
Selected Services	Select one or more of the following services: ● Shell ● PIX Shell ● PPP:IP ● PPP:IPX ● PPP:LCP ● ARAP ● cpass:HTTP ● Wireless-WCS:HTTP ● CiscoWLC:Common ● Aruba:Common ● AMP:https ● NCS:HHHP
Export All TACACS+ Services Dictionaries	Click this link to download the TACACS+ Services dictionary to the local computer.
Authorize Attribute Status	Select one of the following options: ● ADD ● REPLACE
Custom Services	To add new TACACS+ services / attributes or upload the modified XML dictionary, click the **Update TACACS+ Services Dictionary** link.
Service Attributes	

Table 211: *TACACS+ Based Enforcement > Services Parameters (Continued)*

Parameter	Action/Description
Type	Select one of the following Service Attribute types: - PPP:IP - Shell - cpass:HTTP
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.

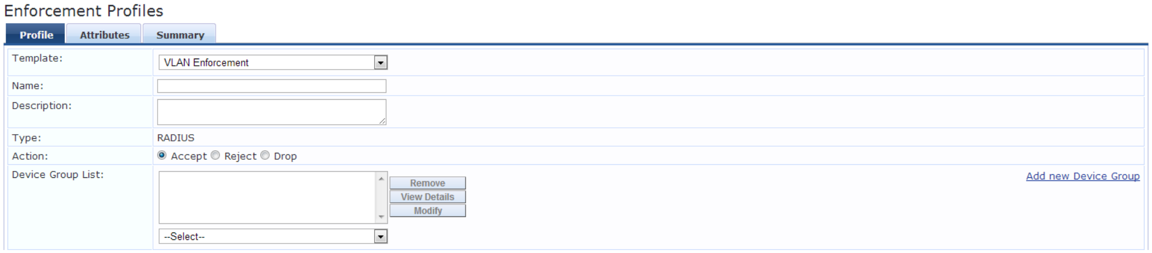
VLAN Enforcement Profile

Use this page to configure the VLAN Enforcement profile.

Profile Configuration

The following figure displays the **VLAN Enforcement** > **Profile** configuration dialog:

Figure 400: *VLAN Enforcement > Profile Configuration Dialog*



Enforcement Profiles

Template:	VLAN Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Specify the **VLAN Enforcement** > **Profile** parameters as described in the following table:

Table 212: *VLAN Enforcement > Profile 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.
Description	Enter a description of the profile.
Type	**RADIUS**. The field is populated automatically.

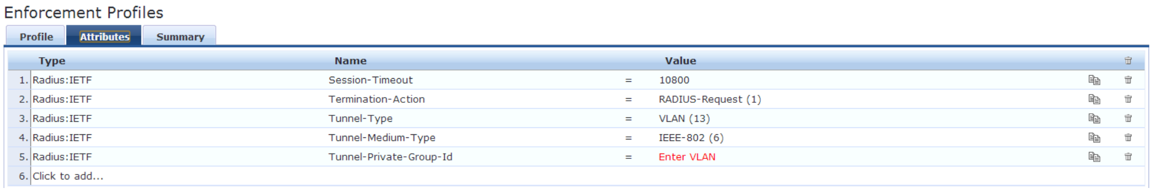
Table 212: *VLAN Enforcement > Profile Parameters (Continued)*

Parameter	Description
Action	To define the action taken on the request, click **Accept**, **Reject**, or **Drop**.
Device Group List	Select a Device Group from the drop-down list. All configured device groups are listed in the **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: ● To delete the selected Device Group List entry, click **Remove**. ● To see the device group parameters, click **View Details**. ● To change the parameters of the selected device group, click **Modify**.
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 459.

Attributes Configuration

The following figure displays the **VLAN Enforcement > Attributes** dialog:

Figure 401: *VLAN Enforcement Attributes Dialog*



Enforcement Profiles

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	10800
2.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
5.	Radius:IETF	Tunnel-Private-Group-Id	=	Enter VLAN
6.	Click to add...			

Specify the **RADIUS Based Enforcement > Attributes** parameters as described in the following table:

Table 213: *VLAN Enforcement Attributes Tab Parameters*

Parameter	Description
Type	Select one of the following attribute types: ■ Radius:Aruba ■ Radius:IETF ■ Radius:Cisco ■ Radius: Hewlett-Packared-Enterprise ■ Radius: Alcatel-Lucent-Enterprise ■ Radius:Microsoft ■ Radius:Avenda For more information, see RADIUS Namespaces on page 884
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.

Chapter 8
Configuring Policy Simulation

This chapter describes the following types of simulations:

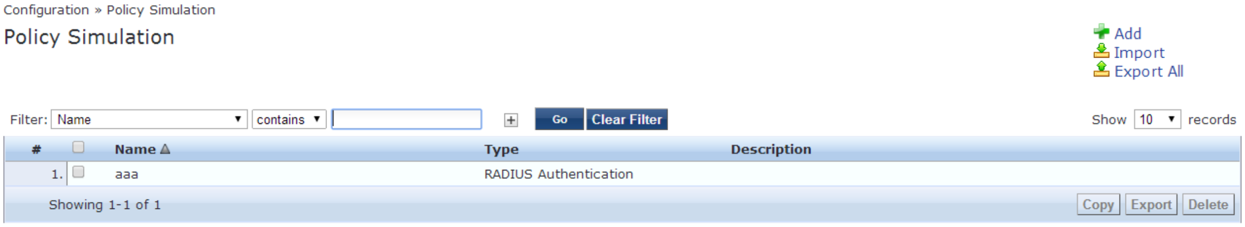
- Active Directory Authentication Simulation
- Application Authentication Simulation
- Audit Simulation
- Chained Simulation
- Enforcement Policy Simulation
- RADIUS Authentication Simulation
- Role Mapping Simulation
- Service Categorization Simulation

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.

The following figure displays the **Policy Simulation** page:

Figure 402: *Policy Simulation Page*



#	□	Name ▲	Type	Description
1.	□	aaa	RADIUS Authentication	

Showing 1-1 of 1

The following table describes the **Policy Simulation** page parameters:

Table 214: *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 Simulation

This section provides the following information:

- Adding an Active Directory Simulation
- Viewing the Simulation Results

This simulation tests authentication against an Active Directory domain or trusted domain to verify that the ClearPass Policy Manager domain membership is valid.

NOTE

The **Attributes** tab is not available for this simulation type.

Adding an Active Directory Simulation

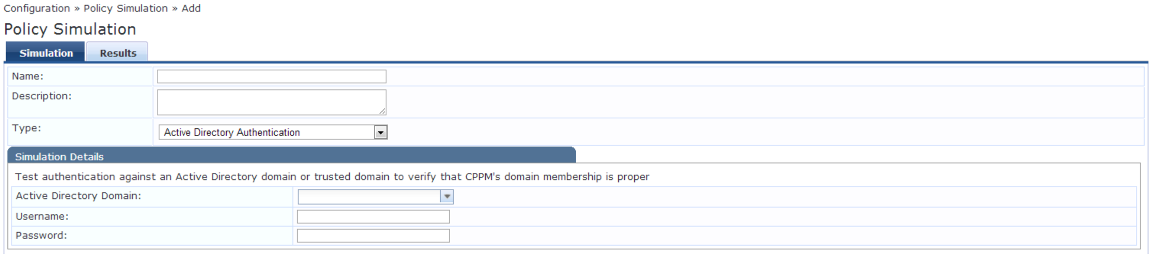
To add the RADIUS authentication server for the authentication test:

1. Navigate to the **Configuration > Policy Simulation > Add** page.

   The **Add Policy Simulation** dialog appears.
2. Enter the **Name** of the simulation.
3. From the **Type** drop-down list, select **Active Directory Authentication**.

   The following figure displays the **Active Directory Authentication Simulation** dialog.

Figure 403: *Active Directory Authentication - Simulation Tab*



Configuration » Policy Simulation » Add

Policy Simulation

Name:

Description:

Type: Active Directory Authentication

Simulation Details

Test authentication against an Active Directory domain or trusted domain to verify that CPPM's domain membership is proper

Active Directory Domain:

Username:

Password:

The following table describes the **Active Directory Authentication - Simulation** tab parameters:

Table 215: *Active Directory Authentication Simulation Tab Parameters*

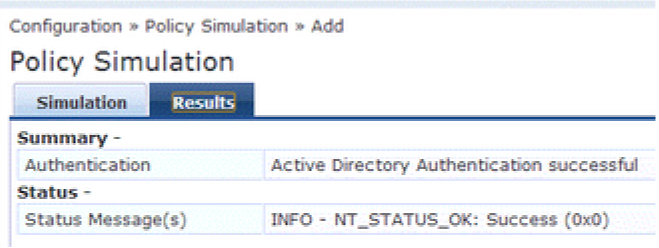
Parameter	Description
Active Directory Domain	Select the domain(s) to which the node is joined.
Username	Enter the username to login to the domain.
Password	Enter the password to login to the domain.

Viewing the Simulation Results

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 404: *Active Directory Authentication Results Tab*



Configuration » Policy Simulation » Add

Policy Simulation

Summary -

Authentication: Active Directory Authentication successful

Status -

Status Message(s): INFO - NT_STATUS_OK: Success (0x0)

Table 216: *Active Directory Authentication Results Tab Parameters*

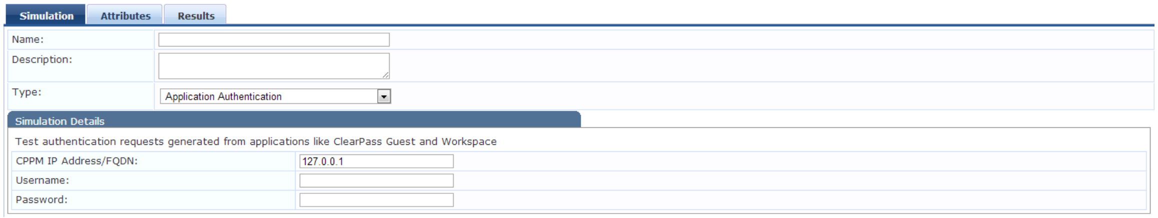
Parameter	Description
Summary	Displays the results of the Active Directory Authentication simulation.
Status	Displays the status message.

Application Authentication Simulation

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 405: *Application Authentication - Simulation Tab*



Name:
Description:
Type: Application Authentication

Simulation Details

Test authentication requests generated from applications like ClearPass Guest and Workspace

CPPM IP Address/FQDN: 127.0.0.1
Username:
Password:

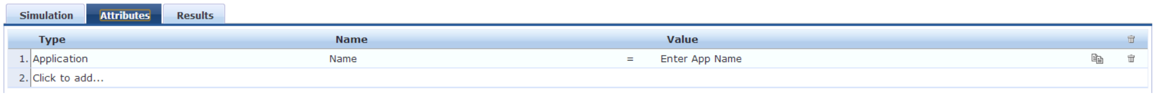
Table 217: *Application Authentication Simulation Tab Parameters*

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 406: *Application Authentication - Attributes Tab*



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

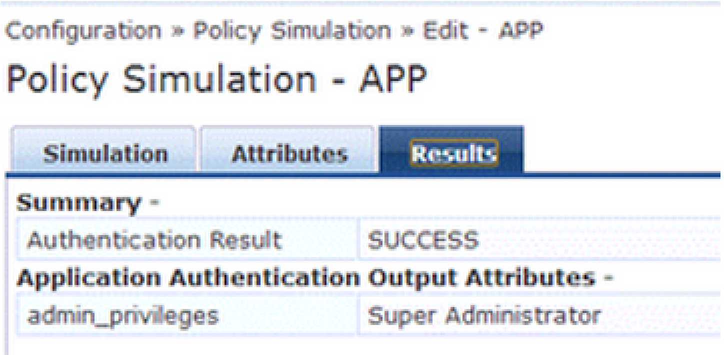
Table 218: *Application Authentication - Attributes Tab Parameters*

Attribute	Parameter
Type	Select Application or select Application:ClearPass. See Application Namespace on page 876
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 407: *Application Authentication Results Tab*



Configuration » Policy Simulation » Edit - APP

Policy Simulation - APP

Summary -

Authentication Result	SUCCESS

Application Authentication Output Attributes -

admin_privileges	Super Administrator

Table 219: *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 Simulation

This simulation allows you to specify an audit against a Nessus Server or Nmap Server with its IP address.

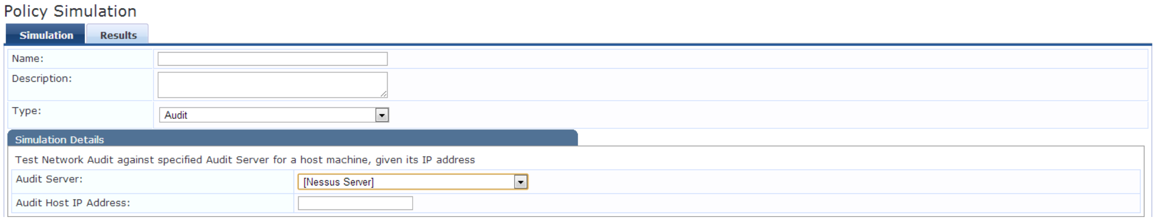
The **Attributes** tab is not available for this simulation type.

NOTE

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 408: *Audit Simulation - Simulation Tab*



Policy Simulation

Name:	
Description:	
Type:	Audit

Simulation Details

Test Network Audit against specified Audit Server for a host machine, given its IP address

Audit Server:	[Nessus Server]
Audit Host IP Address:	

The following table describes the **Audit Simulation - Simulation** tab parameters:

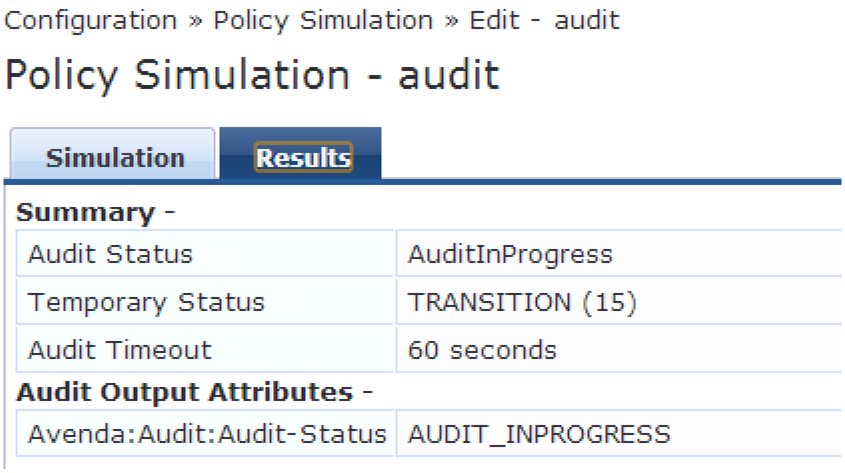
Table 220: *Audit Simulation Tab Parameters*

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 409: *Audit Simulation Results Tab*



Configuration » Policy Simulation » Edit - audit

Policy Simulation - audit

Summary -

Audit Status	AuditInProgress
Temporary Status	TRANSITION (15)
Audit Timeout	60 seconds

Audit Output Attributes -

Avenda:Audit:Audit-Status	AUDIT_INPROGRESS

The following table describes the **Audit Simulation - Results** tab parameters:

Table 221: *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.

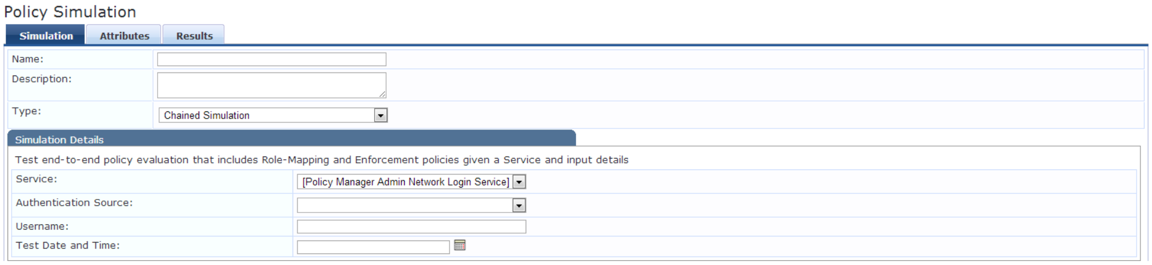
Chained Simulation

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 410: *Chained Simulation Tab*



Policy Simulation

Name:	
Description:	
Type:	Chained Simulation

Simulation Details

Test end-to-end policy evaluation that includes Role-Mapping and Enforcement policies given a Service and input details

Service:	[Policy Manager Admin Network Login Service]
Authentication Source:	
Username:	
Test Date and Time:	

The following table describes the **Chained Simulation - Results** tab parameters:

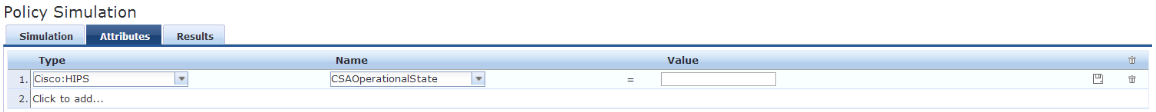
Table 222: *Chained Simulation Tab Parameters*

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 882

Attributes Tab

Enter the attributes of the policy component to be tested.

Figure 411: *Chained Simulation Attributes Tab*



	Type	Name		Value
1.	Cisco:HIPS	CSAOperationalState	=	
2.	Click to add...			

The following table describes the **Chained Simulation Attributes - Results** tab parameters:

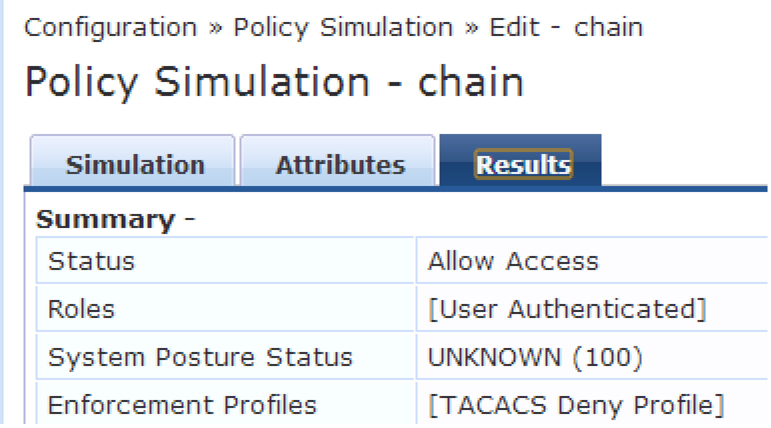
Table 223: *Chained Simulation Attributes tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 883
Authentication	See Authentication Namespaces on page 877
Connection	See Connection Namespaces on page 881
Application	See Application Namespace on page 876
Certificate	See Certificate Namespaces on page 880
● 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 884
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 412: *Chained Simulation Results Tab*



Configuration » Policy Simulation » Edit - chain

Policy Simulation - chain

Summary -

Status	Allow Access
Roles	[User Authenticated]
System Posture Status	UNKNOWN (100)
Enforcement Profiles	[TACACS Deny Profile]

Table 224: *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 Simulation

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.

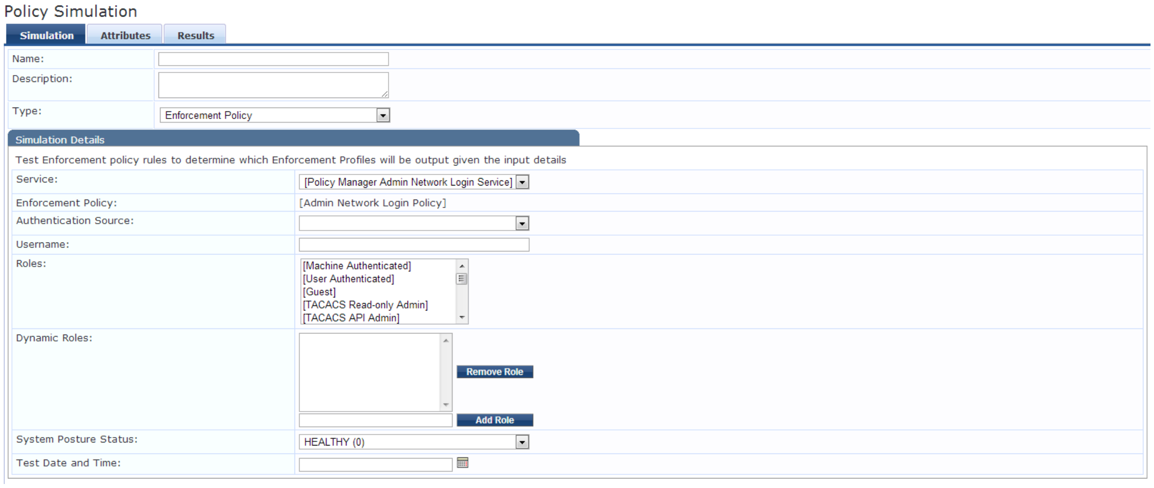
Authentication Source and User Name inputs are used to derive dynamic values in the enforcement profile that are retrieved from the authorization source. These inputs are optional.

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 191.

Simulation Tab

The following figure displays the **Enforcement Policy Simulation** tab:

Figure 413: *Enforcement Policy Simulation Tab*



Name:

Description:

Type: Enforcement Policy

Test Enforcement policy rules to determine which Enforcement Profiles will be output given the input details

Service: [Policy Manager Admin Network Login Service]

Enforcement Policy: [Admin Network Login Policy]

Authentication Source:

Username:

Roles: [Machine Authenticated]
[User Authenticated]
[Guest]
[TACACS Read-only Admin]
[TACACS API Admin]

Dynamic Roles:

System Posture Status: HEALTHY (0)

Test Date and Time:

The following table describes the **Enforcement Policy Simulation** tab parameters:

Table 225: *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

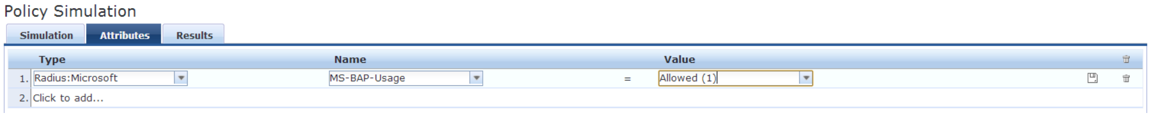
Table 225: *Enforcement Policy Simulation tab Parameters (Continued)*

Parameter	Description
	Values = [Local User Repository] *or* [Guest Device Repository] if you select Guest Operator Logins
Username	Enter username.
Roles	Select from: - [Machine Authenticated] - [User Authenticated] - [Guest] - [TACACS Read-only Admin] - [TACACS API Admin] - [TACACS Help Desk] - [TACACS Receptionist] - [TACACS Network Admin] - [TACACS Super Admin] - [Contractor] - [Other] - [Employee] - [MAC Caching - [Onboard Android] - [Onboard Windows] - [Onboard Mac OS X] - Onboard iOS] - [Aruba TACACS root Admin] - [Aruba TACACS read-only Admin] - [Device Registration] - [BYOD Operator] - [AirGroup V1] - [AirGroup v2]
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 884
Test Date and Time	Click calendar icon to select start date and time for simulation test. See Date Namespaces on page 882

Attributes tab

Enter the attributes of the policy component to be tested. The following figure displays the **Enforcement Policy - Attributes** tab:

Figure 414: *Enforcement Policy Attributes Tab*



	Type	Name		Value
1.	Radius:Microsoft	MS-BAP-Usage	=	Allowed (1)
2.	Click to add...			

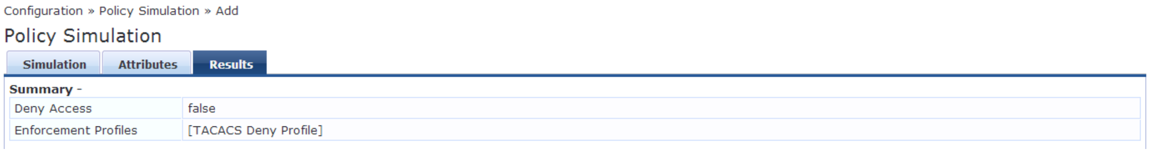
Table 226: *Enforcement Policy Attributes tab Parameters*

Attribute	Description
Type:	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 883
Authentication	See Authentication Namespaces on page 877
Connection	See Connection Namespaces on page 881
Application	See Application Namespace on page 876
● Radius:IETF ● Radius:Cisco ● Radius:Microsoft ● Radius:Avenda ● Radius:Aruba	See RADIUS Namespaces on page 884
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 415: *Policy Simulation Results Tab*



Summary -

Deny Access	false
Enforcement Profiles	[TACACS Deny Profile]

Table 227: *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 Simulation

This section provides the following information:

- Adding a RADIUS Authentication Simulation
- Setting the Attributes to Be Tested
- Viewing the Simulation Results

Dictionaries in the RADIUS namespace come prepackaged with the ClearPass Policy Manager. The administration interface does provide a way to add dictionaries into the system (see RADIUS Dictionary on page 664 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. The same vendor can have multiple dictionaries, in which case the "Vendor" portion includes a suffix or some other unique string by the name of the device to differentiate the dictionaries.

Adding a RADIUS Authentication Simulation

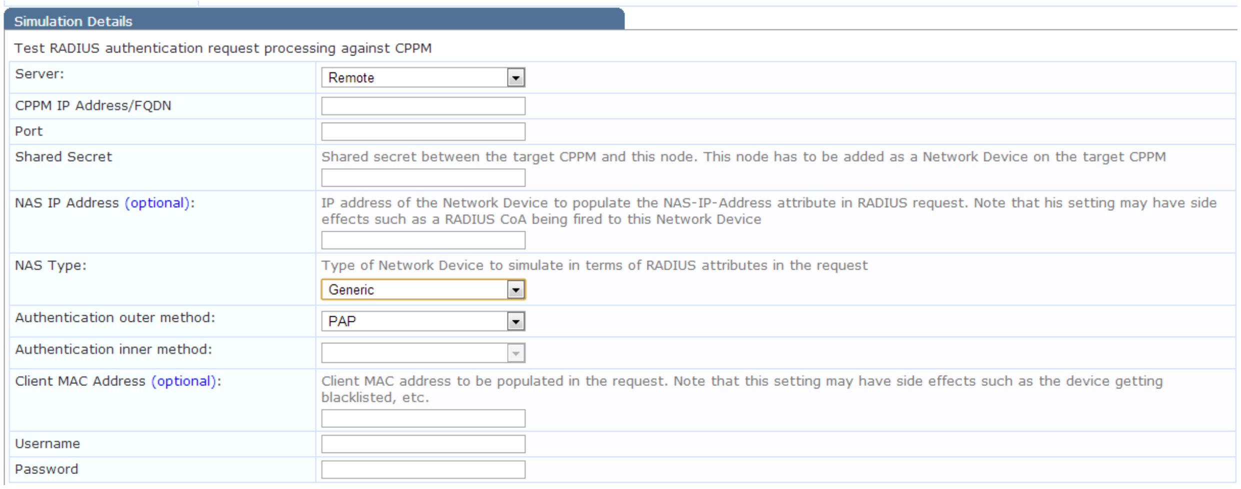
To add the RADIUS authentication server for the authentication test:

1. Navigate to the **Configuration > Policy Simulation > Add** page.

   The **Add Policy Simulation** dialog opens.
2. Enter the **Name** of the simulation.
3. From the **Type** drop-down list, select **RADIUS Authentication**.

   Figure 416 displays the **RADIUS Authentication Simulation Details** dialog, with the **Server** parameter set to **Remote**.

Figure 416: *RADIUS Authentication Simulation Details Dialog*



Simulation Details

Test RADIUS authentication request processing against CPPM

Server:	Remote
CPPM IP Address/FQDN	
Port	
Shared Secret	Shared secret between the target CPPM and this node. This node has to be added as a Network Device on the target CPPM
NAS IP Address (optional):	IP address of the Network Device to populate the NAS-IP-Address attribute in RADIUS request. Note that his setting may have side effects such as a RADIUS CoA being fired to this Network Device
NAS Type:	Type of Network Device to simulate in terms of RADIUS attributes in the request Generic
Authentication outer method:	PAP
Authentication inner method:	
Client MAC Address (optional):	Client MAC address to be populated in the request. Note that this setting may have side effects such as the device getting blacklisted, etc.
Username	
Password	

4. Enter the values for each of the **RADIUS Simulation** parameters as described in Table 228.

Table 228: *RADIUS Simulation Tab Parameters*

Parameter	Action/Description
Server	1. Specify **Local** or **Remote**.
CPPM IP Address or FQDN	This field is displayed only if **Remote Server** is selected. 2. Enter the IP address or the fully qualified domain name (FQDN) of the remote ClearPass Policy Manager server.
Shared Secret	Displayed only if **Remote Server** is selected. 3. Enter the shared secret between the target ClearPass server and this node. You must add the node as a Network Device on the target ClearPass server. (For details, see Adding a Network Device on page 448).
NAS IP Address (optional)	4. To populate the NAS-IP-Address attribute in a RADIUS request, enter the IP address of the network device.
NAS Type	5. 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	6. Specify one of the following authentication outer methods: • PAP • CHAP • MSCHAPv2 • PEAP: Authentication inner method: *enabled*. Select one of the following PEAP Authentication inner methods: ▪ EAP-MSCHAPv2 ▪ EAP-GTC ▪ EAP-TLS • TTLS: Authentication inner method field: *enabled*. Select one of the following TTLS Authentication inner methods: ▪ PAP ▪ CHAP ▪ MSCHAPv2 ▪ EAP-MSCHAPv2 ▪ EAP-GTC ▪ EAP-TLS • TLS
Client MAC Address (optional)	7. Enter the client MAC address of the network device to populate the NAS-IP address attribute in the RADIUS request.
Username	8. Enter the user name.
CA Certificate (optional)	This is the optional Root CA certificate needed to verify the RADIUS server's

Table 228: *RADIUS Simulation Tab Parameters (Continued)*

Parameter	Action/Description
	certificate. 9. Click **Browse** and navigate to the optional Root CA certificate. Click **Open**, then click **Upload**.
Client Certificate PKCS12 (PFX)*	This is the client certificate that is used for TLS in PKCS12 (Public-Key Cryptography Standards). Formats: .pfx or .p12 10. Click **Browse** and navigate to the Client Certificate PKCS12. Click **Open**, then click **Upload**.
Passphrase for PFX file*	11. Enter the pass phrase for the selected PFX file.
* These fields are displayed only if you select **TTLS** or **PEAP** as the authentication outer method *and* you select **EAP-TLS** as the authentication inner method.	
	12. Click **Save**, or click **Next** to proceed to the **Attributes** tab.

Setting the Attributes to Be Tested

NOTE

The attributes that you can set depend on the **NAS Type** selected on the **Policy Simulation** page (see Figure 416).

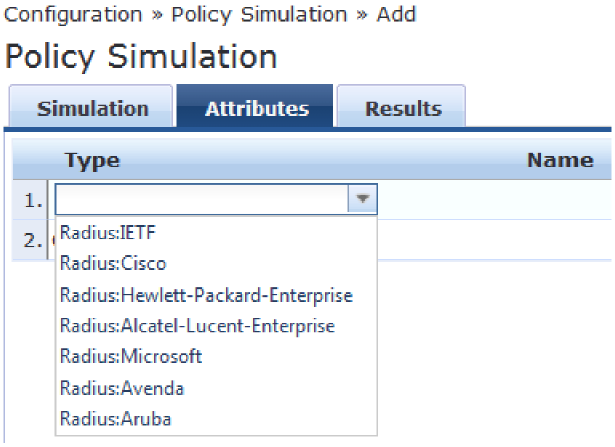
To set the attributes to be tested:

1. From the **Attributes** tab, click **Click to add**.

   The **Add Policy Simulation Attributes** dialog opens.

2. From the **Type** drop-down, select the attribute **Type**.

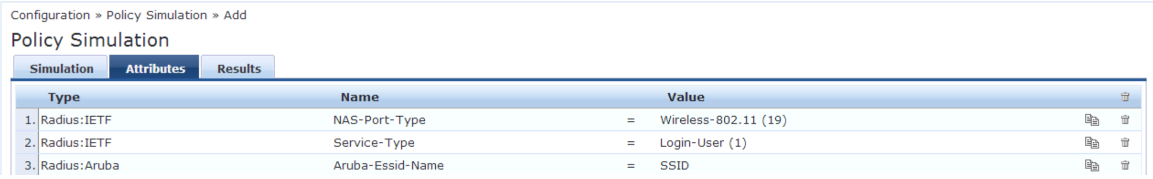
Figure 417: *Specifying Policy Simulation Attributes*



3. Select the attribute **Name**.
4. Select the attribute **Value**.
5. Repeat these steps for each additional attribute you wish to add.
6. Click **Save**, or click **Next** to proceed to the **Results** tab.

NAS Type: Aruba Wireless Controller

Figure 418: *Aruba Wireless Controller Type - Attributes*



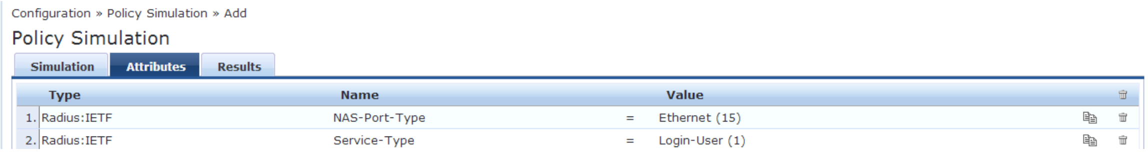
	Type	Name		Value
1.	Radius:IETF	NAS-Port-Type	=	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	=	Login-User (1)
3.	Radius:Aruba	Aruba-Essid-Name	=	SSID

Table 229: *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 419: *NAS Type: Aruba Wired Switch Controller Attributes Tab*



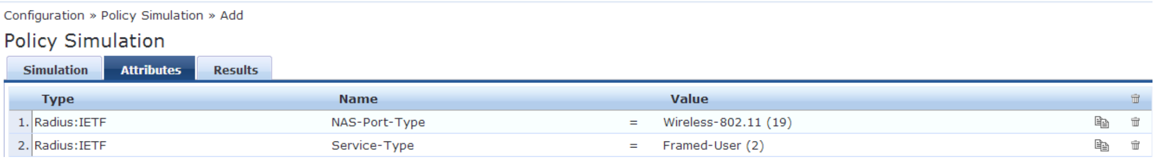
	Type	Name		Value
1.	Radius:IETF	NAS-Port-Type	=	Ethernet (15)
2.	Radius:IETF	Service-Type	=	Login-User (1)

Table 230: *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 420: *NAS Type: Cisco Wireless Switch Attributes*



	Type	Name		Value
1.	Radius:IETF	NAS-Port-Type	=	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	=	Framed-User (2)

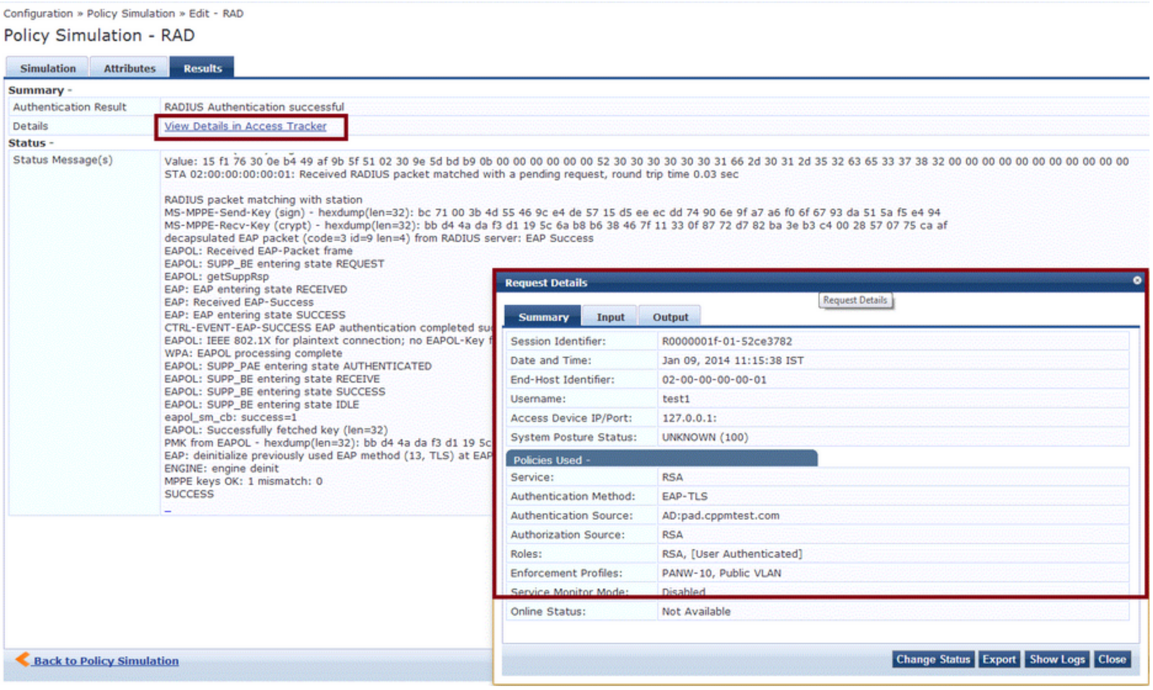
Table 231: *NAS Type: Cisco Wireless Switch Required Attribute Settings*

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)	

Viewing the Simulation Results

The following figure displays the **Policy Simulation RADIUS - Results** dialog:

Figure 421: *Results Tab*


Configuration » Policy Simulation » Edit - RAD
Policy Simulation - RAD
Simulation
Attributes
Results
Back to Policy Simulation

Summary -

Authentication Result	RADIUS Authentication successful
Details	View Details in Access Tracker

Status -

Status Message(s)

```
Value: 15 f1 76 30 0e b4 49 af 9b 5f 51 02 30 9e 5d bd b9 0b 00 00 00 00 00 00 52 30 30 30 30 30 30 31 66 2d 30 31 2d 35 32 63 65 33 37 38 32 00 00 00 00 00 00 00 00 00 00
STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.03 sec

RADIUS packet matching with station
MS-MPPE-Send-Key (sign) - hexdump(len=32): bc 71 00 3b 4d 55 46 9c e4 de 57 15 d5 ee ec dd 74 90 6e 9f a7 a6 f0 6f 67 93 da 51 5a f5 e4 94
MS-MPPE-Recv-Key (crypt) - hexdump(len=32): bb d4 4a da f3 d1 19 5c 6a b8 b6 38 46 7f 11 33 0f 87 72 d7 82 ba 3e b3 c4 00 28 57 07 75 ca af
decapsulated EAP packet (code=3 id=9 len=4) from RADIUS server: EAP Success
EAPOL: Received EAP-Packet frame
EAPOL: SUPP_BE entering state REQUEST
EAPOL: getSuppRsp
EAP: EAP entering state RECEIVED
EAP: Received EAP-Success
EAP: EAP entering state SUCCESS
CTRL-EVENT-EAP-SUCCESS EAP authentication completed su
EAPOL: IEEE 802.1X for plaintext connection; no EAPOL-Key f
WPA: EAPOL processing complete
EAPOL: SUPP_PAE entering state AUTHENTICATED
EAPOL: SUPP_BE entering state RECEIVE
EAPOL: SUPP_BE entering state SUCCESS
EAPOL: SUPP_BE entering state IDLE
eapol_sm_cb: success=1
EAPOL: Successfully fetched key (len=32)
PMK from EAPOL - hexdump(len=32): bb d4 4a da f3 d1 19 5c
EAP: deinitialize previously used EAP method (13, TLS) at EAP
ENGINE: engine deinit
MPPE keys OK: 1 mismatch: 0
SUCCESS
```

Session Identifier:	R0000001f-01-52ce3782
Date and Time:	Jan 09, 2014 11:15:38 IST
End-Host Identifier:	02-00-00-00-00-01
Username:	test1
Access Device IP/Port:	127.0.0.1:
System Posture Status:	UNKNOWN (100)
Service:	RSA
Authentication Method:	EAP-TLS
Authentication Source:	AD:pad.cppmtest.com
Authorization Source:	RSA
Roles:	RSA, [User Authenticated]
Enforcement Profiles:	PANW-10, Public VLAN
Service Monitor Mode:	Disabled
Online Status:	Not Available

Table 232: *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 dialog that provides details about the Authentication test. You can take the following actions: ● Click the **Summary**, **Input**, or **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 Simulation

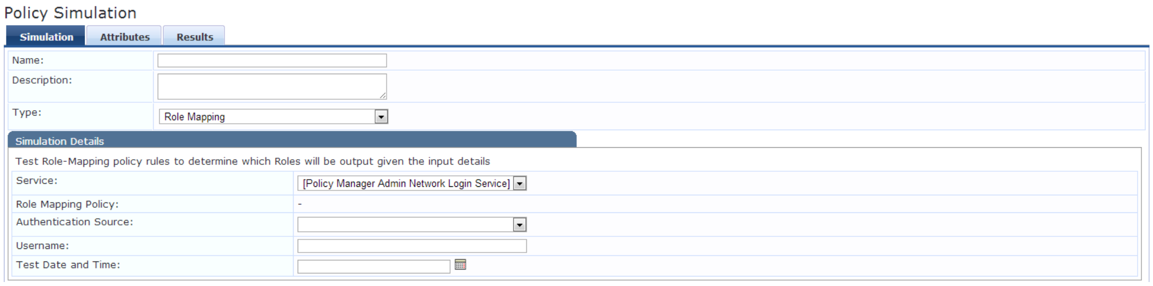
The role mapping simulation tests Role-Mapping policy rules to determine which roles will be output, given the service name (and associated role mapping policy), the authentication source and the user name.

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 422: *Role Mapping Simulation Tab*



Policy Simulation

Name:	
Description:	
Type:	Role Mapping

Simulation Details

Test Role-Mapping policy rules to determine which Roles will be output given the input details

Service:	[Policy Manager Admin Network Login Service]
Role Mapping Policy:	-
Authentication Source:	
Username:	
Test Date and Time:	

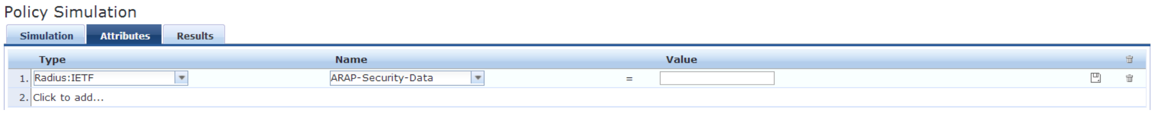
Table 233: *Role Mapping Simulation Tab Parameters*

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 882

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the **Role Mapping Simulation Attributes** tab:

Figure 423: *Role Mapping Simulation Attributes Tab*



	Type	Name		Value
1.	Radius:IETF	ARAP-Security-Data	=	
2.	Click to add...			

The following table describes the **Role Mapping Simulation Attributes** tab parameters:

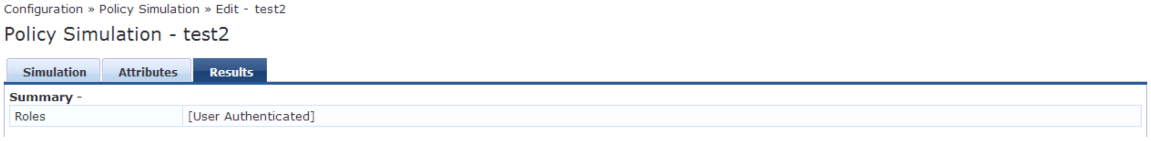
Table 234: *Role Mapping Simulation Attributes Tab Parameters*

Attribute	Parameter
Type	Select the type of attributes from the drop-down list.
Host	See Host Namespaces on page 883
Authentication	See Authentication Namespaces on page 877
Connection	See Connection Namespaces on page 881
Application	See Application Namespace on page 876
Certificate	See Certificate Namespaces on page 880
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Avenda • Radius:Aruba	See RADIUS Namespaces on page 884
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 424: *Results Tab*


Configuration » Policy Simulation » Edit - test2

Policy Simulation - test2

Summary -

Roles	[User Authenticated]

The following table describes the **Role Mapping Simulation - Results** tab parameters:

Table 235: *Role Mapping Results Tab Parameters*

Parameter	Description
Summary	Displays the results of the simulation.

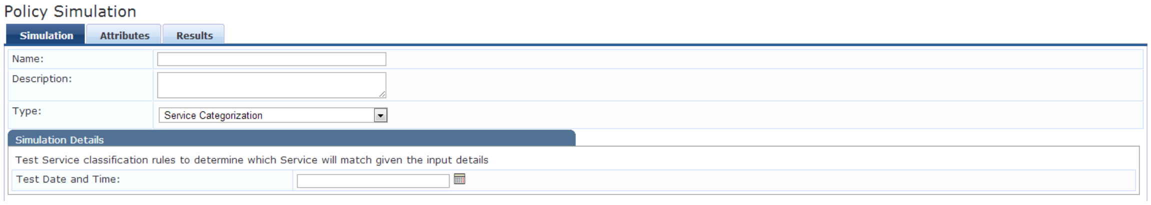
Service Categorization Simulation

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 425: *Service Categorization Simulation Tab*



Name:

Description:

Type: Service Categorization

Test Service classification rules to determine which Service will match given the input details

Test Date and Time:

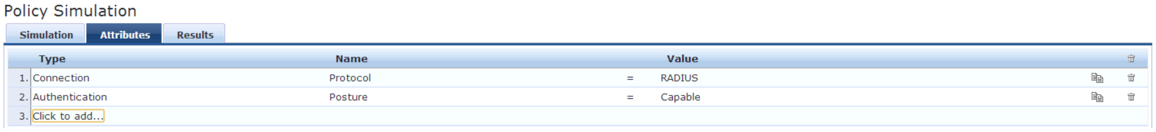
Table 236: *Service Categorization Simulation Tab Parameter s*

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 426: *Service Categorization Attributes Tab*



	Type	Name		Value
1.	Connection	Protocol	=	RADIUS
2.	Authentication	Posture	=	Capable
3.	Click to add...			

Table 237: *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 883
Authentication	See Authentication Namespaces on page 877
Connection	See Connection Namespaces on page 881
Application	See Application Namespace on page 876

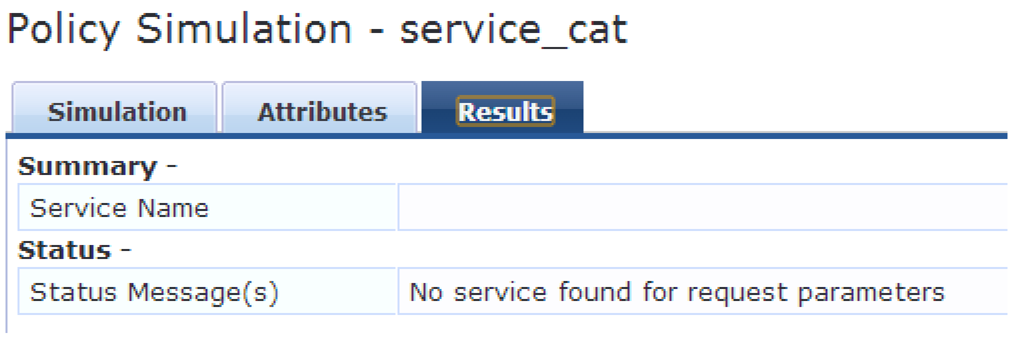
Table 237: *Service Categorization Simulation Attributes Tab Parameters (Continued)*

Attribute	Parameter
• Radius:IETF • Radius:Cisco • Radius:Microsoft • Radius:Aruba	See RADIUS Namespaces on page 884
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 427: *Results Tab*



Policy Simulation - service_cat

Summary -

Service Name	

Status -

Status Message(s)	No service found for request parameters

The following table describes the **Service Categorization Simulation Results** tab parameters:

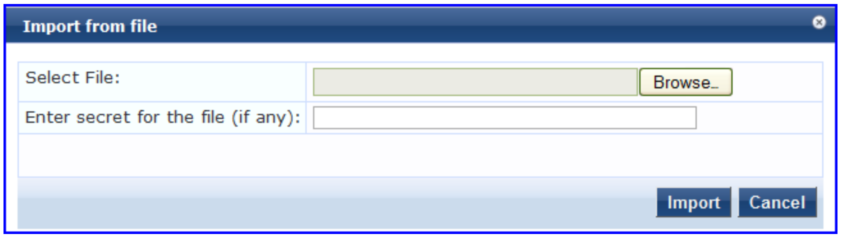
Table 238: *Service Configuration Results Tab Parameters*

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 428: *Import Simulations*



Import from file

Select File:	
Enter secret for the file (if any):	

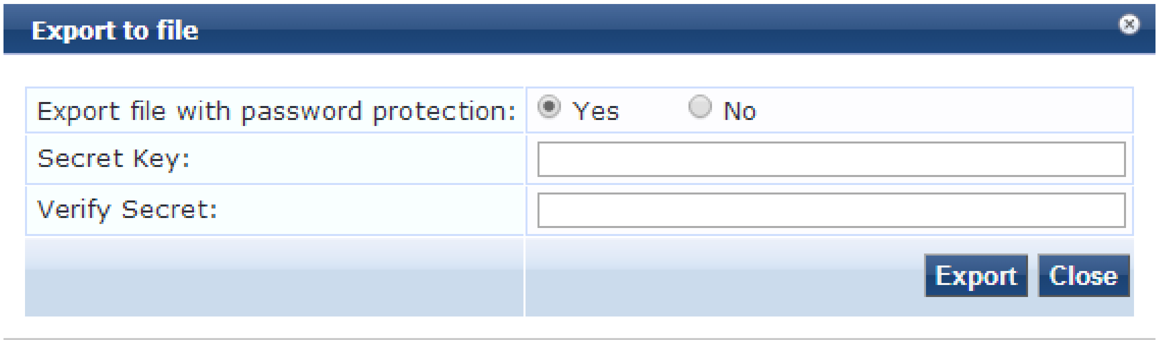
Table 239: *Import from file page Parameters*

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 429: *Export Simulations*



Export to file

Export file with password protection: ● Yes ○ No

Secret Key:

Verify Secret:

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 240: *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 9
ClearPass Policy Manager Profile

This chapter contains the following information:

ClearPass Profile Overview

This section contains the following information:

Introduction

ClearPass Profile is a ClearPass Policy Manager module that automatically classifies endpoints using attributes obtained from software components called *Collectors*.

ClearPass Profile associates an endpoint with a specific user or location and offers an efficient and accurate way to differentiate access by endpoint type (for example, laptop or tablet).

Profiling allows you to gather device type and operating system information by inspecting packets that are sent by these devices in the network. For example, you can identify that a device is a smart device, a laptop, or a printer or IP phone.

You can use this information to implement Bring Your Own Device (BYOD) flows during enforcement, assigning the appropriate privileges and access to users based on their device type and the identity of the user.

Enabling Endpoint Classification

When you enable ClearPass Profile on a ClearPass server, you enable the server for endpoint classification. This associates each endpoint with a specific user or location and secures access for devices.

To enable ClearPass Profile:

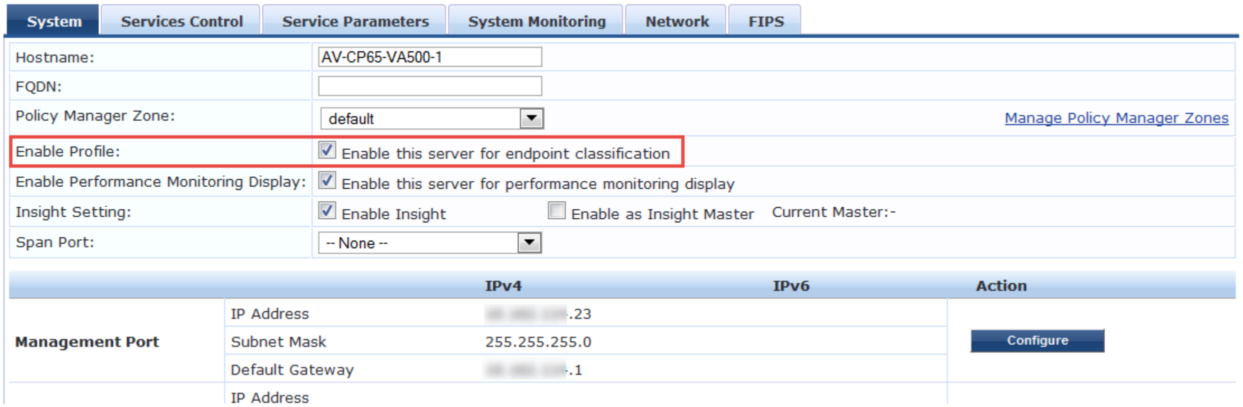
1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.

   The Server Configuration page appears.

2. Select the ClearPass node in the zone that you want to designate as a Profiler.

   The **System** tab for the **Server Configuration** page appears.

Figure 430: *Enable Profile Option*



Hostname:	AV-CP65-VA500-1
FQDN:	
Policy Manager Zone:	default
Enable Profile:	☑ Enable this server for endpoint classification
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	☑ Enable Insight ☐ Enable as Insight Master Current Master:-
Span Port:	-- None --

		IPv4	IPv6	Action
Management Port	IP Address	[redacted].23		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	[redacted].1		
	IP Address			

3. If it is not already enabled, select the **Enable this server for endpoint classification** check box, then click **Save**.

Configuring CoA for an Endpoint-Connected Device

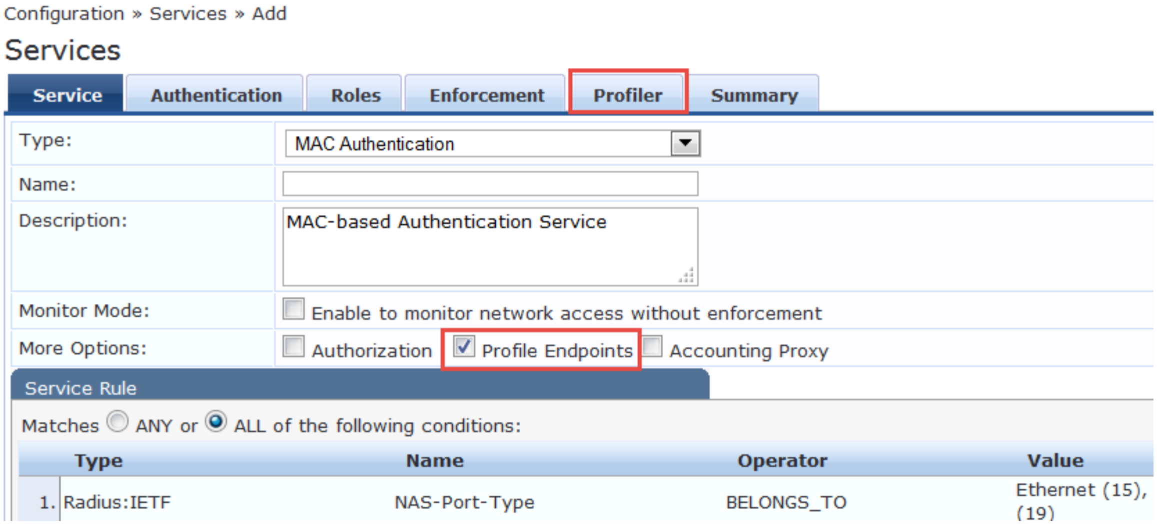
After profiling an endpoint, use the **Profiler** page to configure Change of Authorization (CoA) on the network device to which an endpoint is connected.

The **Profiler** tab is not displayed by default. To access the **Profiler** tab:

1. Navigate to **Configuration** > **Services**, then click **Add**.
2. Enter the name of the service.
3. From the **More Options** field on the **Service** tab, enable the **Profile Endpoints** check box .

   The **Profiler** tab is added to the **Services** tabs:

Figure 431: *Adding the Profiler Page*



Type:	MAC Authentication
Name:	
Description:	MAC-based Authentication Service
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☑ Profile Endpoints ☐ Accounting Proxy

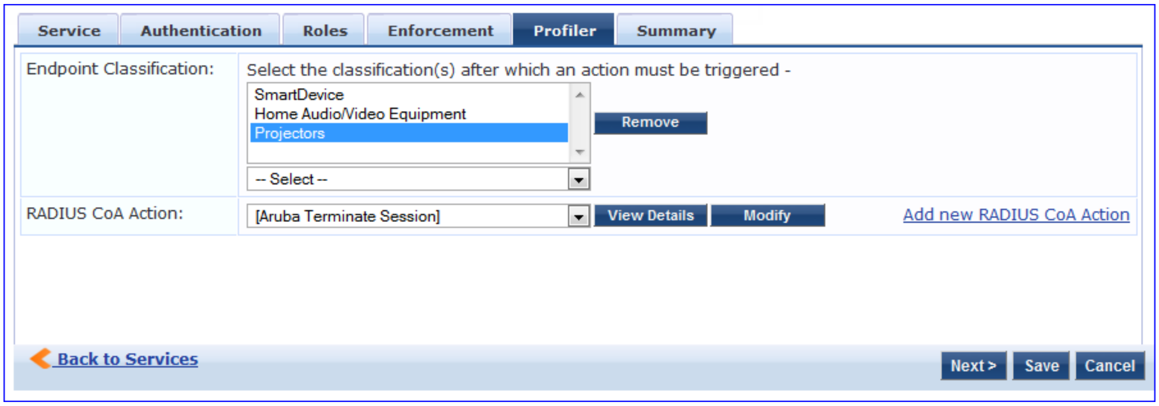
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), (19)

4. Select the **Profiler** tab.

   The **Profiler** page appears.

Figure 432: *Profiler Page*



Endpoint Classification: Select the classification(s) after which an action must be triggered -

SmartDevice
Home Audio/Video Equipment
Projectors

-- Select --

RADIUS CoA Action: [Aruba Terminate Session]

5. You 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. You can use any option from Endpoint Classification to invoke CoA on a change of any one of the fields (category, family, and name).

   Table 241 describes the **Profiler** page parameters:

Table 241: *Profiler Page Parameters*

Parameter	Action/Description
Endpoint Classification	1. Select one or more endpoint classification items from the drop-down list. You can select a new action, or remove a current action.
RADIUS CoA Action	2. Select the RADIUS CoA action from the drop-down list. 3. To view the **Policy Manager Entity Details** page with the summary of enforcement profile details, click **View Details**. 4. To view the **Summary** tab with profile details, click **Modify**.
Add new RADIUS CoA Action	5. To create a new RADIUS CoA action, click the **Add New RADIUS CoA Action** link.

6. When finished, click **Save**.

How ClearPass Profile Classifies Endpoints

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

Stage 1: Deriving Device Profiles

During Stage 1, ClearPass Profile derives 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 profile order of priority, from highest priority to lowest:

a. OnGuard/ActiveSync plugin

b. HTTP User-Agent

c. SNMP

d. DHCP

e. MAC OUI

Stage 2: Refining Results

ClearPass Policy Manager includes a set of rules that evaluates a device profile. The 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 refines the results of profiling.

Example

With DHCP options, Stage 1 can identify an Android device. Stage 2 uses rules to combine this with the MAC OUI to further classify an Android device as Samsung Android and HTC Android.

Fingerprint Dictionaries

ClearPass Policy Manager uses a set of dictionaries and rules to perform device fingerprinting.

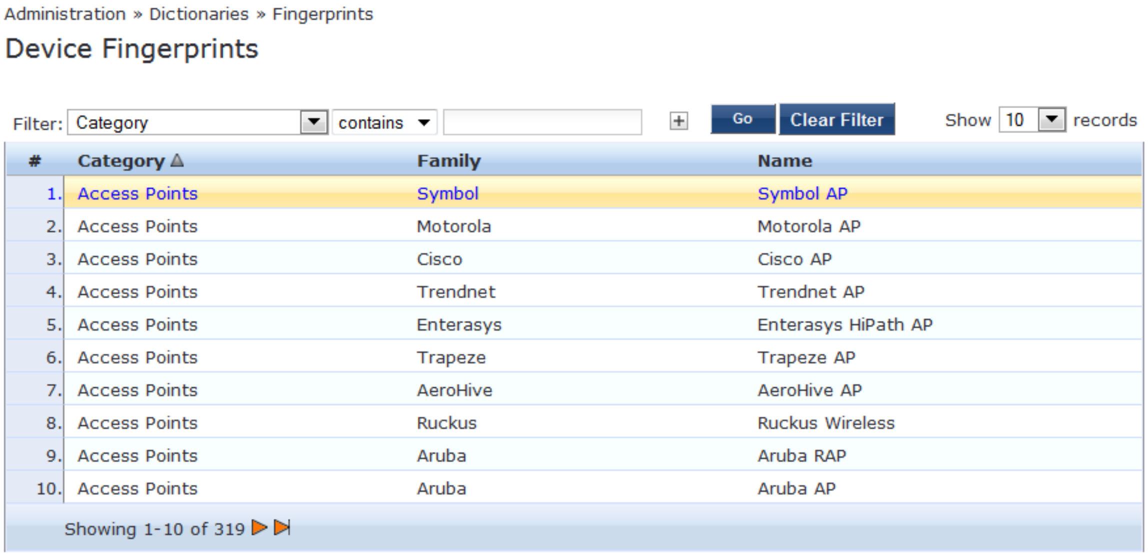
Because these dictionaries can change frequently, ClearPass Policy Manager provides a way to automatically update fingerprints from a hosted portal. The device fingerprints are updated from the Aruba ClearPass Update Portal (for more information, see Updating Policy Manager Software on page 673).

To view the contents of the fingerprints dictionary:

1. Navigate to **Administration > Dictionaries > Fingerprints**.

   The **Device Fingerprints** page appears. This page lists all the device fingerprints recognized by the Profile module.

Figure 433: *Device Fingerprints Page*



Administration » Dictionaries » Fingerprints

Device Fingerprints

Filter: Category contains

Show 10 records

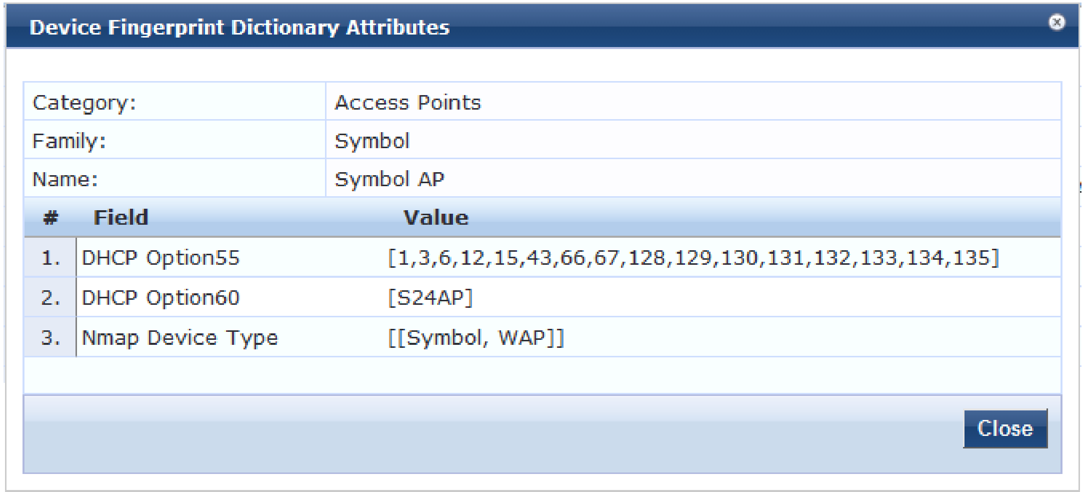
#	Category	Family	Name
1.	Access Points	Symbol	Symbol AP
2.	Access Points	Motorola	Motorola AP
3.	Access Points	Cisco	Cisco AP
4.	Access Points	Trendnet	Trendnet AP
5.	Access Points	Enterasys	Enterasys HiPath AP
6.	Access Points	Trapeze	Trapeze AP
7.	Access Points	AeroHive	AeroHive AP
8.	Access Points	Ruckus	Ruckus Wireless
9.	Access Points	Aruba	Aruba RAP
10.	Access Points	Aruba	Aruba AP

Showing 1-10 of 319

2. To view the device fingerprint dictionary attributes, select the device fingerprint of interest.

   The attributes for the selected Device Fingerprint Dictionary are displayed:

Figure 434: *Device Fingerprint Dictionary Attributes Page*



Device Fingerprint Dictionary Attributes

Category:	Access Points
Family:	Symbol
Name:	Symbol AP

#	Field	Value
1.	DHCP Option55	[1,3,6,12,15,43,66,67,128,129,130,131,132,133,134,135]
2.	DHCP Option60	[S24AP]
3.	Nmap Device Type	[[Symbol, WAP]]

3. To exit, click **Close**.

Viewing Live Endpoint Information for a Specific Device

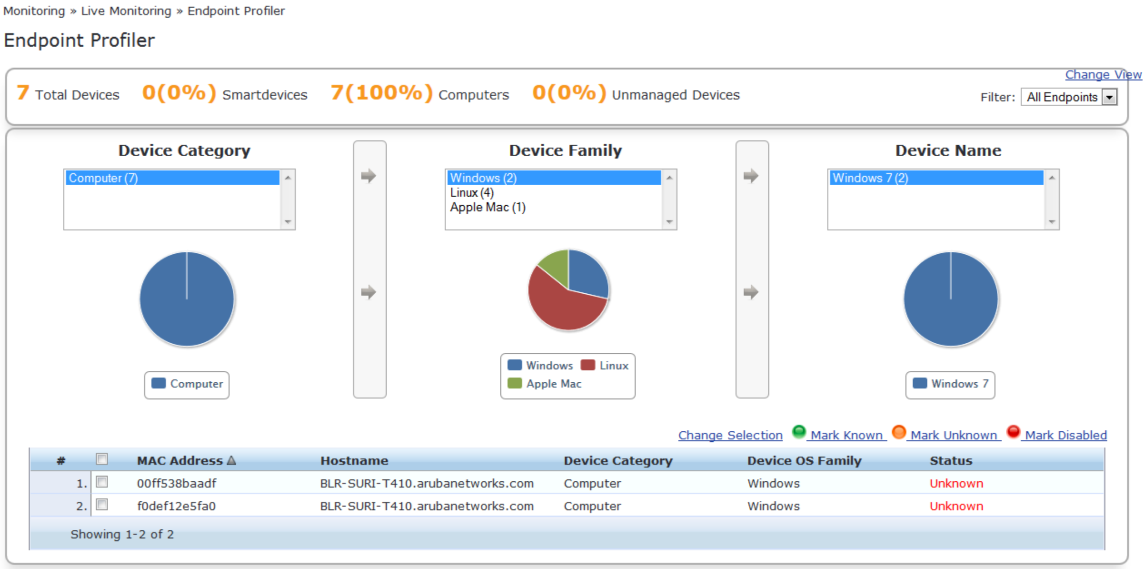
The ClearPass Live Monitoring feature allows you to view endpoint information in graphic format for the device category, device family, and device name items you selected. You can also examine the endpoint details and attributes about a specific device .

To access the Endpoint Profiler Live Monitoring information:

1. Navigate to **Monitoring** > **Profile and Discovery** > **Endpoint Profiler**.

   The Endpoint Profiler appears.

Figure 435: *Endpoint Profiler*



Monitoring » Live Monitoring » Endpoint Profiler

Endpoint Profiler

7 Total Devices 0(0%) Smartdevices 7(100%) Computers 0(0%) Unmanaged Devices

#	□	MAC Address ▲	Hostname	Device Category	Device OS Family	Status
1.	□	00ff538baadf	BLR-SURI-T410.arubanetworks.com	Computer	Windows	Unknown
2.	□	f0def12e5fa0	BLR-SURI-T410.arubanetworks.com	Computer	Windows	Unknown

Showing 1-2 of 2

2. To view endpoint details about a specific device, click a device in the table below the graphs.
3. To return to the **Endpoint Profiler** page, click **Cancel**.

   For more information, see:

   - Profiler and Discovery: Endpoint Profiler on page 133

   The Cluster Status Dashboard widget shows basic distribution of device types. For more information, see:

- Using the Policy Manager Dashboard on page 25

About the Device Profile

A device profile is a hierarchical model consisting of three elements that are derived by the endpoint attributes—*DeviceCategory*, *DeviceFamily*, and *DeviceName*.

Table 242: *Elements of a Device Profile*

Endpoint Attributes	Description
DeviceCategory	Denotes the type of the device, for example, Computer, Smart Device, Printer, or Access Point.
DeviceFamily	Classifies devices based on the type of operating system or vendor. For example, when the category is *Computer*, ClearPass Policy Manager shows a device family of Windows, Linux, or Mac OS X.
DeviceName	Denotes the name of the device. Devices in a family are organized based on characteristics such as their operating system version. For example, in a DeviceFamily of *Windows*, ClearPass Policy Manager shows a DeviceName of *Windows 8.1* or *Windows Server 2012*.

This hierarchical model provides a structured view of all endpoints accessing the network. In addition to these, a device profile also collects and stores the following:

- IP address
- Host name
- Device vendor (via MAC OUI)
- Timestamp indicating when the device was first discovered
- Timestamp indicating when the device was last seen

Endpoint Information Collectors

Collectors are the network elements that provide data in order to profile endpoints. This section provide the following information:

- DHCP Collector
- NetFlow Collector
- ClearPass Onboard Collector
- HTTP User-Agent Strings Collector
- MAC OUI Collector
- ActiveSync Plug-in Collector
- ClearPass OnGuard Agent
- About the Subnet Scan Collector
- Configuring Subnet Scans
- SNMP Configuration for Wired Network Profiling
- Accessing SSH and WMI Configuration Information

DHCP Collector

Dynamic Host Configuration Protocol (DHCP) attributes such as *option 55* (parameter request list), *option 60* (vendor class), and the 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.

You can configure switches and controllers to forward DHCP Discover, Request, and Inform packets to ClearPass. These DHCP packets are decoded by ClearPass Policy Manager to arrive at the appropriate device category, OS family, and device name. In addition to fingerprints, DHCP also provides the host name and IP address.

Sending DHCP Traffic to the ClearPass Server

To configure your Aruba controller and Cisco switch to send DHCP traffic to the ClearPass server, enter the following CLI commands:

```
interface <vlan_name>
ip address <ip_addr> <netmask>
ip helper-address <dhcp_server_IO>
ip helper-address <clearpass_IP> end
end
```

You can configure multiple *ip helper-address* statements to send DHCP packets to servers other than the DHCP server.

NetFlow Collector

NetFlow provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.

The ClearPass Policy Manager NetFlow Collector provides the ability to identify the open ports of a device connected to a network by analyzing the received NetFlow packets.

Supported versions are NetFlow v5 through v9 and IPFIX (Internet Protocol Flow Information eXport).

ClearPass Onboard Collector

ClearPass Onboard collects authentic device information from all devices during the onboarding process. Onboard then posts this information to the ClearPass Profile.

Because the information collected is definitive, ClearPass Profile can directly classify these devices into their appropriate category, OS family, and name without having to rely on any other fingerprinting information.

HTTP User-Agent Strings Collector

In some cases, DHCP fingerprinting alone cannot fully classify a device. A common example is the Apple family of smart devices; for example, DHCP fingerprints cannot distinguish between an iPad and an iPhone.

In these scenarios, user-agent strings sent by browsers in the HTTP protocol are useful to further refine classification results.

User-agent strings are collected from the following:

- ClearPass Guest
- ClearPass Onboard
- Aruba controller through an IF-MAP (Interface for Metadata Access Points) interface

MAC OUI Collector

The MAC OUI (Organization Unique Identifier) is expressed in the first 24 bits of a MAC address for a network-connected device. Thus, the MAC OUI indicates the specific vendor for that device. The MAC OUI is acquired through various authentication mechanisms, such as 802.1X and MAC address authentication.

The MAC OUI can be useful to more accurately classify endpoints. An example is Android™ devices where DHCP fingerprints can only classify a device as generic Android, but it cannot provide more details regarding the vendor.

Combining this information with MAC OUI, the ClearPass Profiler can classify a device as HTC™ Android, Samsung™ Android, or Motorola® Droid, etc.

The MAC OUI is also useful to profile devices such as printers that might be configured with static IP addresses.

ActiveSync Plug-in Collector

You can install the ActiveSync plug-in provided by Aruba on Microsoft Exchange servers.

When a device communicates with an Exchange server using the Active Sync protocol, the device provides attributes such as device-type and user-agent.

These attributes are collected by the ActiveSync plug-in and sent to the ClearPass Profiler. Profiler uses dictionaries to derive profiles from these attributes.

ClearPass OnGuard Agent

The ClearPass OnGuard agent performs advanced endpoint posture assessment. This agent can collect and send operating system details from endpoints during authentication.

The Policy Manager Profiler uses the OnGuard **os_type** attribute to derive a profile.

SNMP Collector

Endpoint information obtained by reading the Simple Network Management Protocol (SNMP) MIBs of network devices is used to discover and profile static IP devices in the network. For related information, see SNMP Configuration for Wired Network Profiling on page 443.

Table 243 describes the MIBs used by the SNMP Collector.

Table 243: *SNMP MIBs Used by the SNMP Collector*

MIB	Description
SysDescr	A textual description of the entity used both for profiling switches, controllers, and routers configured in ClearPass, and for profiling printers and other static IP devices discovered through SNMP or subnet scans (RFC1213).
cdpCacheTable	Provides the cached information obtained via receiving CDP (Cisco Discovery Protocol) messages from CDP-capable devices. Used to discover neighbor devices connected to the switch or controller configured in ClearPass.
lldpRemTable	This table contains one or more rows per physical network connection known to this agent read from LLDP (Link Layer Discovery Protocol)-capable devices. Used to discover and profile neighbor devices connected to the switch or controller configured in ClearPass.
ARPtable	Address Resolution Protocol (ARP) information read from the network devices. Used as a means to discover endpoints in the network.

Setting SNMP Community Attributes

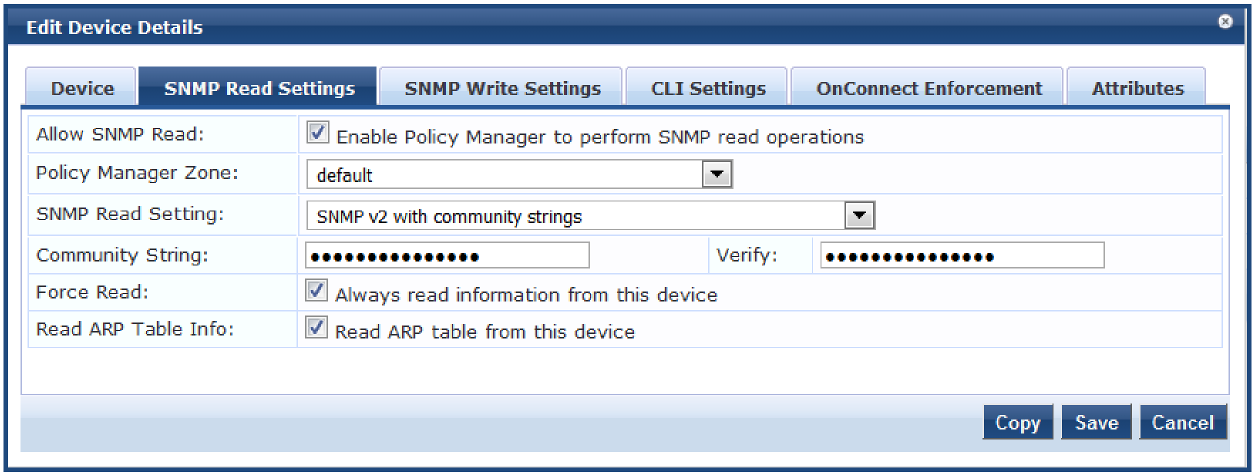
The SNMP-based mechanism is capable of profiling devices only if they respond to SNMP, or if the device advertises its capability via LLDP (Link Layer Discovery Protocol). When performing SNMP reads for a device, ClearPass uses SNMP Read credentials configured in the network devices, or defaults to using SNMPv2 with "public" community strings specified.

To specify SNMPv2 with community strings:

1. Navigate to **Configuration** > **Network** > **Devices**.
2. From the **Network Devices** page, select the appropriate device.

   The **Edit Device Details** dialog opens.
3. Select the **SNMP Read Settings** tab.

Figure 436: *Specifying SNMP v2 with Community Strings*



Edit Device Details

Allow SNMP Read: ☑ Enable Policy Manager to perform SNMP read operations

Policy Manager Zone: default

SNMP Read Setting: SNMP v2 with community strings

Community String: ••••••••••••••• Verify: •••••••••••••••

Force Read: ☑ Always read information from this device

Read ARP Table Info: ☑ Read ARP table from this device

4. Specify the SNMP Read Settings parameters as described in the following table, then click **Save**.

Table 244: *SNMP Read Settings Parameters*

Parameter	Action/Description
Allow SNMP Read	If not already enabled, enable the **Allow SNMP Read** check box. The SNMP Read Settings parameter fields are now enabled for configuration.
Policy Manager Zone	Select the Policy Manager Zone. If no Policy Manager Zone is configured, select **default**.
SNMP Read Setting	Select **SNMPv2 with community strings**.

Table 244: *SNMP Read Settings Parameters (Continued)*

Parameter	Action/Description
Community String	Enter the **Community String** value, then reenter the string to verify it.
Force Read	Enable the **Force Read** check box to ensure that all ClearPass nodes in the cluster will read the SNMP information from this device, regardless of the trap configuration on the device. **NOTE:** This option is especially useful when demonstrating static IP-based device profiling because the **Force Read** option does not require any trap configuration on the network device.
Read ARP Table Info	If this is a Layer-3 device, and you want to use the ARP table on this device as a way to discover endpoints in the network, enable the **Read ARP Table Info** check box. **NOTE:** Static IP endpoints discovered in this way are further probed via SNMP to profile the device.

Configuring the Device Info Poll Interval

Network devices configured with **SNMP Read** enabled are polled periodically for updates based on the time interval configured in the **Device Info Poll Interval**.

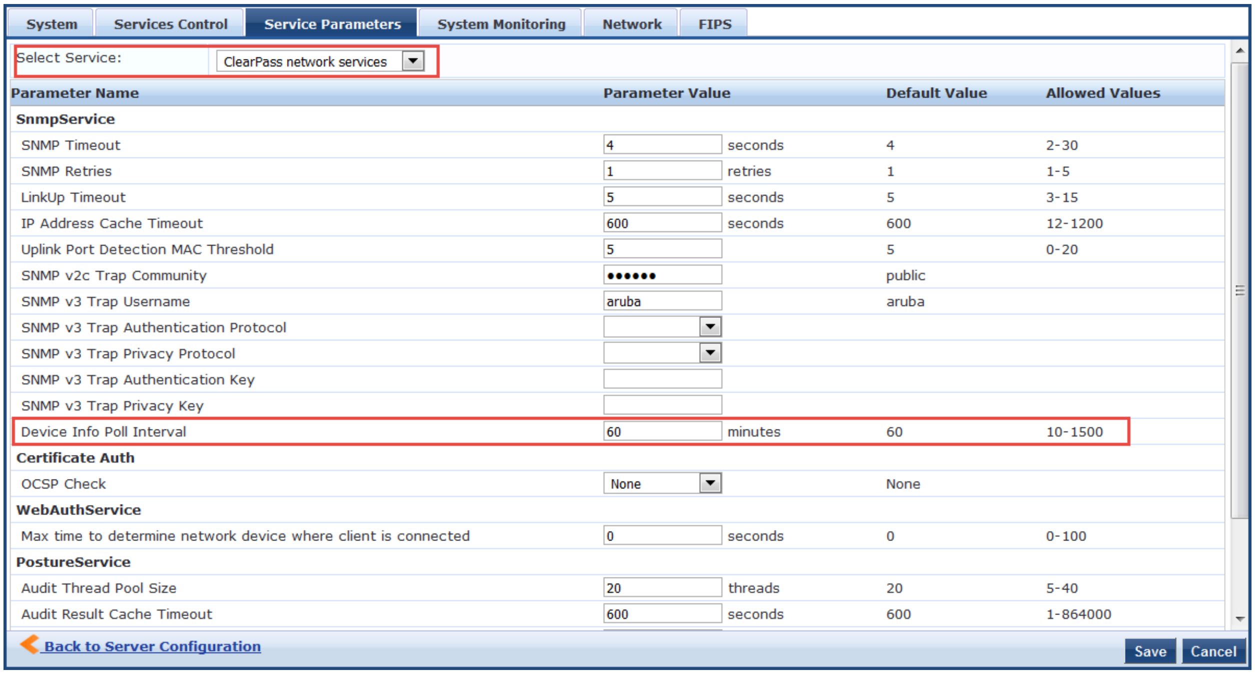
To set the Device Info Poll Interval:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.
2. Select the ClearPass server of interest.

   The **Server Configuration** page opens.
3. Select the **Service Parameters** tab.
4. From the **Select Service** drop-down, select **ClearPass network services**.

   The **ClearPass network services** page opens.

Figure 437: *Specifying the Device Info Poll Interval*



Select Service: ClearPass network services

Parameter Name	Parameter Value		Default Value	Allowed Values
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 MAC 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
Certificate Auth				
OCSP Check	None		None	
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

5. In the **minutes** field, enter the **Device Info Poll Interval**, then click **Save**.

About the Subnet Scan Collector

A network subnet scan discovers the IP addresses of devices in the network.

The devices discovered in this way are further probed using SNMP to fingerprint and assign a profile to the device. Network subnets to be scanned are configured per Policy Manager Zone.

This is particularly useful in deployments that are geographically distributed. In such deployments, it is recommended that you complete the following tasks:

1. Assign the ClearPass Policy Managernodes in a cluster to multiple zones depending on the geographical area served by that node.

   To set up Policy Manager Zones, navigate to **Administration** > **Server Manager** > **Server Configuration** > **Manage Policy Manager Zones.**
2. Then enable the profile for a minimum of one node per zone.

   For more information, see Managing Policy Manager Zones on page 522.

Configuring Subnet Scans

When you configure subnet scans, you specify the IP subnets that you want to be scanned for discovering hosts in the network and their capabilities. You have two options:

- Schedule a subnet scan
- Initiate an on-demand subnet scan

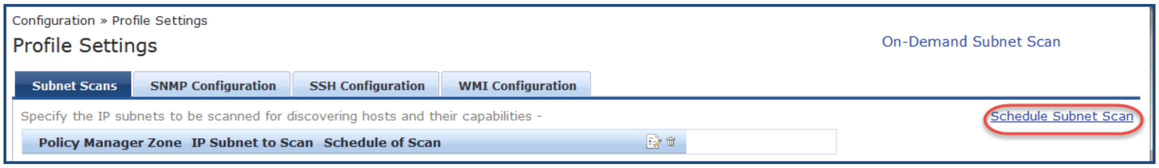
Scheduling a Subnet Scan

To schedule a subnet scan:

1. Navigate to the **Configuration** > **Profile Settings** page.

   The **Profile Settings** page opens to the **Subnet Scans** page.

Figure 438: *Subnet Scans Page*



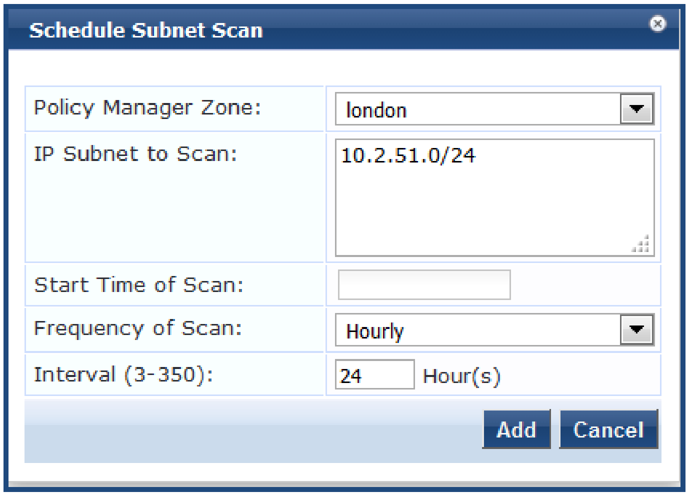
Specify the IP subnets to be scanned for discovering hosts and their capabilities -

Policy Manager Zone	IP Subnet to Scan	Schedule of Scan

2. Click the **Schedule Subnet Scan** link.

   The **Schedule Subnet Scan** dialog opens.

Figure 439: *Scheduling a Subnet Scan*



Schedule Subnet Scan

Policy Manager Zone:	london
IP Subnet to Scan:	10.2.51.0/24
Start Time of Scan:	
Frequency of Scan:	Hourly
Interval (3-350):	24 Hour(s)

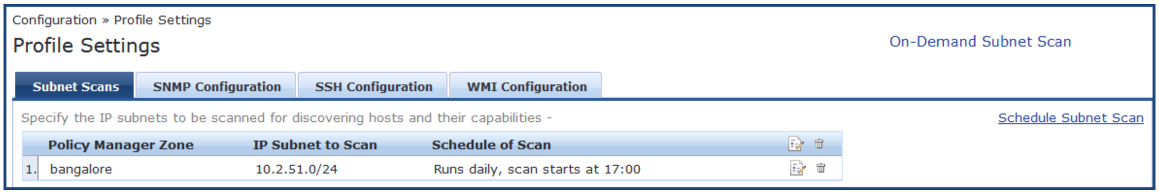
3. Configure the **Schedule Subnet Scan** parameters as described in the following table. When finished, click **Add**.

Table 245: *Schedule Subnet Scan Parameters*

Parameter	Action/Description
Policy Manager Zone	Select the Policy Manager Zone. **NOTE:** If Policy Manager Zones have not yet been set up, you can select the **default** zone, which will allow you to proceed with the subnet scan configuration procedure. For details, see Managing Policy Manager Zones on page 522.
IP Subnet to Scan	Enter the IP addresses for the subnets you wish to scan (using comma-separated values).
Start Time of Scan	Specify the time at which the subnet scan should start the first time. When you click this field, a time calendar opens, from which you can select the start time.
Frequency of Scan	Choose one of the following options to specify the subnet scan's frequency: ● Hourly: This is the default setting. ● Daily ● Weekly: When you select **Weekly**, the **Select Day of Week** field appears. Select the day of the week you want the scans to occur.
Interval	This option is displayed when you select **Hourly** for the scan frequency. Specify the profile subnet scan interval in hours. The default value is **24 hours**. The range is from **3** to **350 hours**.

You return to the **Subnet Scans** page, where the IP subnets are listed, along with their Policy Manager zone (if specified) and the subnet scan schedule:

Figure 440: *Subnet Scan Configured*



Configuration » Profile Settings

Profile Settings

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

	Policy Manager Zone	IP Subnet to Scan	Schedule of Scan
1.	bangalore	10.2.51.0/24	Runs daily, scan starts at 17:00

Initiating an On-Demand Subnet Scan

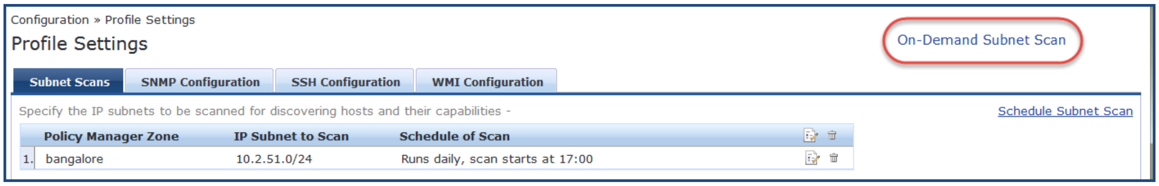
In cases in which you wish to initiate a subnet scan without saving the configuration, you can run an On-Demand Subnet Scan.

To run an On-Demand Subnet Scan:

1. Navigate to **Configuration** > **Profile Setting**s.

   The **Profile Settings** page opens to the **Subnet Scans** tab.

Figure 441: *Initiating an On-Demand Subnet Scan*



Configuration » Profile Settings

Profile Settings

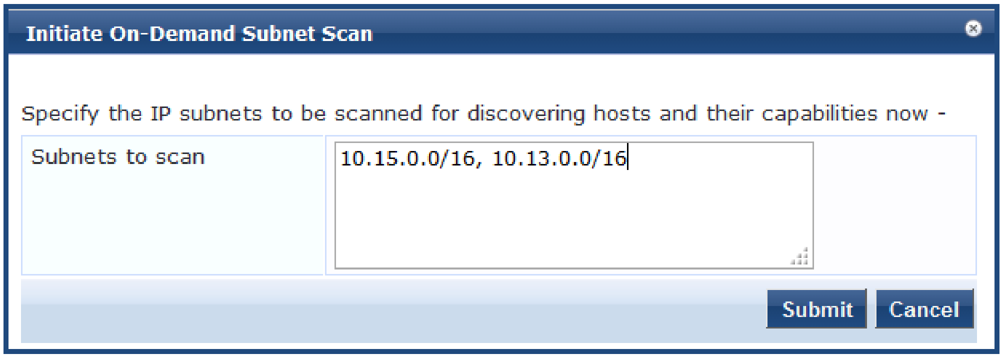
Specify the IP subnets to be scanned for discovering hosts and their capabilities -

	Policy Manager Zone	IP Subnet to Scan	Schedule of Scan
1.	bangalore	10.2.51.0/24	Runs daily, scan starts at 17:00

2. Click the **On-Demand Subnet Scan** link.

   The **Initiate On-Demand Subnet Scan** dialog opens.

Figure 442: *Initiate On-Demand Subnet Scan Dialog*



Initiate On-Demand Subnet Scan

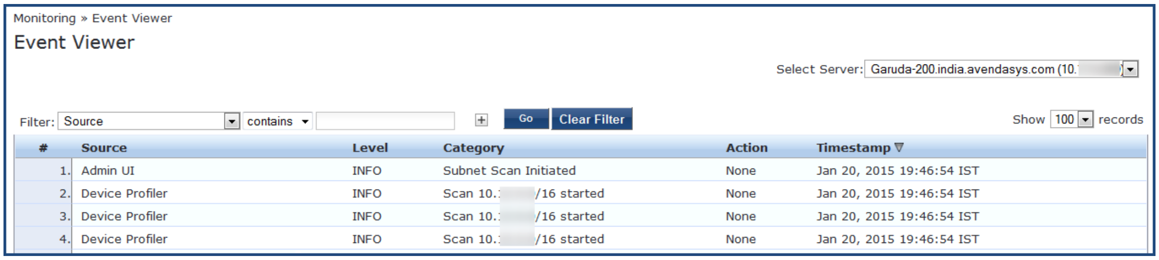
Specify the IP subnets to be scanned for discovering hosts and their capabilities now -

Subnets to scan: 10.15.0.0/16, 10.13.0.0/16

3. To discover hosts, specify the IP subnets to be scanned in the **Subnets to scan** text field. Separate multiple subnets with commas.
4. Click **Submit**.

   The subnet scan progress is shown on the **Profile Settings** page. You can view the subnet scan events in the **Monitoring** > **Event Viewer** page.

Figure 443: *Subnet Scan Logs*



Monitoring » Event Viewer

Event Viewer

Select Server: Garuda-200.india.avendasys.com (10.[redacted])

Filter: Source contains

Show 100 records

#	Source	Level	Category	Action	Timestamp ▽
1.	Admin UI	INFO	Subnet Scan Initiated	None	Jan 20, 2015 19:46:54 IST
2.	Device Profiler	INFO	Scan 10.[redacted]/16 started	None	Jan 20, 2015 19:46:54 IST
3.	Device Profiler	INFO	Scan 10.[redacted]/16 started	None	Jan 20, 2015 19:46:54 IST
4.	Device Profiler	INFO	Scan 10.[redacted]/16 started	None	Jan 20, 2015 19:46:54 IST

SNMP Configuration for Wired Network Profiling

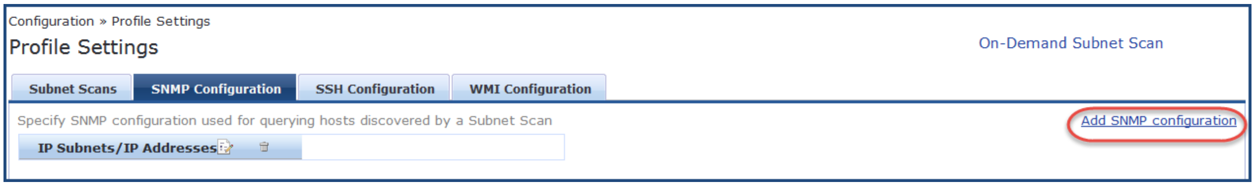
For wired network profiling, you can configure a list of multiple SNMP community strings to query static IP address devices discovered by the Profiler.

If a static IP address 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.

To configure SNMP for wired network profiling:

1. Navigate to **Configuration** > **Profile Settings**.
2. Click the **SNMP Configuration** tab.

Figure 444: *Profile Settings > SNMP Configuration Page*



Configuration » Profile Settings

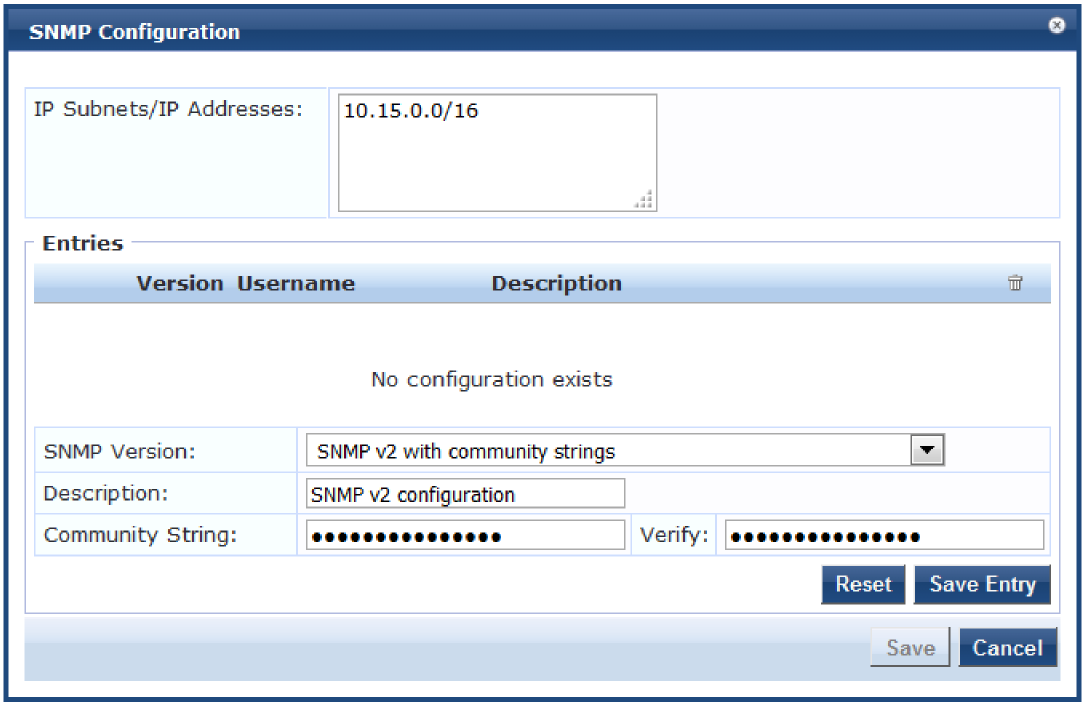
Profile Settings

Specify SNMP configuration used for querying hosts discovered by a Subnet Scan

3. Click **Add SNMP Configuration**.

   The **SNMP Configuration** dialog opens.

Figure 445: *Configuring SNMP Community Strings*



SNMP Configuration

IP Subnets/IP Addresses: 10.15.0.0/16

Entries

Version	Username	Description

No configuration exists

SNMP Version: SNMP v2 with community strings

Description: SNMP v2 configuration

Community String: ●●●●●●●●●●●●●●● Verify: ●●●●●●●●●●●●●●●

4. Specify the **SNMP Configuration** parameters as described in the following table, click **Save Entry**, then click **Save**:

Table 246: *SNMP Configuration Parameters*

Parameter	Action/Description
IP Subnets/ IP Addresses	Enter one or more IP subnet addresses and their subnet masks. For multiple entries, separate multiple IP addresses with commas.
SNMP Version	From the drop-down, select the appropriate SNMP version.
Description	Optionally, enter a description of this SNMP configuration (recommended).
Community String	Enter the community string, then reenter the communty string in the **Verify** field.

Accessing SSH and WMI Configuration Information

For information on configuring SSH and WMI credentials:

- **SSH credentials**

  For Linux server or network device discovery, specify SSH configuration credentials. For more information, see SSH Credentials Configuration on page 137.

- **WMI credentials**

  For Windows device discovery, specify WMI (Windows Management Instrumentation) credentials. For more information, see WMI Credentials Configuration on page 139.

Network Access Devices

This chapter describes the following tasks that you can perform by using the Policy Manager user interface:

- Adding and Modifying Network Devices on page 448
- Adding and Modifying Device Groups on page 459
- Adding and Modifying Proxy Targets on page 458
- Configuring the Ingress Event Sources on page 704

Introduction

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 related information, see SNMP Private MIB, SNMP Traps, System Events, Error Codes on page 807.

For the 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. For details, see SNMP Credentials Configuration on page 135.
- Configure SNMP trap configurations on the network device to send SNMP traps to the Policy Manager server. For details, see SNMP Trap Receivers on page 558.
- 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 user interface.
- Configure SNMPTRAPD on the Policy Manager server to receive SNMP traps. For details, see SNMP Private MIB, SNMP Traps, System Events, Error Codes on page 807.

  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 a phantom login to network devices. For details, see SSH Credentials Configuration on page 137.

- Configure DHCP Relay configuration on the network device to ensure that DHCP requests are forwarded from the clients. For more information, see DHCP Collector on page 437.

Adding and Modifying Network Devices

This section provides the following information:

- Adding a Network Device
- Adding and Modifying Proxy Targets
- Adding and Modifying Device Groups
- Configuring the Ingress Event Sources

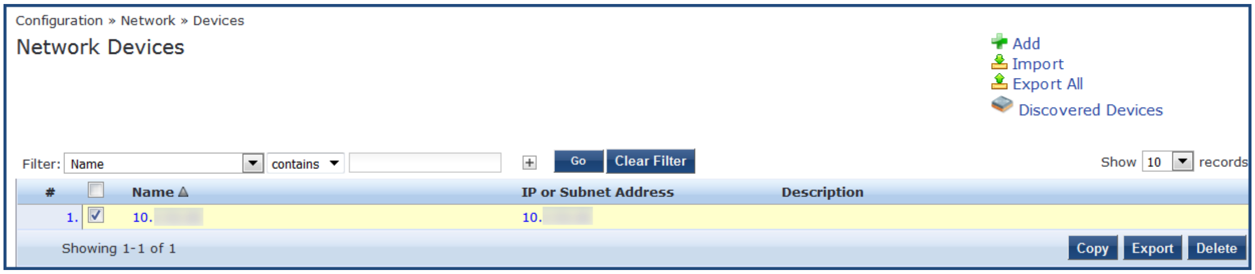
A Network Access Device (NAD) must belong to the global list of devices in the Policy Manager database in order to connect to Policy Manager using any of the supported protocols.

The Policy Manager **Network Devices** page displays the device name, IP address or subnet address, and a brief description of each configured device.

1. To view this page, navigate to **Configuration > Network > Devices**.

   The **Network Devices** page opens:

Figure 446: *Network Devices Page*



Configuration » Network » Devices

Network Devices

#	□	Name ▲	IP or Subnet Address	Description
1.	☑	10.[redacted]	10.[redacted]	

Showing 1-1 of 1

For information on configuring a new network device, see Adding a Network Device on page 448.

Adding a Network Device

This section describes how to configure a new network device:

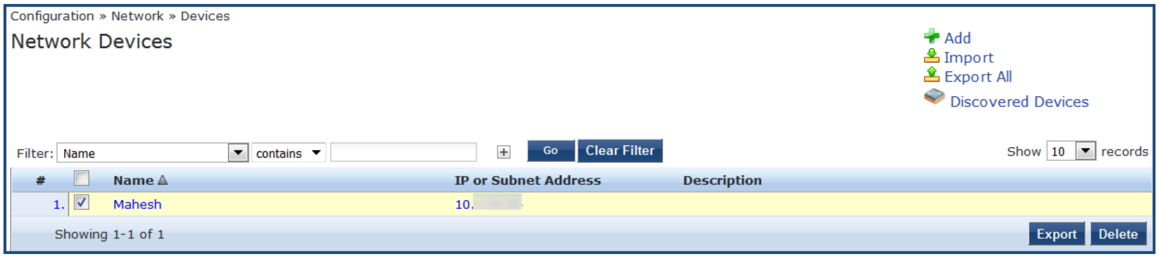
- Device Parameters
- SNMP Read Settings Parameters
- SNMP Write Settings Parameters
- CLI Settings Parameters
- Enabling ClearPass OnConnect Enforcement on a Network Device
- Querying and Selecting Port Names for OnConnect Enforcement
- Attributes Parameters

To add a network device:

1. Navigate to the **Configuration** > **Network** > **Devices** page.

   The **Network Devices** page opens.

Figure 447: *Network Devices Page*



Configuration » Network » Devices

Network Devices

#	☐	Name △	IP or Subnet Address	Description
1.	☑	Mahesh	10.[redacted]	

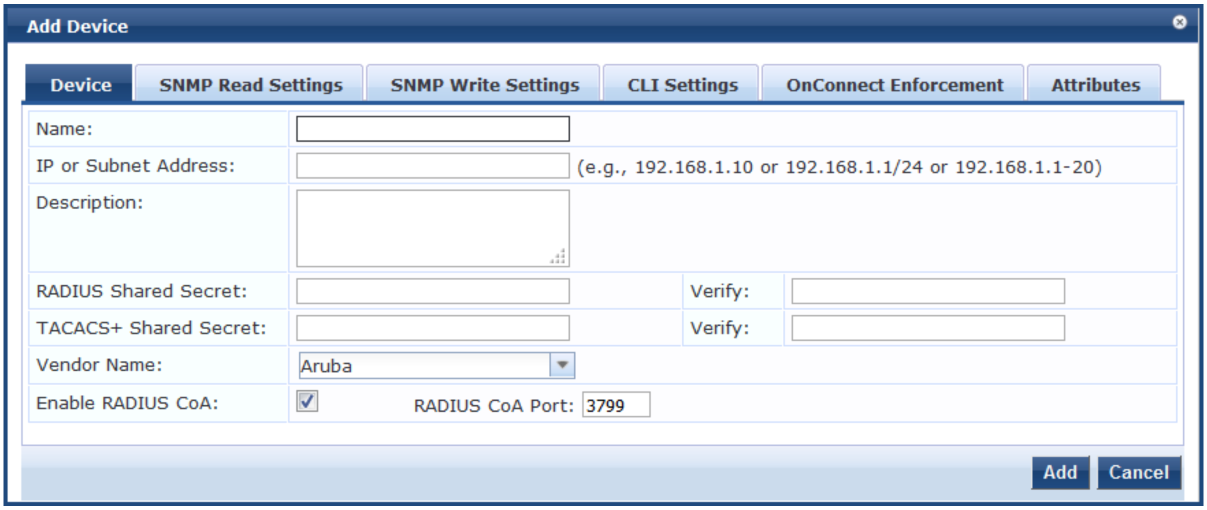
Showing 1-1 of 1

2. Click the **Add** link at the top-right corner.

   The **Add Device** page opens.

Device Parameters

Figure 448: *Add Device > Device Dialog*



Add Device

Name:

IP or Subnet Address: (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description:

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Aruba

Enable RADIUS CoA: ☑ RADIUS CoA Port: 3799

3. Enter the **Add Device** > **Device** parameters as described in Table 247:

Table 247: *Add Device > Device Parameters*

Parameter	Action/Description
Name	Enter the name of 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**.
Description	Enter a description that provides additional information to identify the device.
RADIUS Shared Secret	Enter the RADIUS shared secret.

Table 247: *Add Device > Device Parameters (Continued)*

Parameter	Action/Description
TACACS+ Shared Secret	Enter the TACACS+ shared secret.
Vendor Name	Specify the name of the vendor to load the dictionary associated with this vendor 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	To configure the UDP port on the device to send CoA (Change of Authorization) actions, enable RADIUS CoA for this device. **RADIUS CoA Port**: The default value is **3799**.

SNMP Read Settings Parameters

Use the **SNMP Read Settings** tab to define values that allow ClearPass Policy Manager to read information from the device using SNMPv1, SNMPv2, or SNMPv3.

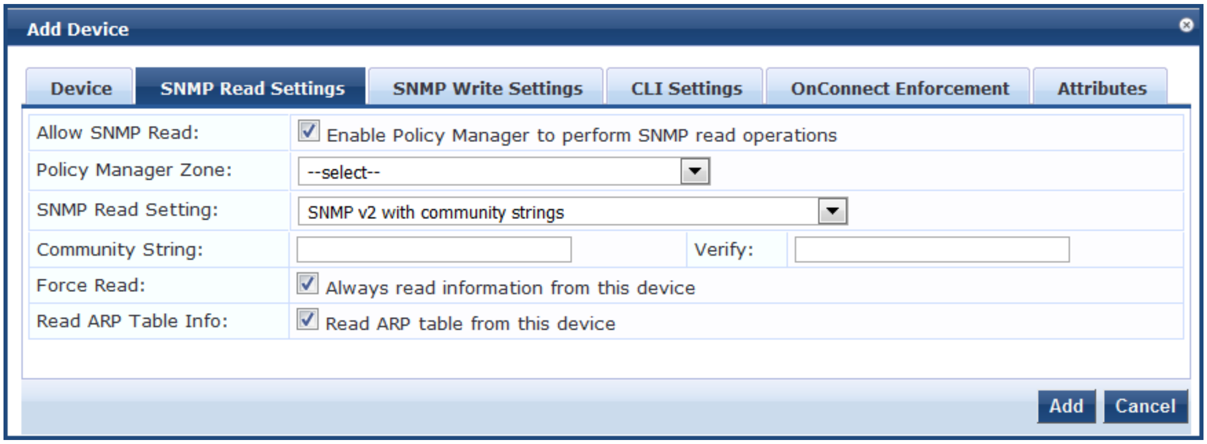
NOTE

Large or geographically-spread cluster deployments typically do not require each ClearPass node to probe all SNMP configured devices. By default, a ClearPass node in a cluster only reads network device information for devices configured to send traps to that node.

1. From the **Add Device** page, select the **SNMP Read Settings** tab.

   The **SNMP Read Settings** dialog opens:

Figure 449: *Add Device > SNMP Read Settings Dialog*



Allow SNMP Read:	☑ Enable Policy Manager to perform SNMP read operations
Policy Manager Zone:	--select--
SNMP Read Setting:	SNMP v2 with community strings
Community String:	Verify:
Force Read:	☑ Always read information from this device
Read ARP Table Info:	☑ Read ARP table from this device

2. Enter the **SNMP Read Settings** parameters as described in Table 248:

Table 248: *Add Device > SNMP Read Settings Parameters*

Parameter	Action/Description
Allow SNMP Read	Toggle to enable or disable SNMP Read operations.
Policy Manager Zone	You can assign Network Access Devices to a zone, allowing the SNMP service to poll or query only the NADs that are in its zone. ● From the Policy Manager Zone drop-down, select the zone assigned to the network device that is being added. OnConnect Enforcement is triggered when a trap from a NAD is received by a ClearPass node. If the zone assigned to a ClearPass node is not same as the zone configured here, then OnConnect Enforcement is not triggered on that ClearPass node. **NOTE:** This setting can be empty or null.
SNMP Read Setting	Specify one of the following SNMP Read Settings: ■ 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 when you use ClearPass Policy Manager in **FIPS** mode.
Community String	Enter the community string for sending the traps. **NOTE:** Available in SNMP v2 only.
Verify	Reenter the community string for sending the traps.
Force Read	Enable **Force Read** to ensure that all 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. **NOTE:** Available in SNMP v1 and SNMP v2 only.
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 that are discovered this way are probed using SNMP to profile the device.
Username	Specify the Admin user name to use for SNMP read operations. **NOTE:** Available in SNMP v3 only.

Table 248: *Add Device > SNMP Read Settings Parameters (Continued)*

Parameter	Action/Description
Authentication Key	Specify the SNMP v3 with authentication option (SHA or MD5). **NOTE:** The **EAP-MD5** authentication type is not supported if you run ClearPass Policy Manager in FIPS mode. **NOTE:** Authentication Key is available in SNMP v3 only.
Privacy Key	Specify the SNMP v3 with privacy option. **NOTE:** Available in SNMP v3 only.
Privacy Protocol	Choose one of the available privacy protocols: ▪ DES-CBC ▪ AES-128 **NOTE:** Available in SNMP v3 with Privacy only. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data.

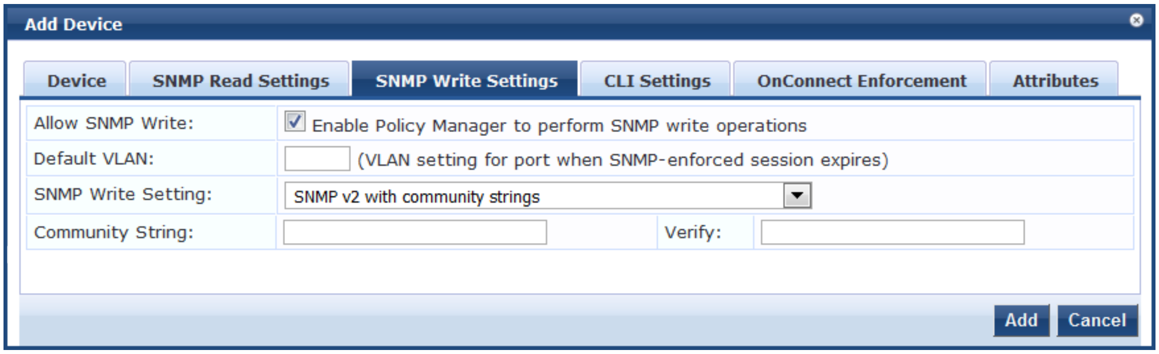
SNMP Write Settings Parameters

Use the **SNMP Write Settings** tab to define values that allow ClearPass Policy Manager to write to (manage) the device using SNMPv1, SNMPv2, or SNMPv3.

1. From the **Add Device** page, select the **SNMP Write Settings** tab.

   The **SNMP Write Settings** dialog opens:

Figure 450: *Add Device > SNMP Write Settings Dialog*



Allow SNMP Write: ☑ Enable Policy Manager to perform SNMP write operations

Default VLAN: (VLAN setting for port when SNMP-enforced session expires)

SNMP Write Setting: SNMP v2 with community strings

Community String: Verify:

2. Enter the **SNMP Write Settings** parameters as described in Table 249.

Table 249: *Add Device > SNMP Write Settings Parameters*

Parameter	Action/Description
Allow SNMP Write	Toggle to enable or disable SNMP write.
Default VLAN	Specify the VLAN port setting after the SNMP-enforced session expires.
SNMP Write Setting	Specify the SNMP Write setting for the device. You can set any of the following options: ▪ SNMP v1 with community strings ▪ SNMP v2 with community strings

Table 249: *Add Device > SNMP Write Settings Parameters (Continued)*

Parameter	Action/Description
	■ 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 ClearPass Policy Manager in **FIPS** mode.
Community String	Enter the community string for sending the traps.
Verify	Reenter the community string for sending the traps.

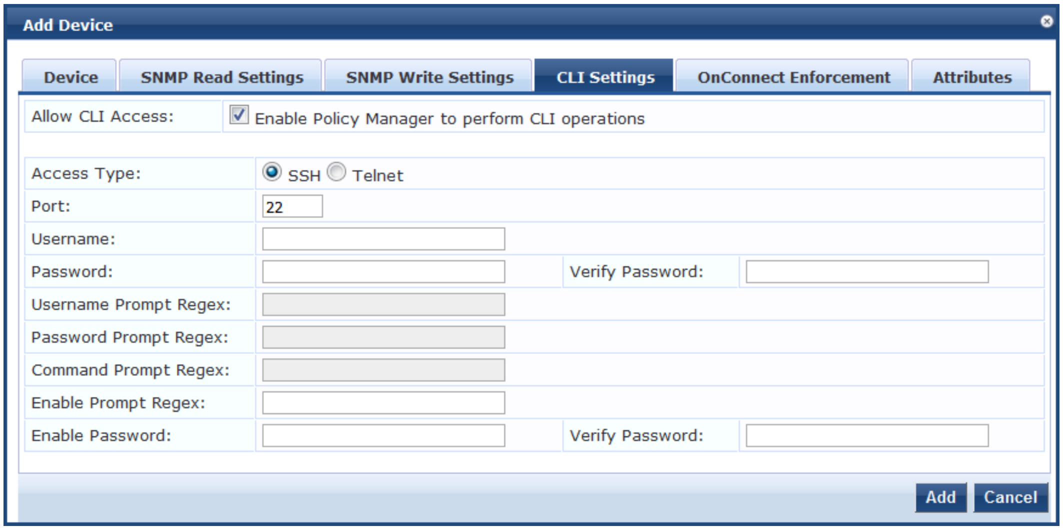
CLI Settings Parameters

Use the **CLI Settings** tab to enable or disable the CLI, and define user names, passwords, and port settings for accessing the CLI.

1. From the **Add Device** page, select the **CLI Settings** tab.

   The **CLI Settings** dialog opens:

Figure 451: *Add Device > CLI Settings Dialog*



Allow CLI Access:	☑ Enable Policy Manager to perform CLI operations		
Access Type:	● SSH ○ Telnet		
Port:	22		
Username:			
Password:		Verify Password:	
Username Prompt Regex:			
Password Prompt Regex:			
Command Prompt Regex:			
Enable Prompt Regex:			
Enable Password:		Verify Password:	

2. Enter the **CLI Settings** parameters as described in Table 250:

Table 250: *Add Device > CLI Parameters*

Parameter	Action/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 then reenter the credentials for the **Enable** password in the CLI.

Enabling ClearPass OnConnect Enforcement on a Network Device

OnConnect Enforcement is an enforcement model that allows you to use non-802.1X methods for device scans, VLAN placement, and so on. OnConnect Enforcement allows enforcement in non-802.1X environments without the need for an agent, such as OnGuard, on the endpoint.

When this feature is enabled, ClearPass performs the following actions:

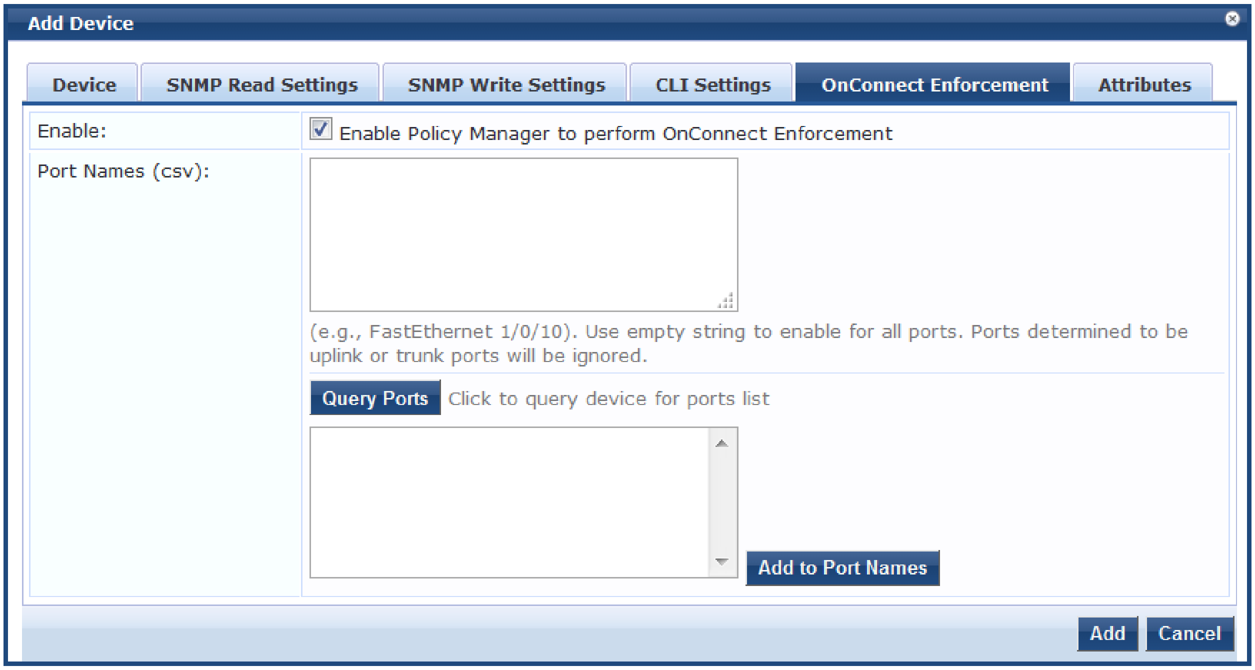
- Detects when a new endpoint connects to the network.
- Scans the endpoint to identify the logged-in user and other device-specific information.
- Triggers a Web-based authentication (WebAuth) for the device.
- Performs SNMP-based enforcement to change the network access profile for the device.

To enable ClearPass OnConnect Enforcement on a Network Device:

1. From the **Add Device** page, select the **OnConnect Enforcement** tab.

   The **OnConnect Enforcement** dialog opens:

Figure 452: *Add Device > OnConnect Enforcement Dialog*



Enable: ☑ Enable Policy Manager to perform OnConnect Enforcement

Port Names (csv):

(e.g., FastEthernet 1/0/10). Use empty string to enable for all ports. Ports determined to be uplink or trunk ports will be ignored.

Query Ports Click to query device for ports list

2. Enter the **OnConnect Enforcement** parameters as described in Table 251.

Table 251: *Add Device > OnConnect Enforcement Parameters*

Parameter	Action/Description
Enable	Select this check box to enable ClearPass OnConnect on the network access device being added.
Port Names	Specify the names and descriptions of the ports to be enabled for OnConnect Enforcement (see the next section for details). You can do so in two ways: ● Click **Query Ports**. ● You can also a enter port names manually as a comma-separated list. Only the ports added in the **Port Names** field will have OnConnect Enforcement enabled. For example, if you add the port names **Fa1/0/3,Fa1/0/5**, when clients connect to any of these ports on the specified network device, OnConnect Enforcement is triggered on that network device. **NOTE:** Use an empty string to enable OnConnect Enforcement for all ports. Ports determined to be uplink ports or trunk ports will be ignored; multiple clients behind a Hub-connected port are also ignored.
Query Ports	To display the list of ports on the current server, click **Query Ports**.
Add to Port Names	Once the list of ports are displayed, select the desired ports from the displayed list, then click **Add to Port Names**. The selected ports are added to the **Port Names** field.

Querying and Selecting Port Names for OnConnect Enforcement

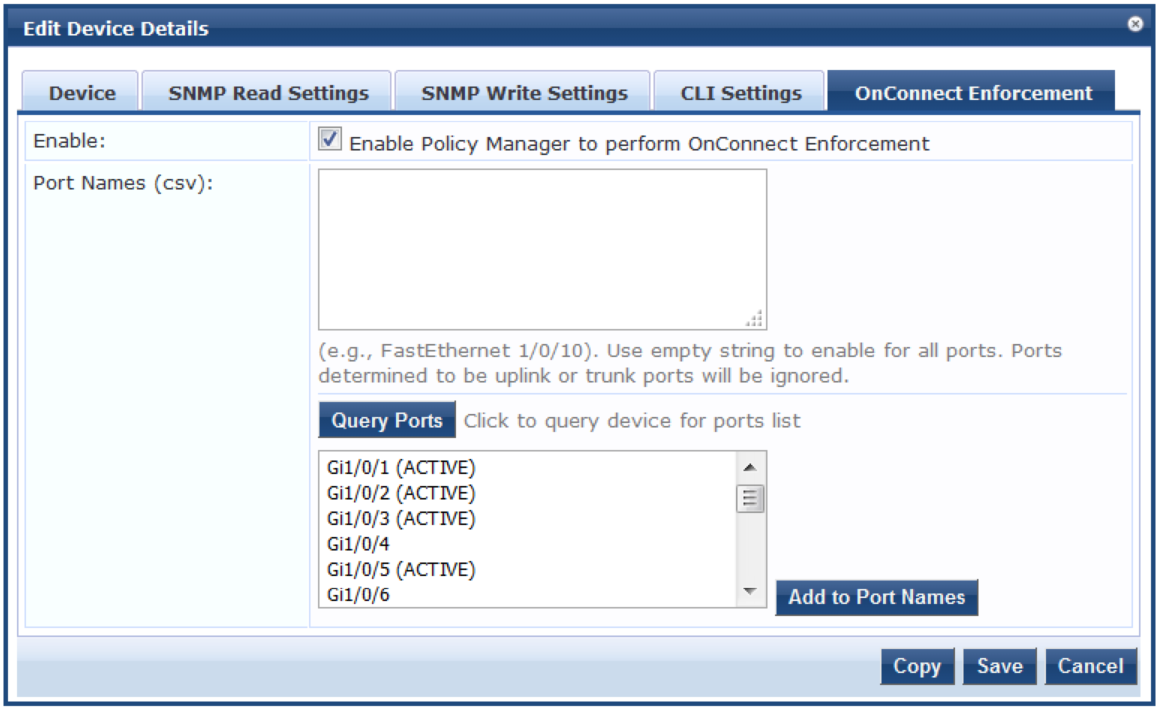
To query and select port names for a Network Access Device for OnConnect Enforcement:

1. From the **Configuration** > **Network** > **Devices** page, select the network device.
2. From the **Edit Device Details** page, select the **SNMP Read Settings** tab (see Table 248 above).

3. In the **Allow SNMP Read** parameter, select the **Enable Policy Manager to perform SNMP read operations** check box.
4. Select the **OnConnect Enforcement** tab.
5. Click the **Query Ports** button.

   The list of ports are displayed, as shown in Figure 453.

Figure 453: *Querying Ports*



Enable: ☑ Enable Policy Manager to perform OnConnect Enforcement

Port Names (csv):

(e.g., FastEthernet 1/0/10). Use empty string to enable for all ports. Ports determined to be uplink or trunk ports will be ignored.

Click to query device for ports list

```
Gi1/0/1 (ACTIVE)
Gi1/0/2 (ACTIVE)
Gi1/0/3 (ACTIVE)
Gi1/0/4
Gi1/0/5 (ACTIVE)
Gi1/0/6
```

6. Select the ports to use, then click **Add to Port Names**.

   The selected port names are added to the **Port Names** list. Only the ports added in the **Port Names** field will have OnConnect Enforcement enabled.
7. Click **Save**.

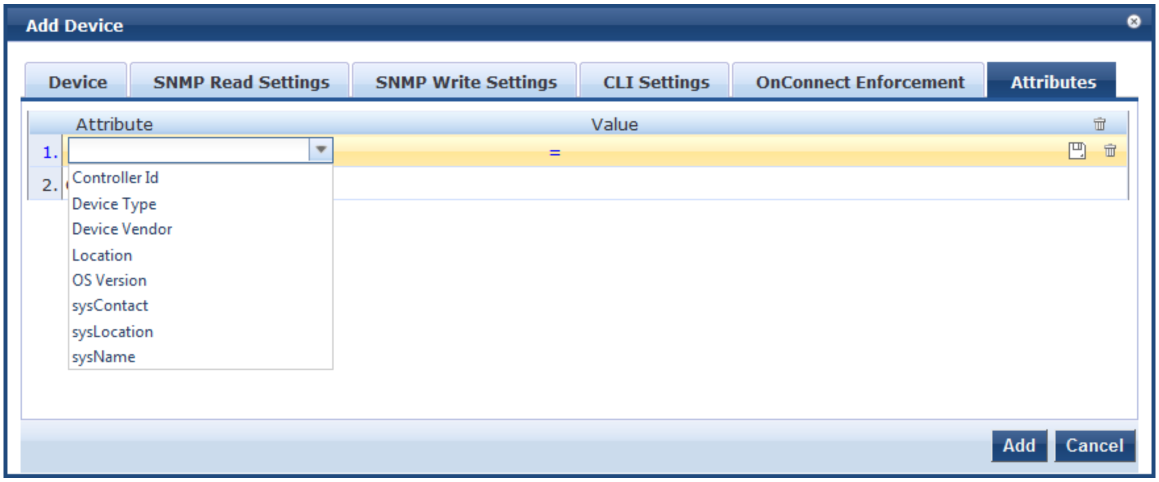
Attributes Parameters

To add custom attributes for this device:

1. From the **Add Device** page, select the **Attributes** tab.

   The **Attributes** dialog opens:

Figure 454: *Adding Custom Device Attributes*



2. From the **Attribute** field, click **Click to add...**.

   By default, the following custom attributes appear in the **Attribute** drop down:

   - Controller ID
   - Device Type
   - Device Vendor
   - Location
   - OS Version
   - sysContact
   - sysLocation
   - sysName

3. Select one of the defalt attributes or enter a new attribute.

   You can enter any name in the **Attribute** field. All attributes are of *string* datatype.

4. Specify the attribute's value.

   You can populate the **Value** field with any string.

5. Repeat this procedure as necessary.
6. When finished adding custom attributes, click **Add**.

   All attributes entered for a device are available in the role-mapping Rules Editor under the Device namespace.

Additional Network Device Tasks

Importing a Device

To import a device:

1. Click **Import**.
2. In the **Import from File** page, browse to select a file, and then click **Import**.
3. If you entered a secret key to encrypt the exported file, enter the same secret key to import the device back.

Exporting All Devices

To export all devices from the configuration:

1. Click **Export**.
2. In the **Export to File** page, specify a file path, then click **Export**.

3. 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.

Exporting a Single Device

To export a single device from the configuration:

1. Select it (using the check box on the left).
2. click **Export**.
3. In the **Save As** dialog, specify a file path, then click **Export**.

Adding and Modifying Proxy Targets

A *proxy server* is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service. The proxy server can exist in the same machine as a firewall server or it canbe on a separate server, which forwards requests through the firewall.

In ClearPass Policy Manager, a *proxy target* represents a RADIUS server (Policy Manager or a 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 appends the domain to the username.

Proxy targets are configured at a global level. They can be used in configuring RADIUS proxy services. For more information, refer to Configuring Policy Manager Services on page 70.

Adding a Proxy Target

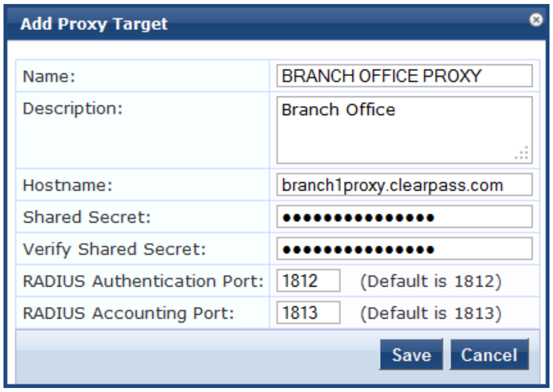
To add a proxy target:

1. Navigate to **Configuration > Network > Proxy Targets**.

   The **Proxy Targets** page opens. Policy Manager lists all configured proxy servers in the **Proxy Targets** page.
2. Click **Add**.

   The **Add Proxy Target** dialog opens.

Figure 455: *Add Proxy Target Dialog*



Add Proxy Target

Name:	BRANCH OFFICE PROXY
Description:	Branch Office
Hostname:	branch1proxy.clearpass.com
Shared Secret:	•••••••••••••••
Verify Shared Secret:	•••••••••••••••
RADIUS Authentication Port:	1812 (Default is 1812)
RADIUS Accounting Port:	1813 (Default is 1813)

3. Specify the **Add Proxy Target** parameters as described in the following table, then click **Save**:

Table 252: *Add Proxy Target Parameters*

Parameter	Action/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.
Shared Secret Verify Shared Secret	Enter the shared secret, then verify it. **NOTE:** Use the same shared 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. The default value for this port is **1812**.
RADIUS Accounting Port	Enter the UDP port to send the RADIUS accounting request. The default value for this port is **1813**.

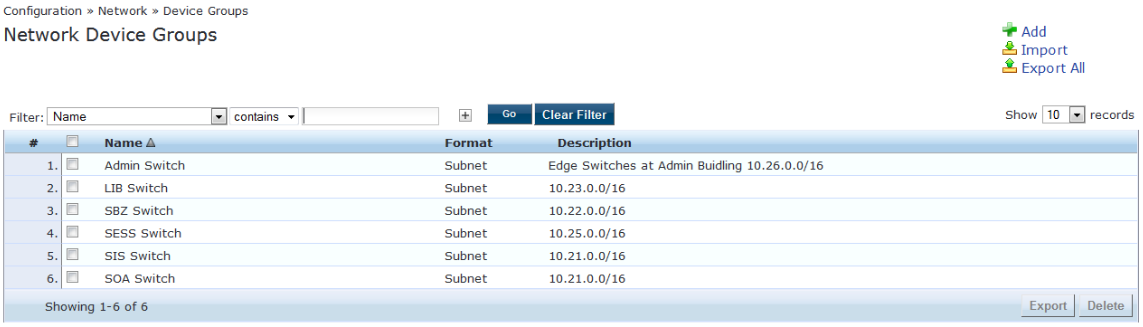
Adding and Modifying Device Groups

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** page (**Configuration > Network > Device Groups**) . The following figure displays the **Network Device Groups** page:

Figure 456: *Device Groups Page*



Configuration » Network » Device Groups

Network Device Groups

Filter: Name contains

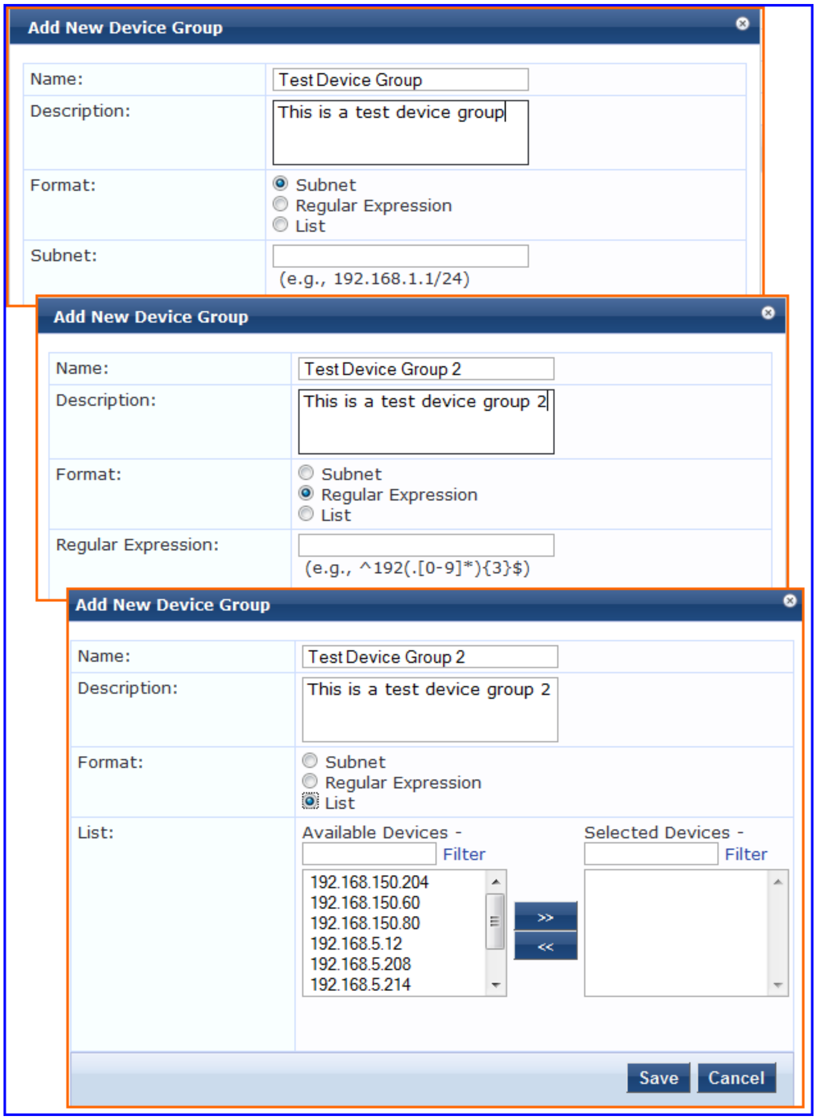
Show 10 records

#	□	Name	Format	Description
1.	□	Admin Switch	Subnet	Edge Switches at Admin Buidling 10.26.0.0/16
2.	□	LIB Switch	Subnet	10.23.0.0/16
3.	□	SBZ Switch	Subnet	10.22.0.0/16
4.	□	SESS Switch	Subnet	10.25.0.0/16
5.	□	SIS Switch	Subnet	10.21.0.0/16
6.	□	SOA Switch	Subnet	10.21.0.0/16

Showing 1-6 of 6

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 457: *Add New Device Group Page*



Add New Device Group

Name: Test Device Group

Description: This is a test device group

Format: ● Subnet ○ Regular Expression ○ List

Subnet: (e.g., 192.168.1.1/24)

Add New Device Group

Name: Test Device Group 2

Description: This is a test device group 2

Format: ○ Subnet ● Regular Expression ○ List

Regular Expression: (e.g., ^192(.[0-9]*){3}$)

Add New Device Group

Name: Test Device Group 2

Description: This is a test device group 2

Format: ○ Subnet ○ Regular Expression ● List

List: Available Devices - Filter

192.168.150.204
192.168.150.60
192.168.150.80
192.168.5.12
192.168.5.208
192.168.5.214

Selected Devices - Filter

The following table describes the **Add New Device Group** page parameters:

Table 253: *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 253: *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.

Configuring the Ingress Event Sources

The Event Source is the device that sends Syslog events to ClearPass. Any events sent that are not from configured event sources are ignored.

To configure the Event Source (in this example, a Juniper Networks SRX gateway):

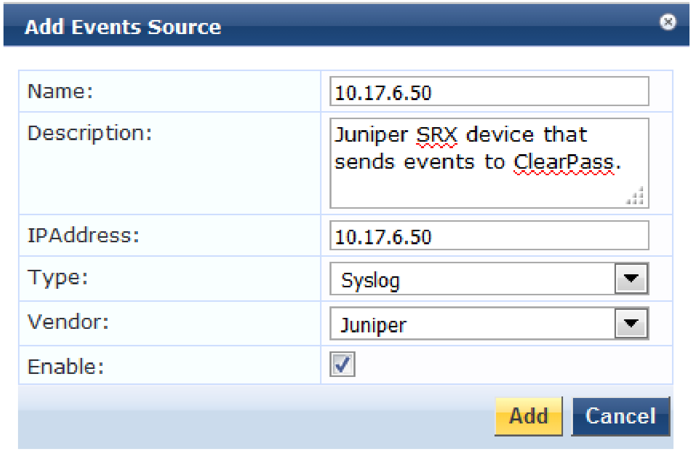
1. Navigate to **Configuration** > **Network** > **Event Sources**.

   The **Event Sources** page opens.

2. To add the Event Source for the desired vendor, click **Add**.

   The **Add Events Source** dialog opens.

Figure 458: *Adding an Event Source*



Add Events Source

Name:	10.17.6.50
Description:	Juniper SRX device that sends events to ClearPass.
IPAddress:	10.17.6.50
Type:	Syslog
Vendor:	Juniper
Enable:	☑

3. Specify the **Add Event Source** parameters as described in Table 254.

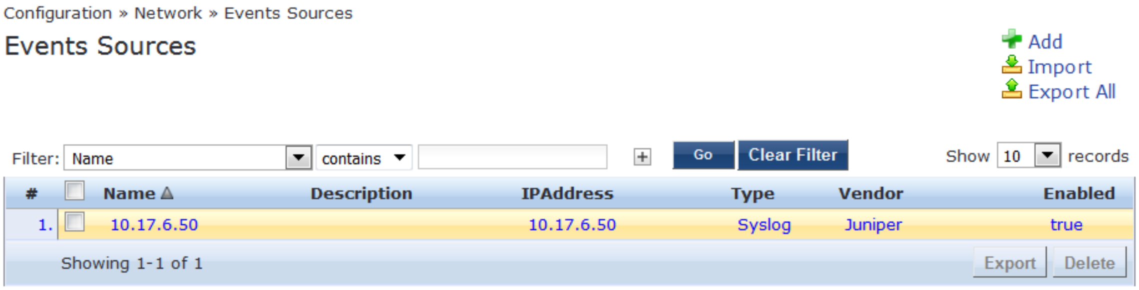
Table 254: *Configuring the Event Source Parameters*

Parameter	Action/Description
Name	1. Enter the IP address of the device that will send Syslog events to ClearPass.
Description	Optionally, enter a description of this Event Source.
IP Address	2. Enter the IP address of the device that will send Syslog events to ClearPass.
Type	3. From the drop-down, select the Event Source **Type**.
Vendor	4. From the drop-down, select the Event Source **Vendor**.
Enable	5. Select this check box to enable the device as an Event Source.

6. When finished, click **Add**.

   The **Event Sources** page now displays the new Event Sources (see Figure 459).

Figure 459: *Event Sources Page*



Filter: Name contains

Show 10 records

#	□	Name ▵	Description	IPAddress	Type	Vendor	Enabled
1.	□	10.17.6.50		10.17.6.50	Syslog	Juniper	true

Showing 1-1 of 1

The IP address displayed in Figure 459 is the IP address and host name of the Juniper SRX gateway that sends Syslog events to ClearPass.

Chapter 11
Administration

You can access all ClearPass administrative activities, including server configuration, log management, certificate and dictionary maintenance, portal definitions, and administrator user account maintenance from the following Administration sections:

- ClearPass Portal
  - ClearPass Portal on page 464
- Users and Privileges
  - Managing Admin Users on page 465
  - Managing Admin Privileges on page 469
- Server Manager
  - Server Configuration on page 477
  - Log Configuration on page 548
  - Downloading Local Shared Folders on page 551
  - License Management on page 552
- External Servers
  - SNMP Trap Receivers on page 558
  - Syslog Targets on page 563
  - Syslog Export Filters on page 567
  - Messaging Setup on page 579
  - Endpoint Context Servers on page 582
  - File Backup Servers on page 646
- Certificates
  - Server Certificates on page 648
  - Certificate Trust List on page 659
  - Certificate Revocation Lists on page 661
- Dictionaries
  - RADIUS Dictionary on page 664
  - TACACS+ Services Dictionary on page 665
  - Fingerprints Dictionary on page 667
  - Dictionary Attributes on page 668
  - Applications Dictionaries on page 672
  - Configuring Endpoint Context Server Actions on page 590
- Agents and Software Updates
  - OnGuard Settings on page 679
  - Updating Policy Manager Software on page 673
- Support
  - Contacting Support on page 1
  - Remote Assistance on page 1
  - Accessing Documentation on page 1

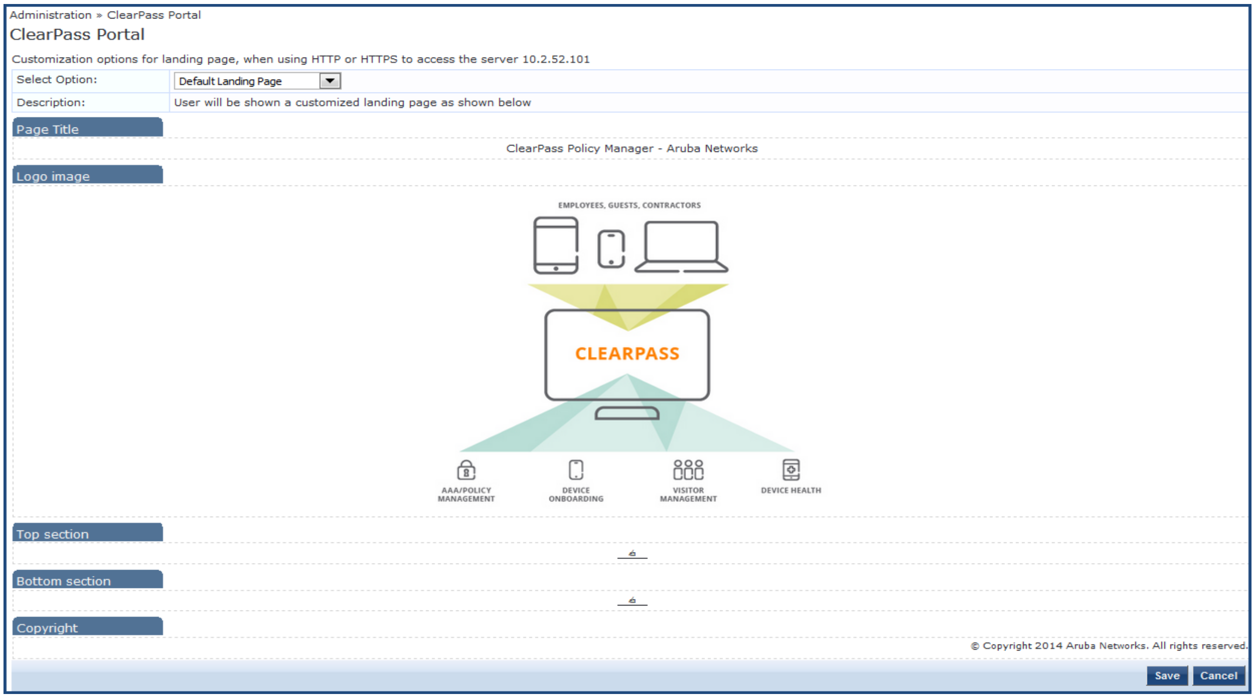
ClearPass Portal

To customize the ClearPass Portal content for your enterprise:

1. Navigate to the **Administration > ClearPass Portal** page.

   The following figure displays the ClearPass Portal page:

Figure 460: *ClearPass Portal*



Administration » ClearPass Portal

ClearPass Portal

Customization options for landing page, when using HTTP or HTTPS to access the server 10.2.52.101

Select Option: Default Landing Page

Description: User will be shown a customized landing page as shown below

Page Title

ClearPass Policy Manager - Aruba Networks

Logo image

Top section

Bottom section

Copyright

© Copyright 2014 Aruba Networks. All rights reserved.

2. Specify the ClearPass Portal parameters as described in the following table, then click **Save**:

Table 255: *ClearPass Portal Parameters*

Parameter	Action/Description
Select Option	Select the page that the user first sees after logging in to ClearPass: - Default Landing Page - Application Login Page: - Guest Portal
Page Title	Click and enter 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 enter the text to appear as the header in the default landing page.
Bottom section	Click and enter the text to appear as the footer in the default landing page.
Copyright	Click and enter the copyright text to appear in the default landing page.

NOTE

Both the HTTP and HTTPS protocols are supported for ClearPass Portal redirection.

Managing Admin Users

This section describes the following topics:

- Changing the Administration Password
- Adding an Admin User
- Importing and Exporting Admin Users
- Setting Password Policy for Admin Users
- Disabling Admin User Accounts

Changing the Administration Password

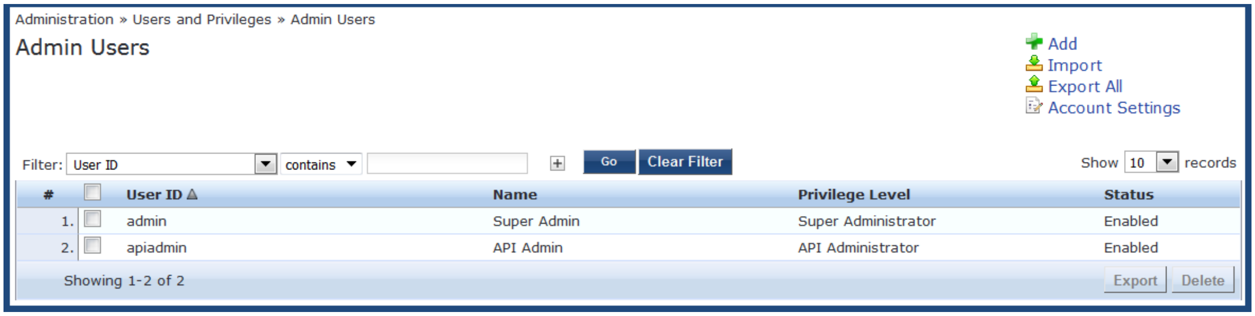
After activating the ClearPass appliance, the recommended next task is to change the administration password for the newly-activated ClearPass server.

To change the administration password:

1. Navigate to **Administration** > **Users and Privileges** > **Admin Users**.

   The **Admin Users** page opens.

Figure 461: *Admin Users Page*



#		User ID	Name	Privilege Level	Status
1.	□	admin	Super Admin	Super Administrator	Enabled
2.	□	apiadmin	API Admin	API Administrator	Enabled

Showing 1-2 of 2

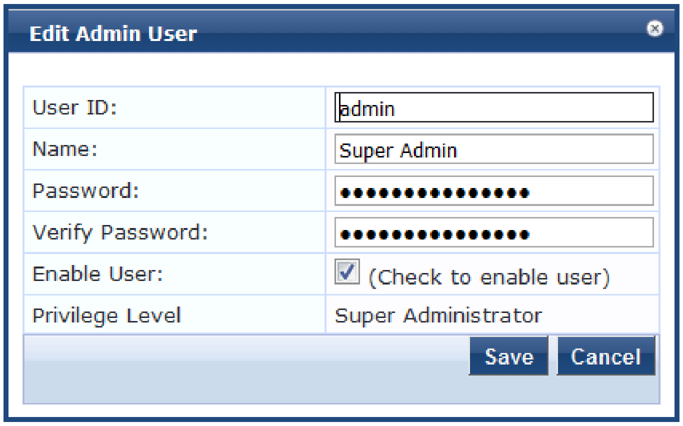
   In this page, you can view the administrator details such as user ID, user name, and privilege level.

   You can also change the admin password, and add, import, export, and set password policies for the admin users by using the links provided at the top-right corner of this page.

2. Select the Admin user you want to modify.

   The **Edit Admin User** dialog opens.

Figure 462: *Changing the Administration Password*



User ID:	admin
Name:	Super Admin
Password:	•••••••••••••••
Verify Password:	•••••••••••••••
Enable User:	☑ (Check to enable user)
Privilege Level	Super Administrator

3. Change the administration password, then click **Save**.

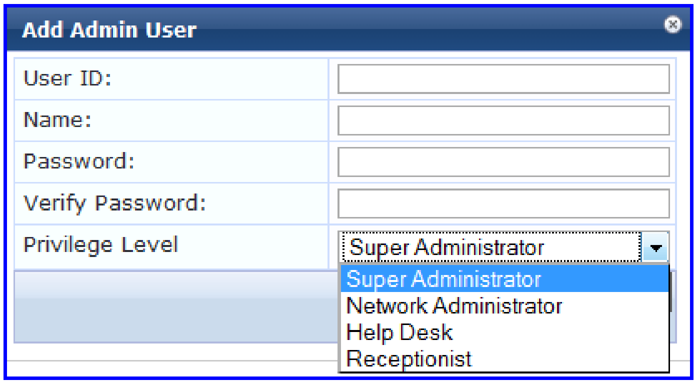
Adding an Admin User

To add a new admin user:

1. Navigate to **Administration > Users and Privileges > Admin Users**.
2. Click the **Add** link at the top-right corner the page.

   The **Add Admin User** dialog opens.

Figure 463: *Adding an Admin User*



Add Admin User

User ID:	
Name:	
Password:	
Verify Password:	
Privilege Level	Super Administrator

3. Specify the **Add Admin User** parameters as described in the following table, then click **Save**:

Table 256: *Adding an Admin User Parameters*

Parameter	Action/Description
User ID	1. Specify a user ID for this administrator.
Name	2. Specify the name for the admin user.
Password/ Verify Password	3. Specify a password for the local user, then verify the password.
Enable User	4. You must enable this check box to enable the admin user account (is is enabled by default). Otherwise, the admin user account is disabled.
Privilege Level	5. From the drop-down list, select one of the following admin user privilege levels: ■ API Administrator ■ Help Desk ■ Network Administrator ■ Read-only Administrator ■ Receptionist ■ Super Administrator

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, refer to Importing and Exporting Information on page 31.

NOTE

The passwords of the admin user accounts are not stored in clear text when exported to an XML file.

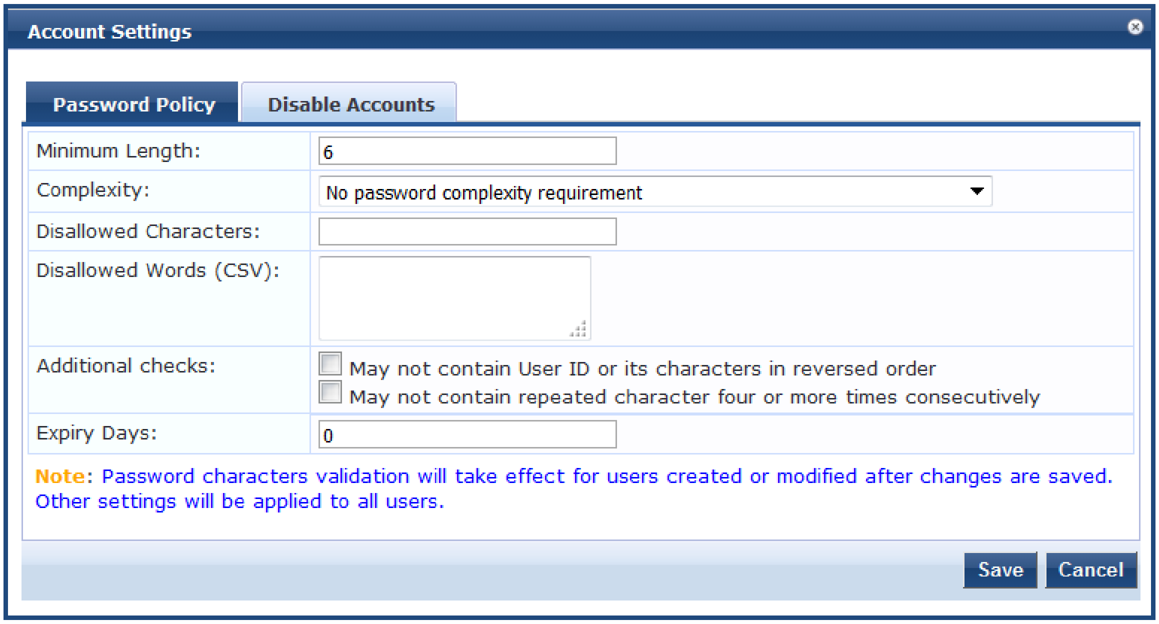
Setting Password Policy for Admin Users

To set password policies for the administrators:

1. Navigate to **Administration > Users and Privileges > Admin Users**.
2. Click the **Account Settings** link at the top-right corner of the **Admin Users** page.

   The **Password Policy Settings** dialog opens.

Figure 464: *Admin Users > Setting Password Policy*



Minimum Length:	6
Complexity:	No password complexity requirement
Disallowed Characters:	
Disallowed Words (CSV):	
Additional checks:	□ May not contain User ID or its characters in reversed order □ May not contain repeated character four or more times consecutively
Expiry Days:	0

Note: Password characters validation will take effect for users created or modified after changes are saved. Other settings will be applied to all users.

3. Specify the **Password Policy** parameters as described in Table 257, then click **Save**:

Table 257: *Password Policy Parameters*

Parameter	Action/Description
Minimum Length	1. Specify the minimum length required for the password.
Complexity	2. 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
Disallowed Characters	3. Specify the characters not to be allowed in the password.

Table 257: *Password Policy Parameters (Continued)*

Parameter	Action/Description
Disallowed Words (CSV)	4. Specify the words not to be allowed in the password
Additional Checks	5. 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.
Expiry Days	6. Set the password expiry time for the local users. The allowed range is **0** to **500** days. The default value is **0**. **NOTE:** If the value is set to **0**, the password never expires. For any other value, local users are forced to reset the expired password when they log in. ClearPass alerts users five days before the password expires.

NOTE

Password Policy settings are effective only for the users created or modified after the changes are saved.

Disabling Admin User Accounts

The Admin user account can be disabled in two ways:

- When the Admin user tries to log in with an invalid password for a configured number of times defined by the **Failed attempts count** parameter, the Admin user account is locked.

NOTE

If the mechanism for logging in to ClearPass Policy Manager is Certificate + Password, the Admin user is allowed to enter the password even if the certificate is invalid.

- When the Admin user tries to log in with an invalid user certificate for a configured number of times defined by the **Failed attempts count** parameter, the Admin user account is disabled.
- To reset the **Failed attempts count** and enable a disabled Admin user account, click the **Reset** button (see Table 258).
- For Admin users whose accounts are locked due to account settings validations, and whose accounts are enabled again after being locked out, entries are logged in both the Audit Viewer (see Audit Viewer on page 148) and the Event Viewer (see Event Viewer on page 150).

The **Disable Account** check occurs every day at midnight.

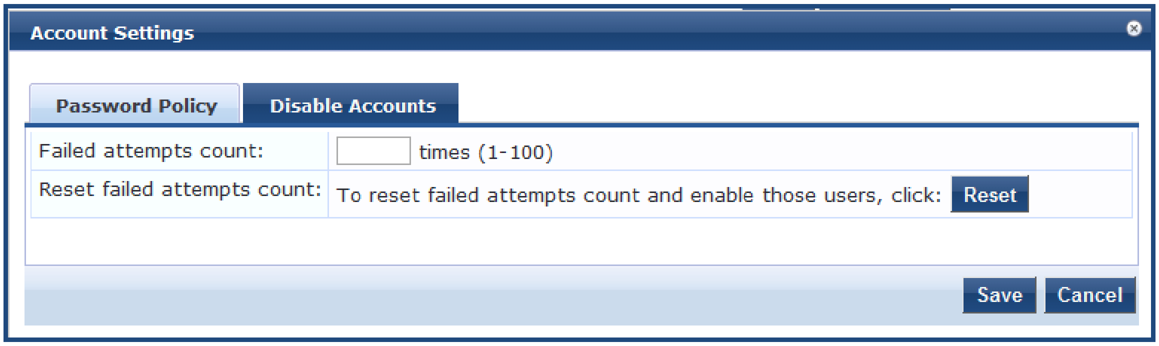
To specify the conditions for disabling admin user accounts:

1. Navigate to **Administration > Users and Privileges > Admin Users**.
2. Click the **Account Settings** link at the top-right corner of the **Admin Users** page.

   The **Account Settings** page opens.
3. Select the **Disable Accounts** tab.

   The **Disable Accounts** dialog opens.

Figure 465: *Admin Users > Disable Accounts Dialog*



Failed attempts count: times (1-100)

Reset failed attempts count: To reset failed attempts count and enable those users, click: Reset

4. Specify the **Disable Accounts** parameters as described in Table 258, then click **Save**.

Table 258: *Admin Users > Disable Accounts Parameters*

Parameter	Action/Description
Failed attempts count	1. Specify the number of failed log-in attempts are allowed before the account is disabled. The range is from **1** to **100** attempts.
Reset failed attempts count	2. To reset the failed attempts count to zero and reenable those admin users who were disabled after exceeding the failed attempts count, click **Reset**.

Managing Admin Privileges

This section provides the following information:

- Overview
- Defining Custom Admin Privileges
- Creating Custom Administrator Privileges on page 472
- Administrator Privilege XML File Structure on page 472
- Administrator Privileges and Task IDs on page 473
- Sample Administrator Privilege XML File on page 476

Overview

ClearPass Policy Manager ships with the following default administrator admin privileges XML files:

- API Administrator
- Help Desk
- Network Administrator
- Read-only Administrator
- Receptionist
- Super Administrator

Each of these default admin privileges administrators, define the admin privileges for Policy Manager and for Insight. The default set of admin privileges cannot be modified.

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 ClearPass Policy Manager on the **Admin Privileges** page.

Defining Custom Admin Privileges

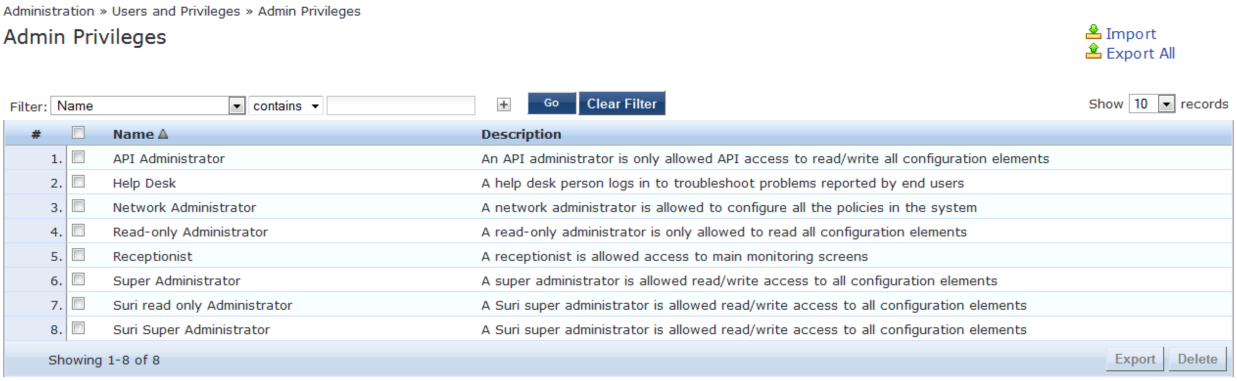
When a different set of admin privileges is needed (for example, if you require different admin privileges for the Report module than the admin privileges defined for the other Insight modules), you must create a new admin privileges administrator.

To define custom admin privileges for ClearPass and Insight:

1. Navigate to the **Administration > Users and Privileges > Admin Privileges** page.

   The **Admin Privileges** page opens:

Figure 466: *Admin Privileges Page*



Administration » Users and Privileges » Admin Privileges

Admin Privileges

Filter: Name contains

Show 10 records

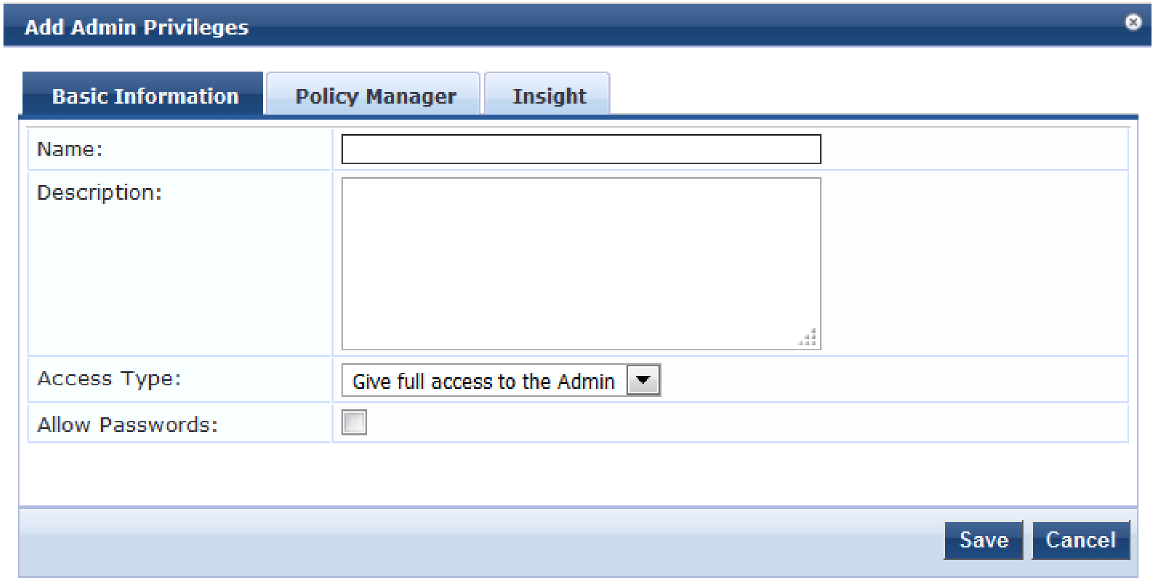
#		Name	Description
1.	□	API Administrator	An API administrator is only allowed API access to read/write all configuration elements
2.	□	Help Desk	A help desk person logs in to troubleshoot problems reported by end users
3.	□	Network Administrator	A network administrator is allowed to configure all the policies in the system
4.	□	Read-only Administrator	A read-only administrator is only allowed to read all configuration elements
5.	□	Receptionist	A receptionist is allowed access to main monitoring screens
6.	□	Super Administrator	A super administrator is allowed read/write access to all configuration elements
7.	□	Suri read only Administrator	A Suri super administrator is allowed read/write access to all configuration elements
8.	□	Suri Super Administrator	A Suri super administrator is allowed read/write access to all configuration elements

Showing 1-8 of 8

2. Click the **Add** link.

   The **Add Admin Privileges** dialog opens.

Figure 467: *Add Admin Privileges Page: Basic Information Tab*



Add Admin Privileges

Name:	
Description:	
Access Type:	Give full access to the Admin
Allow Passwords:	□

3. Specify the parameters in the **Basic Information** tab as described in Table 259.

Table 259: *Add Admin Privileges Parameters: Basic Information Tab*

Parameter	Action/Description
Name	1. Enter the name of the Admin Privileges administrator.
Description	2. Provide a description of this new admin privileges administrator.
Access Type	3. Select one of the following Access Types: ■ Give full access to the Admin ■ Give UI access to the Admin ■ Give API access to the Admin
Allow Passwords	4. Select this check box if you want to allow password access.

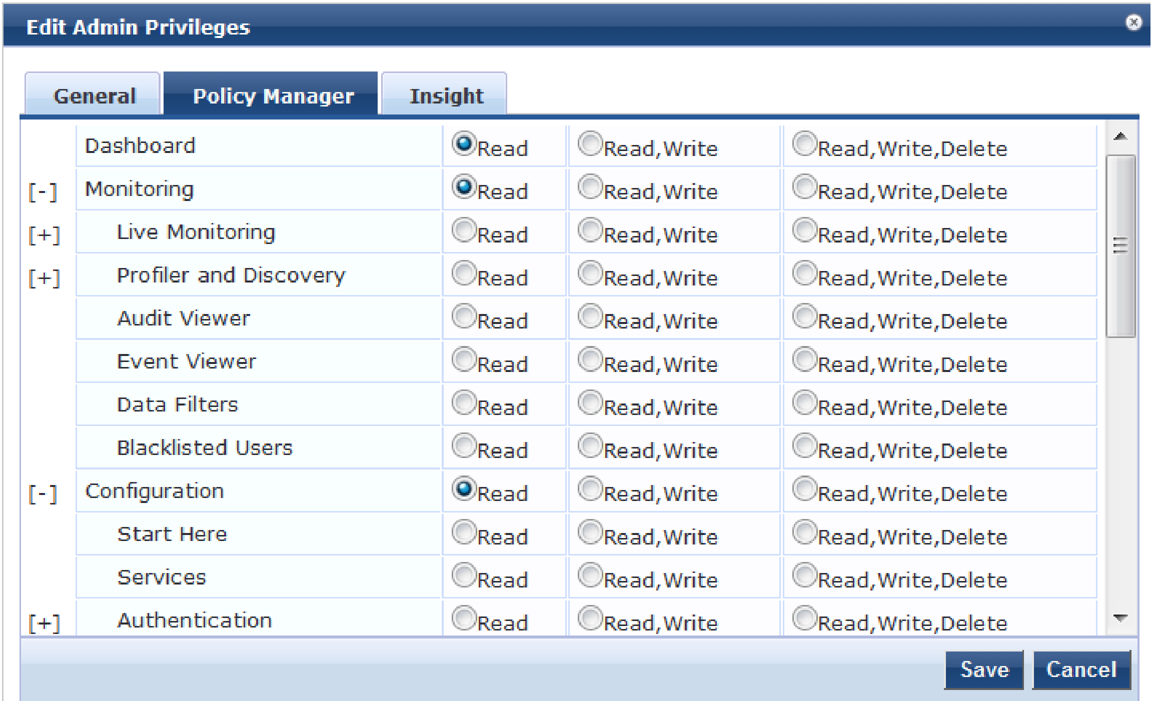
Configuring Policy Manager Admin Privileges

To configure the Policy Manager admin privileges:

1. Select the **Policy Manager** tab.

   The following dialog opens:

Figure 468: *Specifying Policy Manager Admin Privileges*



	Dashboard	● Read	○ Read,Write	○ Read,Write,Delete
[-]	Monitoring	● Read	○ Read,Write	○ Read,Write,Delete
[+]	Live Monitoring	○ Read	○ Read,Write	○ Read,Write,Delete
[+]	Profiler and Discovery	○ Read	○ Read,Write	○ Read,Write,Delete
	Audit Viewer	○ Read	○ Read,Write	○ Read,Write,Delete
	Event Viewer	○ Read	○ Read,Write	○ Read,Write,Delete
	Data Filters	○ Read	○ Read,Write	○ Read,Write,Delete
	Blacklisted Users	○ Read	○ Read,Write	○ Read,Write,Delete
[-]	Configuration	● Read	○ Read,Write	○ Read,Write,Delete
	Start Here	○ Read	○ Read,Write	○ Read,Write,Delete
	Services	○ Read	○ Read,Write	○ Read,Write,Delete
[+]	Authentication	○ Read	○ Read,Write	○ Read,Write,Delete

2. Specify the admin privileges for each of the ClearPass components, then click **Save**.

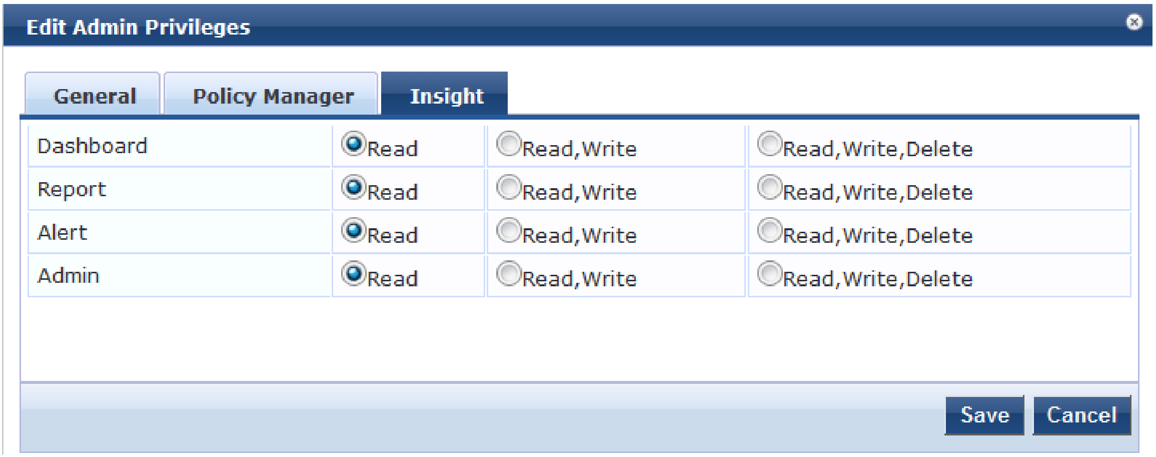
Configuring Insight Admin Privileges

To configure the Insight admin privileges:

1. Select the **Insight** tab.

   The following dialog opens:

Figure 469: *Specifying Insight Admin Privileges*



Dashboard	● Read	○ Read,Write	○ Read,Write,Delete
Report	● Read	○ Read,Write	○ Read,Write,Delete
Alert	● Read	○ Read,Write	○ Read,Write,Delete
Admin	● Read	○ Read,Write	○ Read,Write,Delete

2. Specify the admin privileges for each of the Insight modules, then click **Save**.

Creating Custom Administrator Privileges

To create a custom admin privilege XML file, you must use a plain text or XML editor.

CAUTION

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.

After you complete steps 1 through 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 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 Task IDs

Every element in the ClearPass Policy Manager user interface 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 (read-write) permissions for the task, *Enforcements* (con.en), it is automatically applied to its subtasks, *Policies* (con.en.epo) and *Profiles* (con.en.epr). Hence, you need not explicitly define the same permission for those subtasks.

The following table provides the tasks and subtasks of ClearPass Policy Manager and their associated task IDs:

Table 260: *Administrator Privileges and Task IDs*

Area (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
■ System Monitor	mon.li.sy
● Audit Viewer	mon.av
● Blacklisted Users	mon.bl

Table 260: *Administrator Privileges and Task IDs (Continued)*

Area (ClearPass Policy Manager Menu)	Task ID
● 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
■ Profiles	con.en.epr
● Network	con.nw
■ Devices	con.nw.nd

Table 260: *Administrator Privileges and Task IDs (Continued)*

Area (ClearPass Policy Manager Menu)	Task ID
■ 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
■ Server Certificate	adm.cm.mc
■ Trust List	adm.cm.ctl
■ Revocation List	adm.cm.crl

Table 260: *Administrator Privileges and Task IDs (Continued)*

Area (ClearPass Policy Manager Menu)	Task ID
● 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

Sample Administrator Privilege XML File

This section provides sample XML files with different admin privileges for various user interface elements:

- Read Only (R) Privileges to All Sections
- Read/Write Access
- Read/Write Permissions

Read Only (R) Privileges to All Sections

The following sample provides Read Only (R) privileges 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 2016" version="6.6"/>
 <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="R"/>
   </AdminTask>
   <AdminTask taskid="dnd"> //Refers to DashBoard
    <AdminTaskAction type="R"/>
   </AdminTask>
   <AdminTask taskid="mon"> //Refers to Monitoring
    <AdminTaskAction type="R"/>
   </AdminTask>
```

```
      <AdminTask taskid="adm"> //Refers to Administration
        <AdminTaskAction type="R"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

Read/Write Access

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 2016" version="6.6"/>
  <AdminPrivileges>
    <AdminPrivilege name="Read/Write Access to Guest, Local and Endpoint Repository" description="A read-only
administrator is only allowed to read all configuration elements">
      <AdminTask taskid="con.id.lu"> //Refers to Local Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.gu"> //Refers to Guest Users Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
      <AdminTask taskid="con.id.ep"> //Refers to Endpoints Section
        <AdminTaskAction type="RW"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

Read/Write Permissions

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 2016" version="6.6"/>
  <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="R"/>
      </AdminTask>
    </AdminPrivilege>
  </AdminPrivileges>
</TipsContents>
```

Server Configuration

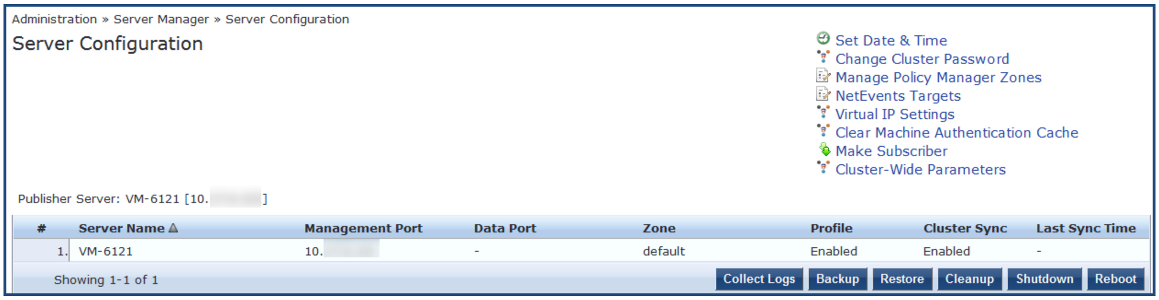
This section describes the following server configuration tasks:

- Editing Server Configuration Settings on page 478
- Configuration Tasks for Disabled Nodes in a Cluster on page 479
- Setting the Date and Time for the Cluster on page 520

- Changing the Cluster-Wide Password on page 521
- Managing Policy Manager Zones on page 522
- Configuring NetEvents Targets on page 524
- Configuring Virtual IP Settings on page 526
- Clearing Machine Authentication Cache on page 526
- Cluster-Wide Parameters on page 528
- Making a Subscriber Node on page 527
- Collecting Logs on page 543
- Backing Up the Policy Manager Database on page 545
- Restoring Policy Manager Configuration Data on page 545
- Performing a System Cleanup on page 547
- Shutting Down or Rebooting the Server on page 548
- Dropping a Subscriber Node on page 548

You can perform numerous server configuration tasks by navigating to **Administration > Server Manager > Server Configuration** page in ClearPass Policy Manager.

Figure 470: *Server Configuration Page*



Publisher Server: VM-6121 [10.[redacted]]

#	Server Name ∆	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	VM-6121	10.[redacted]	-	default	Enabled	Enabled	-

Showing 1-1 of 1

Editing Server Configuration Settings

This section provides the following information:

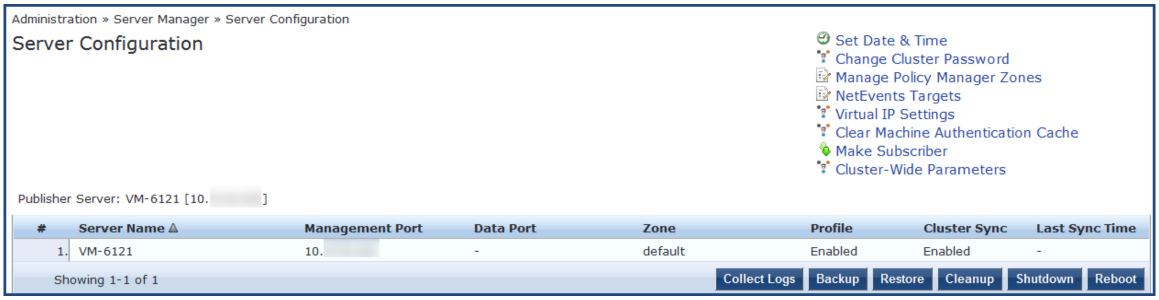
- Cluster-Related Options
- Modifying ClearPass Server Settings
- Configuration Tasks for Disabled Nodes in a Cluster

To modify the configuration settings of a ClearPass server:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.

   The **Server Configuration** page opens.

Figure 471: *Server Configuration Page*



Administration » Server Manager » Server Configuration

Server Configuration

- Set Date & Time
- Change Cluster Password
- Manage Policy Manager Zones
- NetEvents Targets
- Virtual IP Settings
- Clear Machine Authentication Cache
- Make Subscriber
- Cluster-Wide Parameters

Publisher Server: VM-6121 [10.[redacted]]

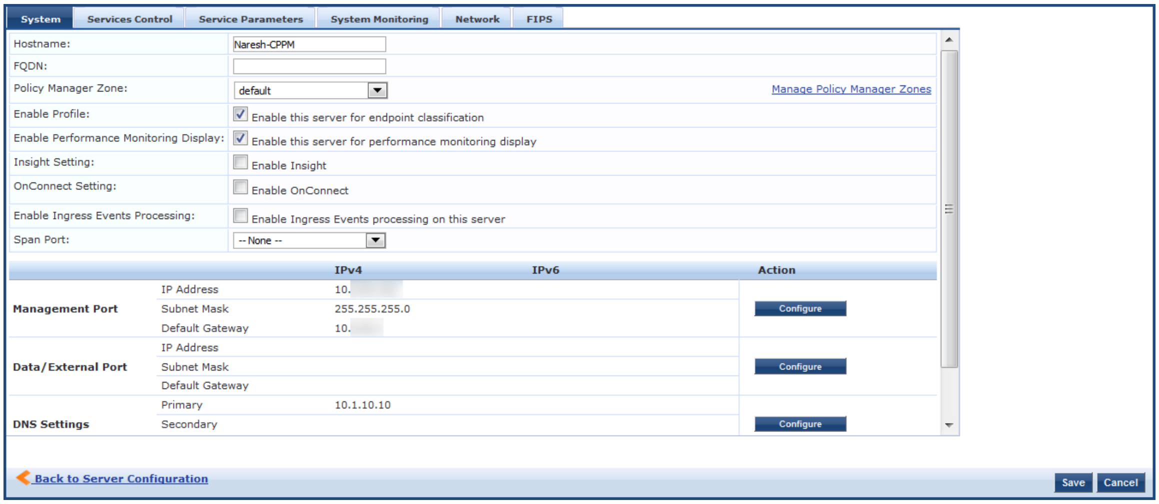
#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	VM-6121	10.[redacted]	-	default	Enabled	Enabled	-

Showing 1-1 of 1

2. Click the ClearPass server name of interest.

   The **Server Configuration** page for the selected server opens:

Figure 472: *Server Configuration Page for the Selected Server*



Hostname:	Naresh-CPPM
FQDN:	
Policy Manager Zone:	default ▾ Manage Policy Manager Zones
Enable Profile:	☑ Enable this server for endpoint classification
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	□ Enable Insight
OnConnect Setting:	□ Enable OnConnect
Enable Ingress Events Processing:	□ Enable Ingress Events processing on this server
Span Port:	-- None -- ▾

		IPv4	IPv6	Action
Management Port	IP Address	10.[redacted]		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	10.[redacted]		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
DNS Settings	Primary	10.1.10.10		Configure
	Secondary			

Cluster-Related Options

For details on the cluster-related options, see Server Configuration Cluster Options on page 520.

Modifying ClearPass Server Settings

For details on modifying ClearPass server settings, refer to the following sections:

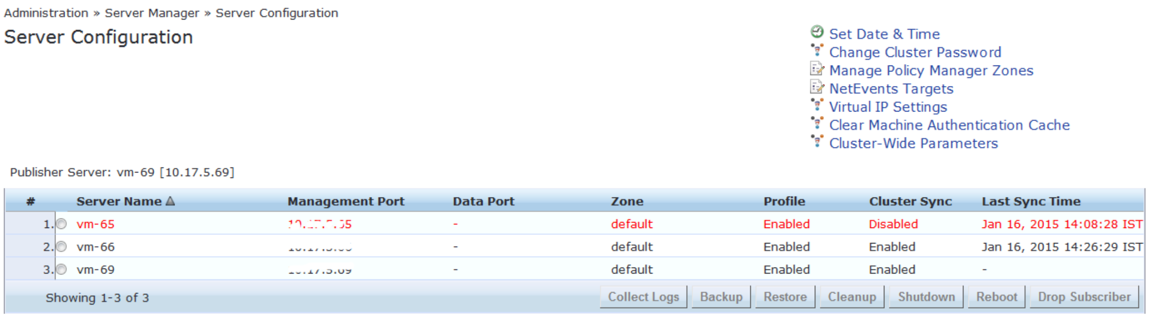
- System Page on page 482
- Services Control Page on page 490
- Service Parameters Page on page 490
- System Monitoring Page on page 506
- Network Page on page 508
- FIPS Page on page 517

Configuration Tasks for Disabled Nodes in a Cluster

You can perform the following configuration tasks only for disabled nodes in a cluster:

- Synchronizing the Cluster Password
- Promoting a ClearPass Subscriber Node to Publisher
- Joining a ClearPass Server Back to the Cluster

Figure 473: *Server Configuration Page with Disabled Nodes*



Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: vm-69 [10.17.5.69]

#	Server Name	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1. ○	vm-65	[redacted]	-	default	Enabled	Disabled	Jan 16, 2015 14:08:28 IST
2. ○	vm-66	[redacted]	-	default	Enabled	Enabled	Jan 16, 2015 14:26:29 IST
3. ○	vm-69	[redacted]	-	default	Enabled	Enabled	-

Showing 1-3 of 3

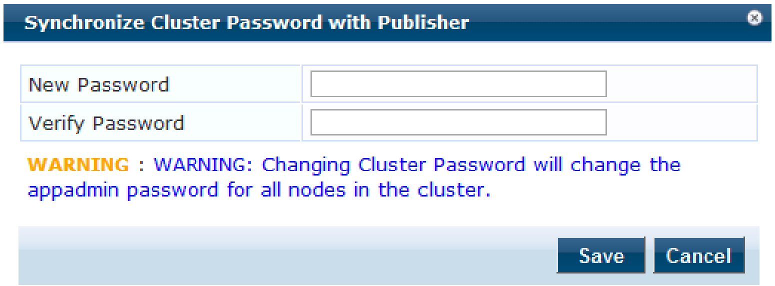
For more information on the **Service Configuration**, see Server Configuration on page 477.

Synchronizing the 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** dialog:

Figure 474: *Synchronize Cluster Password with Publisher Dialog*



Synchronize Cluster Password with Publisher

New Password	
Verify Password	

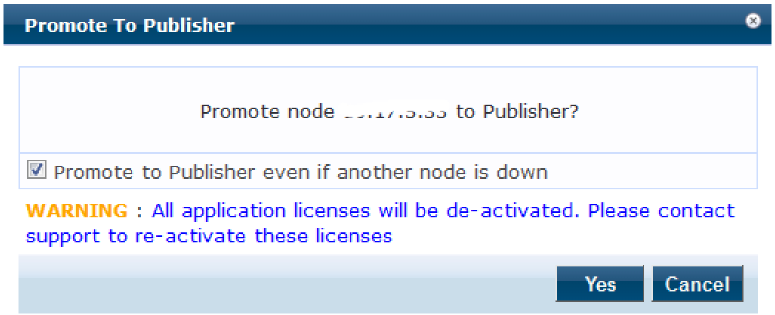
WARNING : WARNING: Changing Cluster Password will change the appadmin password for all nodes in the cluster.

Promoting a ClearPass Subscriber Node 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 that is part of the same cluster.

All application licenses will be deactivated; you need to contact Aruba Support to reactivate these licenses. The following figure displays the **Promote to Publisher** window:

Figure 475: *Promote Node to Publisher*



Promote To Publisher

Promote node [redacted] to Publisher?

☑ Promote to Publisher even if another node is down

WARNING : All application licenses will be de-activated. Please contact support to re-activate these licenses

Joining a ClearPass Server Back to the Cluster

Use the **Join server back to cluster** link to join a ClearPass server back to the cluster.

You can use this option only for a server that is in the **Cluster Sync** > **Disabled** state.

NOTE

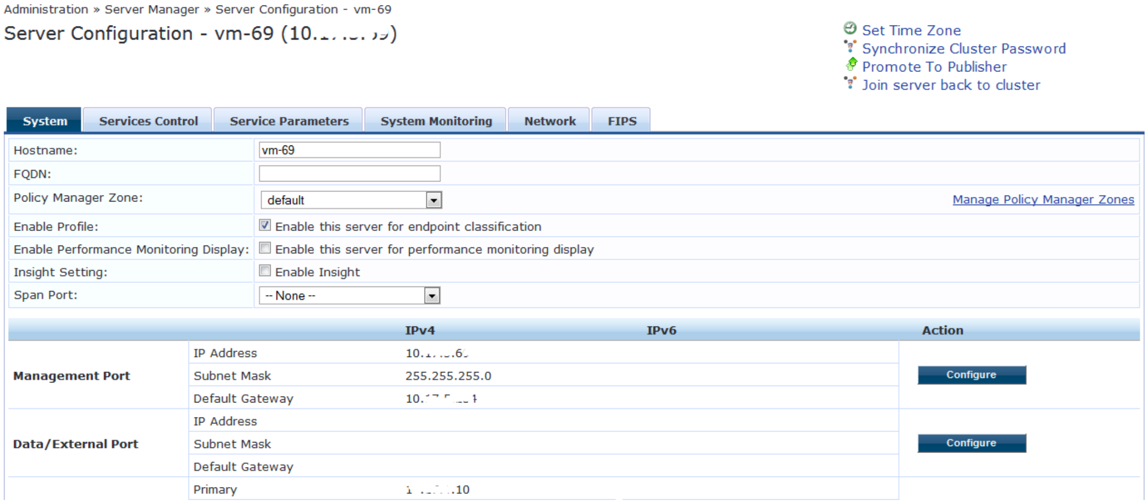
Only users with Admin access can join a ClearPass node back to a cluster.

To join a server back to the cluster:

1. Select a subscriber node that is in **Disabled** state.

   The **Server Configuration > System** tab opens.

Figure 476: *Server Configuration > Join Server Back to Cluster Link*


Administration » Server Manager » Server Configuration - vm-69
Set Time Zone
Synchronize Cluster Password
Promote To Publisher
Join server back to cluster
System
Services Control
Service Parameters
System Monitoring
Network
FIPS
Manage Policy Manager Zones
Configure
Configure

Server Configuration - vm-69 (10.[redacted])

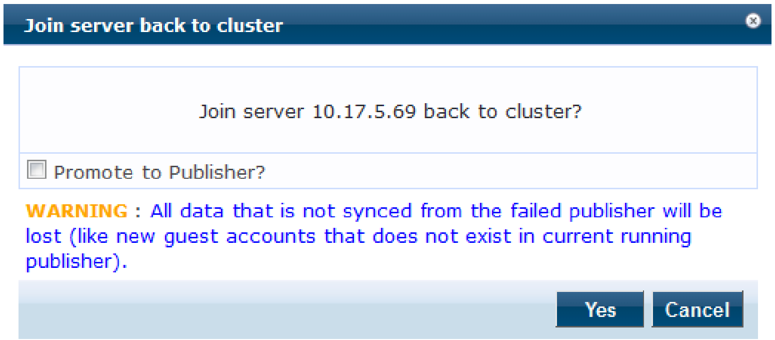
Hostname:	vm-69
FQDN:	
Policy Manager Zone:	default
Enable Profile:	☑ Enable this server for endpoint classification
Enable Performance Monitoring Display:	□ Enable this server for performance monitoring display
Insight Setting:	□ Enable Insight
Span Port:	-- None --

		IPv4	IPv6	Action
Management Port	IP Address	10.[redacted]		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	10.[redacted]		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
	Primary	[redacted].10		

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 477: *Join Server Back to Cluster Confirmation Dialog*



Join server back to cluster

Join server 10.17.5.69 back to cluster?

□ Promote to Publisher?

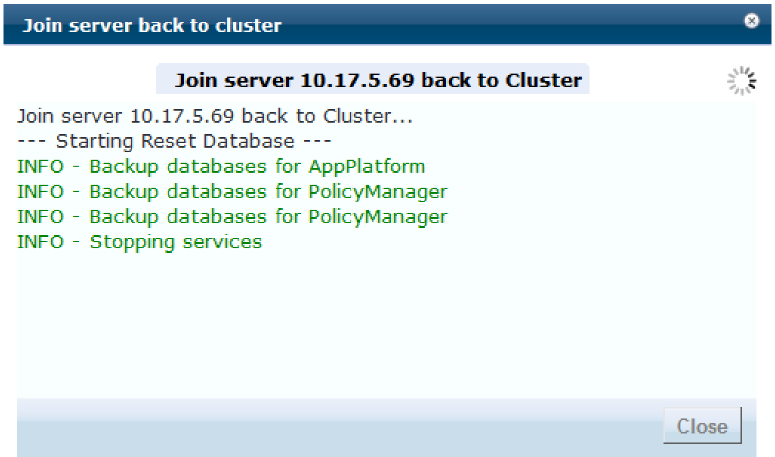
WARNING : All data that is not synced from the failed publisher will be lost (like new guest accounts that does not exist in current running publisher).

3. Click **Yes**.

   A progress indicator shows the progress of the operation.

The following figure displays the Join server back to cluster progress indicator:

Figure 478: *Join Server Back to Cluster Progress Window*



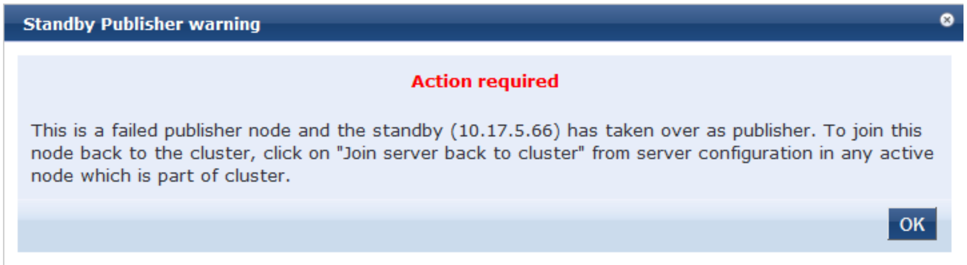
Join server back to cluster

Join server 10.17.5.69 back to Cluster

```
Join server 10.17.5.69 back to Cluster...
--- Starting Reset Database ---
INFO - Backup databases for AppPlatform
INFO - Backup databases for PolicyManager
INFO - Backup databases for PolicyManager
INFO - Stopping services
```

4. For a failed Publisher node, the following message will be displayed in the **Dashboard** page:

Figure 479: *Publisher Warning Message*



Standby Publisher warning

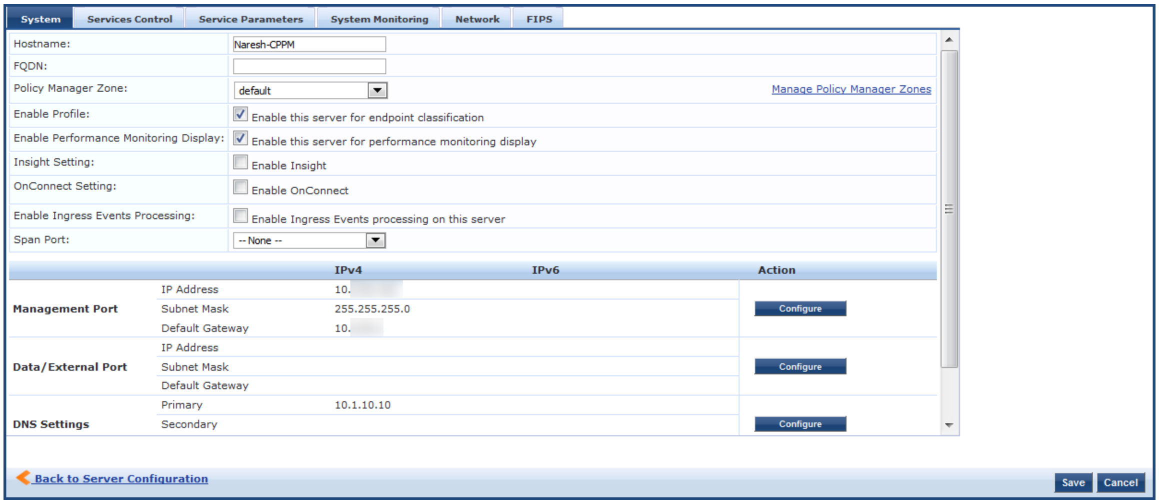
Action required

This is a failed publisher node and the standby (10.17.5.66) has taken over as publisher. To join this node back to the cluster, click on "Join server back to cluster" from server configuration in any active node which is part of cluster.

System Page

The **Server Configuration** page opens onto the **System** page (see Figure 480).

Figure 480: *Server Configuration > System Page*



Hostname:	Naresh-CPPM
FQDN:	
Policy Manager Zone:	default
Enable Profile:	☑ Enable this server for endpoint classification
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	□ Enable Insight
OnConnect Setting:	□ Enable OnConnect
Enable Ingress Events Processing:	□ Enable Ingress Events processing on this server
Span Port:	-- None --

		IPv4	IPv6	Action
Management Port	IP Address	10.		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	10.		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
DNS Settings	Primary	10.1.10.10		Configure
	Secondary			

1. Specify the **Server Configuration** > **System** page parameters as described in the following table, then click **Save**:

Table 261: *Server Configuration > System Page Parameters*

Parameter	Action/Description
Hostname	1. Specify the host name of the Policy Manager server. **NOTE:** You do not need to enter the fully qualified domain name in this field.
FQDN	2. Enter the Fully-Qualified Domain Name (FQDN) of the Policy Manager server.
Policy Manager Zone	3. To add or delete zones, select a previously configured zone from the drop-down list, then click the **Manage Policy Manager Zones** link. For more information on adding or deleting zones, see Adding Policy Manager Zones.
Enable Profile	4. To enable the Policy Manager server to perform endpoint classifications, select the **Enable Profile** check box.
Enable Performance Monitoring	5. To enable the ClearPass Policy Manager server to perform performance monitoring, select the **Enable Performance Monitoring** check box.
Insight Setting	6. To enable the Insight reporting tool on this node, select the **Enable Insight** check box. **NOTE:** ● When you enable this check box for Insight on a node in a cluster, the [Insight Repository] configuration is updated automatically to point to the management IP address 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 the same order in which the user enables Insight on the server.
OnConnect Setting	7. To enable the OnConnect Enforcement on this node, select the **Enable OnConnect** check box. When you enable **OnConnect**, a drop-down box appears that allows you to specify whether the selected server is the **Primary** or **Secondary master** for agentless OnConnect Enforcement in its zone. **NOTE:** When you enable the Enable OnConnect check box, you must specify the current ClearPass server as a Primary or Secondary Master for OnConnect Enforcement. 8. From the drop-down list, select **Primary master** or **Secondary master**. The first server that is enabled for OnConnect Enforcement in a zone is automatically designated as the Primary master for that zone. After other servers in the zone are enabled for OnConnect Enforcement, if the Primary master fails, the designated Secondary master takes over until the Primary master is back on-line. For information on creating an OnConnect Enforcement service, see ClearPass OnConnect Enforcement Service on page 87. **NOTE:** In order for OnConnect Enforcement to be fully functional, OnConnect must be enabled both the ClearPass server and on any network devices that you wish to use for OnConnnect Enforcement (see Enabling ClearPass OnConnect Enforcement on a Network Device on page 454). **NOTE:** During OnConnect, the domain name and machine name are fetched, along with the logged-in user name. The domain name can be used as an attribute for enforcement policies.

Table 261: *Server Configuration > System Page Parameters (Continued)*

Parameter	Action/Description
Enable Ingress Events Processing	9. Check this check box to enable ingress events processing on this server. For more information, see Configuring Processing for Ingress Events.
Enable as Insight Master	10. To specify the current server in a cluster as an Insight Master, select this check box. **NOTE:** This option is available only when **Insight Setting** > **Enable Insight** is enabled.
Span Port	11. If necessary, select a port for DHCP spanning. On selecting a port, the **Enable TCP/ARP Fingerprinting** check box appears. This field is optional.
Enable TCP/ARP Fingerprinting	12. To enable TCP/ARP fingerprinting, select the Enable **TCP/ARP Fingerprinting** check box. 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 specify a **Span Port**.
Management Port	13. To configure the Management Port parameters, click **Configure.** The **Configure Management Port** dialog opens. For details, see Management Port Configuration on page 484.
Data/External Port	14. To configure the Data/External port, click **Configure.** For details, see Data/External Port Configuration on page 485.
DNS Settings	15. To configure the DNS settings, click **Configure**. For details, see DNS Settings Configuration on page 485.
AD Domains	Displays a list of the joined Active Directory domains. 16. To join an active directory domain, click **Join Domain**. For details on joining an AD domain, see Join AD Domain Configuration on page 486.

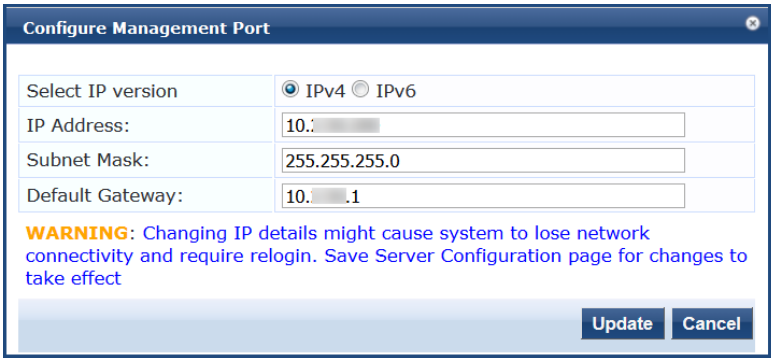
Management Port Configuration

To configure the ClearPass server's Management port:

1. From the **Administration** > **Server Manager** > **Server Configuration** > **System** > **Management Port** section, click **Configure**.

   The **Configure Management Port** dialog opens.

Figure 481: *Configure Management Port Dialog*



Configure Management Port

Select IP version	● IPv4 ○ IPv6
IP Address:	10.[redacted]
Subnet Mask:	255.255.255.0
Default Gateway:	10.[redacted].1

WARNING: Changing IP details might cause system to lose network connectivity and require relogin. Save Server Configuration page for changes to take effect

2. **Select IP Version**: Select the IP version—**IPv4** or **IPv6**.
3. **IP Address**: Specify the IP address (IPv4 or IPv6) to access the ClearPass Policy Manager.
4. **Subnet Mask**: Specify the management interface subnet mask for an IPv4 address.

   IPv6 addresses do not require a netmask as they use Classless Inter-Domain Routing (CIDR).
5. **Default Gateway**: Specify the default gateway for the management interface.
6. Click **Update**.

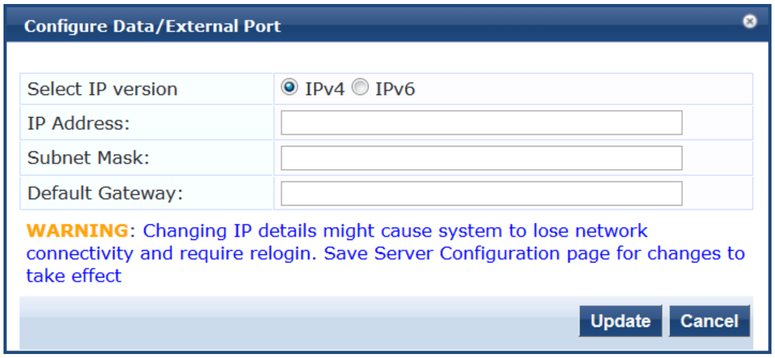
Data/External Port Configuration

To configure the ClearPass server's Data/External port:

1. From the **Server Configuration** > **System** > **Data/External Port** section, click **Configure**.

   The **Configure Data/External Port** dialog opens.

Figure 482: *Configure Data/External Port Dialog*



Configure Data/External Port

Select IP version	● IPv4 ○ IPv6
IP Address:	
Subnet Mask:	
Default Gateway:	

WARNING: Changing IP details might cause system to lose network connectivity and require relogin. Save Server Configuration page for changes to take effect

2. **Select IP Version**: Select the IP version—**IPv4** or **IPv6**.
3. **IP Address**: Specify the IP address (IPv4 or IPv6) of the ClearPass server's data interface.
4. **Subnet Mask**: Specify the data interface subnet mask for an IPv4 address.

   IPv6 addresses do not require a netmask as they use Classless Inter-Domain Routing (CIDR).
5. **Default Gateway**: Specify the default gateway for the data interface.
6. Click **Update**.

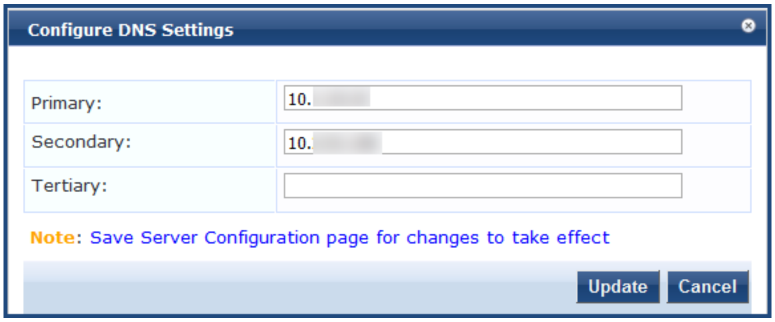
DNS Settings Configuration

To configure the ClearPass server's Data/External port:

1. From the **Server Configuration** page > **System** tab > **DNS Settings**, click **Configure**.

   The **Configure DNS Setting** dialog opens.

Figure 483: *Configure DNS Settings Dialog*



Configure DNS Settings

Primary:	10.[redacted]
Secondary:	10.[redacted]
Tertiary:	

Note: Save Server Configuration page for changes to take effect

2. **Primary**: Specify the primary DNS server for name look-up.

NOTE

A DNS server can be primary for one domain and secondary for another. Only one DNS server should be configured as primary for a domain, but you can have any number of secondary DNS servers.

3. **Secondary**: Specify one or more secondary DNS servers for name look-up.

NOTE

The recommended practice is to configure the primary and secondary DNS servers on separate machines, on separate Internet connections, and in separate geographic locations.

4. **Tertiary**: Optionally, in the rare event of both the primary and secondary DNS servers going down, you can configure a tertiary DNS server.
5. Click **Update**.

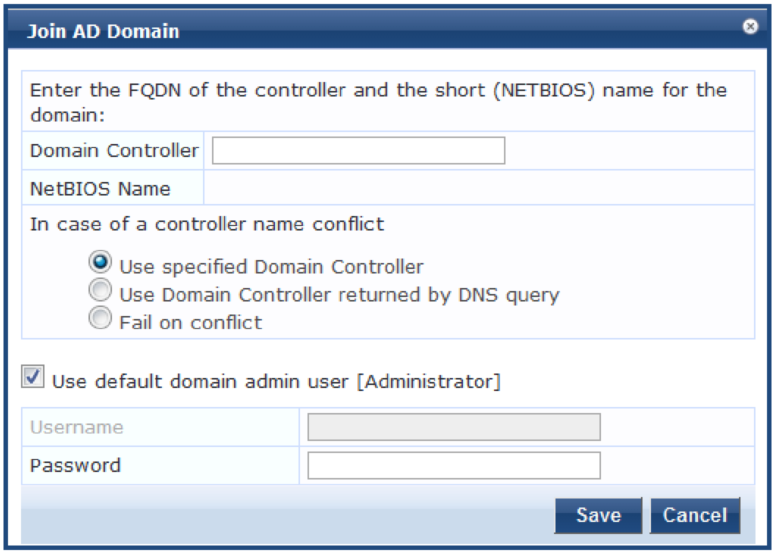
Join AD Domain Configuration

To join the selected ClearPass server to an Active Directory domain:

1. From the **Server Configuration** page > **System** tab > **AD Domains**, click **Join AD Domain**.

   The **Join AD Domain** dialog opens.

Figure 484: *Join AD Domain Dialog*



Join AD Domain

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller	
NetBIOS Name	

In case of a controller name conflict

● Use specified Domain Controller
○ Use Domain Controller returned by DNS query
○ Fail on conflict

☑ Use default domain admin user [Administrator]

Username	
Password	

2. **Domain Controller**: Enter the Fully Qualified Domain Name (FQDN) of the domain controller, then press **Tab**.

   The following message is displayed: *Trying to determine the NetBIOS name...*

   ClearPass searches for the NetBIOS name for the domain.

NOTE

NetBIOS is another term for the short domain name, or the NT4 domain name, also known as the pre-Windows 2000 domain name.

If ClearPass determines the NetBIOS name, the **NetBIOS Name** field is automatically populated.

3. **In case of a controller name conflict**:

   a. **Use specified Domain Controller**: Accept the default setting.

   b. **Use default domain admin user [Administrator]**: Accept the default setting.

NOTE

In a production environment, it is likely that an Administrative username that has permissions to join machines to the domain would be used for the default domain admin user. In that case, 1) disable (that is, uncheck) the **Use default domain admin user [Administrator]** check box and 2) enter the Administrative username and password in the fields provided.

   c. **Password**: Enter the password for the user account that will join ClearPass with the domain, then click **Save**.

   Table 262 displays the characters that are allowed and not allowed for the Active Directory username and passoword:

Table 262: *Characters Allowed and Not Allowed for Active Directory Username and Password*

Field	Characters Allowed	Not Allowed
Username	~ ! @ # $ % ^ * _ - + = { } , . \ ' " ? /	` & ( )
Password	! @ # $ % ^ & * ( ) _ - + = { } < , > . ? /	~ ` [ ] \ | ; : ' "

   The **Join AD Domain** status screen opens. The screen displays the message "*Adding host to AD domain*," and the screen displays status during the joining process.

   When the joining process completes successfully, you see the message "*Added host to the domain*."

4. Click **Close**.

   You return to the **Server Configuration** page, and it now shows that the ClearPass server is joined to the domain.

   Now that the ClearPass Policy Manager server has joined the domain, the server can authenticate users with Active Directory.

   After an Active Directory Domain is added, the domain controller can be setup as a password server. For more information on adding a password server, see Adding a Password Server on page 489.

Join AD Domain

You can join ClearPass Policy Manager to an Active Directory (AD) domain to authenticate users and computers that are members of an Active Directory domain. If you join ClearPass to an Active Directory domain, it creates an account for the ClearPass node in the Active Directory database.

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

If you need to authenticate users belonging to multiple Active Directory forests or domains in your network, and there is no trust relationship between these entities, then you must join ClearPass to each of these untrusted forests or domains.

NOTE

ClearPass does not require to join multiple domains belonging to the same Active Directory forest because a one-way trust relationship exists between those domains. In this case, ClearPass can join the root domain.

ClearPass can join or leave an Active Directory domain by using the following two buttons in the **Server Configuration** page > **System** tab:

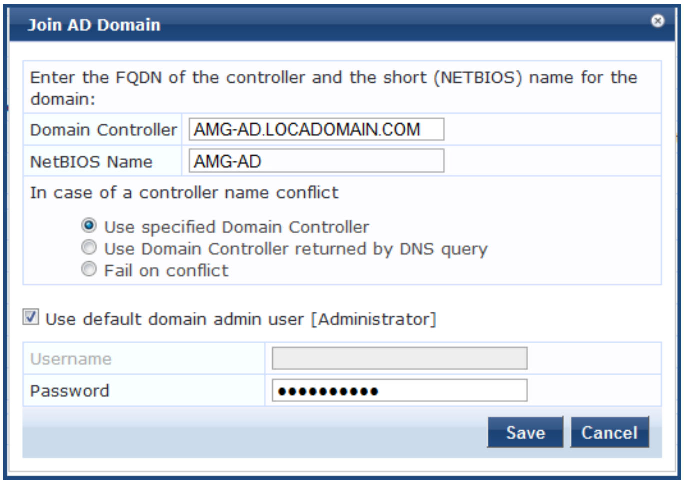
- **Join Domain**: Click **Join Domain** to join this ClearPass appliance to an Active Directory domain. Password servers can be configured after Policy Manager is successfully joined. For more information on adding a password server, see Adding a Password Server on page 489.
- **Leave Domain**: If the server is already part of multiple Active Directory domains, click **Leave Domain** to disassociate this ClearPass 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** dialog:

Figure 485: *Join AD Domain Dialog*



Join AD Domain

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller	AMG-AD.LOCADOMAIN.COM
NetBIOS Name	AMG-AD

In case of a controller name conflict

● Use specified Domain Controller
○ Use Domain Controller returned by DNS query
○ Fail on conflict

☑ Use default domain admin user [Administrator]

Username	
Password	●●●●●●●●●●●

Specify the **Join AD Domain** parameters as described in the following table.

Table 263: *Join AD Domain Parameters*

Parameter	Action/Description
Domain Controller	Enter the fully qualified name of the Active Directory domain controller.
NETBIOS name (optional)	Enter 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 Active Directory administrator about the NetBIOS name. **NOTE:** If you enter an incorrect value for the NetBIOS name, you see a warning message in the user interface. 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 correct NetBIOS name.
Domain	Specify the action to take in the event of a domain controller name conflict.

Table 263: *Join AD Domain Parameters (Continued)*

Parameter	Action/Description
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 can: ● **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	Enter the user ID of the domain administrator account. This field is disabled if the **Use default domain admin user** check box is selected.
Password	Enter the password of the domain administrator account.

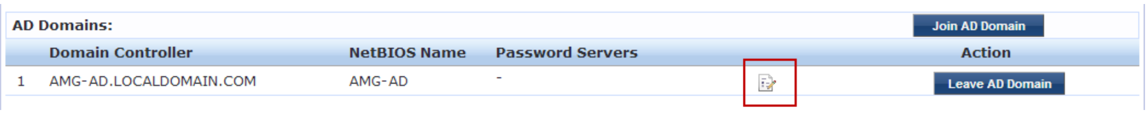
Adding a Password Server

After ClearPass successfully joins an Active Directory domain, you can configure a restricted list of domain controllers to be used for MSCHAP authentication. If this is 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 ClearPass joins at least one Active Directory domain (see Figure 486).

Figure 486: *Add Password Server icon*



AD Domains:

	Domain Controller	NetBIOS Name	Password Servers		Action
1	AMG-AD.LOCALDOMAIN.COM	AMG-AD	-		Leave AD Domain

   The **Configure AD Password Servers** page opens.

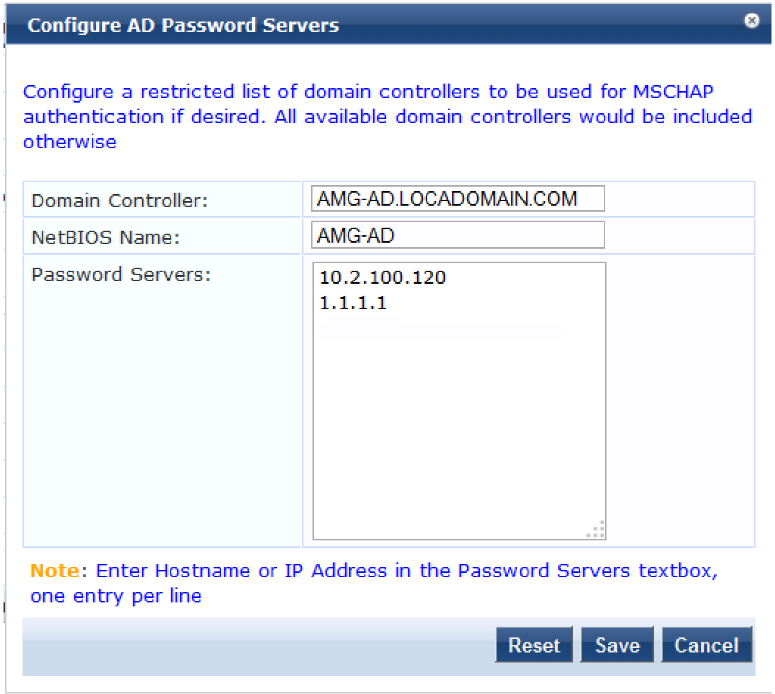
2. Specify the domain name, NetBIOS Name, and the password servers.

   The password servers can be a hostname or an 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** dialog with the password servers added to the configuration:

Figure 487: *Active Directory Password Server Added*



Configure AD Password Servers

Configure a restricted list of domain controllers to be used for MSCHAP authentication if desired. All available domain controllers would be included otherwise

Domain Controller:	AMG-AD.LOCADOMAIN.COM
NetBIOS Name:	AMG-AD
Password Servers:	10.2.100.120 1.1.1.1

Note: Enter Hostname or IP Address in the Password Servers textbox, one entry per line

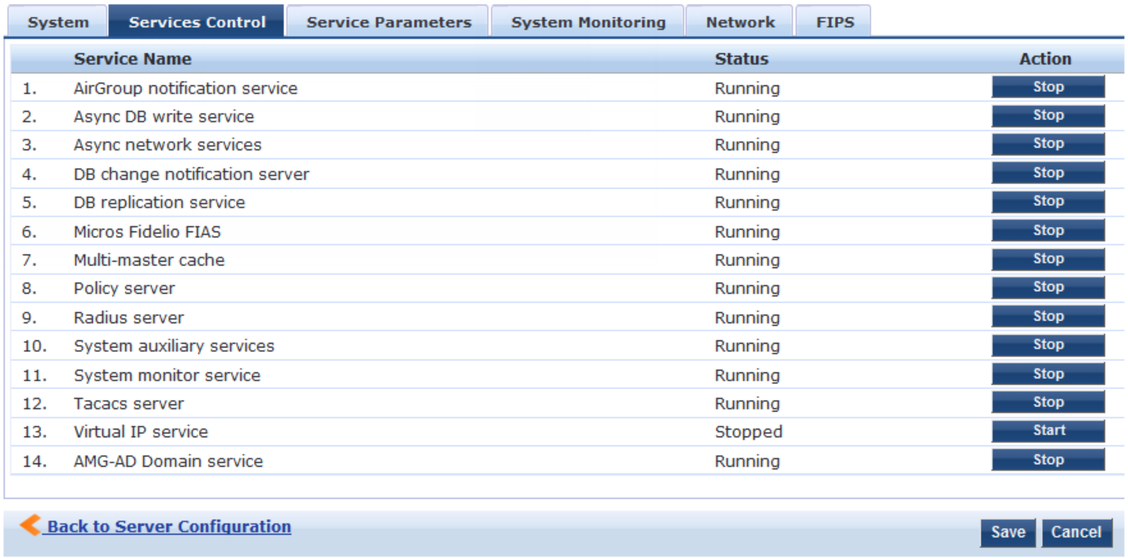
Services Control Page

From the **Services Control** page, you can:

- View the status of all the services: Running or Stopped.
- Stop or start Policy Manager services, including any Active Directory domains that the server joins.

The following figure displays the **Services Control** page:

Figure 488: *Services Control Page*



	Service Name	Status	Action
1.	AirGroup notification service	Running	Stop
2.	Async DB write service	Running	Stop
3.	Async network services	Running	Stop
4.	DB change notification server	Running	Stop
5.	DB replication service	Running	Stop
6.	Micros Fidelio FIAS	Running	Stop
7.	Multi-master cache	Running	Stop
8.	Policy server	Running	Stop
9.	Radius server	Running	Stop
10.	System auxiliary services	Running	Stop
11.	System monitor service	Running	Stop
12.	Tacacs server	Running	Stop
13.	Virtual IP service	Stopped	Start
14.	AMG-AD Domain service	Running	Stop

Service Parameters Page

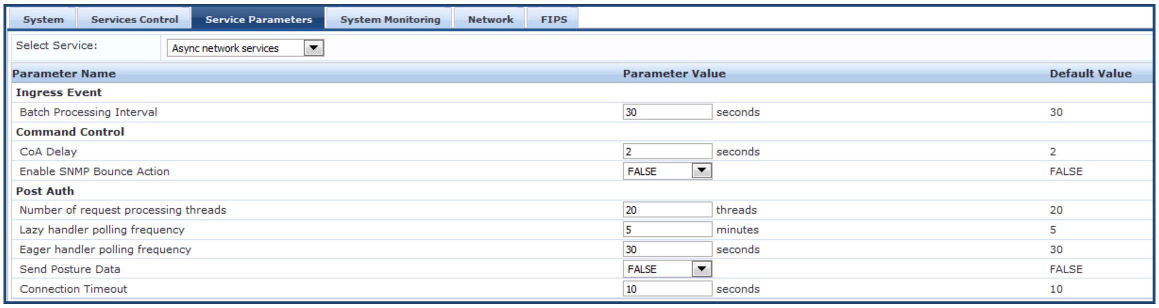
Navigate to the **Administration** > **Server Manager** > **Server Configuration** > **Service Parameters** page to change system parameters of the services listed below.

This section describes the following topics:

- Async Network Services Options on page 491
- ClearPass IPsec Service on page 492
- ClearPass Network Services Options on page 493
- ClearPass System Services Options on page 496
- Ingress Logger Service Ports on page 499
- Policy Server Options on page 500
- RADIUS Server Options on page 501
- Stats Collection Service Options on page 504
- System Monitor Service Options on page 505
- TACACS Server Options on page 506

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

Figure 489: *Service Parameters Page*



Select Service: Async network services

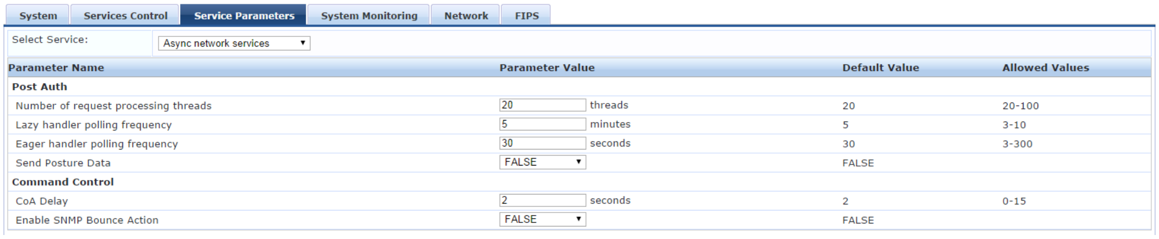
Parameter Name	Parameter Value	Default Value
Ingress Event		
Batch Processing Interval	30 seconds	30
Command Control		
CoA Delay	2 seconds	2
Enable SNMP Bounce Action	FALSE	FALSE
Post Auth		
Number of request processing threads	20 threads	20
Lazy handler polling frequency	5 minutes	5
Eager handler polling frequency	30 seconds	30
Send Posture Data	FALSE	FALSE
Connection Timeout	10 seconds	10

Async Network Services Options

Configure the **Ingress Event**, **Command Control**, and **Post-Auth** parameters for the Async network service.

The following figure displays the **Service Parameters** > **Async network services** parameters:

Figure 490: *Async Network Services*



Select Service: Async network services

Parameter Name	Parameter Value	Default Value	Allowed Values
Post Auth			
Number of request processing threads	20 threads	20	20-100
Lazy handler polling frequency	5 minutes	5	3-10
Eager handler polling frequency	30 seconds	30	3-300
Send Posture Data	FALSE	FALSE	
Command Control			
CoA Delay	2 seconds	2	0-15
Enable SNMP Bounce Action	FALSE	FALSE	

Enter the **Service Parameters** > **Async Network Services** parameters as described in Table 264

Table 264: *Service Parameters > Async Network Services*

Parameter	Action/Description
Ingress Event	
Batch Processing Interval	Specify the batch processing interval for ingress event processing. The default interval is **30** seconds. The range of values is **10** to **300** seconds. **NOTE:** For changes to the Batch Processing Interval to take effect, you must restart the **Async Network** service.
Post Auth	
Number of request processing threads	Set the number of request processing threads. The default value is **20** threads, and the range of values is between **20** and **100**.
Lazy handler polling frequency	Set the **Lazy handler polling frequency** (in minutes). The default value is **5** minutes, and the allowed values are from **3** to **10** minutes. **Lazy handler polling** is employed when an attribute may not require to be updated unless it explicitly asks for it. When it is required, even if there is no available fresh value, it can be fetched by initiating a separate request.
Eager handler polling frequency	Set the **Eager handler polling frequency** (in seconds). The default value is **30** seconds, and the allowed values are from **10** to **300** seconds. **Eager handler polling** is employed when an attribute requires the freshest possible value.
Send Posture Data	To send posture data to the Palo Alto Firewall server, set this to **TRUE**.
Command Control	
CoA Delay	Set the CoA Delay value (in seconds). The default value is **2**, and the allowed values are from **0** to **15** seconds.
Enable SNMP Bounce Action	Set the Enable SNMP Bounce Action value. The default value is **FALSE**.

ClearPass IPsec Service

When a network device requests an IPsec connection between the device and a ClearPass server, ClearPass uses the Online Certificate Status Protocol (OCSP) URI (uniform resource identifier) specified in Figure 491 to contact a third-party server that checks to see if the certificate sent by the requesting device is valid.

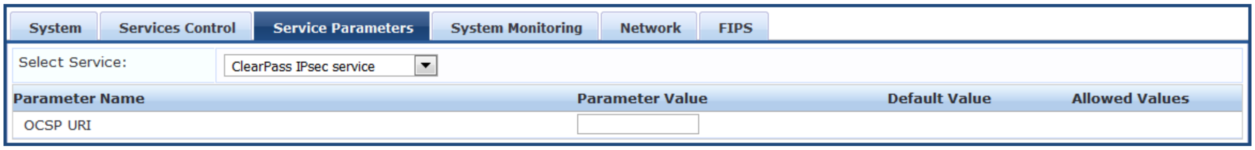
If the certificate is confirmed as valid, an IPsec connection between the ClearPass server and the requesting network device is established.

To configure the ClearPass IPsec service:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**, then select the ClearPass server.
2. Select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **ClearPass IPsec service**.

The following dialog opens:

Figure 491: *ClearPass IPsec Service Dialog*



Select Service: ClearPass IPsec service

Parameter Name	Parameter Value	Default Value	Allowed Values
OCSP URI			

4. Specify the **Service Parameters** > **ClearPass IPsec Service** parameters as described in Table 265, then click **Save**.

Table 265: *Service Parameters > ClearPass IPsec Service Parameters*

Parameter	Action/Description
Strict CRL Policy	You can enable or disable a strict Certificate Revocation List (CRL) policy. This parameter is disabled by default. ● To enable **Strict CRL Policy**, select **Yes** from the **Parameter Value** drop-down. When this option is enabled, a fresh Certificate Revocation List must be available in order for a peer connection to succeed. Whenever **Strict CRL Policy** is modified, existing IPsec tunnels that use Public Key Authentication are brought down and then brought up again.
OCSP URI	In the **Parameter Value** field, specify the **HTTP** or **HTTPS URI** (uniform resource identifier) for the Online Certificate Status Protocol (OCSP). OCSP enables the ClearPass server to determine the revocation state of a certificate presented by a peer—for example a network device requesting an IPsec connection to the ClearPass server. **NOTE:** When you enter the OSCP URI, ClearPass checks that 1) the URI is in the proper format (it must start with HTTP or HTTPS and be syntactically correct), and 2) ClearPass checks to see if the specified OSCP server IP address or host name is reachable from the ClearPass node. A descriptive error message will be displayed in the event of an incorrect OSCP URI.

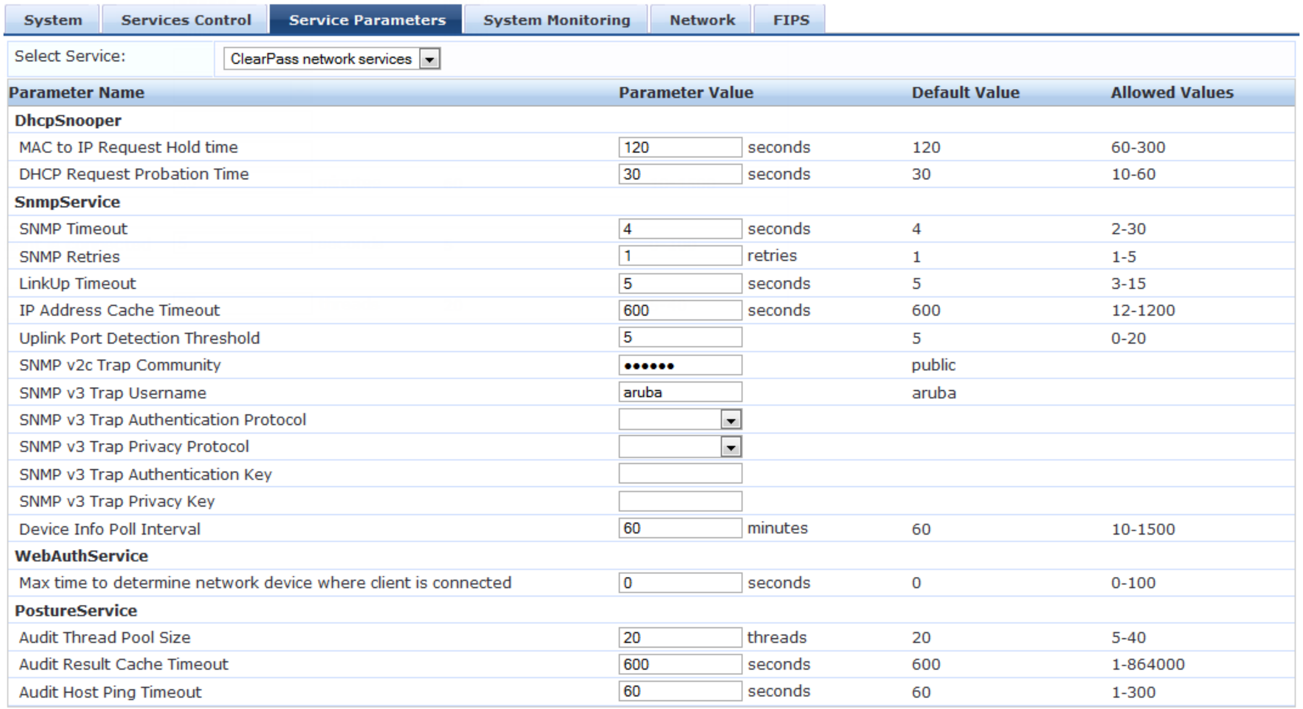
ClearPass Network Services Options

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

- SNMP Service
- Certificate Authentication Service
- Web Authentication Service
- Posture Service
- DHCP Snooper Service

The following figure displays the **Service Parameters** tab > **ClearPass Network Services** parameters (partial view):

Figure 492: *Service Parameters > ClearPass Network Services*

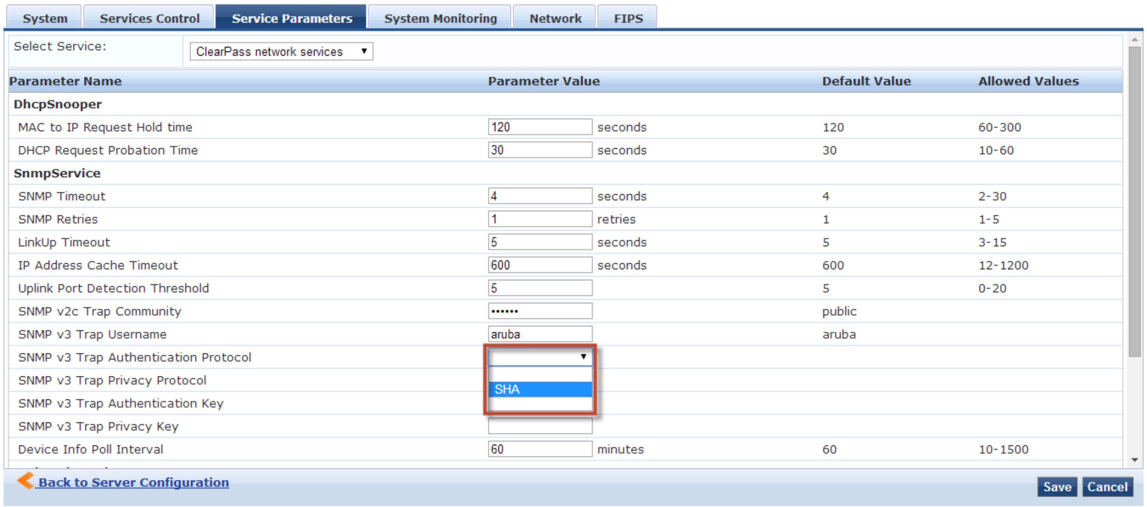


Select Service: ClearPass network services

Parameter Name	Parameter Value		Default Value	Allowed Values
DhcpSnooper				
MAC to IP Request Hold time	120	seconds	120	60-300
DHCP Request Probation Time	30	seconds	30	10-60
SnmpService				
SNMP Timeout	4	seconds	4	2-30
SNMP Retries	1	retries	1	1-5
LinkUp Timeout	5	seconds	5	3-15
IP Address Cache Timeout	600	seconds	600	12-1200
Uplink Port Detection Threshold	5		5	0-20
SNMP v2c Trap Community	••••••		public	
SNMP v3 Trap Username	aruba		aruba	
SNMP v3 Trap Authentication Protocol				
SNMP v3 Trap Privacy Protocol				
SNMP v3 Trap Authentication Key				
SNMP v3 Trap Privacy Key				
Device Info Poll Interval	60	minutes	60	10-1500
WebAuthService				
Max time to determine network device where client is connected	0	seconds	0	0-100
PostureService				
Audit Thread Pool Size	20	threads	20	5-40
Audit Result Cache Timeout	600	seconds	600	1-864000
Audit Host Ping Timeout	60	seconds	60	1-300

The following figure displays the **Service Parameters** tab > **ClearPass Network Services** parameters in FIPS mode:

Figure 493: *Service Parameters > ClearPass Network Services in FIPS Mode*



Select Service: ClearPass network services

Parameter Name	Parameter Value		Default Value	Allowed Values
DhcpSnooper				
MAC to IP Request Hold time	120	seconds	120	60-300
DHCP Request Probation Time	30	seconds	30	10-60
SnmpService				
SNMP Timeout	4	seconds	4	2-30
SNMP Retries	1	retries	1	1-5
LinkUp Timeout	5	seconds	5	3-15
IP Address Cache Timeout	600	seconds	600	12-1200
Uplink Port Detection Threshold	5		5	0-20
SNMP v2c Trap Community	••••••		public	
SNMP v3 Trap Username	aruba		aruba	
SNMP v3 Trap Authentication Protocol	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

Specify the **ClearPass Network Services** parameters as described in the following table:

Table 266: *Service Parameters > ClearPass Network Services*

Service Parameters	Action/Description
SnmpService	
SNMP Timeout	Specify the seconds to wait for an SNMP response from the network device.
SNMP Retries	Specify the number of retries for SNMP requests.
LinkUp Timeout	Specify the seconds to wait before processing link-up traps. If a MAC notification trap arrives in this time, the SNMP service does not try to poll the switch for MAC addresses behind a port for link-up processing.
IP Address Cache Timeout	Specify the duration in seconds for which MAC-to-IP lookup response is cached.
Uplink Port Detection Threshold	Specify 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. The default value is **5**, with a range from **0** to **20**.
SNMP v2c Trap Community	Specify the community string that must be checked in all incoming SNMP v2 traps.
SNMP v3 Trap Username	Specify the SNMP v3 Username to be used for all incoming traps.
SNMP v3 Trap Authentication Protocol	Specify the SNMP v3 Authentication protocol for traps. The options are: **MD5**, **SHA**, or **empty** (to disable authentication). **NOTE:** The **EAP-MD5** authentication type is not supported if you use ClearPass Policy Manager in **FIPS** mode.
SNMP v3 Trap Privacy Protocol	Specify the SNMP v3 Privacy protocol for traps. The options are: **DES_CBC**, **AES_128**, or **empty** (to disable privacy). **NOTE:** The **DES_CBC** privacy protocol is not supported if you use ClearPass Policy Manager in **FIPS** mode.
SNMP v3 Trap Authentication Key	Specify the SNMP v3 authentication key and privacy key for incoming traps.
SNMP v3 Trap Privacy Key	
Device Info Poll Interval	Specify the time (in minutes) between polling for device information.
Certificate Auth	

Table 266: *Service Parameters > ClearPass Network Services (Continued)*

Service Parameters	Action/Description
OCSP Check	Specify one of the following options for initiating an Online Certificate Status Protocol (OCSP) check: - **None** (the default setting) - **Optional** - **Required**
WebAuthService	
Max time to determine network device where client is connected	Specifies the maximum time to wait for Policy Manager to determine the network device to which the 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 process can take some time.
PostureService	
Audit Thread Pool Size	Specify the number of threads to use for connections to audit servers.
Audit Result Cache Timeout	Specify the time (in seconds) for which audit result entries are cached by Policy Manager.
Audit Host Ping Timeout	Specify the number of seconds for which Policy Manager pings an end-host before giving up and deeming the host to be unreachable.
DhcpSnooper	
MAC to IP Request Hold time	Specify 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 address-to-IP address binding. Typically, an audit service requests a MAC-to-IP mapping as soon the RADIUS request is received, but the client may take some more time to receive the IP address through DHCP. This wait period takes into account the latest DHCP IP address that the client received.
DHCP Request Probation Time	Specify 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 a client receives a DHCPNAK for a DHCPREQUEST and receives a new IP address after going through the DHCPDISCOVER process again.

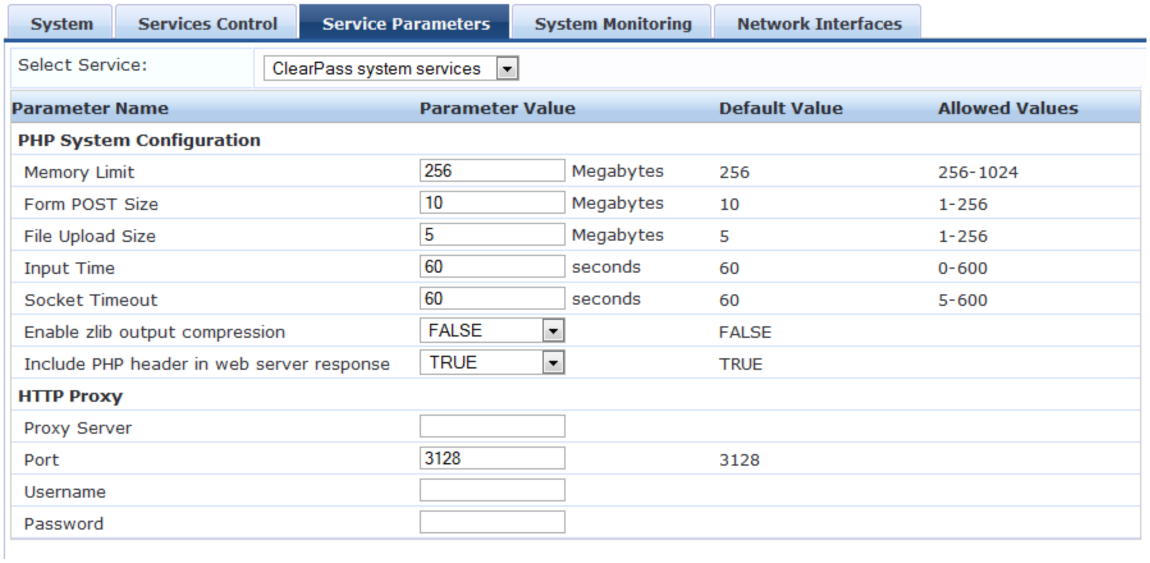
ClearPass System Services Options

You can use the ClearPass system service parameters for PHP configuration and for HTTP traffic flowing through a proxy server.

ClearPass Policy Manager relies on an HTTP connection for the ClearPass Update Portal to download the latest information for system services.

The following figure displays the **Service Parameters** > **ClearPass System Services** parameters (partial view):

Figure 494: *ClearPass System Services Parameters*



Select Service: ClearPass system services

Parameter Name	Parameter Value	Default Value	Allowed Values
PHP System Configuration			
Memory Limit	256 Megabytes	256	256-1024
Form POST Size	10 Megabytes	10	1-256
File Upload Size	5 Megabytes	5	1-256
Input Time	60 seconds	60	0-600
Socket Timeout	60 seconds	60	5-600
Enable zlib output compression	FALSE	FALSE	
Include PHP header in web server response	TRUE	TRUE	
HTTP Proxy			
Proxy Server			
Port	3128	3128	
Username			
Password			

Specify the **Service Parameters** > **ClearPass System Services** parameters as described in the following table.

Table 267: *Service Parameters > ClearPass System Services*

Service Parameter	Action/Description
PHP System Configuration	
Memory Limit	Specify the maximum memory that can be used by the PHP applications.
Form POST Size	Specify the maximum HTTP POST content size that can be sent to the PHP application.
File Upload Size	Specify the maximum file size that can be uploaded into the PHP application.
Input Time	Specify the time limit after which the server will detect no activity from the user and will take some action.
Socket Timeout	Specify the maximum time for any socket connections.
Enable zlib output compression	Specify the setting to compress the output files.
Include PHP header in web server response	Specify the setting to include PHP header in the HTTP responses.
HTTP Proxy	
Proxy Server	Specify the hostname or IP address of the proxy server.

Table 267: *Service Parameters > ClearPass System Services (Continued)*

Service Parameter	Action/Description
Port	Specify the port at which the proxy server listens for HTTP traffic.
Username	Specify the user name to authenticate with the proxy server.
Password	Specify the password to authenticate with the 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 to 86400.
Keep Alive Interval	Specify a value in seconds from 1 to 3600.
Keep Alive Probes	Specify a value from 1 to 100 for the number of probes.
Web Server Configuration	
Maximum Clients	Specify a value from 10 to 20000 for the maximum number of clients allowed.
Timeout	Specify a server timeout value in seconds from 1 to 60.
Keep Alive	To enable or disable keep-alive for the web server, select **TRUE** or **FALSE**.
Request Wait	Specify the request wait time in seconds from 1 to 60. The default value is **4** seconds.

Table 267: *Service Parameters > ClearPass System Services (Continued)*

Service Parameter	Action/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 whether to enable the host header check. 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, ClearPass Policy Manager redirects to https://<ClearPass-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 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 ClearPass Policy Manager.

Ingress Logger Service Ports

When Ingress Event Processing is enabled and configured on ClearPass (see Configuring Processing for Ingress Events on page 703), logging of ingress events occurs automatically.

By default, the ClearPass server listens for Ingress Events on **TCP port 514** and **UDP port 514**.

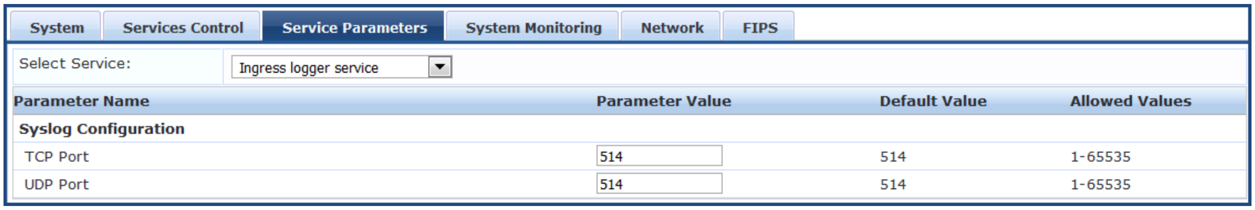
If necessary, you can change these Syslog Ingress Logger ports.

To change the Syslog Ingress Logger ports:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**, then select the ClearPass server.
2. Select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **Ingress Logger Service**.

   The following dialog opens:

Figure 495: *Ingress Logger Service Dialog*



Select Service: Ingress logger service

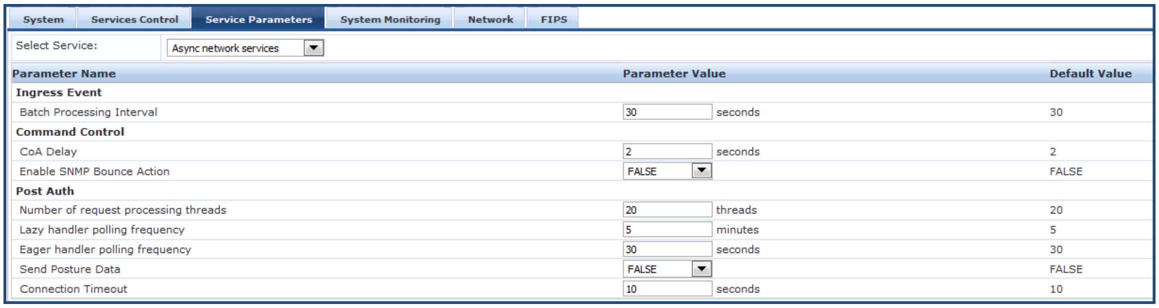
Parameter Name	Parameter Value	Default Value	Allowed Values
Syslog Configuration			
TCP Port	514	514	1-65535
UDP Port	514	514	1-65535

4. To change the Ingress Logger **TCP Port**, enter the new port number in the **Parameter Value** field.
5. To change the Ingress Logger **UDP Port**, enter the new port number.
6. Click **Save**.

Policy Server Options

The following figure displays the **Service Parameters** > **Policy Server** dialog:

Figure 496: *Policy Server Service Parameters*



Select Service: Async network services

Parameter Name	Parameter Value		Default Value
Ingress Event			
Batch Processing Interval	30	seconds	30
Command Control			
CoA Delay	2	seconds	2
Enable SNMP Bounce Action	FALSE		FALSE
Post Auth			
Number of request processing threads	20	threads	20
Lazy handler polling frequency	5	minutes	5
Eager handler polling frequency	30	seconds	30
Send Posture Data	FALSE		FALSE
Connection Timeout	10	seconds	10

Specify the **Service Parameters** > **Policy Server** parameters.

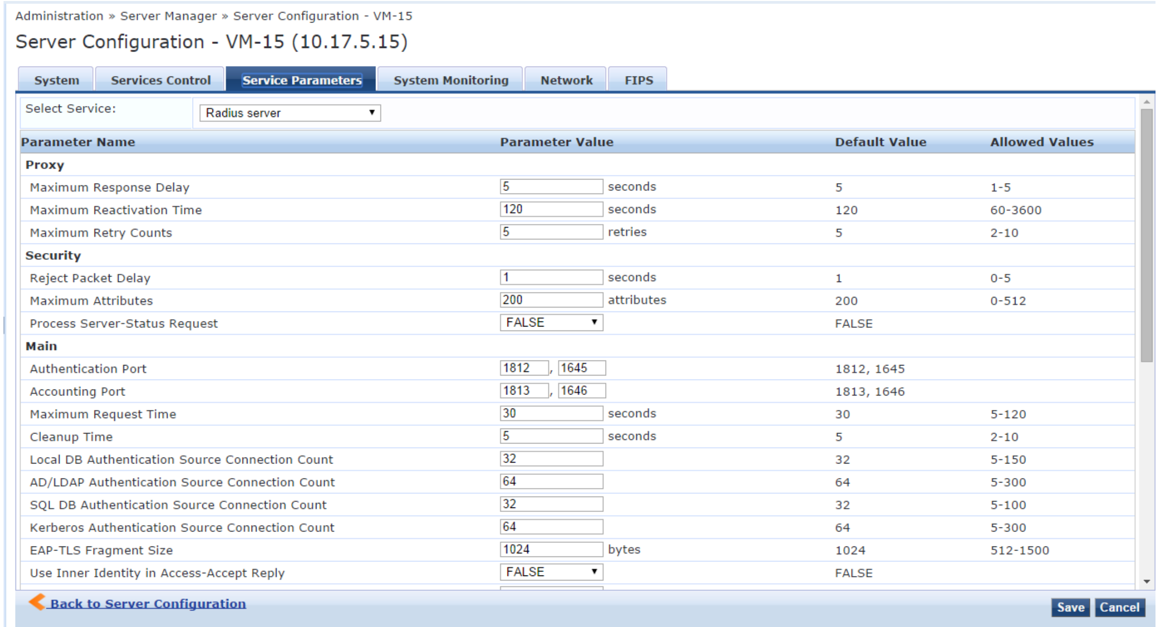
Table 268: *Service Parameters > Policy Server Service*

Service Parameter	Action/Description
Machine Authentication Cache Timeout	1. Specify the time (in hours) for which machine authentication entries are cached by ClearPass Policy Manager. The default is **24 hours**.
LDAP Primary Retry Interval	After a primary LDAP server is down, the ClearPass server connects to one of the backup servers. 2. Specify how long the ClearPass server waits (in seconds) before it tries to connect to the primary server again.
Audit SPT Default Timeout	3. Specify the time (in seconds) for which an Audit success or error response is cached in the Policy server.
Additional time before session deletion from multi-master cache	4. Specify the number of seconds the Policy server will wait before deleting the multi-master entry. The default value is **0**. This parameter handles roaming scenarios where an Accounting-Start occurs without an authentication request. If the value for this parameter is **0**, the Policy server deletes the multi-master entry when an Accounting-Stop is received. The RADIUS server updates the multi-master entry with attribute values from the accounting request. These can be used in the Change of Authorization (CoA). In a roaming scenario, this NAS information update from the accounting request helps ClearPass send the CoA to the correct NAS.
Number of request processing threads	5. Specify the maximum number of threads used to process requests.
HTTP Thread Pool Size	6. Specify the number of threads allotted for the HTTP thread pool.
Authentication Thread Pool Size	7. Specify the number of threads to use for LDAP/AD and SQL connections.
	8. Click **Save**.

RADIUS Server Options

The following figure displays the **Service Parameters** tab > **RADIUS Server** parameters (partial list):

Figure 497: *RADIUS Server Parameters Dialog*



Administration » Server Manager » Server Configuration - VM-15

Server Configuration - VM-15 (10.17.5.15)

Select Service: Radius server

Parameter Name	Parameter Value		Default Value	Allowed Values
Proxy				
Maximum Response Delay	5	seconds	5	1-5
Maximum Reactivation Time	120	seconds	120	60-3600
Maximum Retry Counts	5	retries	5	2-10
Security				
Reject Packet Delay	1	seconds	1	0-5
Maximum Attributes	200	attributes	200	0-512
Process Server-Status Request	FALSE		FALSE	
Main				
Authentication Port	1812, 1645		1812, 1645	
Accounting Port	1813, 1646		1813, 1646	
Maximum Request Time	30	seconds	30	5-120
Cleanup Time	5	seconds	5	2-10
Local DB Authentication Source Connection Count	32		32	5-150
AD/LDAP Authentication Source Connection Count	64		64	5-300
SQL DB Authentication Source Connection Count	32		32	5-100
Kerberos Authentication Source Connection Count	64		64	5-300
EAP-TLS Fragment Size	1024	bytes	1024	512-1500
Use Inner Identity in Access-Accept Reply	FALSE		FALSE	

Specify the **Service Parameters** > **RADIUS server** parameters as described in the following table:

Table 269: *Service Parameters > RADIUS Server Service*

Service Parameter	Action/Description
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 expires. The default is **3 weeks**. If a client presents a PAC (Protected Access Credential) that is encrypted using the master key in this period after its TTL (Time-to-Live), it is accepted and a new PAC encrypted with the latest master key is provisioned on the client.
PACs are valid across cluster	If PACs (Protected Access Credentials) generated by this server are valid across the cluster, set to **TRUE** (the default setting). If not, select **FALSE**.
Proxy	
Maximum Response Delay	If the target server has not responded, specify the time delay before retrying a proxy request. The default is **5** seconds.
Maximum Reactivation Time	Specify the time to elapse before retrying a dead proxy server.
Maximum Retry Counts	If the target server doesn't respond, specify the maximum number of times to retry a proxy request.

Table 269: *Service Parameters > RADIUS Server Service (Continued)*

Service Parameter	Action/Description
Accounting	
Log Accounting Interim-Update Packets	To store the Interim-Update packets in session logs, select **TRUE**. **FALSE** is the default setting.
Thread Pool	
Maximum Number of Threads	Specify the maximum number of threads in the RADIUS server thread pool to process requests.
Number of Initial Threads	Specify the initial number of threads in the RADIUS server thread pool to process requests.
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 to specify the number of Active Directory errors that can occur within the defined Window Size and have the self-healing Recovery Action 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. This is the default. ● **Exit**: To restart the RADIUS server. (The monitoring daemon will restart it.) ● **Restart Domain Service**: To restart the Domain service.
Security	
Reject Packet Delay	Specify the delay time before sending an actual RADIUS Access-Reject message after the server decides to reject the request.
Maximum Attributes	Specify the maximum number of RADIUS attributes allowed in a request. The default is **200**.
Process Server-Status Request	● **TRUE**: Send replies to Status-Server RADIUS packets. ● **FALSE**: Do not send replies to Status-Server RADIUS packets. This is the default setting.
Main	
Authentication Port	Specify the ports on which the RADIUS server listens for authentication requests. Default values are ports **1645** and **1812**. **NOTE:** You can configure the Authentication Port to different values if desired.

Table 269: *Service Parameters > RADIUS Server Service (Continued)*

Service Parameter	Action/Description
Accounting Port	Specify the ports on which the RADIUS server listens for accounting requests. The default values are **1646** and **1813**. **NOTE:** You can configure the Accounting Port to different values if desired.
Maximum Request Time	Specify the maximum time (in seconds) allowed for processing a request after which it is considered timed out. The default is **30 seconds**.
Cleanup Time	Specify the time to cache the response sent to a RADIUS request after sending it. The range is from **2** to **10** seconds. The default is **5** seconds. If the RADIUS server gets a duplicate request for which the response is already sent, and the duplicate request arrives within this time period, the cached response is resent.
Local DB Authentication Source Connection Count	Specify the maximum number of Local DB connections opened.
AD/LDAP Authentication Source Connection Count	Specify the maximum number of Active Directory and LDAP (Lightweight Directory Access Protocol) connections opened. The range is from **5** to **300**. The default is **64**.
SQL DB Authentication Source Connection Count	Specify the maximum number of SQL DB.
Kerberos Authentication Source Connection Count	Specify the maximum number of Kerberos connections opened.
EAP-TLS Fragment Size	Specify the maximum allowed size (in bytes) for the EAP-TLS fragment.
Use Inner Identity in Access-Accept Reply	To use the inner identity in the Access-Accept replies, select **TRUE**. **FALSE** is the default setting.
Reject if OCSP response does not have Nonce	To reject an OCSP response without a nonce, select **TRUE**. Else, select **FALSE**.
Include Nonce in OCSP request	Specify one of the following: ● **TRUE**: Select if the OCSP (Online Certificate Status Protocol) request should include the nonce. This is the default value. ● **FALSE**: To avoid the EAP-TLS authentication failure, select if the OCSP server does not support the nonce.
Enable signing for OCSP Request	To enable signing for OCSP request, select **TRUE**. This determines whether ClearPass should sign an OCSP request with a RADIUS server certificate. The default value is **FALSE**.
Check the validity of all	To check the validity of all certificates in the chain against Certificate Revocation

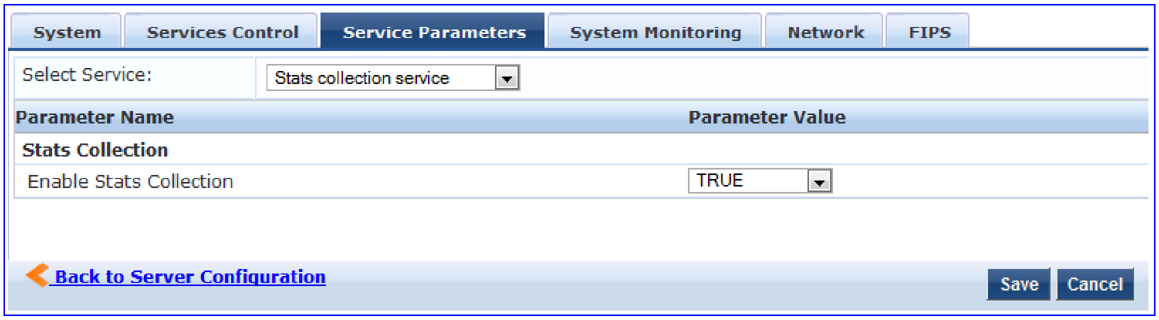
Table 269: *Service Parameters > RADIUS Server Service (Continued)*

Service Parameter	Action/Description
certificates in the chain against CRLs	Lists (CRLs), select **TRUE**. Else, select **FALSE**.
ECDH Curve	Select one of the following ECDH curve (Elliptic Curve Diffie-Helman) 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
Disable TLS 1.2	To disable Transport Layer Security 1.2 (TLS 1.2), select **TRUE**. **FALSE** is the default setting—TLS 1.2 is enabled by default.
Check the validity of intermediary certificates in the chain using OCSP	To check the validity of intermediary certificates in the chain using OCSP, select **TRUE**. The defaOnline Certificate Status Protocolult is **FALSE**.
Maximum Number of AD Authentication Processes	To specify the maximum number of Active Directory authentication processes, enter a number between **1** and **5**. The default is **1**.
Verify OCSP Signing Purpose	Specify one of the following: ● **TRUE**: EAP-TLS authentication will fail unless the OCSP signing certificate also has the OCSP signing purpose set. ● **FALSE**: The OCSP signing certificate does not need to have the OCSP signing purpose set. This is default setting.
TLS Session Cache Limit	Specify the number of TLS sessions to cache before purging the cache (used in TLS based 802.1X EAP Methods). The range is from **1,000** to **100,000**. The default is **10,000**.

Stats Collection Service Options

The following figure displays the **Service Parameters** tab > **Stats Collection Service** parameters:

Figure 498: *Stats Collection Service Parameters*



Select Service: Stats collection service

Parameter Name	Parameter Value
Stats Collection	
Enable Stats Collection	TRUE

The following table describes the **Service Parameters** tab > **Stats Collection Service** parameter:

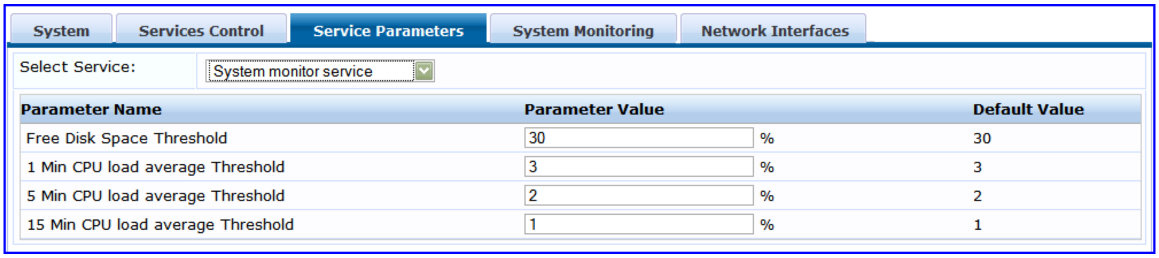
Table 270: *Service Parameters > Stats Collection Service*

Service Parameter	Action/Description
Enable Stats Collection	Enable or disable statistics collection and aggregation. The **Statistics Collection Service** is enabled by default (**TRUE**). If this is not enabled, statistics collection and aggregation services will not run on the node. In addition, if statistics collection and aggregation is not enabled, the following error message is displayed 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 or disabling this parameter requires a restart of the cpass-statsd-server and cpass-carbon-server.

System Monitor Service Options

The following figure displays the **Service Parameters** tab > **System Monitor Service** parameters:

Figure 499: *System Monitor Service Parameters*



Select Service: System monitor service

Parameter Name	Parameter Value		Default Value
Free Disk Space Threshold	30	%	30
1 Min CPU load average Threshold	3	%	3
5 Min CPU load average Threshold	2	%	2
15 Min CPU load average Threshold	1	%	1

The following table describes the **Service Parameters** tab > **System Monitor Service** parameters:

Table 271: *Services Parameters > System Monitor Service*

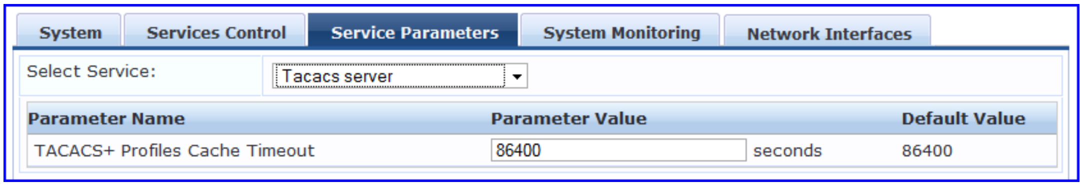
Service Parameter	Action/Description
Free Disk Space Threshold	This parameter monitors the available disk space on the current ClearPass server node. Specify the **Free Disk Space Threshold** (the default is **30%**). If the available disk free space falls below the specified threshold, the ClearPass server 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-minute, 5-minute, and 15-minute averages, respectively. If any of these loads exceed the associated maximum value, the ClearPass server sends traps to the configured trap servers.
5 Min CPU load average Threshold	
15 Min CPU load average Threshold	

TACACS Server Options

The **Service Parameters** >**TACACS Server** dialog provides two parameters:

- TACACS+ Profiles Cache Timeout
- TACACS+ HTTP Thread Pool Size

Figure 500: *Service Parameters > TACACS+ Server Dialog*



Select Service: Tacacs server

Parameter Name	Parameter Value		Default Value
TACACS+ Profiles Cache Timeout	86400	seconds	86400

Specify the **Service Parameters** > **TACACS server** parameters as described in the following table:

Table 272: *Service Parameters > TACACS Server*

Service Parameter	Action/Description
TACACS+ Profiles Cache Timeout	Specify the time (in seconds) for which TACACS+ profile result entries are cached by ClearPass Policy Manager.
TACACS+ HTTP Thread Pool Size	Specify the maximum number of simultaneous requests the server can handle. The default value is **100**. The range is from **5** to **200**. When the server has reached the limit or request threads, it defers processing new requests until the number of active requests drops below the specified amount. Increasing this value reduces HTTP response latency times.

System Monitoring Page

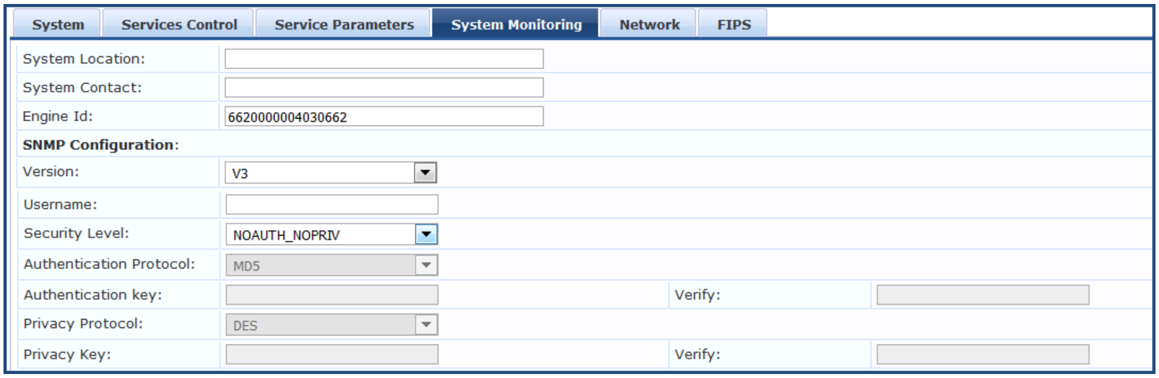
By configuring the **System Monitoring** parameters, you can ensure that the external Management Information Base (MIB) browsers can browse the system-level MIB objects exposed by the ClearPass Policy Manager appliance. The options in this page vary based on the SNMP version that you select.

To configure the System Monitoring parameters:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration** page.
2. Select the ClearPass server of interest.
3. Select the **System Monitoring** tab.

   The **System Monitoring** configuration dialog opens:

Figure 501: *System Monitoring Configuration Dialog*



System Location:			
System Contact:			
Engine Id:	6620000004030662		
SNMP Configuration:			
Version:	V3		
Username:			
Security Level:	NOAUTH_NOPRIV		
Authentication Protocol:	MD5		
Authentication key:		Verify:	
Privacy Protocol:	DES		
Privacy Key:		Verify:	

4. Specify the **System Monitoring** configuration parameters as described in the following table:

Table 273: *System Monitoring Parameters*

Parameter	Action/Description
System Location	Specify the location of the ClearPass Policy Manager appliance.
System Contact	Specify the contact information of the ClearPass Policy Manager appliance.
Engine ID	A unique identifier for the SNMP v3 agent. The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMP v3 messages. The default value for the Engine ID is **6620000004030662**. The Engine ID is automatically generated when you enable the stand-alone SNMP agent.
SNMP Configuration	
Version	Specify the SNMP version from the options **V1**, **V2C**, or **V3**. The SNMP parameters on this page vary based on the SNMP version selected.
Community String	V1 and V2C: Enter and reenter the community string for sending traps. This is applicable only for SNMP V1 and V2C versions.
Username	V3 only: Specify the user name to use for SNMP v3 communication.
Security Level	V3 only: Select any of the following options: ● **NOAUTH_NOPRIV** (No authentication or privacy): When you select this security level, only the **SHA** authentication protocol is available. ● **AUTH_NOPRIV** (Authentication but no privacy): When you select this security level, the **MD5** and **SHA** authentication protocols are available. ● **AUTH _PRIV** (Authenticate and keep the communication private): When you select this security level, the **MD5** and **SHA** authentication protocols are available.
Authentication Protocol	V3 only: Select the authentication protocol from **MD5** or **SHA**. These protocols vary depending on the security level that you selected in the **Security Level** field. **NOTE:** The **MD5** authentication protocol is not supported in **FIPS** mode.

Table 273: *System Monitoring Parameters (Continued)*

Parameter	Action/Description
Authentication key	V3 only: Enter and reenter the authentication key. This field is available only if you selected **V3** as the SNMP version in the **Version** field.
Privacy Protocol	V3 only: Select the privacy protocol from **DES** or **AES**.
Privacy Key	V3 only: Enter the privacy key.

Network Page

This section provides the following information:

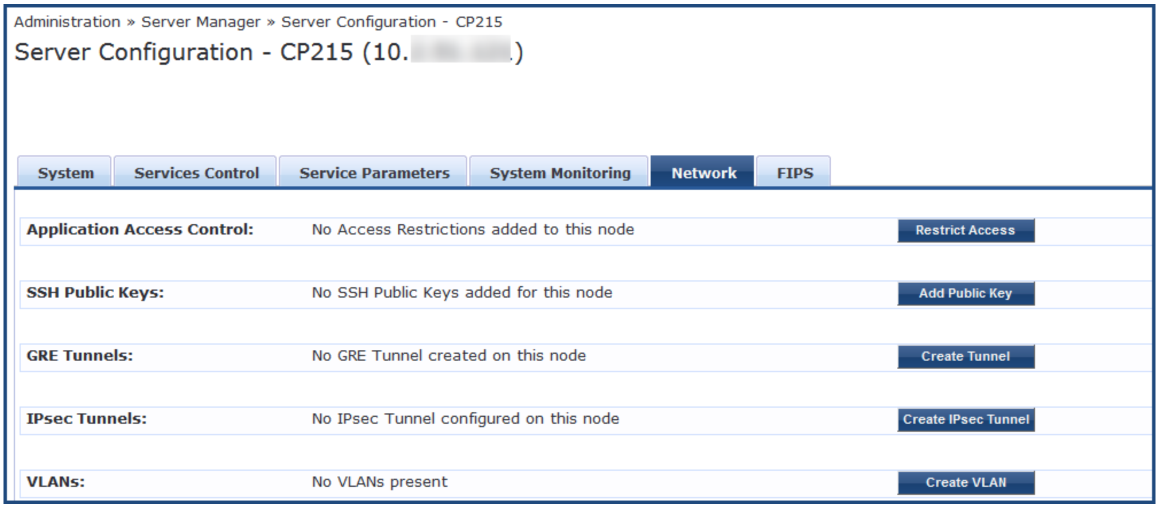
- Defining Application Access Control Restrictions
- Adding an SSH Public Key
- Creating GRE Tunnels
- Creating IPsec Tunnels
- Creating VLANs

To configure the **Server Configuration** > **Network** parameters:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.
2. Select the ClearPass server of interest.
3. Select the **Network** tab.

   The **Server Configuration** > **Network** page opens:

Figure 502: *Server Configuration > Network Page*



Administration » Server Manager » Server Configuration - CP215

Server Configuration - CP215 (10.[redacted])

Application Access Control:	No Access Restrictions added to this node	Restrict Access
SSH Public Keys:	No SSH Public Keys added for this node	Add Public Key
GRE Tunnels:	No GRE Tunnel created on this node	Create Tunnel
IPsec Tunnels:	No IPsec Tunnel configured on this node	Create IPsec Tunnel
VLANs:	No VLANs present	Create VLAN

Defining Application Access Control Restrictions

Use this function to define specific network resources and allow or deny them access to specific applications. You can create multiple definitions.

To configure network application access control restrictions:

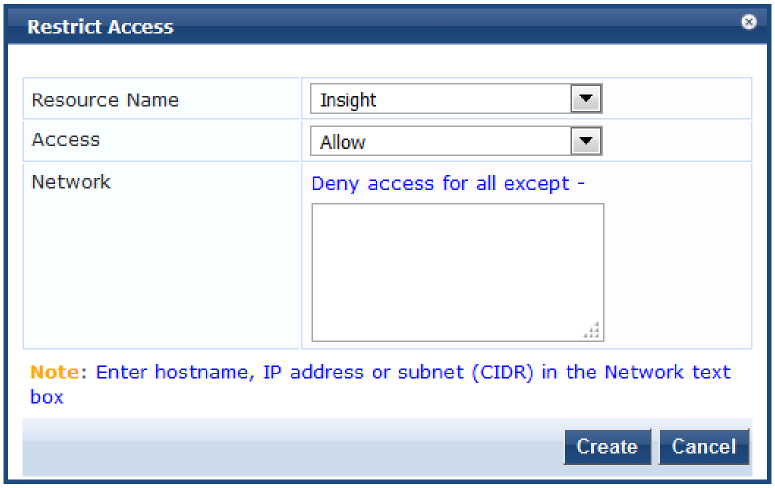
1. Navigate to the **Administration** > **Server Manager** > **Server Configuration**.
2. Select the ClearPass server of interest.
3. From the **Server Configuration** page, select the **Network** tab.

The **Server Configuration** > **Network** page opens.

4. From the **Application Access Control** option, click **Restrict Access**.

   The **Restrict Access** dialog opens.

Figure 503: *Restrict Access Configuration Dialog*



Restrict Access

Resource Name	Insight
Access	Allow
Network	Deny access for all except -

Note: Enter hostname, IP address or subnet (CIDR) in the Network text box

5. Specify the **Restrict Access** parameters as described in the following table, then click **Create**:

Table 274: *Restrict Access Parameters*

Parameter	Action/Description
Resource Name	Select the application to which you want to allow or deny access: ■ OnGuard ■ ClearPass API ■ Policy Manager ■ Graphite ■ Guest Operator ■ Insight
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 host names, IP addresses, or IP subnets (CIDR) per line. The devices defined by what you enter here will be either specifically allowed or specifically denied access to the application you select.

Adding an SSH Public Key

ClearPass supports public key-based SSH logins. This includes public key management and the ability to enable public key authentication in ClearPass on a node-by-node basis.

When you add the SSH public key to the clients, ClearPass allows passwordless SSH public key-based authentication to the appadmin ClearPass console.

NOTE

SSH public key-based authentication will continue to work even when the cluster password or the appadmin password have been changed.

To add an SSH public key:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.

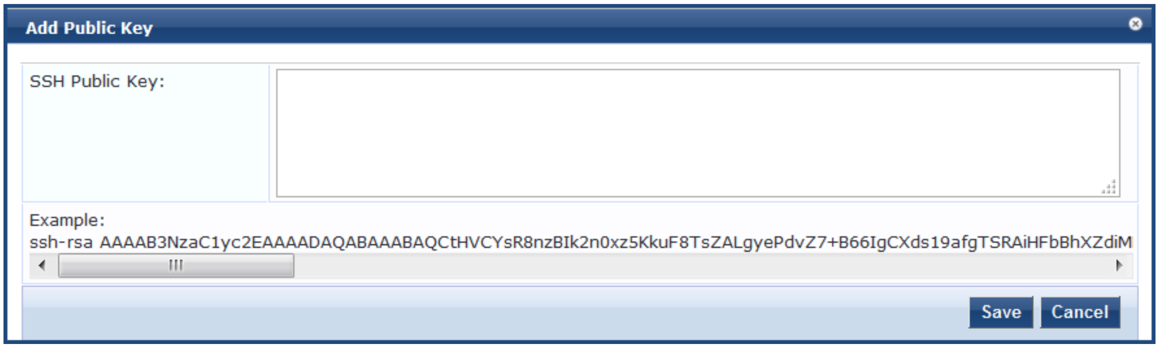
   The **Server Configuration** page opens.
2. Select the ClearPass server for which passwordless SSH is needed.

   The **Server Configuration** dialog for the selected server opens.
3. Select the **Network** tab.

   The **Server Configuration** >**Network** page opens.
4. From the **SSH Public Keys** option, click **Add Public Key**.

   The **Add Public Key** configuration page opens.

Figure 504: *Adding a Public Key*



SSH Public Key:

Example:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCtHVCYsR8nzBIk2n0xz5KkuF8TsZALgyePdvZ7+B66IgCXds19afgTSRAiHFbBhXZdiM

5. In the **SSH Public Key** window, copy and paste the SSH public key of the client, then click **Save**.

NOTE

If the SSH public key is regenerated on the client, passwordless public key-based SSH authentication will cease to work. The existing entry for that client must be deleted. Then copy and paste the new SSH public key.

6. From the **Server Configuration** page, click **Save**.

   The SSH operation to the ClearPass server using a public key is now active, and you can perform passwordless SSH to the ClearPass server appadmin console.

Creating GRE Tunnels

You can use the Generic Routing Encapsulation (GRE) protocol to create a virtual point-to-point link over a standard IP network or the Internet.

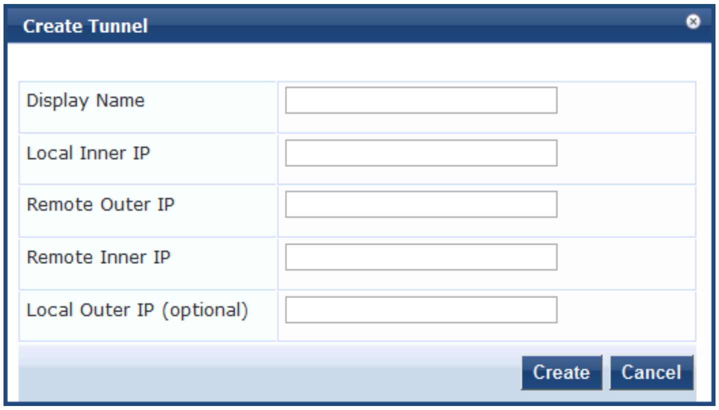
To create a GRE tunnel:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration**.
2. Select the ClearPass server of interest.
3. From the **Server Configuration** page, select the **Network** tab.

   The **Server Configuration** > **Network** page opens.
4. From the **GRE Tunnels** option, click **Create Tunnel.**

   The **Create Tunnel** dialog opens:

Figure 505: *Creating a GRE Tunnel*



5. Specify the **Create Tunnel** parameters as described in the following table, then click **Create**:

Table 275: *Create Tunnel Parameters*

Parameter	Action/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	Enter the local IP address of the tunnel network interface.
Remote Outer IP	Enter the IP address of the remote tunnel endpoint.
Remote Inner IP	Enter the remote IP address of the tunnel network interface. Enter a value to automatically create a route to this address through the tunnel.
Local Outer IP (Optional)	Optionally, enter the local IP address of the tunnel endpoint.

Creating IPsec Tunnels

ClearPass provides the option to configure rules that can determine which IPsec traffic to tunnel, which traffic to drop, and which traffic to encrypt or bypass (see Figure 507).

Thus, ClearPass supports adding traffic selectors based on port number and protocol (TCP/UDP) with rule options *Bypass, Encrypt*, and *Drop* (see Table 277).

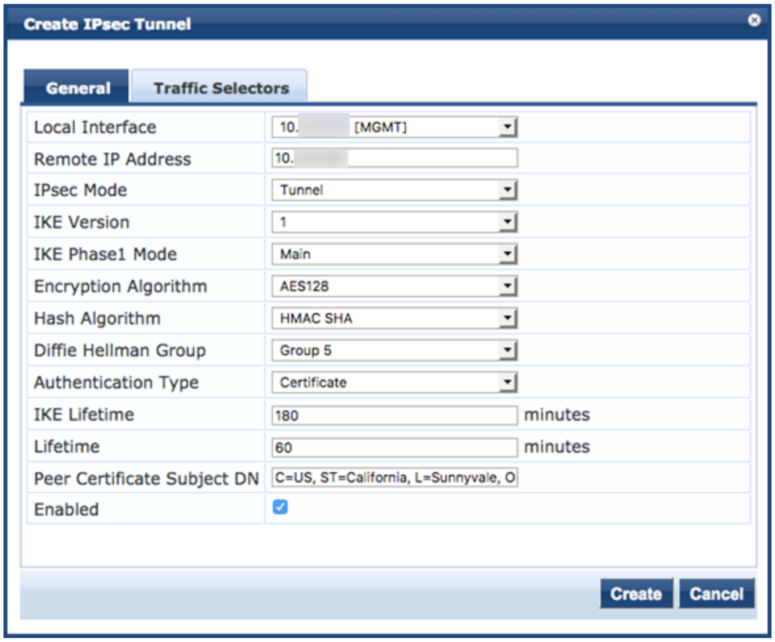
To create an IPsec tunnel:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration**.
2. Select the ClearPass server of interest.
3. From the **Server Configuration** page, select the **Network** tab.

   The **Server Manager** > **Configuration** > **Network** page opens.
4. Click **Create IPsec Tunnel**.

   The **Create IPsec Tunnel** dialog opens to the **General** tab.

Figure 506: *Creating an IPsec Tunnel Dialog*



Local Interface	10.[redacted] [MGMT]
Remote IP Address	10.[redacted]
IPsec Mode	Tunnel
IKE Version	1
IKE Phase1 Mode	Main
Encryption Algorithm	AES128
Hash Algorithm	HMAC SHA
Diffie Hellman Group	Group 5
Authentication Type	Certificate
IKE Lifetime	180 minutes
Lifetime	60 minutes
Peer Certificate Subject DN	C=US, ST=California, L=Sunnyvale, O
Enabled	☑

5. Specify the **Create IPsec Tunnel** parameters as described in the following table, then click **Create**:

Table 276: *Create IPSec Tunnel Parameters*

Parameter	Action/Description
Local Interface	Specify the local Management interface.
Remote IP Address	Specify the IP address of the remote host.
IPsec Mode	Select one of the following IPsec modes: ■ **Tunnel** ■ **Transport**
IKE Version	Select the version of the Internet Key Exchange (IKE) protocol from the options: **1** or **2**.
IKE Phase 1 Mode	This parameter is enabled when you select **IKE Version 1**. **IKE Phase 1 Mode** is set by default to **Main**.
PRF	The **PRF** (pseudorandom function) parameter is enabled when you select **IKE Version 2**. Select one of the following PRF options: ■ PRF-HMAC-SHA1 ■ PRF-HMAC-SHA256 ■ PRF-HMAC-SHA384 ■ PRF-HMAC-MD5
Encryption Algorithm	Select one of the following encryption algorithms: ■ AES128 ■ AES256

Table 276: *Create IPSec Tunnel Parameters (Continued)*

Parameter	Action/Description
Hash Algorithm	Select one of the following hash algorithms: - HMAC SHA - HMAC-SHA256 - HMAC-SHA384 - HMAC-MD5
Diffie Hellman Group	Select one of the following Diffie Hellman groups: - Group 5 - Group 14 - Group 19 - Group 20
Authentication Type	Select one of the following authentication types: - **Pre-Shared Key** - **Certificate**
IKE Shared Secret Verify IKE Shared Secret	Enter the IKE secret key, then verify the secret key.
IKE Lifetime	Specify the number of minutes for the lifetime of the IKE. The default is **180** minutes.
Lifetime	Specify the lifetime of the IPsec tunnel in minutes. The default is **60** minutes.
Peer Certificate Subject DN	When the authentication type is set to **Certificate**, you can configure the **Peer Subject Certificate DN** (Distinguished Name) field, which ensures that the IPsec connection will be successfully established only for peers that have certificates that match the peer certificate subject DN. **NOTE:** Configuring Peer Certificate Subject DN is optional. If it is configured, the Distinguished Name should match with the peer certificate DN in order to complete the authentication.
Enabled	To enable the IPsec tunnel, click the **Enabled** check box.

Traffic Selectors

A traffic selector (also known as a *proxy ID* in IKEv1) is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. Only traffic that conforms to a traffic selector is permitted through the associated IPsec security association (SA).

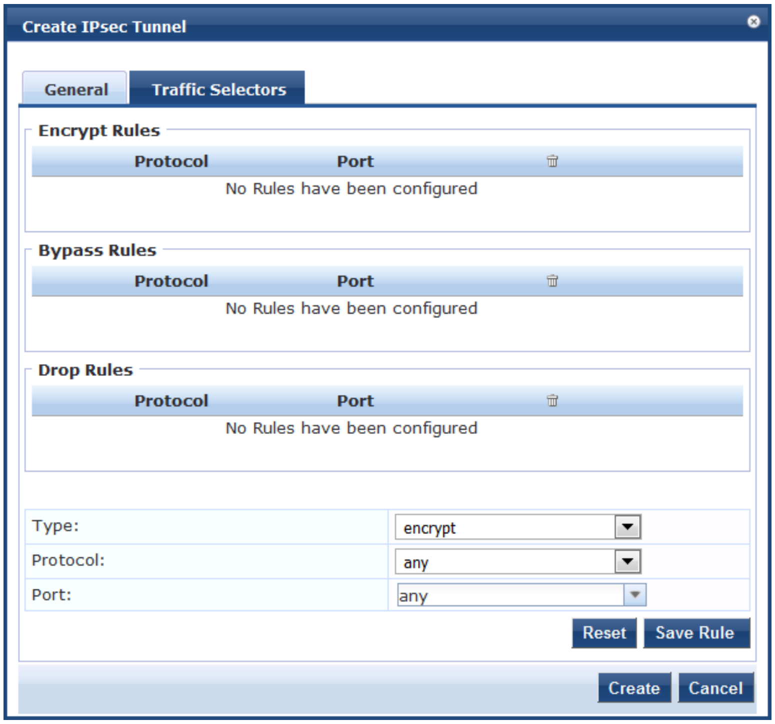
Traffic selectors are retained after a system restart, a service restart of network services, and a service restart of the IPsec service.

To configure the traffic selectors for this IPsec tunnel:

1. From the **Create IPsec Tunnel** dialog, select the **Traffic Selectors** tab.

   The **Traffic Selectors** dialog opens.

Figure 507: *Create IPsec Tunnel > Traffic Selectors Dialog*



2. Specify the **Traffic Selectors** parameters as described in the following table, then click **Create**.

Table 277: *Create IPSec Tunnel > Traffic Selectors Parameters*

Parameter	Action/Description
Encrypt Rules	Displays the IPsec tunnel encryption rules configured for this IPsec tunnel.
Bypass Rules	Displays the IPsec tunnel bypass rules configured for this IPsec tunnel.
Drop Rules	Displays the IPsec tunnel drop rules configured for this IPsec tunnel.
Type	Select one of the following traffic selector types: ■ **Bypass** ■ **Encrypt** ■ **Drop**
Protocol	Select one of the following protocols: ■ **Any** ■ **TCP** ■ **UDP**
Port	From the **Port** drop-down list, select the port.
Reset	To reset the configuration settings to the defaults, click **Reset**.
Save Rule	To save the current Rule configuration, click **Save Rule**.

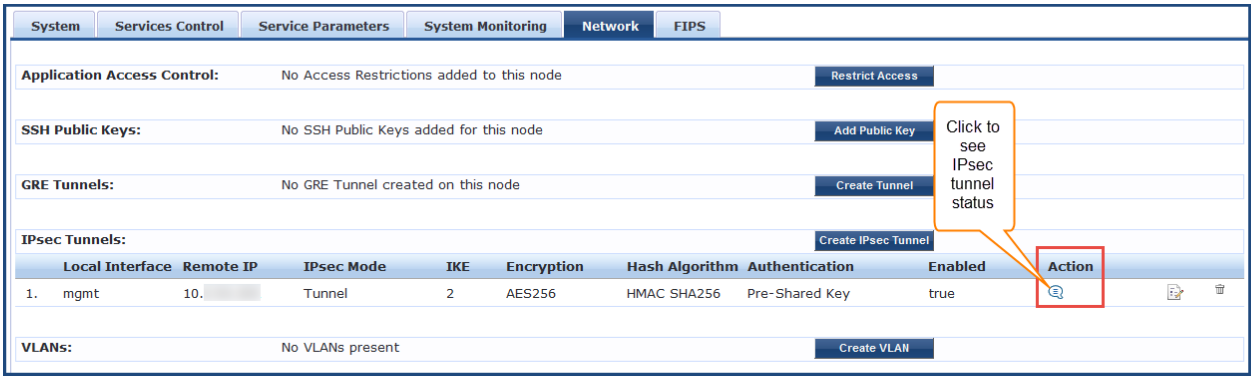
Checking IPsec Tunnel Status

To check the status of an IPsec tunnel:

1. Navigate to the **Server Manager** > **Configuration** > **Network** page.

   The **IPsec Tunnels** section displays the configuration summary for each configured IPsec tunnel, along with an **Action** button to provide each IPsec tunnel's current status.

Figure 508: *IPsec Tunnel Summary and Action Button to See Tunnel Status*



Application Access Control: No Access Restrictions added to this node

SSH Public Keys: No SSH Public Keys added for this node

GRE Tunnels: No GRE Tunnel created on this node

IPsec Tunnels:

	Local Interface	Remote IP	IPsec Mode	IKE	Encryption	Hash Algorithm	Authentication	Enabled	Action
1.	mgmt	10.[redacted]	Tunnel	2	AES256	HMAC SHA256	Pre-Shared Key	true	

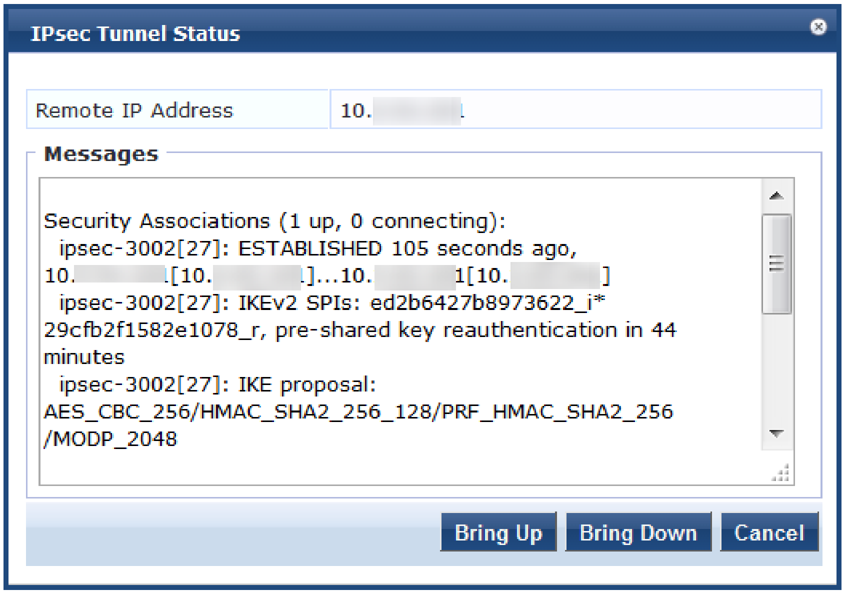
VLANs: No VLANs present

Click to see IPsec tunnel status

2. To see the current status for an IPsec tunnel, click the **Action** button (see Figure 508).

   The **IPsec Tunnel Status** window for the selected tunnel opens:

Figure 509: *IPsec Tunnel Status*



Remote IP Address: 10.[redacted]

Messages

```
Security Associations (1 up, 0 connecting):
  ipsec-3002[27]: ESTABLISHED 105 seconds ago,
10.[redacted][10.[redacted]]...10.[redacted][10.[redacted]]
  ipsec-3002[27]: IKEv2 SPIs: ed2b6427b8973622_i*
29cfb2f1582e1078_r, pre-shared key reauthentication in 44
minutes
  ipsec-3002[27]: IKE proposal:
AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256
/MODP_2048
```

- **Bring Up**

  If the tunnel is down, **Bring Up** brings up the IPsec tunnel. If you select **Bring Up** when the tunnel is up, ClearPass creates a new tunnel.

- **Bring Down**

  If the tunnel is up, **Bring Down** tears down the IPsec tunnel.

  If you select **Bring Down** when the tunnel is down (for example, when the tunnel is still negotiating), ClearPass stops the tunnel from forming.

Understanding the IPsec Tunnel Status Information

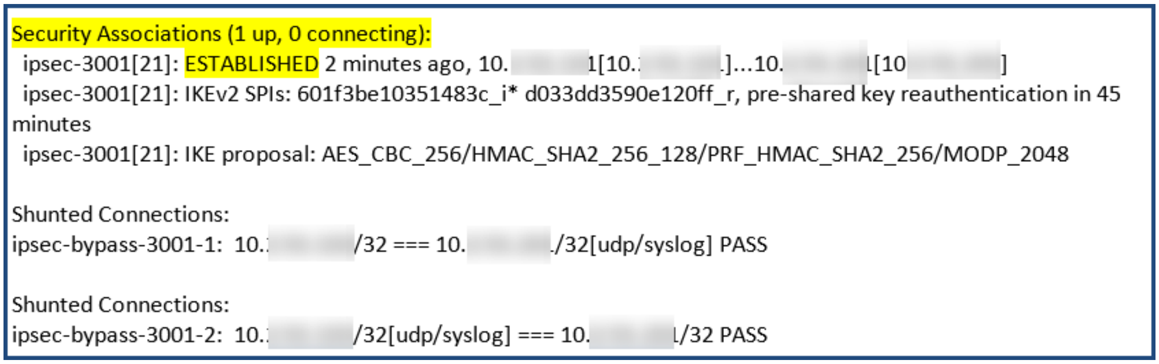
A way to quickly decipher the IPsec tunnel status information is as follows:

- If the tunnel status shows **ESTABLISHED**, only IKE Phase 1 is complete.
- If the tunnel status shows **INSTALLED, Rekeying**, IKE Phase 2 is complete.

Example 1

If tunnel status shows as shown in Figure 510, Phase 1 is complete but Phase 2 is failing. Look at the Audit Viewer events (**Monitoring** > **Audit Viewer**) to find the root cause.

Figure 510: *IPsec Tunnel Status: Only IKE Phase 1 Complete*

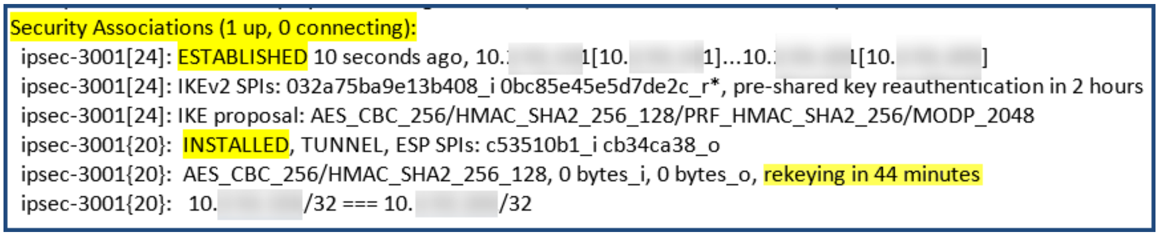


```
Security Associations (1 up, 0 connecting):
  ipsec-3001[21]: ESTABLISHED 2 minutes ago, 10.[redacted][10.[redacted]]...10.[redacted][10[redacted]]
  ipsec-3001[21]: IKEv2 SPIs: 601f3be10351483c_i* d033dd3590e120ff_r, pre-shared key reauthentication in 45
minutes
  ipsec-3001[21]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048

Shunted Connections:
ipsec-bypass-3001-1:  10.[redacted]/32 === 10.[redacted]/32[udp/syslog] PASS

Shunted Connections:
ipsec-bypass-3001-2:  10.[redacted]/32[udp/syslog] === 10.[redacted]/32 PASS
```

Example 2

When the tunnel status displays the information as shown in Figure 511, Phase 2 is also complete.

Figure 511: *IPsec Tunnel Status: IKE Phase 1 and Phase 2 Complete*



```
Security Associations (1 up, 0 connecting):
  ipsec-3001[24]: ESTABLISHED 10 seconds ago, 10.[redacted][10.[redacted]]...10.[redacted][10.[redacted]]
  ipsec-3001[24]: IKEv2 SPIs: 032a75ba9e13b408_i 0bc85e45e5d7de2c_r*, pre-shared key reauthentication in 2 hours
  ipsec-3001[24]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
  ipsec-3001{20}:  INSTALLED, TUNNEL, ESP SPIs: c53510b1_i cb34ca38_o
  ipsec-3001{20}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 44 minutes
  ipsec-3001{20}:   10.[redacted]/32 === 10.[redacted]/32
```

Creating VLANs

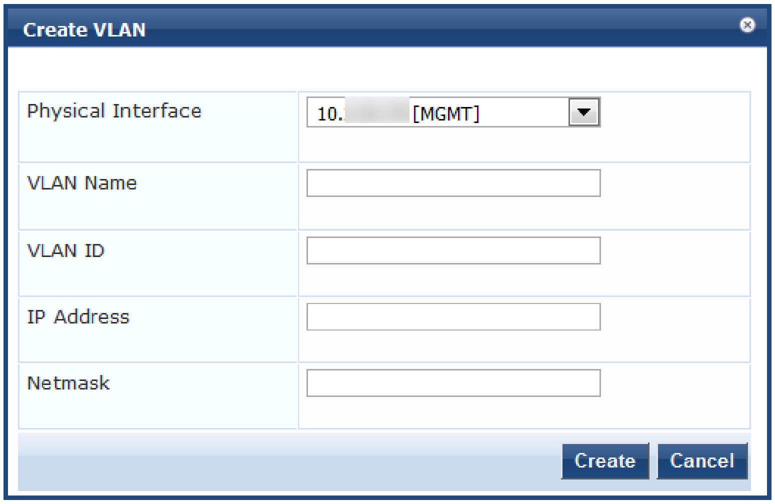
To create VLAN interfaces:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration**.
2. Select the ClearPass server of interest.
3. From the **Server Configuration** page, select the **Network** tab.

   The **Server Configuration** > **Network** page opens.
4. From the **VLANS** option, click **Create VLAN.**

   The **Create VLAN** dialog opens:

Figure 512: *Creating a VLAN*



Create VLAN

Physical Interface	10.[redacted] [MGMT] ▾
VLAN Name	
VLAN ID	
IP Address	
Netmask	

5. Specify the **Create VLAN** parameters as described in the following table, then click **Create**:

Table 278: *Server Configuration > Create VLAN Parameters*

Parameter	Action/Description
Physical Interface	Enter the physical port on which to create the VLAN interface. This is the interface through which the VLAN traffic will be routed. **NOTE:** Make sure your network supports tagged 802.1Q packets on the selected physical interface.
VLAN Name	Enter the name for the VLAN interface. This name is used to identify the VLAN in the list of network interfaces.
VLAN ID	Specify the 802.1Q VLAN identifier. Enter a value between 1 and 4094. The VLAN ID cannot be changed after the VLAN interface has been created. **NOTE: VLAN ID 1** is often reserved for use by network management components. Avoid using this VLAN ID unless you know it will not conflict with a VLAN already defined in your network.
IP Address	Enter the IP address of the VLAN.
Netmask	Enter the netmask for the VLAN.

FIPS Page

This section provides information on using ClearPass Policy Manager in Federal Information Processing Standards (FIPS) 140-2 approved mode.

The U. S. 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 algorithms.

For details on the Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, see:

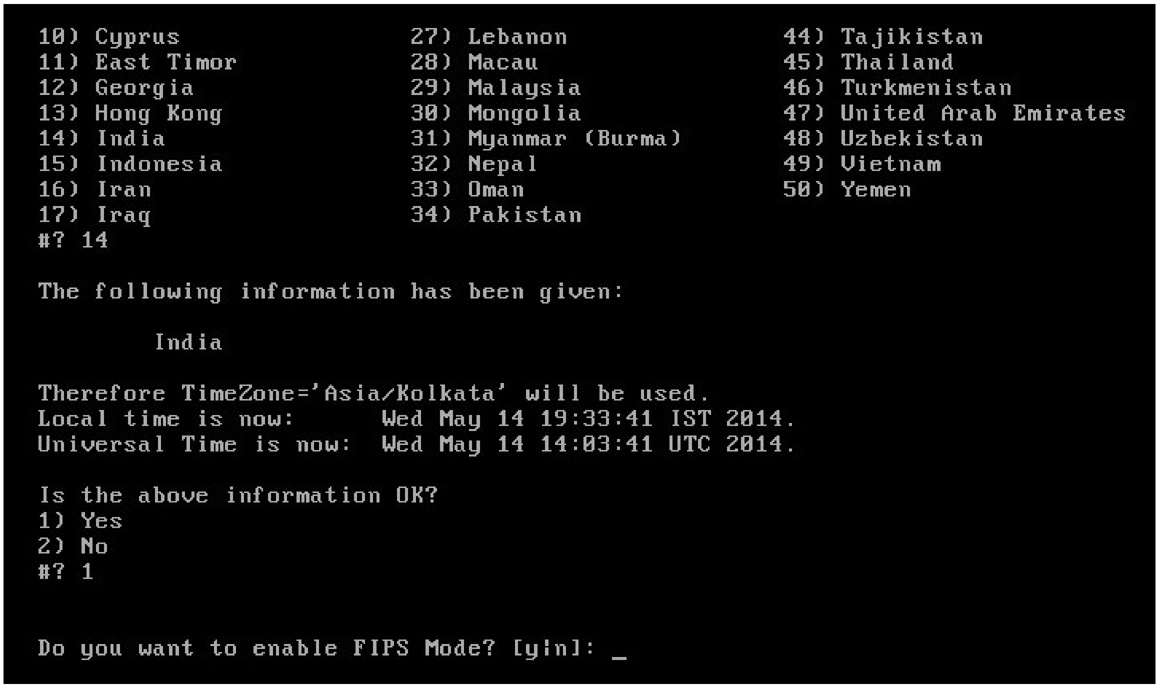
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2577

Enabling FIPS Mode Using CLI

You can enable FIPS mode in ClearPass 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:

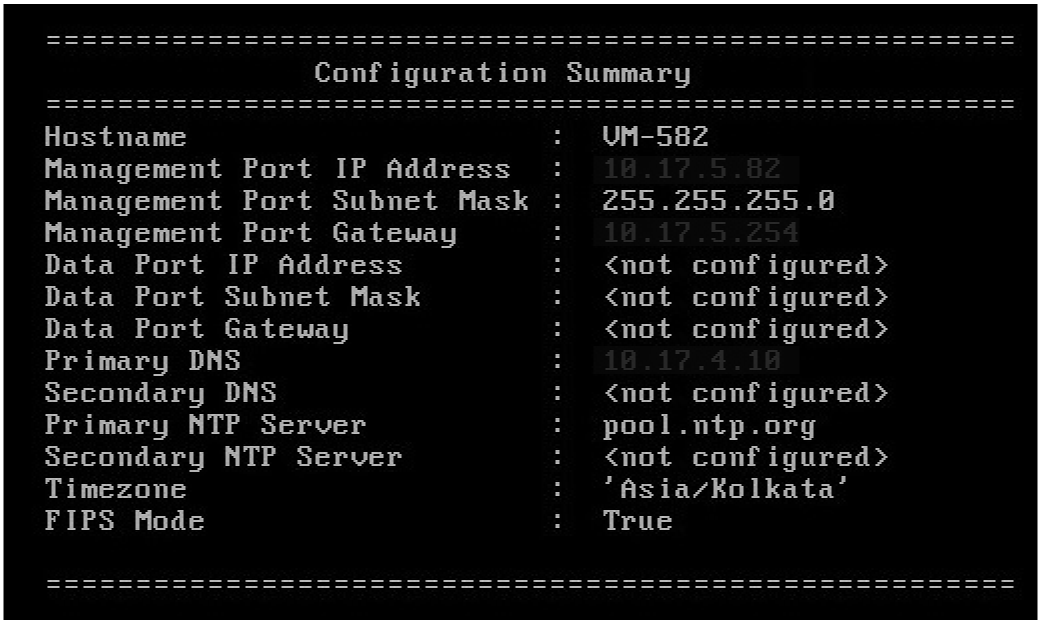
Figure 513: *Enabling FIPS Mode*



```
10) Cyprus                27) Lebanon                44) Tajikistan
11) East Timor            28) Macau                  45) Thailand
12) Georgia               29) Malaysia               46) Turkmenistan
13) Hong Kong             30) Mongolia               47) United Arab Emirates
14) India                 31) Myanmar (Burma)        48) Uzbekistan
15) Indonesia             32) Nepal                  49) Vietnam
16) Iran                  33) Oman                   50) Yemen
17) Iraq                  34) Pakistan
#? 14

The following information has been given:

        India

Therefore TimeZone='Asia/Kolkata' will be used.
Local time is now:      Wed May 14 19:33:41 IST 2014.
Universal Time is now:  Wed May 14 14:03:41 UTC 2014.

Is the above information OK?
1) Yes
2) No
#? 1


Do you want to enable FIPS Mode? [y|n]: _
```

After enabling FIPS mode using the CLI commands, you can verify whether FIPS mode is enabled or not in the **Configuration Summary** page.

Figure 514: *FIPS Mode > Configuration Summary*



```
=====================================================
                  Configuration Summary
=====================================================
Hostname                      :  VM-582
Management Port IP Address    :  [redacted]
Management Port Subnet Mask   :  255.255.255.0
Management Port Gateway       :  [redacted]
Data Port IP Address          :  <not configured>
Data Port Subnet Mask         :  <not configured>
Data Port Gateway             :  <not configured>
Primary DNS                   :  [redacted]
Secondary DNS                 :  <not configured>
Primary NTP Server            :  pool.ntp.org
Secondary NTP Server          :  <not configured>
Timezone                      :  'Asia/Kolkata'
FIPS Mode                     :  True

=====================================================
```

Enabling FIPS Mode in the ClearPass User Interface

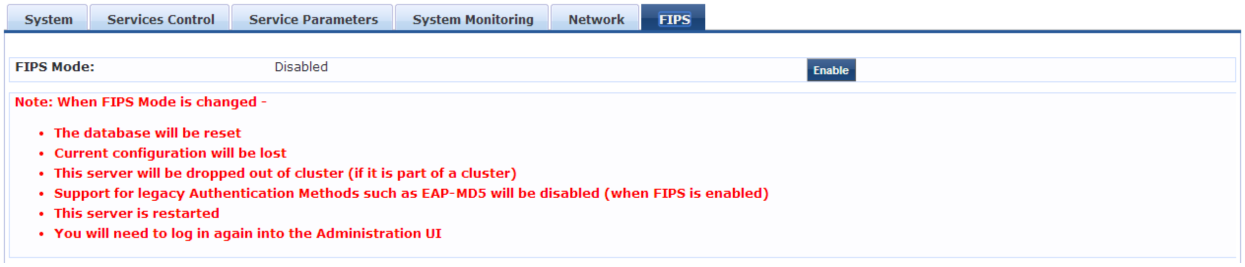
Alternatively, you can enable or disable the FIPS mode in the ClearPass user interface:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.

2. From the **Server Configuration** page, select the server of interest.

   The **Server Configuration** dialog for the selected server opens.
3. Select the **FIPS** tab.

Figure 515: *Server Configuration > FIPS Tab*



FIPS Mode: Disabled

Note: When FIPS Mode is changed -

- The database will be reset
- Current configuration will be lost
- This server will be dropped out of cluster (if it is part of a cluster)
- Support for legacy Authentication Methods such as EAP-MD5 will be disabled (when FIPS is enabled)
- This server is restarted
- You will need to log in again into the Administration UI

Important Points to Remember

Note the following important points, when you enable FIPS mode in the ClearPass Policy Manager user interface:

- The database is reset when you enable the FIPS mode in ClearPass Policy Manager.

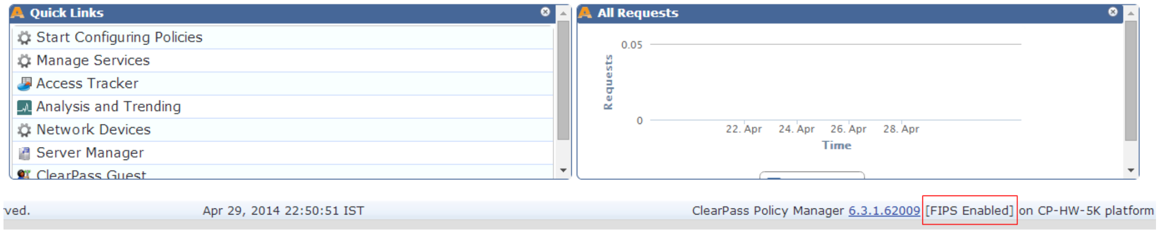
CAUTION

Ensure that you backed up your database before enabling FIPS mode.

- Configuration backup file from the ClearPass Policy Manager in non-FIPS mode cannot be restored on ClearPass Policy Manager in FIPS mode. However, configuration backup file from the ClearPass Policy Manager in FIPS mode can be restored on the 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 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 interface.

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 516: *FIPS Status*



ved. Apr 29, 2014 22:50:51 IST ClearPass Policy Manager 6.3.1.62009 [FIPS Enabled] on CP-HW-5K platform

You can also view the status of the FIPS mode using the CLI commands. For more information, see Show Commands on page 788.

Server Configuration Cluster Options

This section describes the cluster-related options that are available from the **Administration** > **Server Manager** > **Server Configuration** page.

- Setting the Date and Time for the Cluster
- Changing the Cluster-Wide Password
- Managing Policy Manager Zones
- Configuring NetEvents Targets
- Configuring Virtual IP Settings
- Clearing Machine Authentication Cache
- Making a Subscriber Node
- Cluster-Wide Parameters

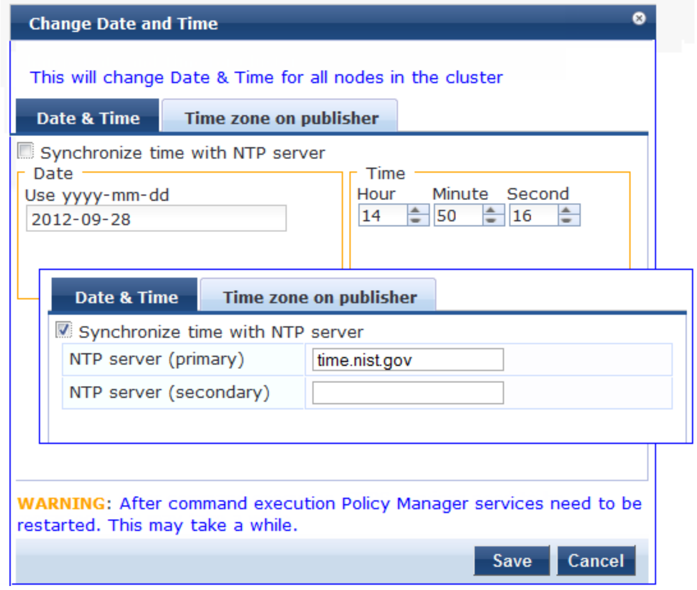
Setting the Date and Time for the Cluster

To set the date and time for all the nodes in a cluster:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Select the **Set Date and Time** link.

   The **Change Date and Time** dialog opens to the **Date & Time** tab.

Figure 517: *Change Date and Time > Date & Time Dialog*



Change Date and Time

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

□ Synchronize time with NTP server

Date

Use yyyy-mm-dd

2012-09-28

Time

Hour	Minute	Second
14	50	16

☑ Synchronize time with NTP server

NTP server (primary)	time.nist.gov
NTP server (secondary)	

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

3. Specify the **Date & Time** parameters as described in the following table, then click **Save**:

Table 279: *Change Date and Time > Date & Time Parameters*

Parameter	Description
Synchronize time with NTP server	To synchronize with a Network Time Protocol (NTP) server, enable this check box (enabled by default). **NOTE:** You can also specify the date and time for the cluster manually by disabling the **Synchronize time with NTP server** check box and entering the current date and time in the dialog provided.
NTP server (primary)	Specify the IP address or host name for the primary NTP server.
NTP server (secondary)	Specify the IP address or host name fore secondary NTP server.

Time Zone on Publisher Tab

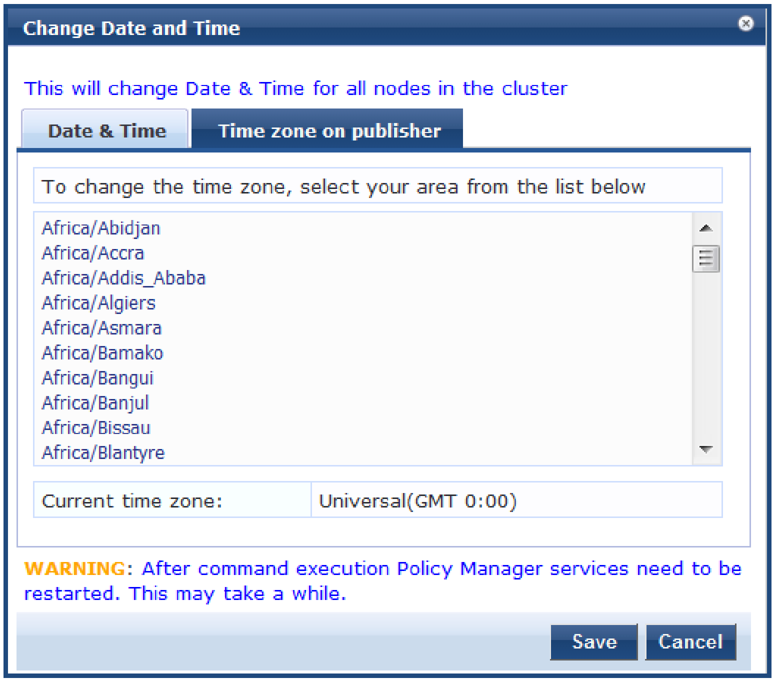
NOTE

This option is available only on the Publisher. To set the time zone on a Subscriber node, select the specific server and set the time zone from the server-specific page.

To specify the time zone on the Publisher node:

1. Click the **Time Zone on Publisher** tab.

Figure 518: *Time Zone on Publisher Dialog*



Change Date and Time

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

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

Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre

Current time zone: Universal(GMT 0:00)

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

The time zones are listed in alphabetical order.

2. Select the time zone where the Publisher node resides, then click **Save**.

Changing the Cluster-Wide Password

To change the cluster-wide password:

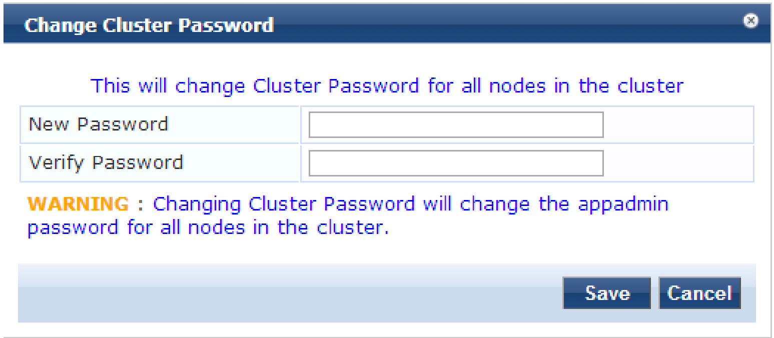
1. Navigate to **Administration > Server Manager > Server Configuration**.

The **Server Configuration** page opens.

2. Click the **Change Cluster Password** link.

   The **Change Cluster Password** dialog opens.

Figure 519: *Change Cluster Password Dialog*



Change Cluster Password

This will change Cluster Password for all nodes in the cluster

New Password	
Verify Password	

WARNING : Changing Cluster Password will change the appadmin password for all nodes in the cluster.

3. Enter the new cluster password, then verify the password.
4. Click **Save**.

NOTE

Changing this password changes the password for the CLI user *appadmin* as well.

Managing Policy Manager Zones

This section provides the following information:

- About Policy Manager Zones
- Adding Policy Manager Zones
- Mapping Policy Manager Zones

About Policy Manager Zones

ClearPass Policy Manager shares a distributed cache of run-time states across all nodes in a cluster. These run-time states include:

- Roles and postures of connected entities
- Connection status of all endpoints running OnGuard
- Endpoint details gathered by OnGuard Agent

ClearPass Policy Manager uses this run-time 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 run-time 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 run-time state to a given geographical area.

You can configure zones in 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 ClearPass Policy Manager nodes that share their run-time state.

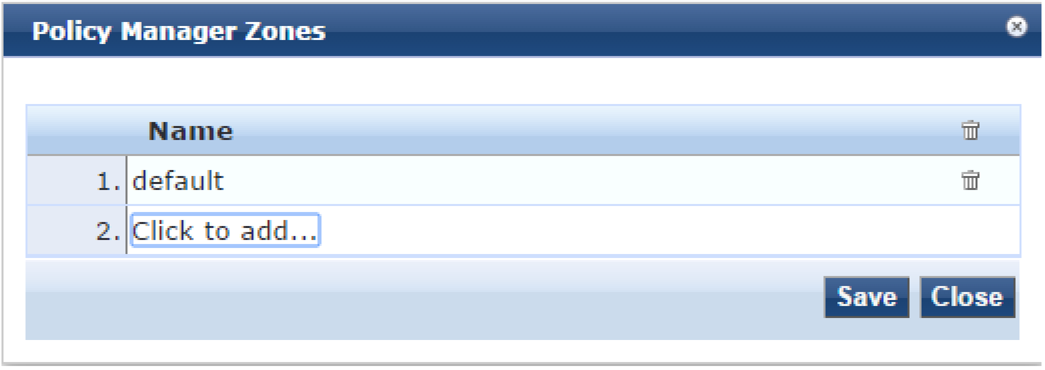
Adding Policy Manager Zones

To add or delete a Policy Manager Zone:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Click the **Manage Policy Manager Zones** link.

   Figure 520 displays the **Policy manager Zones** dialog:

Figure 520: *Policy Manager Zones Dialog*



Policy Manager Zones

	Name
1.	default
2.	Click to add...

3. To add a new Policy Manager Zone, click **Click to add...** and enter the name of the Policy Manager Zone to be added, click the **Save** icon, then click **Save**.
4. To delete a zone, click the trash can icon—🗑.

Mapping Policy Manager Zones

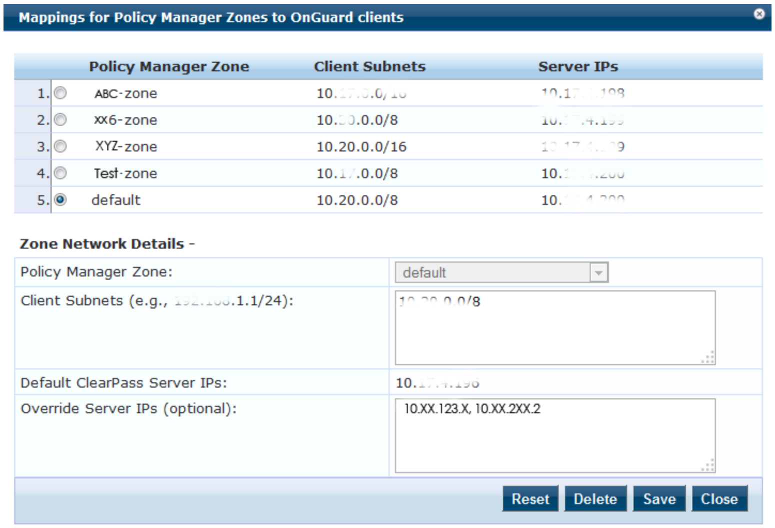
To configure the Policy Manager Zone you created:

1. Navigate to **Administration** > **Agents and Software Updates** > **OnGuard Settings**.

   The **OnGuard Settings** page opens.
2. Click **Policy Manager Zones**.

   The **Mappings for Policy Manager Zones to OnGuard Clients** page opens.

Figure 521: *Mappings for Policy Manager Zones to OnGuard Clients Page*



Mappings for Policy Manager Zones to OnGuard clients

		Policy Manager Zone	Client Subnets	Server IPs
1.	○	ABC-zone	10.17.0.0/16	10.17.4.198
2.	○	xx6-zone	10.30.0.0/8	10.17.4.199
3.	○	XYZ-zone	10.20.0.0/16	10.17.4.199
4.	○	Test-zone	10.17.0.0/8	10.17.4.200
5.	●	default	10.20.0.0/8	10.17.4.200

Zone Network Details -

Policy Manager Zone:	default
Client Subnets (e.g., 192.168.1.1/24):	10.20.0.0/8
Default ClearPass Server IPs:	10.17.4.196
Override Server IPs (optional):	10.XX.123.X, 10.XX.2XX.2

3. Specify the **Mappings for Policy Manager Zones to OnGuard Clients** parameters as described in the following table:

Table 280: *OnGuard Settings > Policy Manager Zones Parameters*

Parameter	Action/Description
Policy Manager Zone	Lists the Policy Manager zones with radial buttons for selection.
Client Subnets	Displays the client subnet addresses specific to the Policy Manager zone.
Server IPs	Displays the server IP addresses specific to the Policy Manager zone.
Zone Network Details	
Policy Manager Zone	1. Select the Policy Manager zone from the drop-down list that are created from the **Administration** > **Server Manager** > **Server Configuration** > **Manage Policy Manager Zones** page. If no Policy Manager zone is configured, the default Policy Manager zone is displayed in this field.
Client Subnets	2. Specify the client subnets that are configured for the selected Policy Manager zone.
Default ClearPass Server IPs	3. Specify the IP address of the default ClearPass server.
Override Server IPs	4. Optionally, specify the IP addresses or the Fully Qualified Domain Name (FQDN) to which you want the OnGuard agent to send request in the sequence. You can specify the data port or load balancer IP address in this field. The IP addresses configured here will override the IP address configured in the **Default ClearPass Server IPs** field. For example, if you have configured the IP addresses 10.17.XXX.1, 10.17.XXX.2, and 10.17.XXX.3, OnGuard agent will send the request in the same sequence.

Configuring NetEvents Targets

NetEvents are a collection of information regarding various 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.

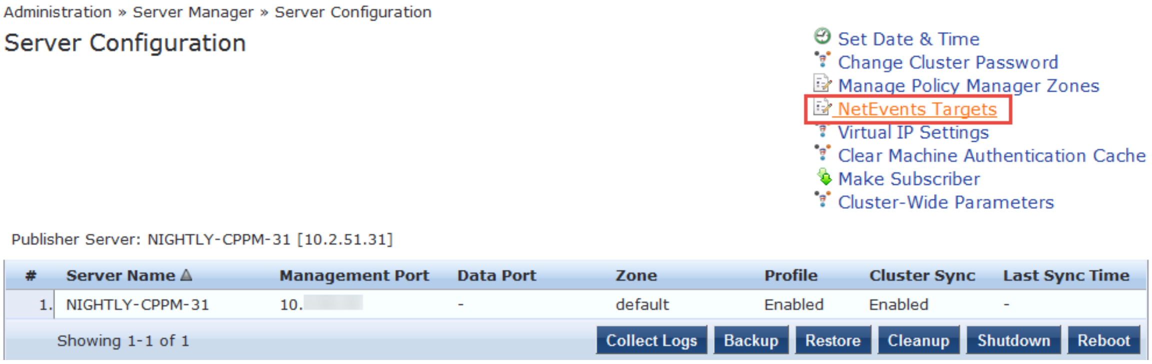
If ClearPass Insight is enabled on a ClearPass Policy Manager server (see Enabling Insight and Specifying a Master Insight Node on page 712), it will receive net events from all other server nodes within the same ClearPass cluster.

If you want to post these details to an external server that can aggregate these events or to an external dedicated ClearPass Insight server for multiple ClearPass clusters, you have to configure an external NetEvents Target.

To configure an external NetEvents Target:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.

Figure 522: *NetEvents Target Link on Server Configuration Page*


Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: NIGHTLY-CPPM-31 [10.2.51.31]

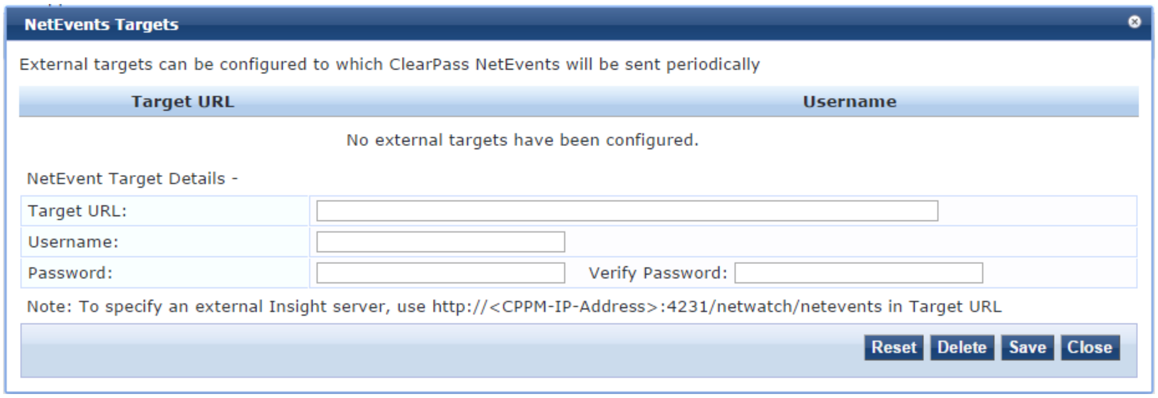
#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	NIGHTLY-CPPM-31	10.[redacted]	-	default	Enabled	Enabled	-

Showing 1-1 of 1

2. Click the **NetEvents Targets** link.

   The **NetEvents Targets** configuration dialog opens.

Figure 523: *NetEvents Targets Configuration Dialog*


NetEvents Targets

External targets can be configured to which ClearPass NetEvents will be sent periodically

Target URL	Username
No external targets have been configured.	

NetEvent Target Details -

Target URL:

Username:

Password: Verify Password:

Note: To specify an external Insight server, use http://<CPPM-IP-Address>:4231/netwatch/netevents in Target URL

3. Specify the **NetEvents Targets** parameters as described in the following table, then click **Save**:

Table 281: *NetEvents Targets Parameters*

Parameter	Action/Description
Target URL	1. Enter the HTTP URL for the service that supports posting to the NetEvents target and requires authentication using username and password. 2. To specify an external Insight server, use the following Target URL: **https://<ClearPass-IP-address>netwatch/netevents**.
Username/Password	3. Enter the ClearPass admin credentials configured for authentication for the HTTP service that is provided in the Target URL.
Reset button	Resets the values entered in this configuration dialog.
Delete button	Deletes the specified Target URL.

Configuring 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.

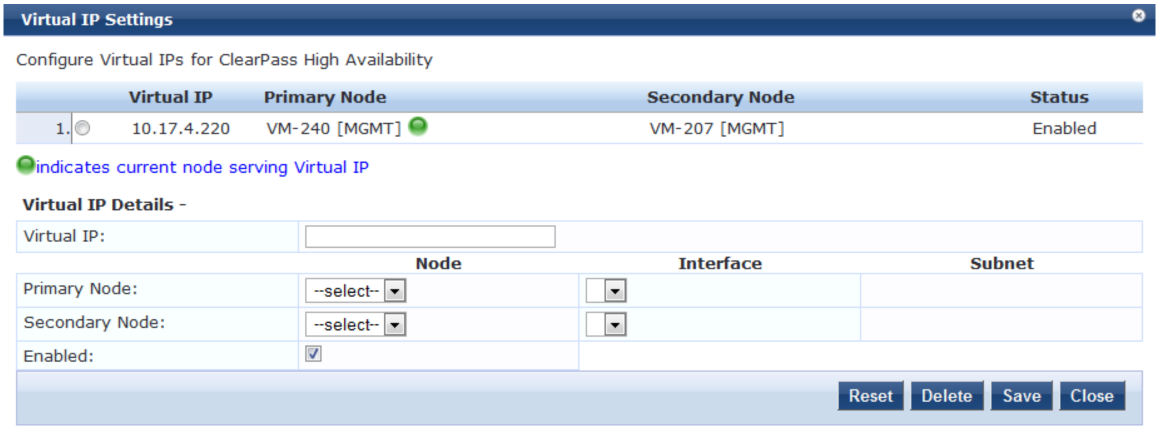
> NOTE
>
> In a virtual machine deployment of ClearPass Policy Manager, you must enable forged transmits on the VMWare distributed virtual switch for the Virtual IP feature to be effective.

To configure a virtual IP address:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Click the **Virtual IP Settings** link.

   The **Virtual IP Settings** dialog opens:

Figure 524: *Virtual IP Settings*



Virtual IP Settings

Configure Virtual IPs for ClearPass High Availability

	Virtual IP	Primary Node	Secondary Node	Status
1. ○	10.17.4.220	VM-240 [MGMT] ●	VM-207 [MGMT]	Enabled

● indicates current node serving Virtual IP

Virtual IP Details -

	Node	Interface	Subnet
Virtual IP:			
Primary Node:	--select--		
Secondary Node:	--select--		
Enabled:	☑		

3. Specify the **Virtual IP Settings** parameters as described in the following table, then click **Save**:

Table 282: *Virtual IP Settings Parameters*

Parameter	Action/Description
Virtual IP	Enter the IP address you want to define as the virtual IP address.
Primary Node	Select the server to use as the primary node.
Secondary Node	Select the server to use as the secondary node.
Interface	When you select the primary node and the secondary node, the **Interface** field is populated with that node's management interface IP address.
Subnet	The **Subnet** value for the management interface IP address is automatically populated when you select the primary node and secondary node.
Enabled	This parameter is enabled by default.

Clearing Machine Authentication Cache

The **Clear Machine Authentication Cache** option clears the machine authentication cache from the local node; this operation is synced during battery replication. On confirmation, machine authentication cache is cleared from all nodes in the cluster.

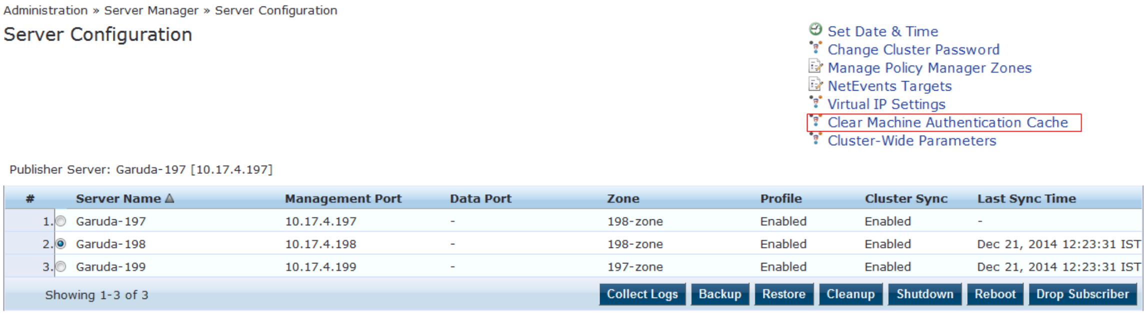
Once the machine authentication cache is cleared, it takes up to 5 seconds to resync the cache.

To clear machine authentication cache on all the nodes in a cluster:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration** page.

   The **Server Configuration** page opens:

Figure 525: *Server Configuration Page > Clear Machine Authentication Cache*



Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: Garuda-197 [10.17.4.197]

#	Server Name △	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1. ○	Garuda-197	10.17.4.197	-	198-zone	Enabled	Enabled	-
2. ●	Garuda-198	10.17.4.198	-	198-zone	Enabled	Enabled	Dec 21, 2014 12:23:31 IST
3. ○	Garuda-199	10.17.4.199	-	197-zone	Enabled	Enabled	Dec 21, 2014 12:23:31 IST

Showing 1-3 of 3

2. Click the **Clear Machine Authentication Cache** link.

   The following prompt is displayed:

   Are you sure you want to clear machine authentication cache?

3. To proceed with the operation, click **Yes**.

   The following message appears:
   Machine authentication cache cleared from all nodes

Making a Subscriber Node

In the Policy Manager cluster environment, the Publisher node acts as the master node. A Policy Manager cluster can contain only one Publisher node. Administration, configuration, and database write operations can occur only on the Publisher 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, the **Make Subscriber** link is not displayed.

Note the following caveats when adding a Subscriber node:

- As part of this operation, configuration changes are blocked on the Publisher node during the initial cluster sync process.
- All the application licenses on this server will be removed. To add and reactivate these application licenses, contact Support—navigate to **Administration** > **Support** > **Contact Support** for contact information.

To add a Subscriber node:

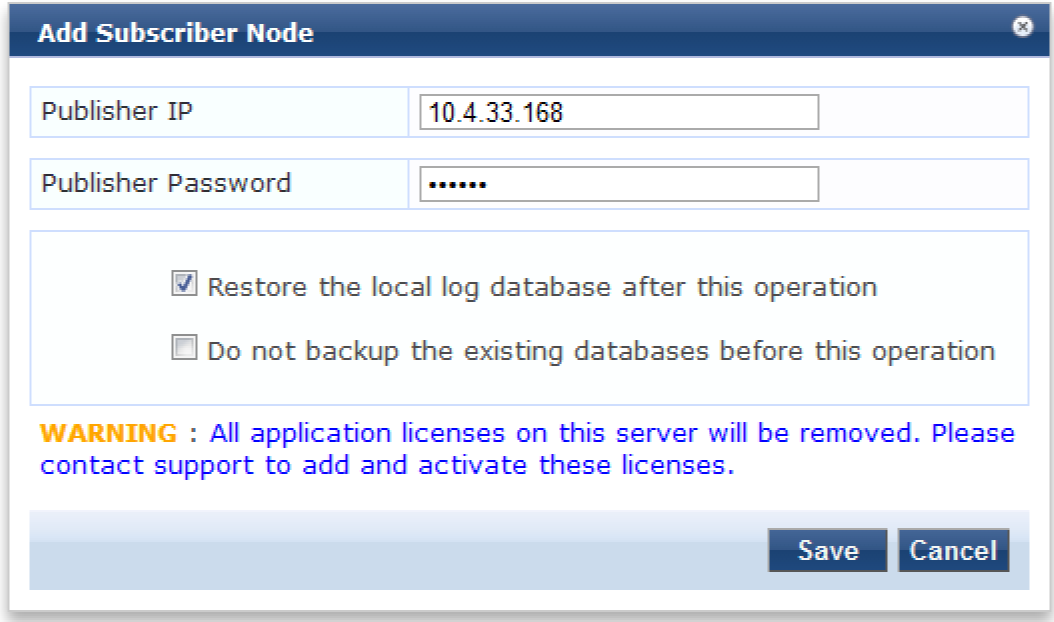
1. On a Publisher node, navigate to the **Administration > Server Manager > Server Configuration** page.

   The **Server Configuration** page opens.

2. Click the **Make Subscriber** link.

   The **Add Subscriber Node** page opens:

Figure 526: *Adding a Subscriber Node*



Publisher IP: 10.4.33.168

Publisher Password: ••••••

☑ Restore the local log database after this operation

☐ Do not backup the existing databases before this operation

WARNING : All application licenses on this server will be removed. Please contact support to add and activate these licenses.

3. Specify the **Add Subscriber Node** parameters as described in the following table, then click **Save**:

Table 283: *Add Subscriber Node Parameters*

Parameter	Action/Description
Publisher IP	Enter the Publisher node's IP address.
Publisher Password	Specify the Publisher node's password. **NOTE:** The password specified here is the password for the CLI user *appadmin*.
Restore the local log database after this operation	To restore the log database after the Subscriber node has been added, select the check box.
Do not backup the existing databases before this operation	If you do not require a backup to the existing databases on this node, select the check box.

Cluster-Wide Parameters

This section describes the following **Cluster-Wide Parameters** features:

- General Parameters
- Cleanup Intervals Parameters
- Notifications Parameters
- Standby Publisher Parameters
- Virtual IP Parameters
- Mode Parameters
- Database Parameters
- Profiler Parameters

General Parameters

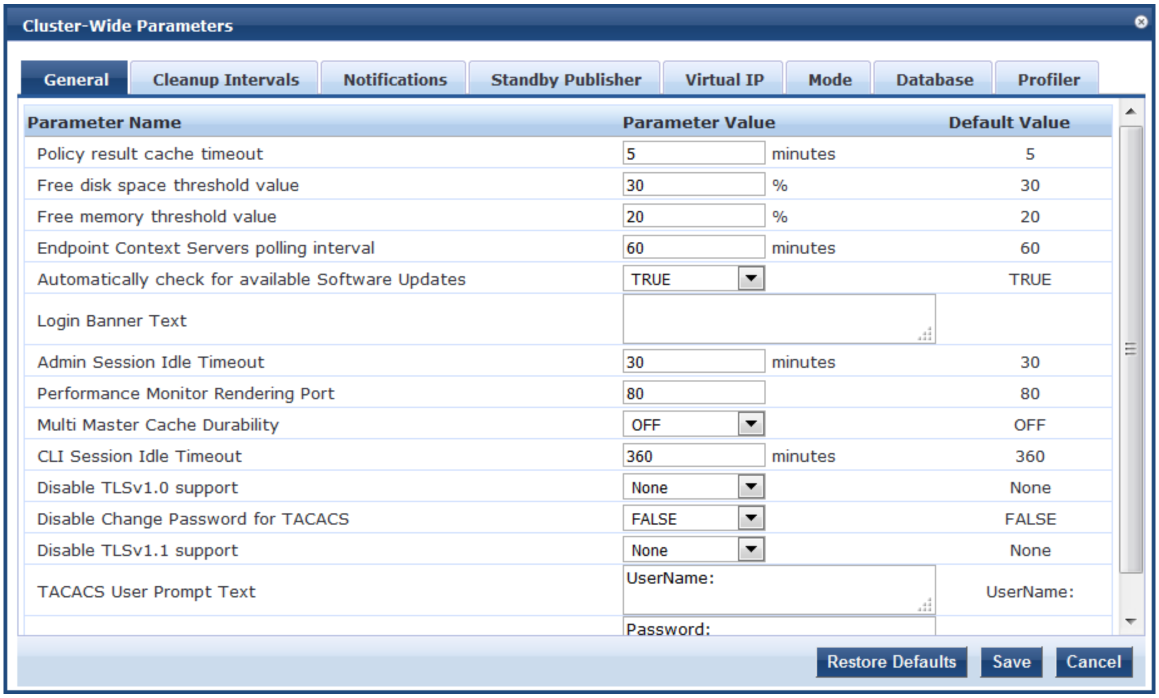
You can configure the parameters that apply to all the nodes in a ClearPass cluster by configuring the **Cluster-Wide Parameters**.

To configure Cluster-Wide parameters:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration** page.
2. Select the **Cluster-Wide Parameters** link.

   The **Cluster-Wide Parameters** page opens to the **General** page:

Figure 527: *Cluster-Wide Parameters > General Page*



Parameter Name	Parameter Value		Default Value
Policy result cache timeout	5	minutes	5
Free disk space threshold value	30	%	30
Free memory threshold value	20	%	20
Endpoint Context Servers polling interval	60	minutes	60
Automatically check for available Software Updates	TRUE		TRUE
Login Banner Text			
Admin Session Idle Timeout	30	minutes	30
Performance Monitor Rendering Port	80		80
Multi Master Cache Durability	OFF		OFF
CLI Session Idle Timeout	360	minutes	360
Disable TLSv1.0 support	None		None
Disable Change Password for TACACS	FALSE		FALSE
Disable TLSv1.1 support	None		None
TACACS User Prompt Text	UserName:		UserName:
	Password:		

3. Configure the **Cluster-Wide Parameters** > **General** parameters as described in the following table, then click **Save**.

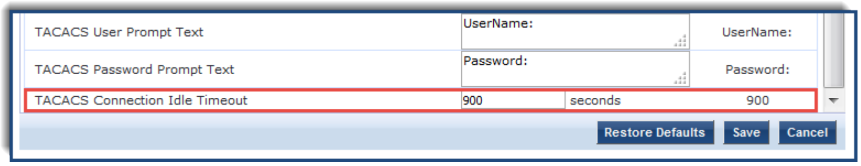
Table 284: *Cluster-Wide Parameters > General Page Parameters*

Parameter	Action/Description
Policy result cache timeout	Specify the duration allowed in minutes to store the role mapping and posture results derived by the policy engine during a policy evaluation. A value of **0** disables caching. 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. **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	Specify 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. An error message similar to the following may appear in the **System Event Details** dialog: *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	Specify the percentage below which RAM usage warnings are issued in the ClearPass Event Viewer. For example, a value of **30** indicates that a warning is issued only when the available RAM is 30% or lower.
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	Specify whether to enable automatic checking for available software updates. The default it **TRUE**.
Login Banner Text	Customize the banner text that appears on the ClearPass login screen and CLI access window.
Admin Session Idle Timeout	Specify the maximum idle time permitted for admin users, beyond which the session times out. The default value is **30 minutes**. The allowed range is **5** to **1440** minutes (24 hours).

Table 284: *Cluster-Wide Parameters > General Page Parameters (Continued)*

Parameter	Action/Description
Performance Monitor Rendering Port	Specify the port for performance monitor rendering. The default value is **80**.
Multi Master Cache Durability	For the Multi-Master Cache to survive most abrupt shutdowns, set this to **Normal** or **Full**. The default value is **OFF**. **NOTE:** Enabling this feature may result in some performance degradation.
CLI Session Idle Timeout	Specify the maximum idle time permitted for CLI users, beyond which the session times out. The default value is **30 minutes**. The allowed range is **5** to **1440** minutes (24 hours). When this parameter is changed, the changes take effect when the client opens a new CLI session. Any active CLI sessions will continue to use the old timeout setting—they have to be disconnected and reconnected for the updated timeout value to take effect.
Disable TLSv1.0 support	To disable Transport Layer Security (TLS) v1.0 support, select one of the following options: ● None ● Admin ● Network ● All
Disable Change Password for TACACS	When logging in for TACACS user authentication: ● If set to **FALSE** (the default setting), after entering a blank password, you are presented with an option to change the TACACS user password. ● If set to **TRUE**, the option to enter the TACACS user password is displayed. The option to change the TACACS password is **not** displayed.

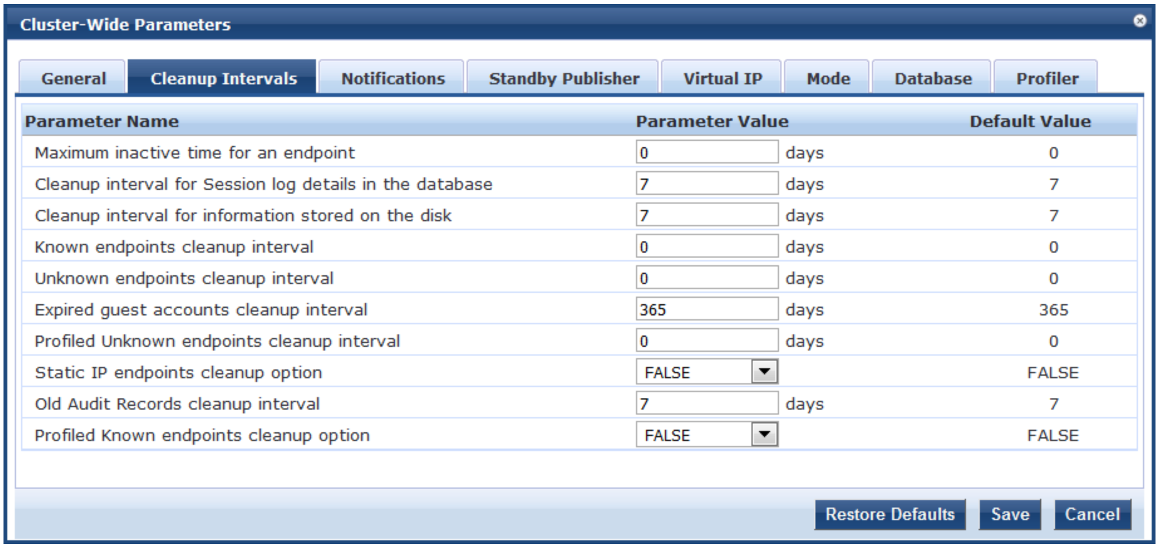
Table 284: *Cluster-Wide Parameters > General Page Parameters (Continued)*

Parameter	Action/Description
Disable TLSv1.0 support	To disable Transport Layer Security (TLS) v1.1 support, select one of the following options: ● None ● Admin ● Network ● All
TACACS User Prompt Text TACACS Password Prompt Text	You can modify the text to be used for the TACACS username and password prompts as needed. The default TACACS prompts are as follows: *UserName:* *Password*:
TACACS Connection Idle Timeout	An idle TACACS login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. To close idle sessions automatically, you must configure a time limit for each login class. Specify the TACACS Connection Idle Timeout duration in seconds as needed. ● The default value is **900 seconds** (15 minutes). ● The minimum allowed value is **60 seconds**. ● The maximum allowed value is **172800 seconds** (two days).  TACACS User Prompt Text UserName: UserName: TACACS Password Prompt Text Password: Password: TACACS Connection Idle Timeout 900 seconds 900

Cleanup Intervals Parameters

The following figure displays the **Cluster-Wide Parameters** > **Cleanup Intervals** dialog:

Figure 528: *Cluster-Wide Parameters > Cleanup Intervals Dialog*



Parameter Name	Parameter Value		Default Value
Maximum inactive time for an endpoint	0	days	0
Cleanup interval for Session log details in the database	7	days	7
Cleanup interval for information stored on the disk	7	days	7
Known endpoints cleanup interval	0	days	0
Unknown endpoints cleanup interval	0	days	0
Expired guest accounts cleanup interval	365	days	365
Profiled Unknown endpoints cleanup interval	0	days	0
Static IP endpoints cleanup option	FALSE		FALSE
Old Audit Records cleanup interval	7	days	7
Profiled Known endpoints cleanup option	FALSE		FALSE

1. Specify the **Cluster-Wide Parameters** > **Cleanup Intervals** parameters as described in the following table:

Table 285: *Cluster-Wide Parameters > Cleanup Intervals Parameters*

Parameter	Action/Description
Maximum inactive time for an endpoint	Specify the duration in number of days to which an endpoint is retained in the endpoints table since its last authentication. A value of **0** specifies that no time limit is configured. If the endpoint is not authenticated for this period, the entry is removed from the endpoint table.
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 database: ● Session logs (found on the **Monitoring** > **Live Monitoring** > **Access Tracker** page) ● Event logs (found on the **Monitoring** > **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 day**s. 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. A value of **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**.

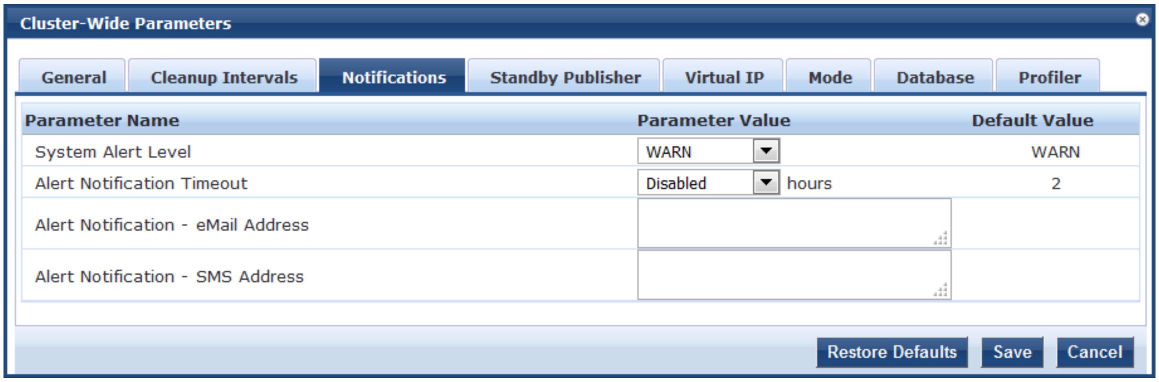
Table 285: *Cluster-Wide Parameters > Cleanup Intervals Parameters (Continued)*

Parameter	Action/Description
Static IP endpoints cleanup option	Specify whether to enable the option to cleanup static IP endpoints. The default option 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 Parameters

The following figure displays the **Cluster-Wide Parameters** > **Notifications** dialog:

Figure 529: *Cluster-Wide Parameters > Notifications Dialog*



Parameter Name	Parameter Value	Default Value
System Alert Level	WARN	WARN
Alert Notification Timeout	Disabled hours	2
Alert Notification - eMail Address		
Alert Notification - SMS Address		

1. Specify the **Cluster-Wide Parameters > Notifications** parameters as described in the following table:

Table 286: *Cluster-Wide Parameters > Notifications Parameters*

Parameter	Action/Description
System Alert Level	Specify the alert notifications that are generated for system events logged at this level or higher. ● **INFO**: Alerts that provide Information, Warnings, and Error messages are generated. ● **WARN**: Alerts that provide Warnings and Error messages are generated. ● **ERROR**: Alerts that provide Error messages only are generated. ● The default value is **WARN**.
Alert Notification Timeout	Specify the timeout in hours that determines how often alert messages are generated and distributed. If you select **Disabled**, alert generation is disabled. The default value is **2 hours**.
Alert Notification - eMail Address	Enter a comma-separated list of email addresses to which alert messages are sent.

Table 286: *Cluster-Wide Parameters > Notifications Parameters (Continued)*

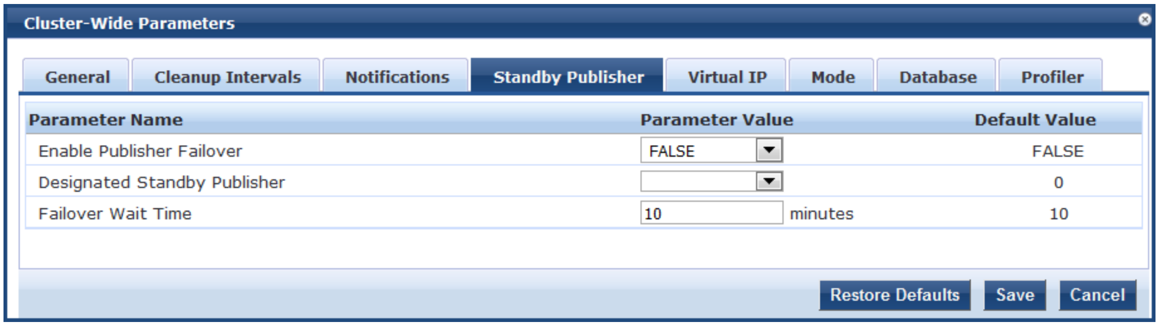
Parameter	Action/Description
Alert Notification - SMS Address	Enter a comma-separated list of phone numbers to which alert messages are sent.

Standby Publisher Parameters

The Standby Publisher is the Publisher node in the cluster that is configured to come up in the event that the Publisher node goes down.

The following figure displays the **Cluster-Wide Parameters** > **Standby Publisher** dialog:

Figure 530: *Cluster-Wide Parameters > Standby Publisher Dialog*



Parameter Name	Parameter Value	Default Value
Enable Publisher Failover	FALSE	FALSE
Designated Standby Publisher		0
Failover Wait Time	10 minutes	10

1. Specify the **Cluster-Wide Parameters** > **Standby Publisher** parameters as described in the following table:

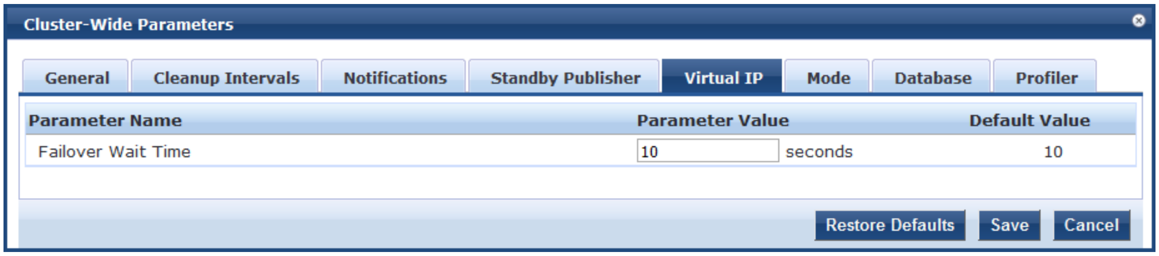
Table 287: *Cluster-Wide Parameters > Standby Publisher Parameters*

Parameter	Action/Description
Enable Publisher Failover	To authorize a node in a cluster on the system to act as a publisher if the primary publisher fails, select **TRUE**. 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 subnets is available to avoid unwanted network segmentation and potential data loss from a false failover.
Failover Wait Time	Specify the time (in minutes) for which the secondary node must wait before it acquires a virtual IP address after the primary node fails. The default failover wait time is **10 minutes**. This prevents the secondary node from taking over when the primary node is temporarily unavailable during a restart.

Virtual IP Parameters

The following figure displays the **Cluster-Wide Parameters** > **Virtual IP** dialog:

Figure 531: *Cluster-Wide Parameters > Virtual IP Dialog*



Parameter Name	Parameter Value		Default Value
Failover Wait Time	10	seconds	10

1. Specify the **Cluster-Wide Parameters > Virtual IP** parameter as described in the following table:

Table 288: *Cluster-Wide Parameters > Virtual IP Configuration Parameter*

Parameter	Action/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 fail-over wait time is 10 seconds in order for the secondary node to take over and respond quickly to authentication access requests.

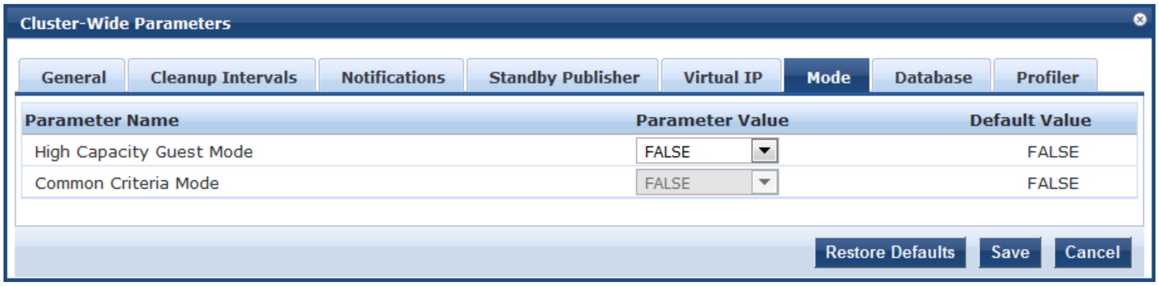
NOTE

You can define a virtual IP address with a primary server only (that is, without a secondary server) if required. This can be used to add an additional IP address to the ClearPass Policy Manager server without introducing any redundancy.

Mode Parameters

The **Mode** tab in the **Cluster-Wide Parameters** page allows you to enable or disable High Capacity Guest **Mode** and **Common Criteria Mode**.

Figure 532: *Cluster-Wide Parameters Page*



Parameter Name	Parameter Value	Default Value
High Capacity Guest Mode	FALSE	FALSE
Common Criteria Mode	FALSE	FALSE

1. Specify the **Cluster-Wide Parameters > Mode** parameters as described in the following table:

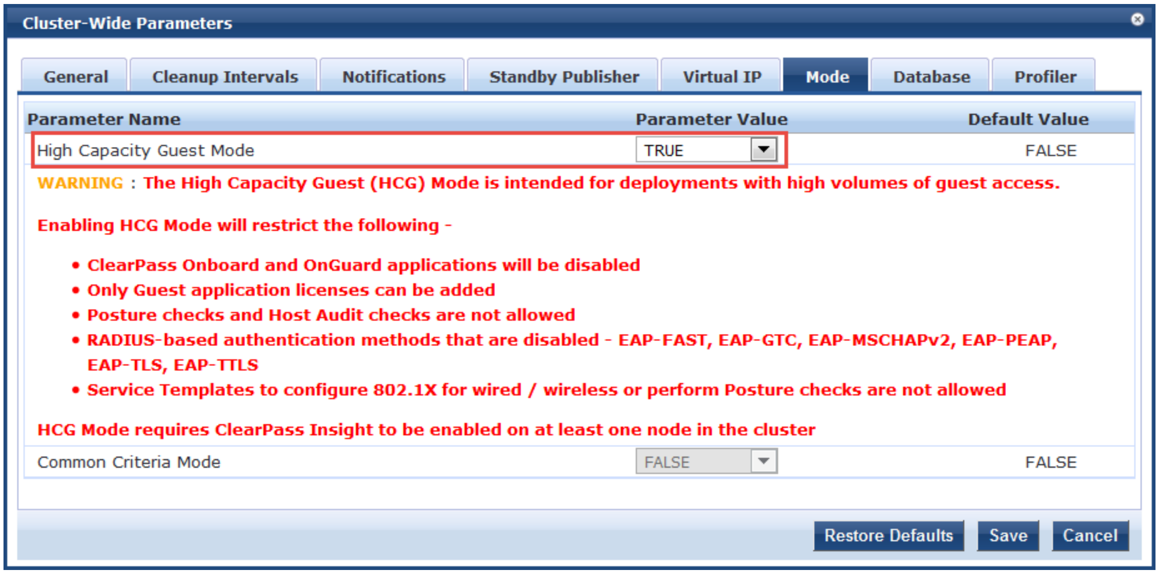
Table 289: *Cluster-Wide Parameters > Mode Parameter*

Parameter	Action/Description
High Capacity Guest Mode	To enable or disable **High Capacity Guest Mode**, select **TRUE** or **FALSE**. The default is **FALSE**.
Common Criteria Mode	**Common Criteria Mode** is for specific deployments that require strict compliance to Common Criteria requirements. To enable or disable **Common Criteria Mode**, select **TRUE** or **FALSE**. The default is **FALSE**. When you set **Common Criteria Mode** to **TRUE**, the following Warning message is displayed: **WARNING:** Setting this value to TRUE enables strict validation of Certificates and changes to modules to comply to Common Criteria requirements.

High Capacity Guest Mode

High Capacity Guest mode addresses the high-volume licensing requirements in the public-facing enterprises environment, where a large volume of unique endpoints need wireless access.

Figure 533: *High Capacity Guest Mode Page*



Parameter Name	Parameter Value	Default Value
High Capacity Guest Mode	TRUE	FALSE

WARNING : The High Capacity Guest (HCG) Mode is intended for deployments with high volumes of guest access.

Enabling HCG Mode will restrict the following -

- ClearPass Onboard and OnGuard applications will be disabled
- Only Guest application licenses can be added
- Posture checks and Host Audit checks are not allowed
- RADIUS-based authentication methods that are disabled - EAP-FAST, EAP-GTC, EAP-MSCHAPv2, EAP-PEAP, EAP-TLS, EAP-TTLS
- Service Templates to configure 802.1X for wired / wireless or perform Posture checks are not allowed

HCG Mode requires ClearPass Insight to be enabled on at least one node in the cluster

Parameter Name	Parameter Value	Default Value
Common Criteria Mode	FALSE	FALSE

The licensing scheme in High Capacity Guest mode supports a high volume of user traffic in the following public-facing enterprises where the number of endpoints changes every day:

- **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, ClearPass Policy Manager licensing accumulates the unique endpoint count for seven days, which can cause the number of licenses to exceed their limit.

To address this license limit in the public-facing enterprises environment, you can enable High Capacity Guest mode on a cluster.

In High Capacity Guest mode, the count of unique endpoints is reset every day, instead of accumulating the count for seven days. In High Capacity Guest mode, only you can view the supported guest authentication methods supported in the **Authentication Methods** page.

RADIUS Authentication Methods That Cannot Be Enabled

When **High Capacity Guest** mode is enabled, you *cannot* enable the RADIUS services with the following authentication methods:

- EAP-FAST
- EAP-GTC
- EAP-MSCHAPv2
- EAP-PEAP
- EAP-TLS
- EAP-TTLS

Licensing Restrictions

You can add only guest licenses to High Capacity Guest mode. This mode is intended to handle only a high volume of guest users in PFE environments. After enabling 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 High Capacity Guest mode, a maximum of 2x licenses are allowed. For example, if you use the CP-HW-5K platform (which supports 5,000 licenses), a maximum of 10,000 licenses are allowed.

Cluster Restrictions

When 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 High Capacity Guest mode.
- Restoring configuration is allowed only with the backup files from servers that have High Capacity Guest mode enabled.
- High Capacity Guest mode is intended only for high volumes of guest access.
- Use-case-related settings other than those for High Capacity Guest mode are restricted.
- OnGuard and Onboard access is restricted.
- The default cleanup interval values are reset.
- Only Guest application licenses are supported.

Insight Requirement

High Capacity Guest mode requires ClearPass Insight to be enabled on at least one node in the cluster.

1. Specify the default cleanup interval values when High Capacity Guest mode is enabled as described in the following table:

Table 290: *Cleanup Interval Values in High Capacity Guest Mode*

Parameter	Action/Description
Cleanup interval for Session log details in the database	The default value is **3days**.
Known endpoints cleanup interval	The default value of the known endpoints cleanup interval is **3days**.
Unknown endpoints cleanup interval	The default value of the unknown endpoints cleanup interval is **3days**.
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**.

Service Templates Supported in High Capacity Guest Mode

The following service templates are supported when High Capacity Guest 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

Service Types Supported in High Capacity Guest Mode

The following service types are supported when High Capacity Guest mode is enabled:

- MAC Authentication
- RADIUS Authorization
- RADIUS Enforcement
- RADIUS Proxy
- Aruba Application Authentication
- Aruba Application Authorization
- TACACS+ Enforcement
- Web-based Authentication

- Web-based Open Network Access

Authentication Methods Supported in High Capacity Guest Mode

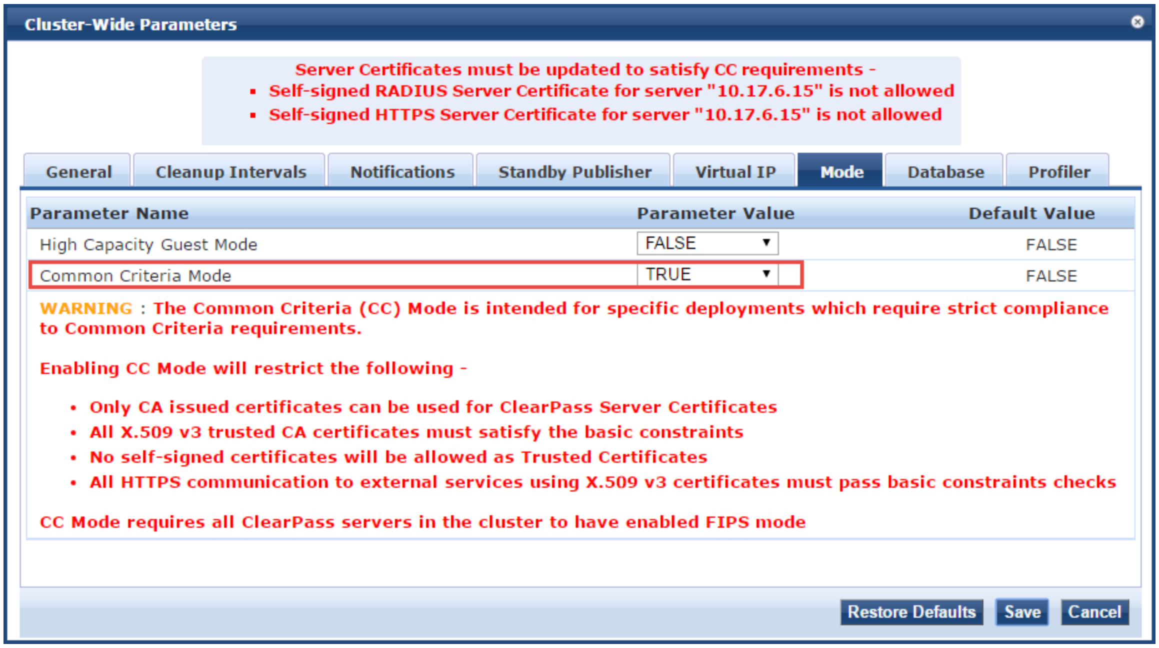
The following authentication methods are used in service templates in High Capacity Guest mode:

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

Common Criteria Mode

Use Common Criteria Mode for deployments that require strict compliance to Common Criteria requirements. Common Criteria is an international standard for security certification.

Figure 534: *Cluster-Wide Parameters > Mode > Common Criteria Mode Page*



Server Certificates must be updated to satisfy CC requirements -

- Self-signed RADIUS Server Certificate for server "10.17.6.15" is not allowed
- Self-signed HTTPS Server Certificate for server "10.17.6.15" is not allowed

Parameter Name	Parameter Value	Default Value
High Capacity Guest Mode	FALSE	FALSE
Common Criteria Mode	TRUE	FALSE

WARNING : The Common Criteria (CC) Mode is intended for specific deployments which require strict compliance to Common Criteria requirements.

Enabling CC Mode will restrict the following -

- Only CA issued certificates can be used for ClearPass Server Certificates
- All X.509 v3 trusted CA certificates must satisfy the basic constraints
- No self-signed certificates will be allowed as Trusted Certificates
- All HTTPS communication to external services using X.509 v3 certificates must pass basic constraints checks

CC Mode requires all ClearPass servers in the cluster to have enabled FIPS mode

Common Criteria Mode has the following restrictions and requirements:

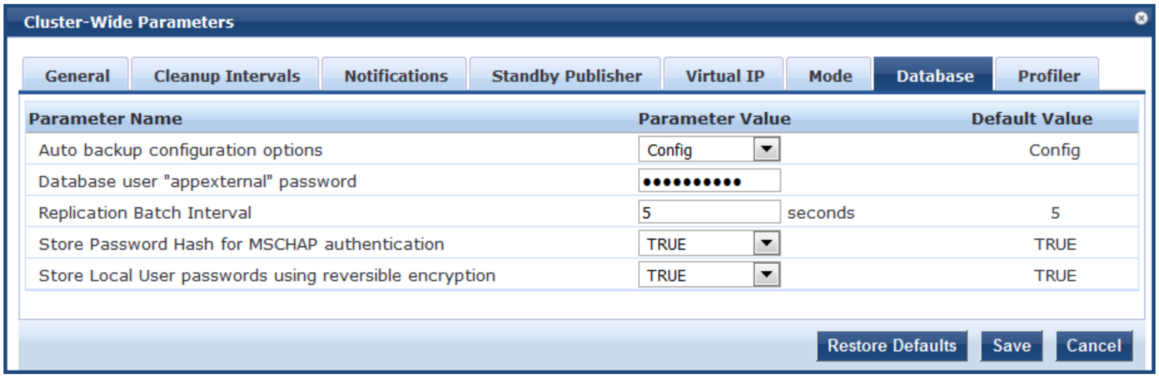
- Common Criteria Mode requires that all the ClearPass servers in the cluster must have FIPS mode enabled.
- Server certificates must be updated before you enable Common Criteria Mode .
- Only CA-issued certificates can be used for ClearPass server certificates.
- No self-signed certificates are allowed as trusted certificates.
- All X.509 v3 trusted CA certificates must satisfy the basic constraints.

  X.509 is an important standard for a public key infrastructure to manage digital certificates and public-key encryption. X.509 is a key part of the Transport Layer Security protocol used to secure web and email communication.
- All HTTPS communication to external services using X.509 v3 certificates must pass the basic constraint checks.

Database Parameters

The following figure displays the **Cluster-Wide Parameters** > **Database** dialog:

Figure 535: *Cluster-Wide Parameters > Database Dialog*



Parameter Name	Parameter Value		Default Value
Auto backup configuration options	Config		Config
Database user "appexternal" password	••••••••••		
Replication Batch Interval	5	seconds	5
Store Password Hash for MSCHAP authentication	TRUE		TRUE
Store Local User passwords using reversible encryption	TRUE		TRUE

1. Configure the **Cluster-Wide Parameters** > **Database** parameters as described in the following table:

Table 291: *Cluster-Wide Parameters > Database Parameters*

Parameter	Action/Description
Auto backup configuration options	Select any of the following auto-backup configuration options: ● **Off**: Select this to not to perform periodic backups. ● Select **Off** before upgrading 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 can 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 (in seconds) at which the subscribers synchronize with the Publisher. The default value is **5 seconds**. The allowed range is 1 to 60 seconds.

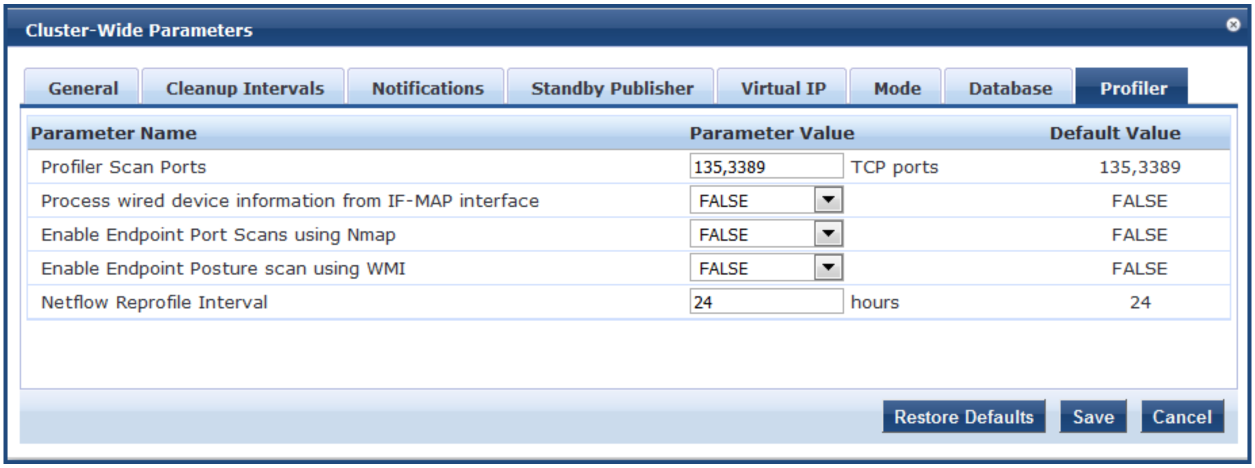
Table 291: *Cluster-Wide Parameters > Database Parameters (Continued)*

Parameter	Action/Description
Store Password Hash for MSCHAP authentication	To store passwords for admin and local users to Hash and NTLM hash formats (which enables RADIUS MSCHAP authentications against admin or local repositories), set this to **TRUE**. If you set this to **FALSE**, RADIUS MSCHAP authentications are not possible because the NTLM hash passwords are removed for all the users. **NOTE:** When you set this value to **TRUE**, you must reset all the passwords to reenable RADIUS MSCHAP authentication against the user repositories.
Store Local User Passwords using reversible encryption	To enable cleartext password comparison against local users, set this to **TRUE**. If you set this to **FALSE**, cleartext password comparison against local users is not possible because the reversible passwords for local users are removed. **NOTE:** After setting this value to **TRUE**, you must reset all the local user passwords to reenable cleartext password comparison against local users.

Profiler Parameters

The following figure displays the **Cluster-Wide Parameters** > **Profiler** dialog:

Figure 536: *Cluster-Wide Parameters > Profiler Dialog*



Cluster-Wide Parameters

Parameter Name	Parameter Value		Default Value
Profiler Scan Ports	135,3389	TCP ports	135,3389
Process wired device information from IF-MAP interface	FALSE		FALSE
Enable Endpoint Port Scans using Nmap	FALSE		FALSE
Enable Endpoint Posture scan using WMI	FALSE		FALSE
Netflow Reprofile Interval	24	hours	24

1. Configure the **Cluster-Wide Parameters** > **Profiler** parameters as described in the following table:

Table 292: *Cluster-Wide Parameters > Profiler Tab Parameters*

Parameter	Action/Description
Profiler Scan Ports	To change the list of ports to scan and add custom fingerprints to classify based on them, enter the new TCP port numbers. The TCP ports scanner checks to see if the specified Profiler Scan Ports are open. The default TCP ports are **135** and **3389**.
Process wired device information from IF-MAP interface	Choose whether to process wired device information from the IF-MAP interface. The default is **FALSE**.
Enable Endpoint Port Scans using Nmap	Set this option to **TRUE** to enable Endpoint scans using Nmap (Network Mapper). **NOTE:** The Open Ports scanner is disabled when Nmap-based port scanning is enabled. When Nmap scan is enabled, the following warning is displayed: **WARNING**: Setting this value to **TRUE** enables active scan of the host for open ports. This can be resource intensive. Also, the **Profiler Scan Ports** value is ignored when Nmap scan is enabled.
Enable Endpoint Port Scans using WMI	Set this option to **TRUE** to enable Endpoint scans using WMI (Windows Management Instrumentation).
Netflow Reprofile Interval	Specify the interval after which endpoints will be reprofiled. The default value is 24 hours. The minimum value is one hour.

Collecting 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 (see Downloading Local Shared Folders on page 551).

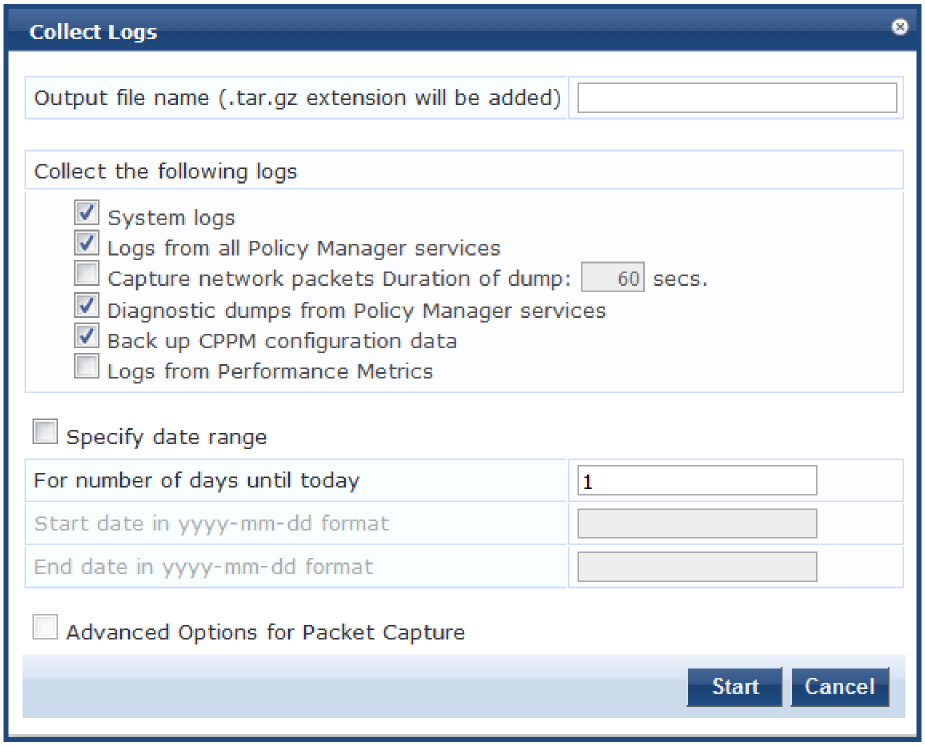
To collect logs:

1. Navigate to **Administration > Server Manager > Server Configuration**.

   The **Server Configuration** page opens.
2. Click **Collect Logs**.

   The **Collect Logs** dialog opens.

Figure 537: *Collect Logs Dialog*



Collect Logs

Output file name (.tar.gz extension will be added)	

Collect the following logs

- ☑ System logs
- ☑ Logs from all Policy Manager services
- ☐ Capture network packets Duration of dump: 60 secs.
- ☑ Diagnostic dumps from Policy Manager services
- ☑ Back up CPPM configuration data
- ☐ Logs from Performance Metrics

☐ Specify date range

For number of days until today	1
Start date in yyyy-mm-dd format	
End date in yyyy-mm-dd format	

☐ Advanced Options for Packet Capture

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 in seconds.

CAUTION

Use this option only when you want to debug a problem. System performance can be severely impacted.

   - Diagnostic dumps from Policy Manager services
   - Back up Policy Manager 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.
   - To collect logs for the specified time period, select the **Specify date range** check box and enter a start date and end date in yyyy-mm-dd format in the respective fields.
6. Click **Start**.

   You'll see the progress of the information collection.
7. To finish, click **Close**
8. To save the log file to your computer, click **Download File**.

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.

Backing Up the Policy Manager Database

The backup file is automatically placed in the *Shared Local Folder* under folder type *Backup Files* (for details, see Downloading Local Shared Folders).

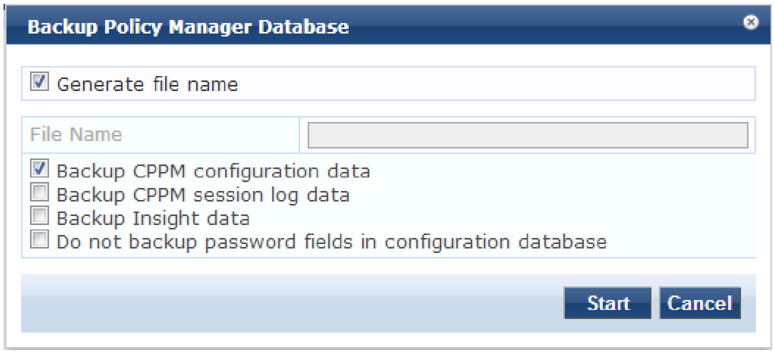
Backup files are in the gzipped tar format (tar.gz extension).

To back up the Policy Manager database:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Click the **Back Up** button.

   The **Back up Policy Manager Database** dialog opens:

Figure 538: *Backup Policy Manager Database Dialog*



Backup Policy Manager Database

☑ Generate file name

File Name

☑ Backup CPPM configuration data
☐ Backup CPPM session log data
☐ Backup Insight data
☐ Do not backup password fields in configuration database

3. Specify the **Back up Policy Manager Database** parameters as described in the following table, then click **Start**:

Table 293: *Back up Policy Manager Database Parameters*

Parameter	Action/Description
Generate file name	To enable Policy Manager to generate a file name for the database backup, select this check box. This option is enabled by default.
File Name	To manually specify the backup file name, click this check box, then enter the desired file name.
Backup CPPM configuration data	The option to back up Policy Manager configuration data is enabled by default.
Backup CPPM session log data	To enable back up of Policy Manager session log data, select this check box.
Backup Insight data	To enable back up of ClearPass Insight data, select this check box.
Do not backup password fields in configuration database	If you don't want to backup the password fields in the configuration database, select this check box.

Restoring Policy Manager Configuration Data

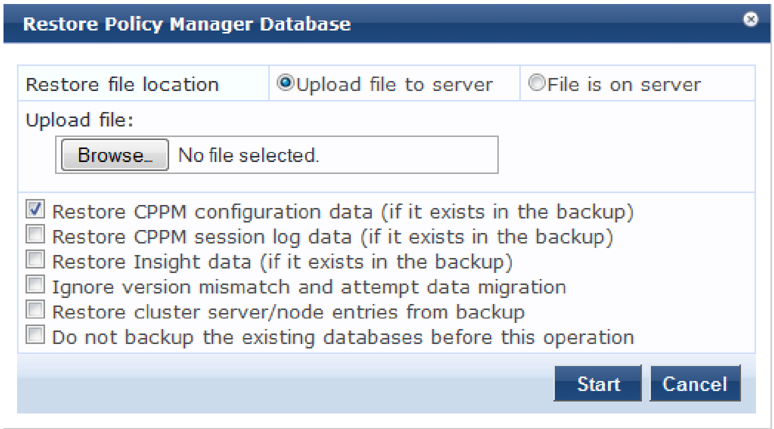
To restore the ClearPass Policy Manager configuration data:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.

2. Click the **Restore** button.

   The **Restore Policy Manager Database** dialog opens:

Figure 539: *Restore Policy Manager Database Dialog*



Restore Policy Manager Database

Restore file location ● Upload file to server ○ File is on server

Upload file:

Browse... No file selected.

☑ Restore CPPM configuration data (if it exists in the backup)
☐ Restore CPPM session log data (if it exists in the backup)
☐ Restore Insight data (if it exists in the backup)
☐ Ignore version mismatch and attempt data migration
☐ Restore cluster server/node entries from backup
☐ Do not backup the existing databases before this operation

3. Specify the **Restore Policy Manager Database** parameters as described in the following table, then click **Start**:

Table 294: *Restore Policy Manager Database*

Parameter	Action/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 Downloading 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.

Parameter	Action/Description
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.

Performing a System Cleanup

You can perform a system cleanup operation to purge the following records:

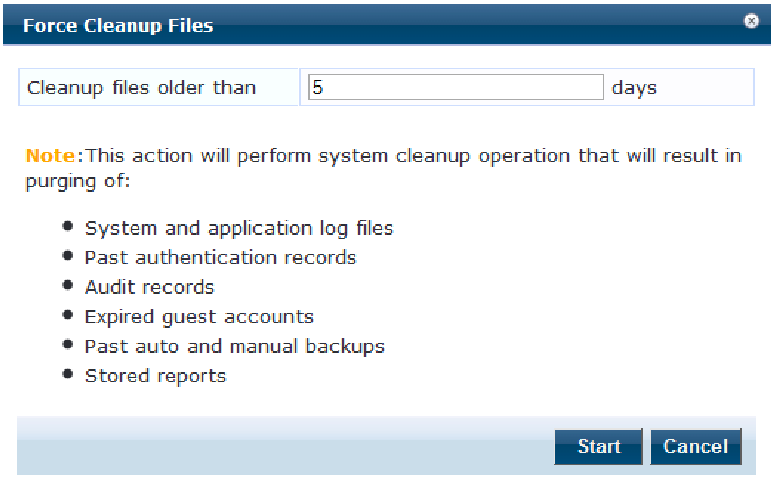
- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

To perform a system cleanup:

1. Navigate to the **Administration** > **Server Manager** > **Server Configuration** page.
2. Click the **Cleanup** button.

   The **Force Cleanup Files** dialog opens.

Figure 540: *Force Cleanup Files Dialog*



Force Cleanup Files

Cleanup files older than	5	days

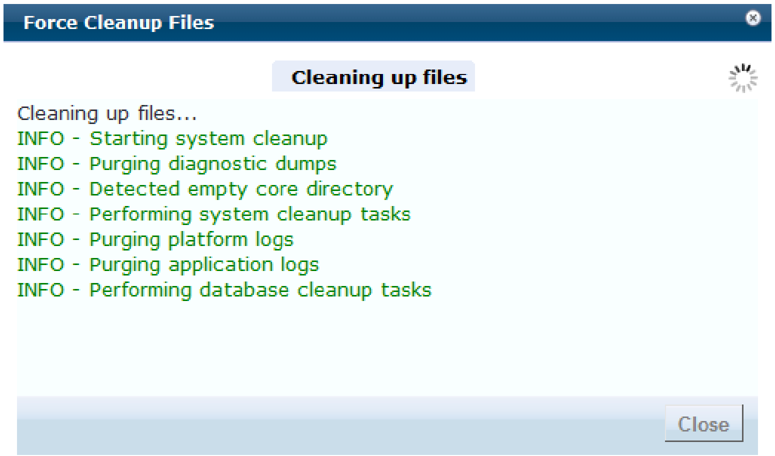
Note:This action will perform system cleanup operation that will result in purging of:

- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

3. Enter the number of days system files can remain before they are removed. The allowed range is 0 to 15 days.
4. To initiate the cleanup process, click **Start**.

   The **Force Cleanup Files** status report opens:

Figure 541: *Force Cleanup Files Status Report*



```
Cleaning up files...
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
```

Shutting Down or Rebooting the Server

To shut down the current ClearPass server:

1. Navigate to the **Administration > Server Manager > Server Configuration** page .
2. Click the **Shutdown** button.

To reboot the current ClearPass server:

1. Navigate to the **Administration > Server Manager > Server Configuration** page .
2. Click the **Reboot** button.

Dropping a Subscriber Node

To drop a Subscribe node from the cluster:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Select the node you want to drop from the cluster.
3. Click the **Drop Subscriber** button.

NOTE

This option is not available in a single-node deployment.

Log Configuration

To configure logs for services and system level, navigate to the **Administration > Server Manager > Log Configuration** page.

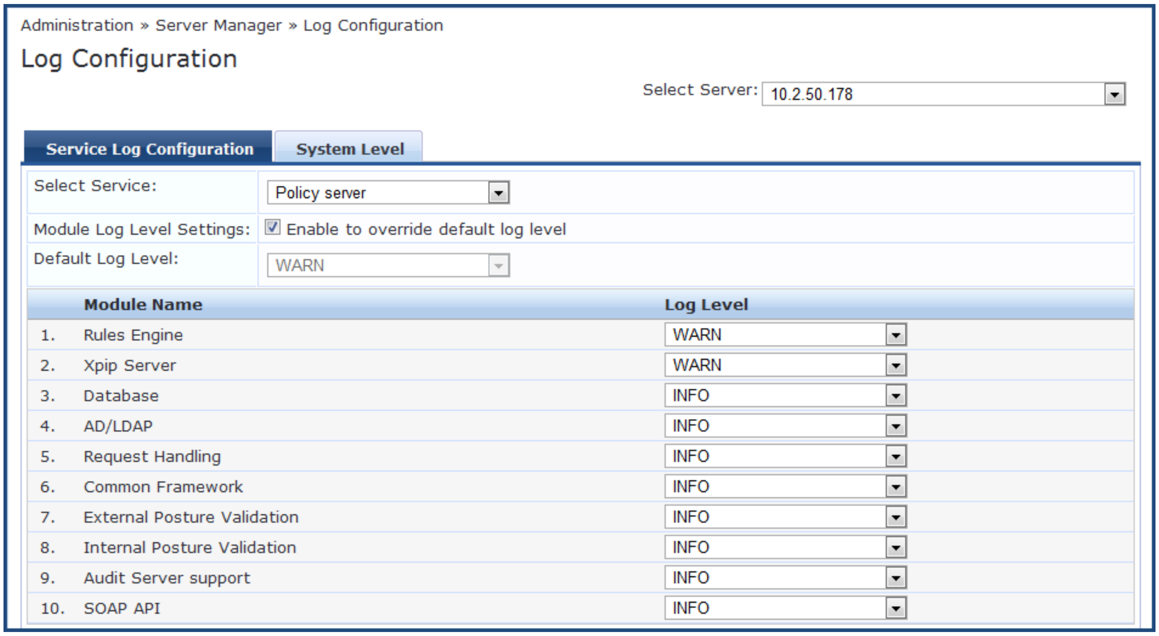
This section provides the following information:

- Service Log Configuration
- System Level Configuration

Service Log Configuration

The following figure displays the **Service Log Configuration** dialog:

Figure 542: *Log Configuration > Service Log Configuration Tab*



Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 10.2.50.178

Select Service:	Policy server
Module Log Level Settings:	☑ Enable to override default log level
Default Log Level:	WARN

	Module Name	Log Level
1.	Rules Engine	WARN
2.	Xpip Server	WARN
3.	Database	INFO
4.	AD/LDAP	INFO
5.	Request Handling	INFO
6.	Common Framework	INFO
7.	External Posture Validation	INFO
8.	Internal Posture Validation	INFO
9.	Audit Server support	INFO
10.	SOAP API	INFO

The following table describes the **Service Log Configuration** parameters:

Table 295: *Log Configuration > Service Log Configuration Parameters*

Parameter	Action/Description
Select Server	1. From the **Select Server** drop-down, specify the server for which you want to configure logs. All nodes in the cluster appear in the drop-down list.
Select Service	2. Specify the service for which you want to configure logs.
Module Log Level Settings	3. Select the **Module Log Level Settings** 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 the 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	4. Specify the default logging level for all modules. The **Default Log Level** drop-down list is available if the **Module Log Level Settings** option is disabled. Available options include the following: ■ DEBUG ■ INFO

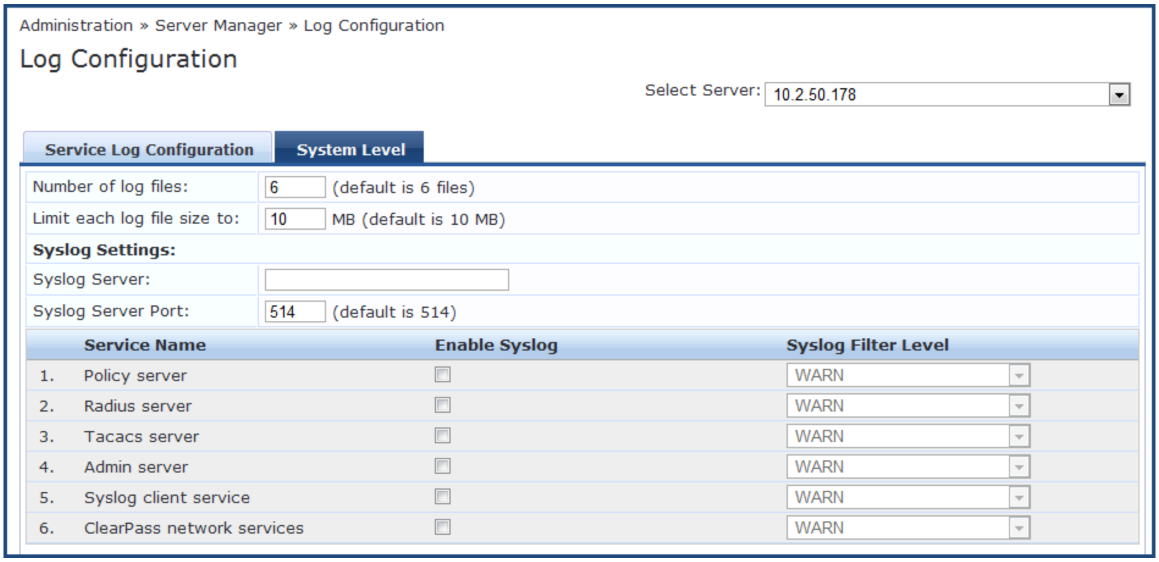
Table 295: *Log Configuration > Service Log Configuration Parameters (Continued)*

Parameter	Action/Description
	■ WARN ■ ERROR ■ FATAL **NOTE:** Set this option first, and then override any specific modules as necessary.
Restore Defaults/Save	5. Click **Save** to save changes. ■ To restore the default settings, click **Restore Defaults**.

System Level Configuration

The following figure displays the **System Level** dialog:

Figure 543: *Log Configuration - System Level tab*



Administration » Server Manager » Log Configuration

Log Configuration

Select Server: 10.2.50.178

Number of log files:	6	(default is 6 files)
Limit each log file size to:	10	MB (default is 10 MB)
Syslog Settings:		
Syslog Server:		
Syslog Server Port:	514	(default is 514)

	Service Name	Enable Syslog	Syslog Filter Level
1.	Policy server	□	WARN
2.	Radius server	□	WARN
3.	Tacacs server	□	WARN
4.	Admin server	□	WARN
5.	Syslog client service	□	WARN
6.	ClearPass network services	□	WARN

The following table describes the **System Level** tab parameters:

Table 296: *Log Configuration > System Level Parameters*

Parameter	Action/Description
Select Server	1. Specify the server for which you want to configure logs.
Number of log files	2. 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 L**imit each log file size to**), 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	3. Specify the size of each log file before the log rolls over to the next file. The default value is 50 MB.

Table 296: *Log Configuration > System Level Parameters (Continued)*

Parameter	Action/Description
Syslog Settings	
Syslog Server	4. Specify the name of the syslog server. Policy Manager sends the configured module logs to this syslog server.
Syslog Server Port	5. Specify the syslog server port number. The default is **514**.
Enable Syslog	6. To override the **Syslog Filter Level** for a service, select the **Enable Syslog** check box.
Syslog Filter Level	7. If desired, change 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	8. Click **Save** to save your changes. ▪ To restore the default settings, click **Restore Defaults**.

Downloading Local Shared Folders

The supported ClearPass folder types are:

- **Backup files**: Database backup files that are backed up manually.
- **Log files**: Log files backed up via the method described in Collecting Logs on page 543.
- **Automated Backup files**: Database backup files that are backed up automatically on a daily basis.

To download a local shared folder:

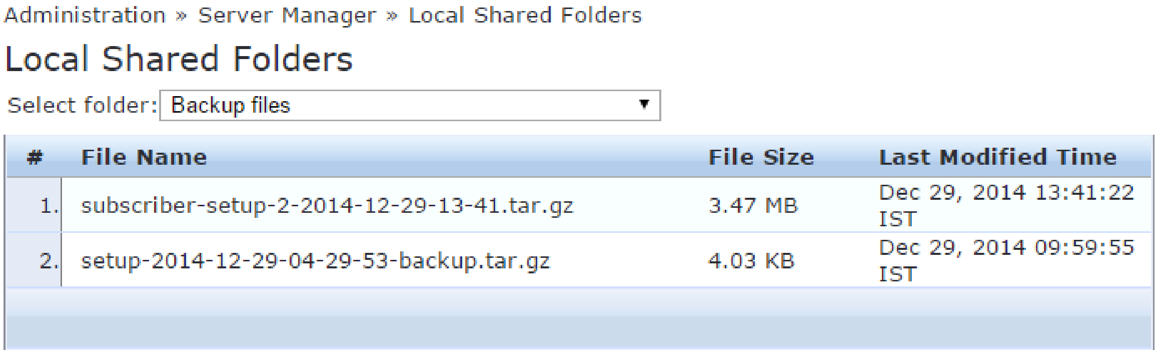
1. Navigate to **Administration > Server Manager > Local Shared Folders**.

   The **Local Shared Folders** page opens.

2. Choose a folder type from the **Select folder** drop-down list.

   The folders in the selected shared folder are displayed.

Figure 544: *Local Shared Folders Page*



Administration » Server Manager » Local Shared Folders

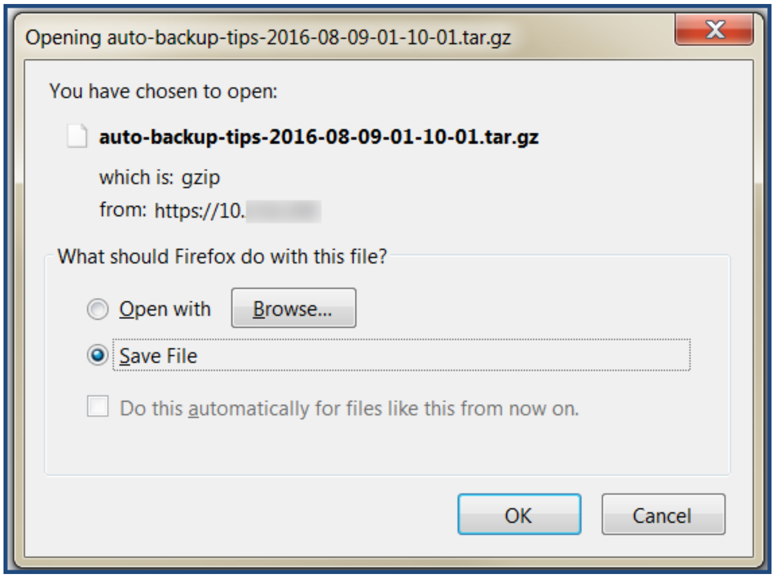
Local Shared Folders

Select folder: Backup files

#	File Name	File Size	Last Modified Time
1.	subscriber-setup-2-2014-12-29-13-41.tar.gz	3.47 MB	Dec 29, 2014 13:41:22 IST
2.	setup-2014-12-29-04-29-53-backup.tar.gz	4.03 KB	Dec 29, 2014 09:59:55 IST

3. Select the folder you want to download.

   The following dialog opens:



Opening auto-backup-tips-2016-08-09-01-10-01.tar.gz

You have chosen to open:

auto-backup-tips-2016-08-09-01-10-01.tar.gz

which is: gzip

from: https://10.[redacted]

What should Firefox do with this file?

○ Open with [Browse...]

● Save File

□ Do this automatically for files like this from now on.

4. You can either browse to an application to open the selected folder or save the tar.gz file to your hard disk:
   a. To open the folder, click **Browse**, select the application to open the tar.gz file, then click **OK**.
   b. To save the file, select **Save File**, then click **OK**.

      The file is downloaded to your system.

License Management

This section describes the following topics:

- Licensing Page on page 552
- Adding an Application License on page 553
- Activating a Server License on page 554
- Activating an Application License on page 555
- Updating a Server License on page 556
- Updating an Application License on page 557

The **Licensing** page shows all the licenses that are activated for the entire ClearPass Policy Manager cluster. You must have a 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 average.

NOTE

On a virtual machine instance of ClearPass, the permanent license must be entered.

Licensing Page

To manage licenses, navigate to **Administration > Server Manager > Licensing**.

The **Licensing** page opens to the **License Summary** tab:

NOTE

The **Applications** tab gets activated on adding an application license such as OnGuard, Guest, or Onboard.

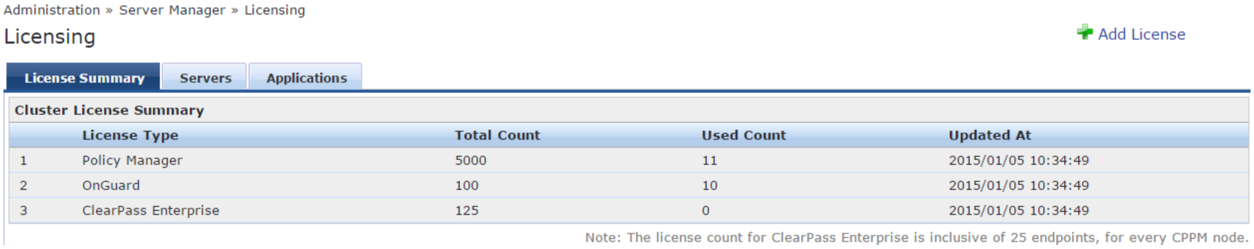
License Summary Tab

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 **Licensing** > **License Summary** tab:

Figure 545: *Licensing > License Summary Tab*



Administration » Server Manager » Licensing

Licensing

Cluster License Summary

	License Type	Total Count	Used Count	Updated At
1	Policy Manager	5000	11	2015/01/05 10:34:49
2	OnGuard	100	10	2015/01/05 10:34:49
3	ClearPass Enterprise	125	0	2015/01/05 10:34:49

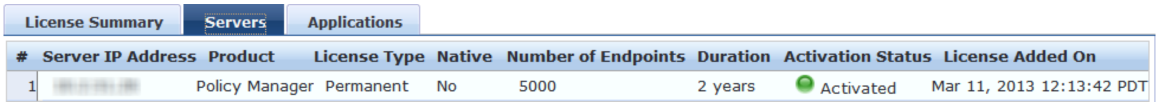
Note: The license count for ClearPass Enterprise is inclusive of 25 endpoints, for every CPPM node.

Licensing > Servers Tab

The **Licensing** > **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 **Licensing** > **Servers** tab:

Figure 546: *Licensing > Servers Tab*



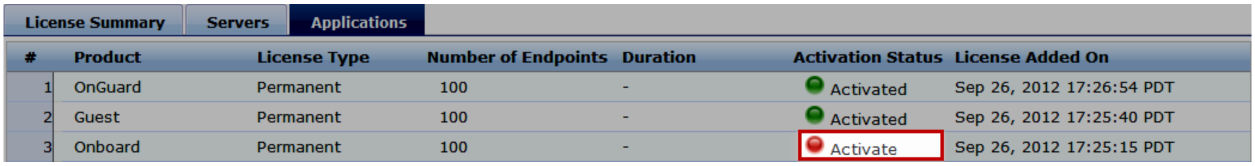
#	Server IP Address	Product	License Type	Native	Number of Endpoints	Duration	Activation Status	License Added On
1	[redacted]	Policy Manager	Permanent	No	5000	2 years	● Activated	Mar 11, 2013 12:13:42 PDT

Licensing > Applications Tab

The **Licensing** > **Applications** tab displays the ClearPass Policy Manager application license details such as product type, license type, number of endpoints, and license activation status.

The following figure displays the **Licensing** > **Applications** tab:

Figure 547: *Licensing > Applications Tab*



#	Product	License Type	Number of Endpoints	Duration	Activation Status	License Added On
1	OnGuard	Permanent	100	-	● Activated	Sep 26, 2012 17:26:54 PDT
2	Guest	Permanent	100	-	● Activated	Sep 26, 2012 17:25:40 PDT
3	Onboard	Permanent	100	-	● Activate	Sep 26, 2012 17:25:15 PDT

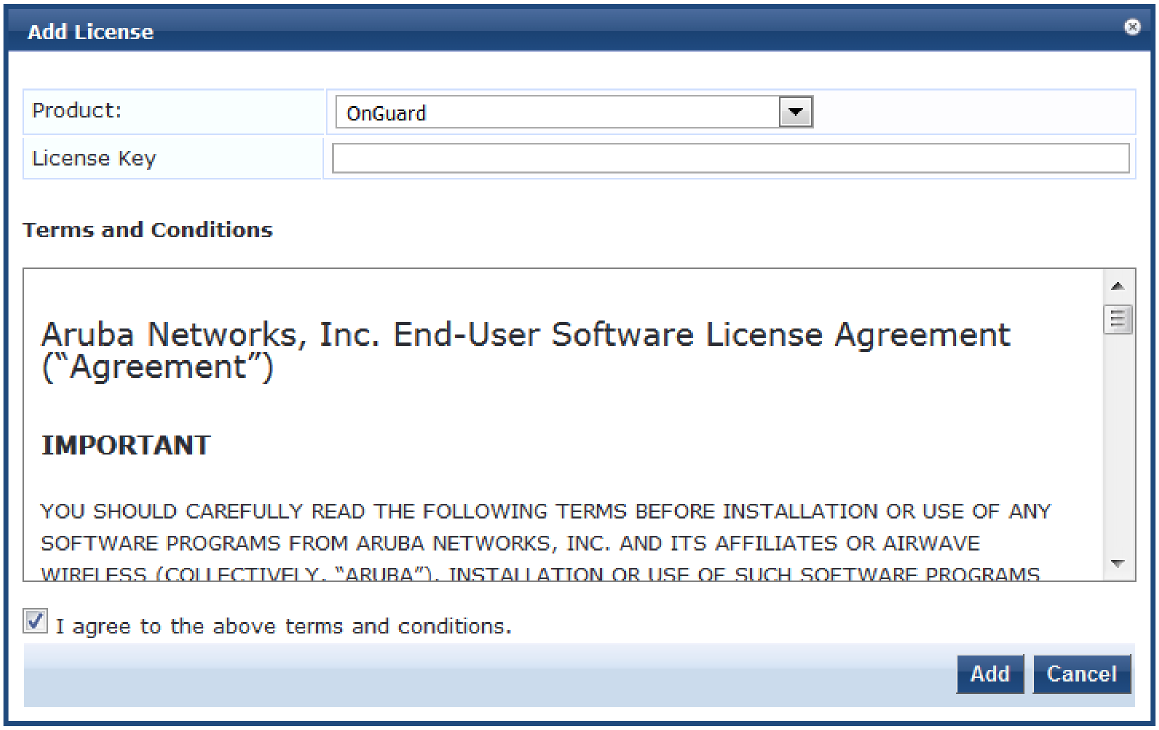
Adding an Application License

To add an application license:

1. Navigate to **Administration > Server Manager > Licensing**.
2. Click the **Add License** link at the top-right section of the page.

   The **Add License** page opens.

Figure 548: *Add License Page*



Add License

Product: OnGuard

License Key

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY, "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS

☑ I agree to the above terms and conditions.

3. **Product**: Choose a product from the **Product** drop-down list:
   - OnGuard
   - Guest
   - Onboard
   - ClearPass Enterprise
4. **License Key:** Enter the license key.
5. Click the **I agree to the above terms and conditions** check box.

   The **Add** button is now enabled.
6. Click **Add**.

   You return to the **Licensing** > **License Summary** page, where the new application license is now listed.

   When you add an application license, the **Applications** tab is enabled to allow you to activate a new application license.

Activating a Server License

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

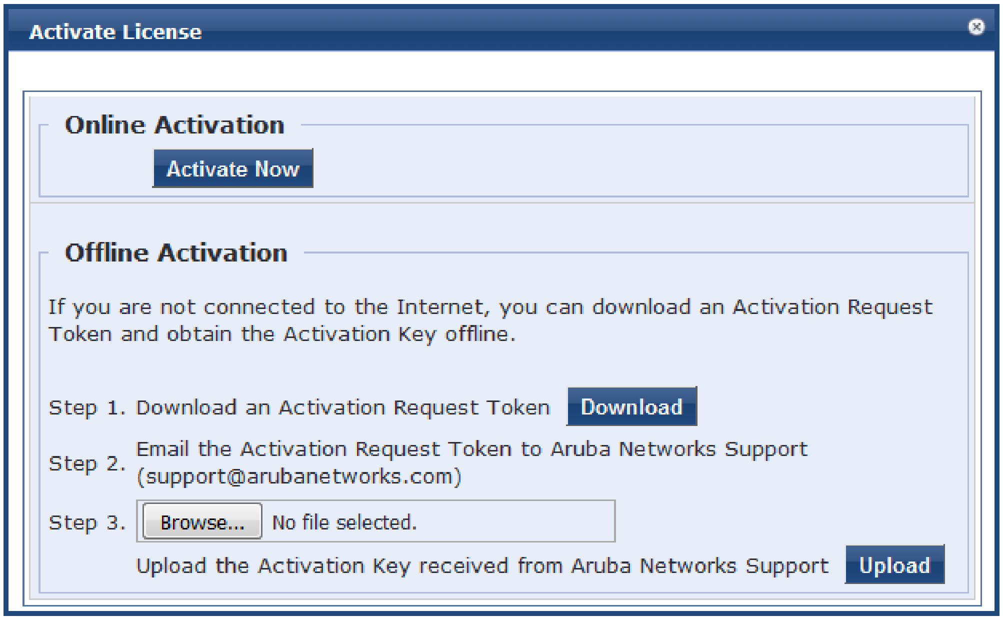
To activate a ClearPass Policy Manager server license:

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

   A ClearPass server that is not activated has the keyword **Activate** next to the red circle in the **Activation Status** column.
3. Click **Activate**.

   The **Activate License** page opens.

Figure 549: *Activate License Page*



Activate License

Online Activation

Activate Now

Offline Activation

If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

Step 1. Download an Activation Request Token Download

Step 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com)

Step 3. Browse... No file selected.

Upload the Activation Key received from Aruba Networks Support Upload

4. In the **Online Activation** section, click **Activate Now**.

   The ClearPass Policy Manager server license is now activated. The **Applications** tab > **Activation Status** column shows a green circle next to the keyword **Activated**.

If You Are Not Connected to the Internet

If you are not connected to the Internet:

1. In the **Offline Activation** section, click **Download** to download an activation request token from the Policy Manager server.
2. Email the activation request token file to the Aruba Support Center.

   You will receive an activation key.
3. Click **Browse** to locate the activation key file on your system, then click **Upload**.

Activating an Application License

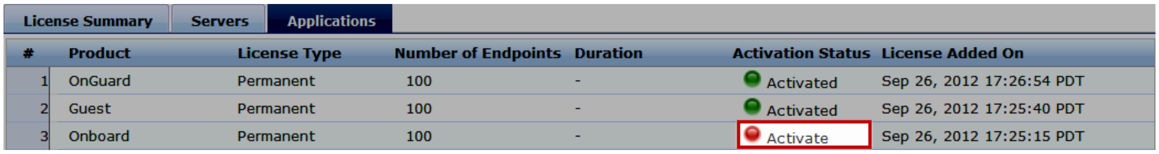
After you add or update an application license, it must be activated. Adding or updating an application license enables the **Applications** tab on the Licensing page.

1. Navigate to **Administration > Server Manager > Licensing**.

   The **Licensing** page opens to the **License Summary** page.
2. Select the **Applications** tab.

   The new application licenses are listed. The **Activation Status** column shows a red circle next to the keyword **Activate**.

Figure 550: *Application Licenses Ready to Be Activated*



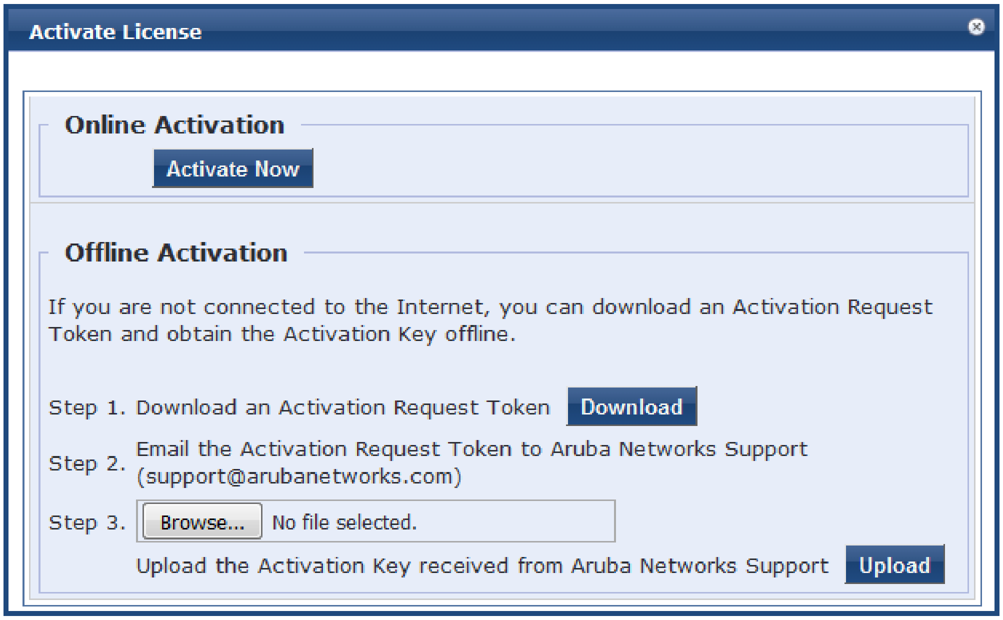
License Summary | Servers | Applications

#	Product	License Type	Number of Endpoints	Duration	Activation Status	License Added On
1	OnGuard	Permanent	100	-	● Activated	Sep 26, 2012 17:26:54 PDT
2	Guest	Permanent	100	-	● Activated	Sep 26, 2012 17:25:40 PDT
3	Onboard	Permanent	100	-	● Activate	Sep 26, 2012 17:25:15 PDT

3. Click **Activate**.

   The **Activate License** page opens.

Figure 551: *Activate License Page*



Activate License

Online Activation

Activate Now

Offline Activation

If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

Step 1. Download an Activation Request Token Download

Step 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com)

Step 3. Browse... No file selected.

Upload the Activation Key received from Aruba Networks Support Upload

4. In the **Online Activation** section, click **Activate Now**.

   The selected application license is now activated. The **Applications** tab > **Activation Status** column shows a green circle next to the keyword **Activated**.

If You Are Not Connected to the Internet

If you are not connected to the Internet:

1. In the **Offline Activation** section, click **Download** to download an activation request token from the Policy Manager server.
2. Email the activation request token file to the Aruba Support Center.

   You will receive an activation key.
3. Click **Browse** to locate the activation key file on your system, then click **Upload**.

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.

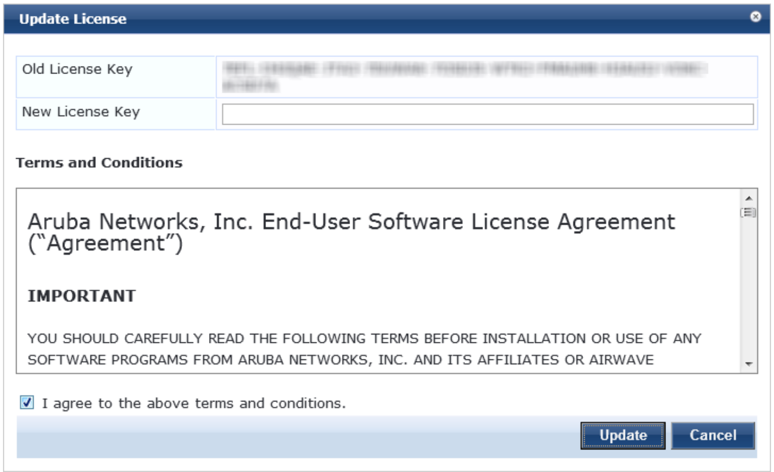
To update a ClearPass Policy Manager server license:

1. Navigate to **Administration > Server Manager > Licensing**.

   The **Licensing** page opens.
2. Select the **Servers** tab.
3. Click the ClearPass server entry.

   The **Update License** dialog opens.

Figure 552: *Update License Dialog*



Old License Key [redacted]

New License Key

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE

☑ I agree to the above terms and conditions.

4. Enter the new license key.
5. Click the **I agree to the above terms and conditions** check box.

   The **Update** button is now activated.
6. Click **Update**.

Updating an Application License

Application licenses typically require updating after they expire, for example, after the evaluation license expires, or when capacity exceeds its licensed amount.

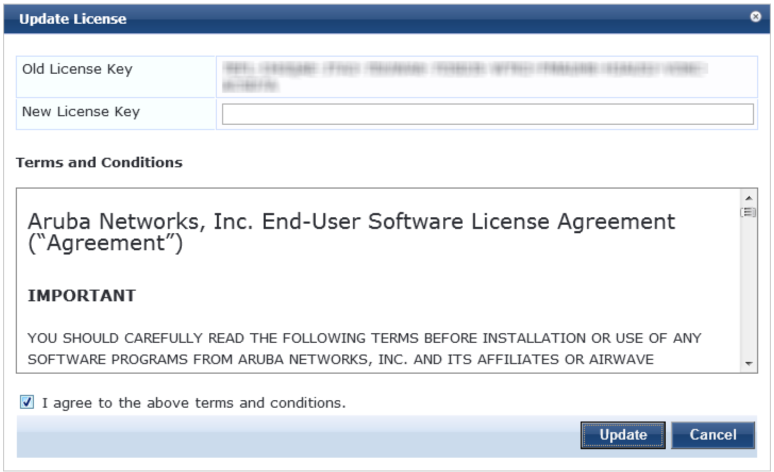
To update an application license:

1. Navigate to **Administration > Server Manager > Licensing**.

   The **Licensing** page opens.
2. Select the **Applications** tab.
3. Select the application license you need to update.

   The **Update License** dialog opens.

Figure 553: *Update License Dialog*



Old License Key [redacted]

New License Key

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE

☑ I agree to the above terms and conditions.

4. Enter the new license key.
5. Click the **I agree to the above terms and conditions** check box.

   The **Update** button is now activated.
6. Click **Update**.

SNMP Trap Receivers

This section provides the following information:

- SNMP Trap Receivers Main Page on page 558
- Adding an SNMP Trap Server on page 558
- Importing an SNMP Trap Server on page 560
- Exporting All SNMP Trap Servers on page 561
- Exporting an SNMP Trap Server on page 562
- Deleting an SNMP Trap Server on page 563

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

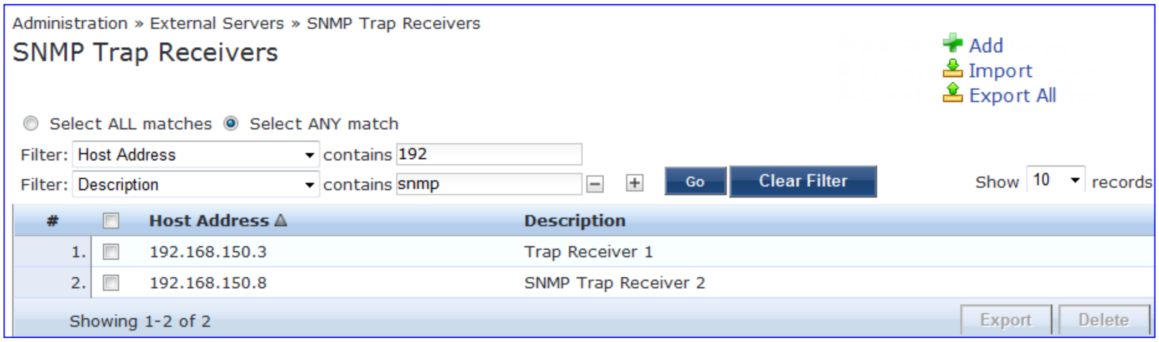
- **System up-time**: Provides information about how long the ClearPass server has been running.
- **Network interface statistics [up/down]**: Provides information about whether the network interface is up or down.
- **Process monitoring information**: Checks for the processes that should be running, including maximum and minimum number of allowed instances. Sends traps if there is a change in value of the maximum and minimum numbers.
- **Disk usage**: Checks for disk space usage of a partition. The agent can check the amount of available disk space and make sure it's 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**: Checks for unreasonable load average values. For example, if CPU load average for one minute exceeds the configured value (in percentage), the ClearPass server sends a trap to the configured destination.
- **Memory usage**: Reports the ClearPass server's memory usage.

SNMP Trap Receivers Main Page

To view a list of SNMP trap receivers configured on the ClearPass Policy Manager server, navigate to **Administration > External Servers > SNMP Trap Receivers**.

The following figure displays the **SNMP Trap Receivers** page:

Figure 554: *SNMP Trap Receivers Page*



Administration » External Servers » SNMP Trap Receivers

SNMP Trap Receivers

Add
Import
Export All

○ Select ALL matches ● Select ANY match

Filter: Host Address contains 192

Filter: Description contains snmp

Go Clear Filter

Show 10 records

#	□	Host Address	Description
1.	□	192.168.150.3	Trap Receiver 1
2.	□	192.168.150.8	SNMP Trap Receiver 2

Showing 1-2 of 2

Export Delete

About the ClearPass SNMP Private MIB

For information about the ClearPass SNMP Private MIB, see ClearPass SNMP Private MIB on page 807.

Adding an SNMP Trap Server

A trap is an SNMP message sent from one application to another (which is typically on a remote host).

For SNMP trap server configuration, ClearPass provides the **Type** parameter to specify whether the SNMP notification is a standard **Trap** notification or an **Inform** notification (see Figure 555). An **Inform** notification is an acknowledged SNMP trap.

When you send an **Inform** notification, ClearPass uses an **SNMP Engine ID** when sending the message. The Engine ID is a unique identifier for the SNMP v3 agent. The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMP v3 messages. The Engine ID is automatically generated when you enable the stand-alone SNMP agent.

The default value for the SNMP Engine ID is *6620000004030662*. This value can be changed in the **Engine ID** field configured in the ClearPass **Server Configuration** > **System Monitoring** page (for details, see System Monitoring Page on page 506).

NOTE

To receive traps, the same Engine ID value must be configured on the trap receiver side.

To add an SNMP trap server:

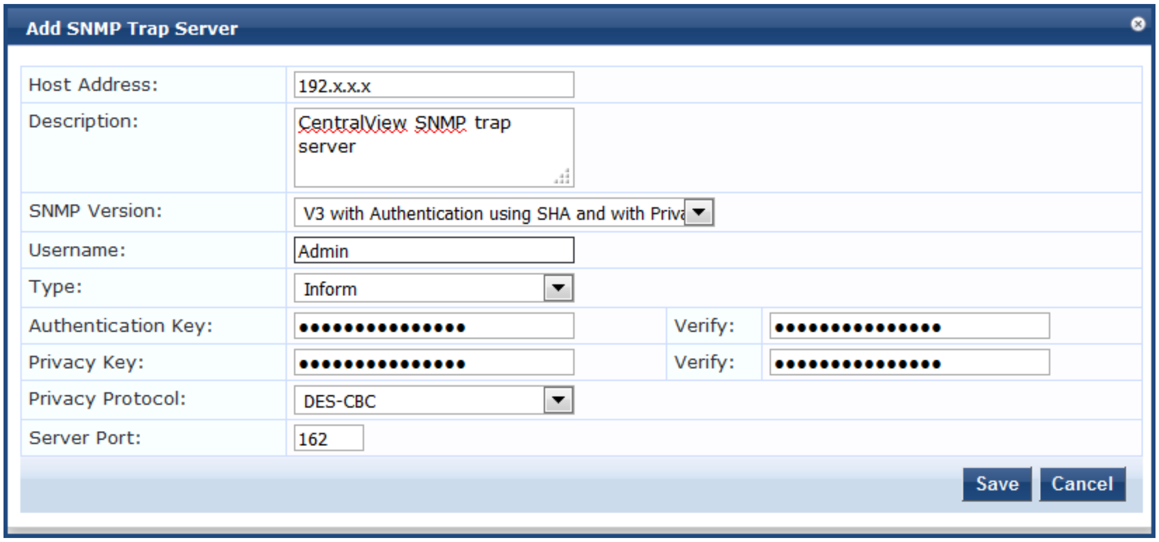
1. Navigate to **Administration > External Servers > SNMP Trap Receivers**.

   The **SNMP Trap Receivers** page opens.

2. Click the **Add** link.

   The **Add SNMP Trap Server** dialog opens.

Figure 555: *Add SNMP Trap Server Dialog*



Add SNMP Trap Server

Host Address:	192.x.x.x		
Description:	CentralView SNMP trap server		
SNMP Version:	V3 with Authentication using SHA and with Priva		
Username:	Admin		
Type:	Inform		
Authentication Key:	•••••••••••••••	Verify:	•••••••••••••••
Privacy Key:	•••••••••••••••	Verify:	•••••••••••••••
Privacy Protocol:	DES-CBC		
Server Port:	162		

3. Specify the **Add SNMP Trap Server** parameters as described in the following table, then click **Save**:

Table 297: *Add SNMP Trap Server Parameters*

Parameter	Action/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 one of the following SNMP versions:

Table 297: *Add SNMP Trap Server Parameters (Continued)*

Parameter	Action/Description
	■ 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 when you use ClearPass Policy Manager in **FIPS** mode.
Username	Specify the Admin user name for SNMP operations. **NOTE:** This parameter is available in SNMP v3 only.
Type	From the **Type** drop-down, select the type of SNMP notification: ■ Inform ■ Trap
Authentication Key	Specify the SNMP v3 with authentication option (SHA or MD5). **NOTE:** The **EAP-MD5** authentication type is not supported if you run ClearPass Policy Manager in FIPS mode. **NOTE:** Authentication Key is available in SNMP v3 only.
Privacy Key	Specify the SNMP v3 with privacy option. **NOTE:** This parameter is available in SNMP v3 only.
Privacy Protocol	Choose one of the available privacy protocols: ■ DES-CBC ■ AES-128 **NOTE:** This parameter is available in SNMP v3 with Privacy only. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data.
Server Port	Specify the port number for sending the traps. By default, the port number is **162**. **NOTE:** Configure the trap server firewall for traffic on this port.

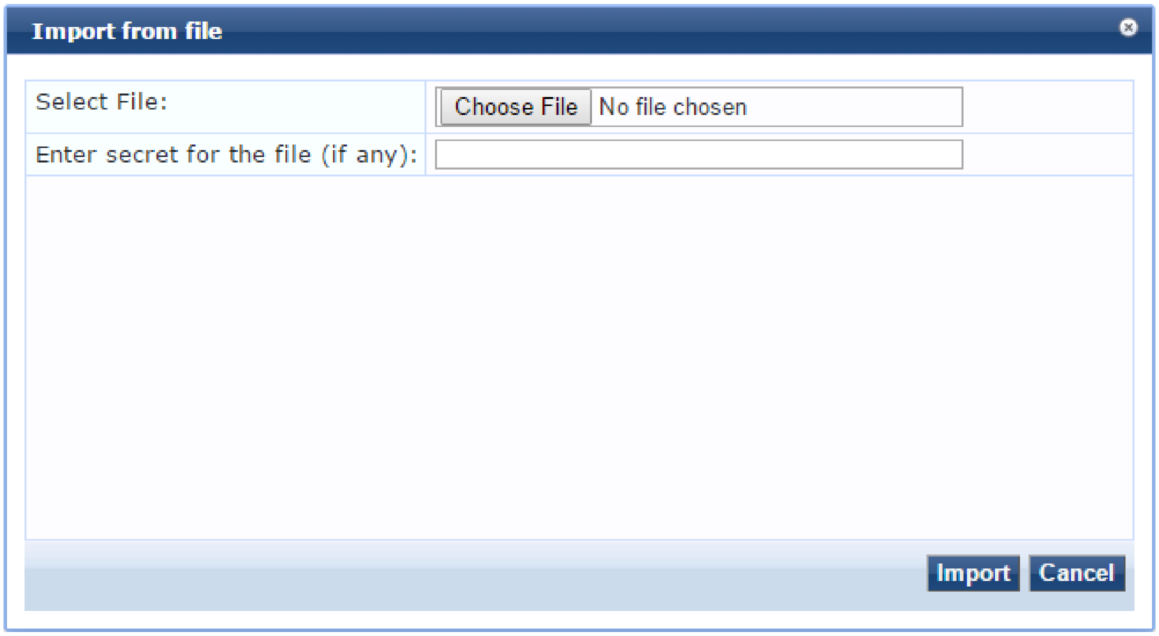
Importing an SNMP Trap Server

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 298.
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 556: *Import from file Pop-up*



Import from file

Select File: Choose File No file chosen

Enter secret for the file (if any):

The following table describes the **Import from file** parameters:

Table 298: *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.

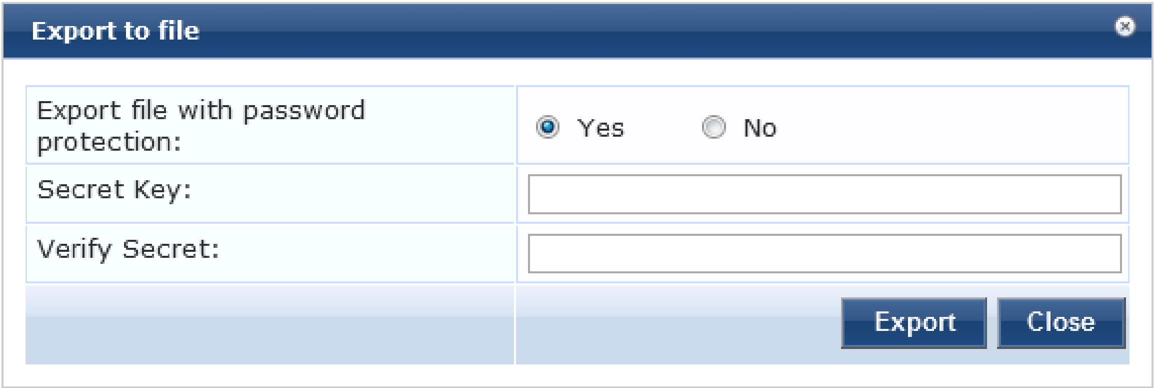
Exporting All SNMP Trap Servers

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 299.
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 557: *Export to file Pop-up*



Export to file

Export file with password protection: ● Yes ○ No

Secret Key:

Verify Secret:

The following table describes the **Export to file** parameters:

Table 299: *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.

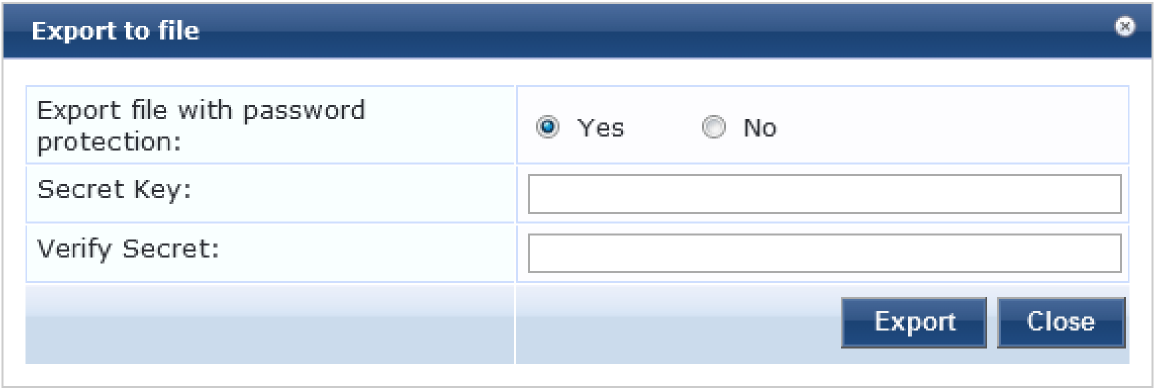
Exporting an SNMP Trap Server

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 300.
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 558: *Export to file Pop-up*



Export to file

Export file with password protection: ● Yes ○ No

Secret Key:

Verify Secret:

The following table describes the **Export to file** parameters:

Table 300: *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

ClearPass Policy Manager can export session data (see Live Monitoring: Access Tracker on page 99), audit records (see Audit Viewer on page 148) and event records (see Event Viewer on page 150). 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**.

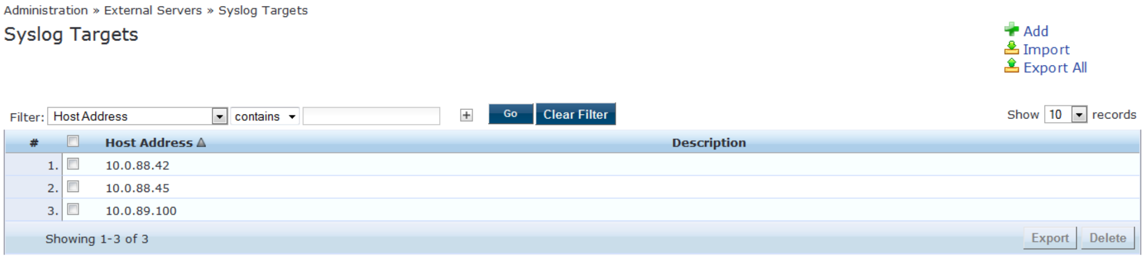
This section describes the following topics:

- Syslog Targets Main Page on page 563
- Adding a Syslog Target on page 564
- Importing a Syslog Target on page 565
- Exporting All Syslog Target on page 566
- Exporting a Syslog Target on page 566
- Exporting a Syslog Target on page 566

Syslog Targets Main Page

The following figure displays the **Syslog Targets** page:

Figure 559: *Syslog Targets Page*



Administration » External Servers » Syslog Targets

Syslog Targets

Filter: Host Address contains

Show 10 records

#	□	Host Address △	Description
1.	□	10.0.88.42	
2.	□	10.0.88.45	
3.	□	10.0.89.100	

Showing 1-3 of 3

The following table describes the **Syslog Targets** parameters:

Table 301: *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.

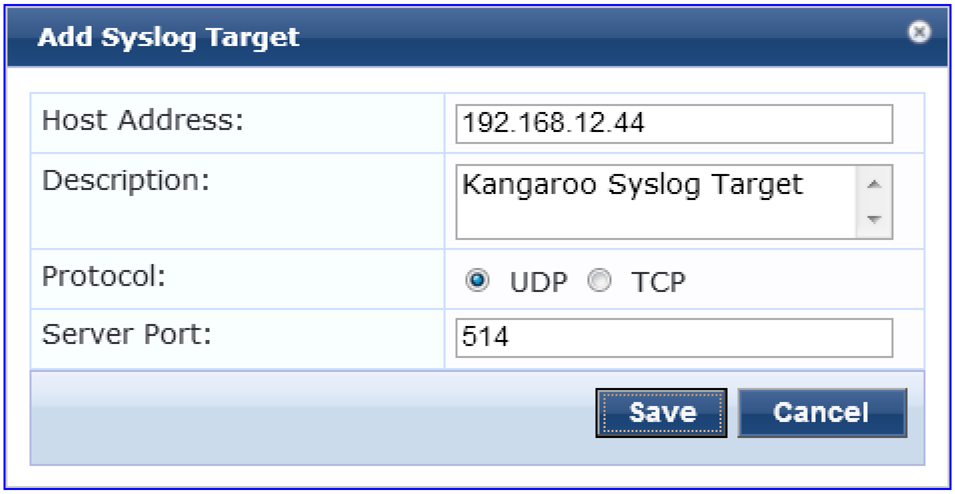
Adding a Syslog Target

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 302.
3. Click **Save**.

The following figure displays the **Add Syslog Target** pop-up:

Figure 560: *Add Syslog Target Pop-up*



Add Syslog Target

Host Address: 192.168.12.44

Description: Kangaroo Syslog Target

Protocol: ● UDP ○ TCP

Server Port: 514

The following table describes the **Add Syslog Target** parameters:

Table 302: *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.

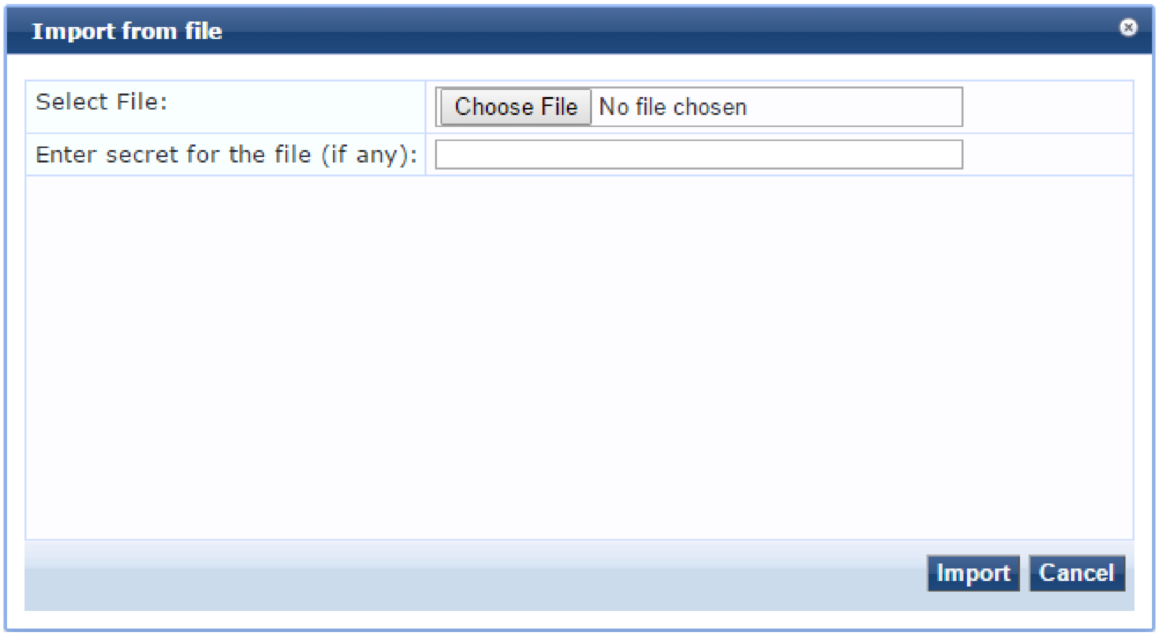
Importing a Syslog Target

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 303.
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 561: *Import from file Pop-up*



Import from file

Select File:	Choose File No file chosen
Enter secret for the file (if any):	

The following table describes the **Import from file** parameters:

Table 303: *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.

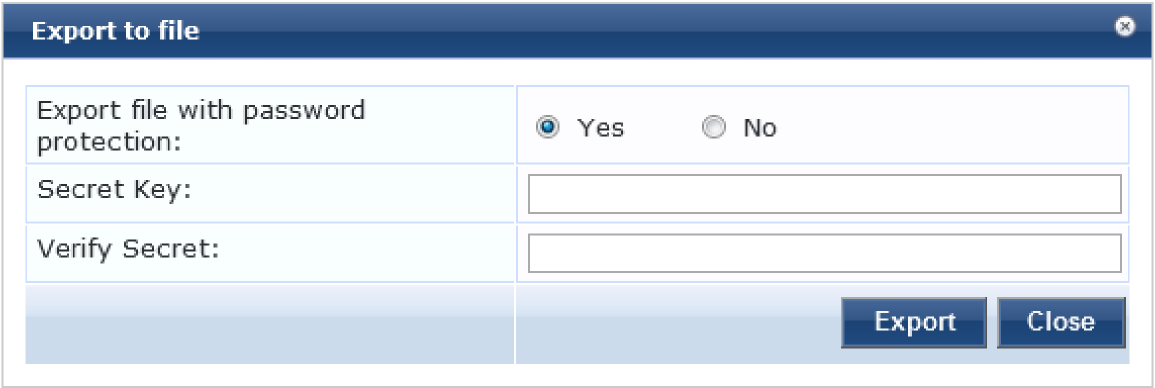
Exporting All Syslog Target

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 304.
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 562: *Export to file Pop-up*



Export to file

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

The following table describes the **Export to file** parameters:

Table 304: *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

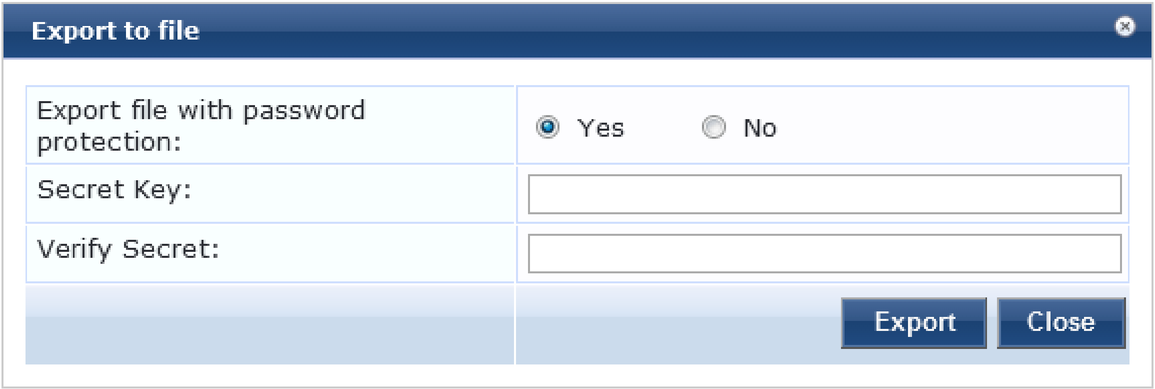
To export a syslog target:

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 304.
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 563: *Export to file Pop-up*



Export to file

Export file with password protection: ● Yes ○ No

Secret Key:

Verify Secret:

The following table describes the **Export to file** parameters:

Table 305: *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

This section describes the following topics:

- About Syslog Export Filters
- Syslog Export Filters Page on page 568
- Adding a Syslog Export Filter on page 568
- Importing a Syslog Filter on page 577
- Exporting All Syslog Filter on page 578
- Exporting a Syslog Filter on page 578
- Deleting a Syslog Filter on page 579

About Syslog Export Filters

Policy Manager can export session data (see Live Monitoring: Access Tracker on page 99), audit records (see Audit Viewer on page 148), and event records (see Event Viewer on page 150).

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.

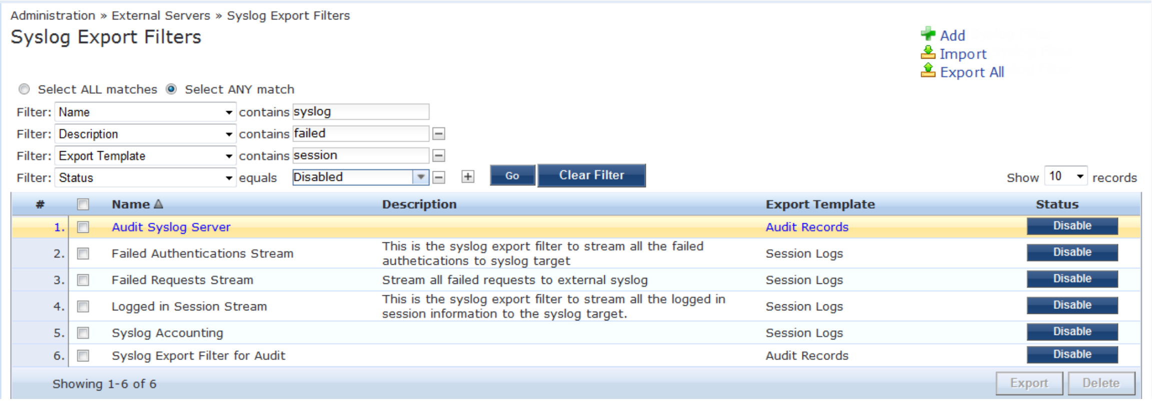
Syslog Export Filters Page

To configure syslog export filters:

1. Navigate to **Administration** > **External Servers** > **Syslog Export Filters**.

   The **Syslog Export Filters** page opens.

Figure 564: *Syslog Export Filters Page*



Administration » External Servers » Syslog Export Filters

Syslog Export Filters

○ Select ALL matches ● Select ANY match

Filter: Name contains syslog

Filter: Description contains failed

Filter: Export Template contains session

Filter: Status equals Disabled

Show 10 records

#	□	Name	Description	Export Template	Status
1.	□	Audit Syslog Server		Audit Records	Disable
2.	□	Failed Authentications Stream	This is the syslog export filter to stream all the failed authetications to syslog target	Session Logs	Disable
3.	□	Failed Requests Stream	Stream all failed requests to external syslog	Session Logs	Disable
4.	□	Logged in Session Stream	This is the syslog export filter to stream all the logged in session information to the syslog target.	Session Logs	Disable
5.	□	Syslog Accounting		Session Logs	Disable
6.	□	Syslog Export Filter for Audit		Audit Records	Disable

Showing 1-6 of 6

The following table describes the **Syslog Export Filters** parameters:

Table 306: *Syslog Export Filters Page Parameters*

Parameter	Action/Description
Name	Displays the name of the syslog export filter.
Description	Displays the description of the syslog export filter.
Export Template	Displays the name of the **Export Template** selected in the **Add Syslog Export Filter** dialog (see Adding a Syslog Export Filter on page 568).
Export Event Format	Displays the **Export Event Format Type** selected in the **Add Syslog Export Filter** dialog.
Enable/Disable	Enable or disable the syslog export filter.
Export	Opens the **Export to file** dialog. With this option, you can export individual syslog export filters.
Delete	Deletes a syslog export filter.

Adding a Syslog Export Filter

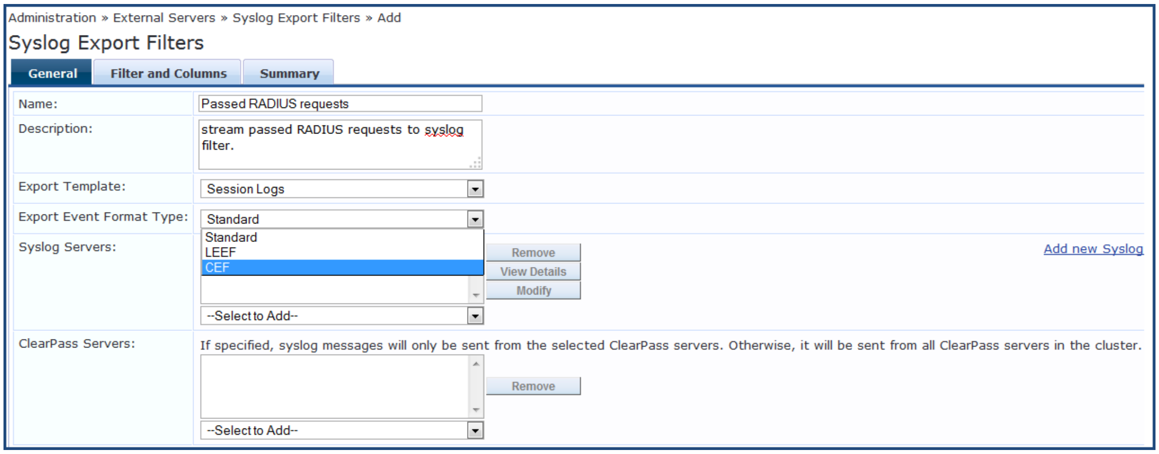
You can use filters to select the data sent from the Log server to the Syslog server. First add a Syslog Filter as described below. You can then export and apply the Syslog filters separately to different kinds of logs.

To add a syslog export filter:

1. Navigate to **Administration** > **External Servers** > **Syslog Export Filters**.
2. From the **Syslog Export Filters** page, click **Add**.

   The **Add Syslog Filters** page opens to the **General** tab.

Figure 565: *Add Syslog Export Filters Page > General Tab*



Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

Name:	Passed RADIUS requests
Description:	stream passed RADIUS requests to syslog filter.
Export Template:	Session Logs
Export Event Format Type:	Standard Standard LEEF CEF
Syslog Servers:	--Select to Add--
ClearPass Servers:	If specified, syslog messages will only be sent from the selected ClearPass servers. Otherwise, it will be sent from all ClearPass servers in the cluster. --Select to Add--

> **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. For more information, see Filter and Columns Tab on page 573.

The following table describes the **Add Syslog Export Filters** > **General** tab parameters:

Table 307: *Add Syslog Export Filters > General Tab Parameters*

Parameter	Action/Description
Name	Enter the name of the syslog export filter.
Description	Enter the description that provides additional information about the syslog export filter (recommended).
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 573.

Table 307: *Add Syslog Export Filters > General Tab Parameters (Continued)*

Parameter	Action/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 570.
Syslog Servers	Syslog servers define the receivers of syslog messages sent by servers in the ClearPass cluster. - To add a ClearPass syslog server, select it from the **Select to Add** drop-down list. - To add a new ClearPass syslog server, click the **Add New Syslog Target** link (for more information, see Adding a Syslog Target on page 564). - 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 more information, see Adding a Syslog Target on page 564. - To remove a syslog server (from receiving syslog messages), select the syslog server, then click **Remove**.
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 provides several examples of Standard, LEEF, and CEF event format types for the syslog export filter templates.

Standard Event Format Type > Audit Events

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 2017-01-19 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, 2017 21:18:54 IST
Mar 20 21:20:56 10.17.5.228 2017-01-19 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, 2017 21:20:22 IST
Mar 21 09:28:59 10.17.5.228 2017-01-20 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, 2017 09:29:13 IST
```

Standard Event Format Type > System Events

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 2017-01-20 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 2017-01-20 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, 2017 16:48:53 IST
2015-01-20 16:50:05,210 [pool-6-thread-1] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2017-
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, 2017 16:48:57 IST
2015-01-20 16:50:05,211 [pool-6-thread-1] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2017-
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, 2017 16:49:00 IST
```

Standard Event Format Type > Session Events

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 2017-01-20 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=2017-01-20
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]
```

LEEF Event Format Type > Insight Logs

The following example describes the LEEF event format type for the **Insight Logs** syslog export filter template:

```
Dec 03 2017 16:50:44.085 IST 10.17.4.208 LEEF:1.0|Aruba Networks|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=2017-12-03 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
```

CEF Event Format Type > Insight Logs

The following example describes the CEF event format type for the **Insight Logs** syslog export filter template:

```
Dec 03 2017 16:31:28.861 IST 10.17.4.208 CEF:0|Aruba Networks|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=2017-12-03 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
```

CEF Event Format Type > Audit Logs

The following example describes the CEF event format type for the **Audit Logs** syslog export filter template:

```
Nov 19 2017 18:22:40.700 IST 10.17.4.221 CEF:0|Aruba Networks|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
```

LEEF Event Format Type > Audit Logs

The following example describes the LEEF event format type for the **Audit Logs** syslog export filter template:

```
Nov 19 2017 14:31:10.422 IST 10.17.4.221 LEEF:1.0|Aruba Networks|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
```

CEF Event Format Type > System Events

The following example describes the CEF event format type for the **System Events** syslog export filter template:

```
Nov 19 2017 17:15:52.348 IST 10.17.4.221 CEF:0|Aruba Networks|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, 2017 17:15:12 IST src=ClearPass Firmware Update Checker act=None
```

LEEF Event Format Type > System Events

The following example describes the LEEF event format type for the **System Events** syslog export filter template:

```
Dec 02 2017 20:38:40.901 IST 10.17.4.206 LEEF:1.0|Aruba Networks|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
```

CEF Event Format Type > Session Logs

The following example describes the CEF event format type for the **Session Logs** syslog export filter template:

```
Dec 01 2017 15:28:40.540 IST 10.17.4.206 CEF:0Aruba Networks|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
```

LEEF Event Format Type > Session Logs

The following example describes the LEEF event format type for the **Session Logs** syslog export filter template:

```
Dec 02 2017 15:35:14.944 IST 10.17.4.206 LEEF:1.0Aruba Networks|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=2017-12-02
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** page of the **Syslog Export Filters > Add** page.

This page provides two methods for configuring data filters: **Insight Logs** or **Session Logs**. These methods are visible only if you select **Insight Logs** or **Session Logs** as the export template.

Insight Logs

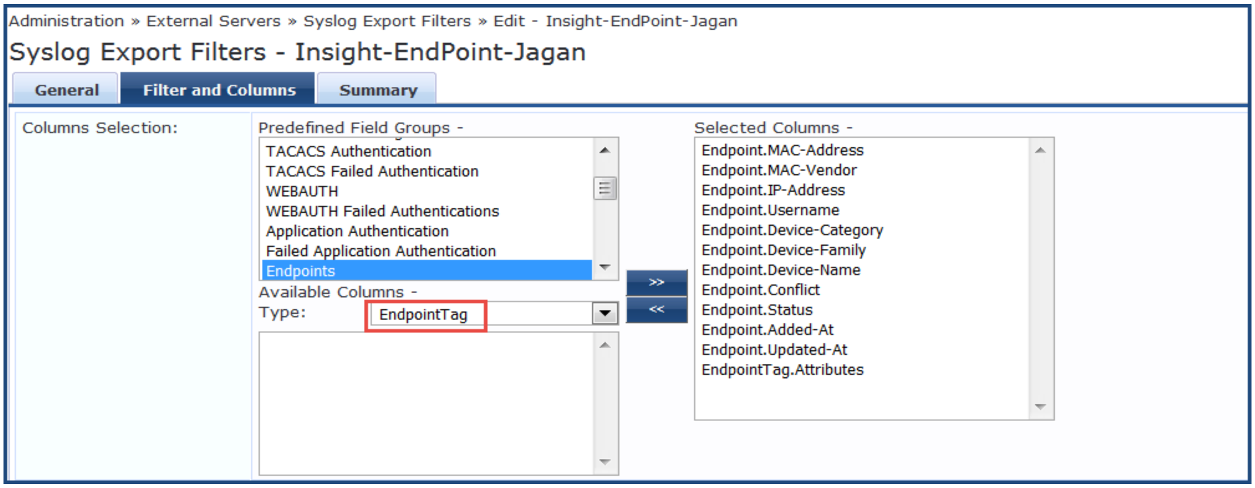
This section describes the options if you select **Insight Logs** as the export template in the **General** tab.

NOTE

The **Insight Logs** option is enabled only if you enable Insight on the current ClearPass server. To do so, navigate to the **Administration** > **Server Manager** > **Server Configuration** > **System** tab, then enable the **Enable Insight** check box.

Figure 566 displays the **Syslog Export Filters** > **Filter and Columns > Insight Logs**.

Figure 566: *Syslog Export Filters > Filter and Columns >Insight Logs*



Administration » External Servers » Syslog Export Filters » Edit - Insight-EndPoint-Jagan

Syslog Export Filters - Insight-EndPoint-Jagan

Columns Selection:

Predefined Field Groups -

TACACS Authentication
TACACS Failed Authentication
WEBAUTH
WEBAUTH Failed Authentications
Application Authentication
Failed Application Authentication
Endpoints

Available Columns -

Type: EndpointTag

Selected Columns -

Endpoint.MAC-Address
Endpoint.MAC-Vendor
Endpoint.IP-Address
Endpoint.Username
Endpoint.Device-Category
Endpoint.Device-Family
Endpoint.Device-Name
Endpoint.Conflict
Endpoint.Status
Endpoint.Added-At
Endpoint.Updated-At
EndpointTag.Attributes

As shown in Figure 566, administrators can select **EndpointTag** attributes as a column in Syslog Export Filters.

Custom attributes fetched by users and recorded in an endpoint are sent in syslog export filters to the Syslog server. When there is a update on endpoints, syslog events are generated.

NOTE

The data collection interval for Insight logs is -4 to -2 minutes from the current time.

Specify the **Syslog Export Filters** > **Filter and Columns** > **Insight Logs** parameters as described in the following table:

Table 308: *Syslog Export Filters > Filter and Columns > Insight Logs Parameters*

Parameter	Action/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 addition.
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

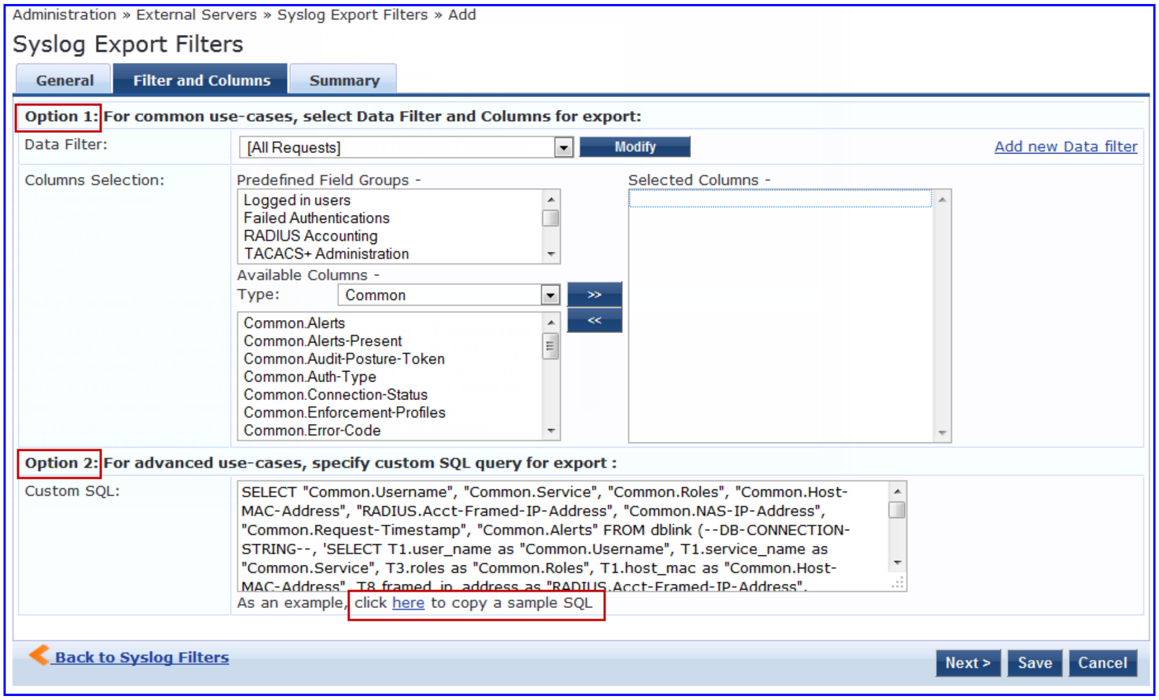
This section describes the options if you select **Session Logs** as the export template in the **General** tab. On selecting **Session Logs**, the following options are available:

- **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 567: *Syslog Export Filters - Filter and Columns (Session Logs) Tab*



Option 1: For common use-cases, select Data Filter and Columns for export:

Data Filter: [All Requests]

Columns Selection:

Predefined Field Groups -
Logged in users
Failed Authentications
RADIUS Accounting
TACACS+ Administration

Available Columns -
Type: Common

Common.Alerts
Common.Alerts-Present
Common.Audit-Posture-Token
Common.Auth-Type
Common.Connection-Status
Common.Enforcement-Profiles
Common.Error-Code

Selected Columns -

Option 2: For advanced use-cases, specify custom SQL query for export :

Custom SQL:

```
SELECT "Common.Username", "Common.Service", "Common.Roles", "Common.Host-
MAC-Address", "RADIUS.Acct-Framed-IP-Address", "Common.NAS-IP-Address",
"Common.Request-Timestamp", "Common.Alerts" FROM dblink (--DB-CONNECTION-
STRING--, 'SELECT T1.user_name as "Common.Username", T1.service_name as
"Common.Service", T3.roles as "Common.Roles", T1.host_mac as "Common.Host-
MAC-Address", T8.framed_ip_address as "RADIUS.Acct-Framed-IP-Address",
```

As an example, click here to copy a sample SQL

The following table describes the **Syslog Export Filters** > **Filter and Columns** > **Session Logs** parameters:

Table 309: *Syslog Export Filters > Filter and Columns > Insight Logs Parameters*

Parameter	Action/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 filter, see Adding a Data Filter on page 155.
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.

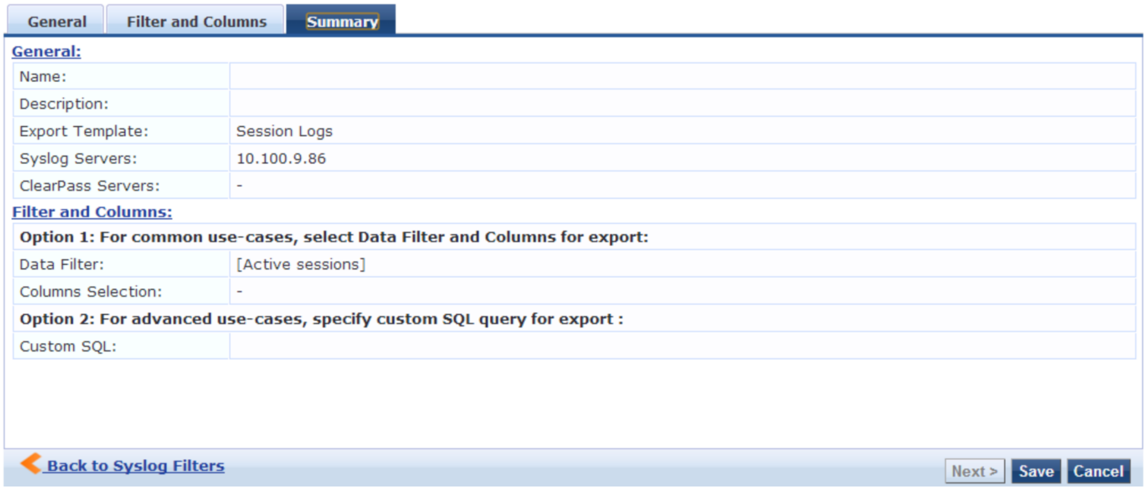
Table 309: *Syslog Export Filters > Filter and Columns > Insight Logs Parameters (Continued)*

Parameter	Action/Description
Custom SQL	Specify custom SQL query for export. This option is for advanced use cases. **NOTE:** If you choose this option, contact Aruba Support at **Administration** > **Support** > **Contact Support**. 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 568: *Syslog Export Filters - Summary Tab*



General:

Name:	
Description:	
Export Template:	Session Logs
Syslog Servers:	10.100.9.86
ClearPass Servers:	-

Filter and Columns:

Option 1: For common use-cases, select Data Filter and Columns for export:	
Data Filter:	[Active sessions]
Columns Selection:	-
Option 2: For advanced use-cases, specify custom SQL query for export :	
Custom SQL:	

The following table describes the **Syslog Export Filters - Summary** tab parameters:

Table 310: *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	

Table 310: *Syslog Export Filters - Summary Tab Parameters (Continued)*

Parameter	Description
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.

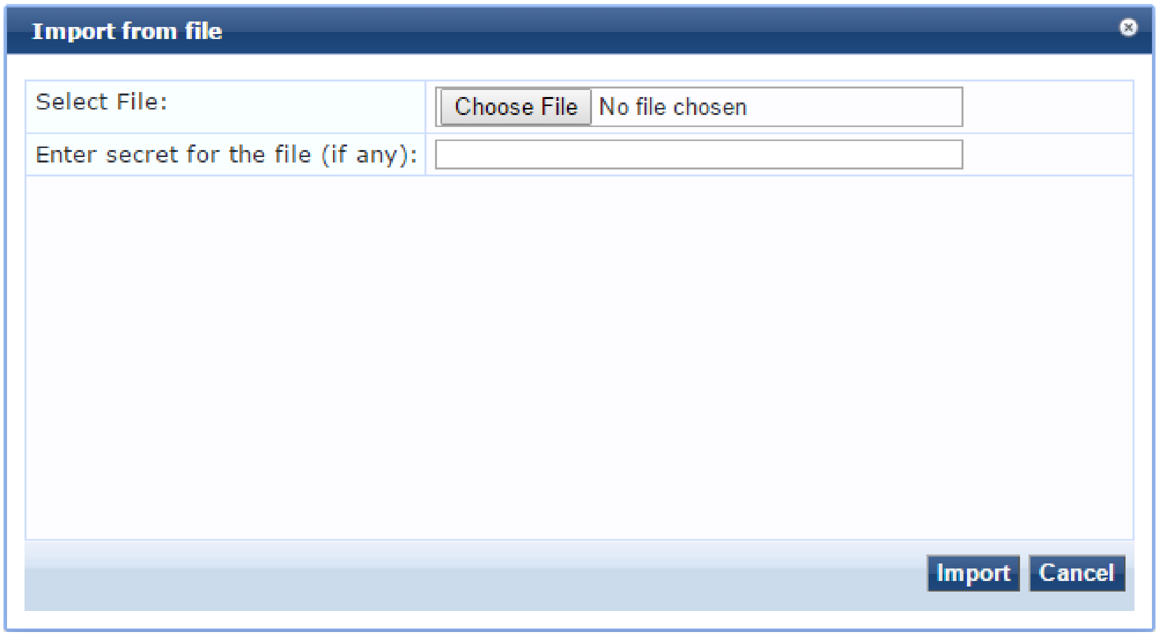
Importing a Syslog Filter

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 311.
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

Figure 569: *Import from file Pop-up*



Import from file

Select File:	Choose File No file chosen
Enter secret for the file (if any):	

The following table describes the **Import from file** parameters:

Table 311: *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.

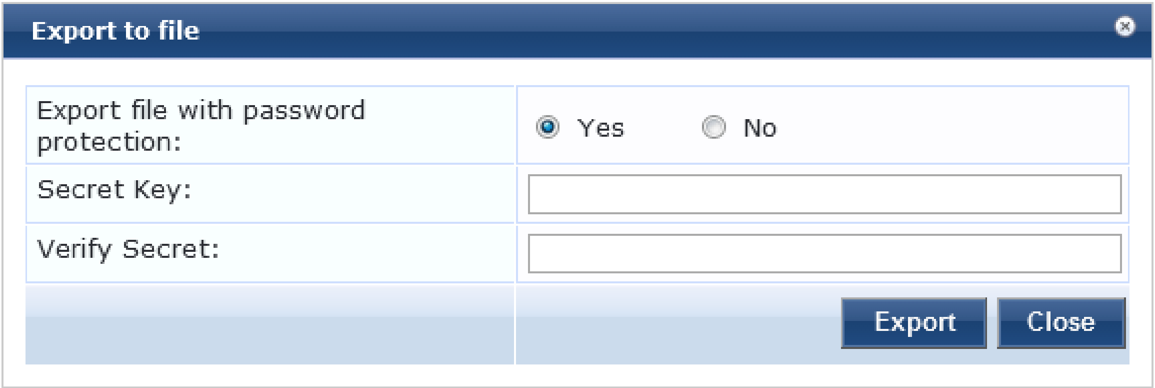
Exporting All Syslog Filter

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 312.
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 570: *Export to file Pop-up*



Export to file

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

The following table describes the **Export to file** parameters:

Table 312: *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.

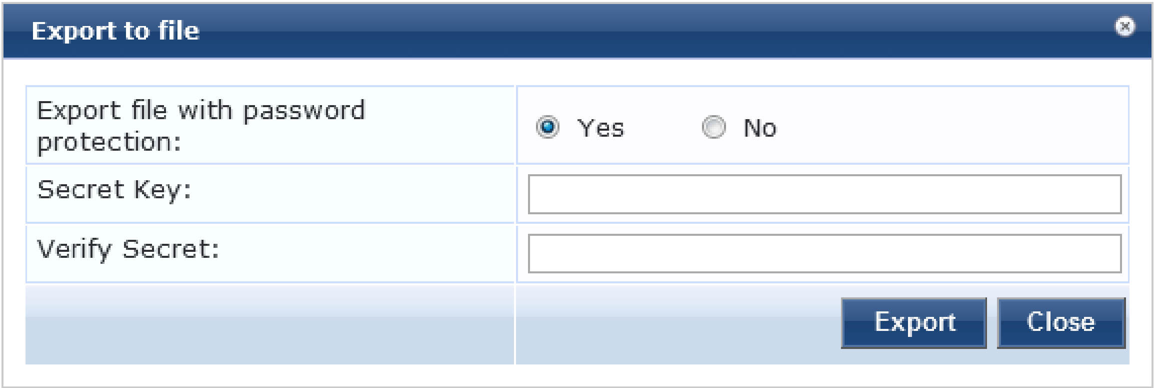
Exporting a Syslog Filter

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 313.
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 571: *Export to file Pop-up*



Export to file

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

The following table describes the **Export to file** parameters:

Table 313: *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

This section provides the following information:

- Configuring Messaging
- Sending a Test Email Message
- Sending a Test SMS Message

ClearPass messaging setup provides an interface to configure the Simple Mail Transfer Protocol (SMTP) server for email and SMS notifications.

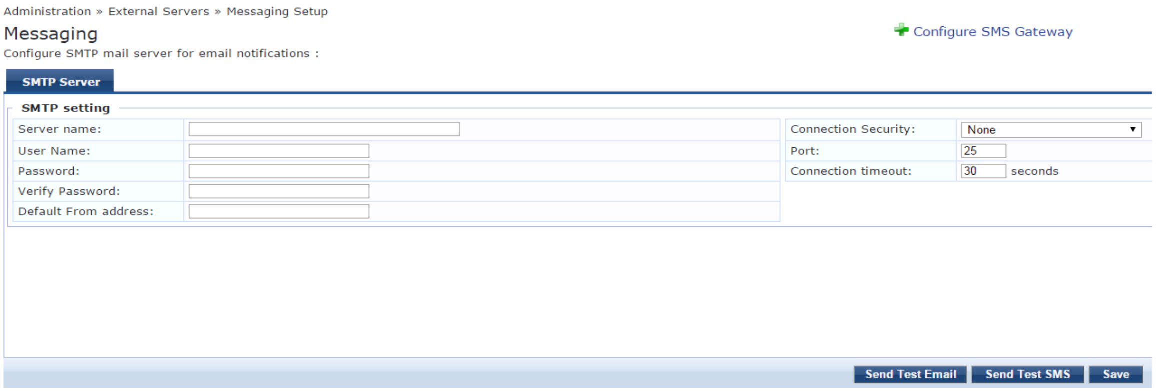
Configuring Messaging

To configure messaging:

1. Navigate to **Administration** > **External Servers** > **Messaging Setup**.

The **Messaging** > **SMTP Server** page opens.

Figure 572: *Messaging > SMTP Server Page*



Messaging

Configure SMTP mail server for email notifications :

SMTP setting

Server name:		Connection Security:	None
User Name:		Port:	25
Password:		Connection timeout:	30 seconds
Verify Password:			
Default From address:			

2. To configure a new SMS gateway using the ClearPass Guest portal, click the **Configure SMS Gateway** link at the top right section of the page.

   The following table describes the **Messaging > SMTP Server** page parameters:

Table 314: *Messaging > SMTP Server Page Parameters*

Parameter	Action/Description
Server name	1. Enter the Fully Qualified Domain Name (FQDN) or the IP address of the SMTP server.
User Name	2. Enter the username if your email server requires authentication for sending email messages.
Password	3. Enter the password for the specified username, then verify the password.
Default From address	4. Enter the email address that must to be displayed as the sender’s address in the message.
Connection Security	5. To establish the communication with the SMTP 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	6. Enter the TCP port number that the SNMP server listens on. The default value of the port is **25**.
Connection timeout	7. Enter the timeout value for connection to the SMTP server (in seconds). The default value is **30** seconds.

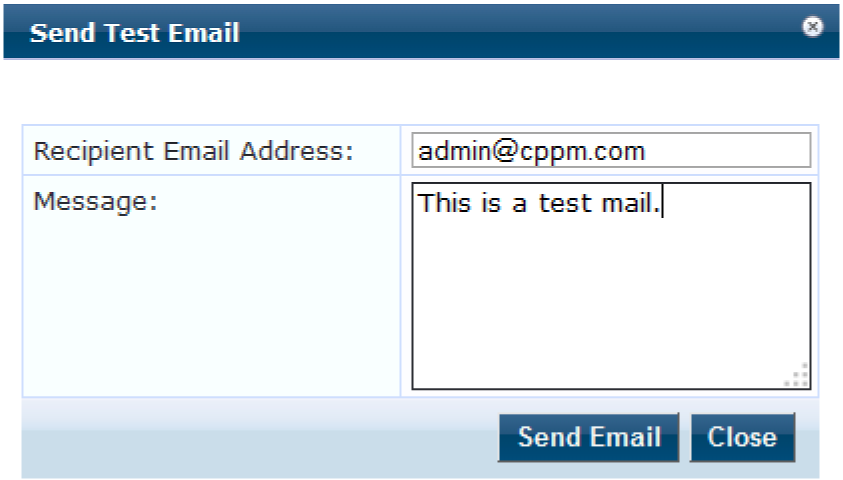
Sending a Test Email Message

To send a test mail message to the preferred email address:

1. Click **Send Test Email**.

   The **Send Test Email** dialog opens.

Figure 573: *Send Test Email Dialog*



Send Test Email

Recipient Email Address: admin@cppm.com

Message: This is a test mail.

2. **Recipient Email Address**: Enter the email address of the recipient.
3. **Message**: Enter the test message.
4. Click **Send Email**.

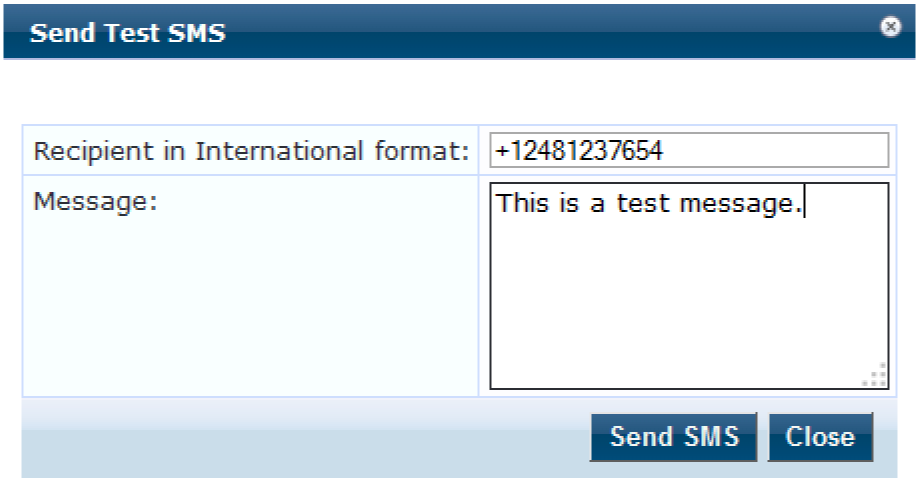
Sending a Test SMS Message

To send a test SMS message to the preferred email address:

1. Click **Send Test SMS**.

   The **Send Test SMS** dialog opens.

Figure 574: *Send Test SMS Dialog*



Send Test SMS

Recipient in International format: +12481237654

Message: This is a test message.

2. **Recipient in International format**: Enter the mobile phone number of the recipient in international format.

   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).
3. **Message**: Enter the test message.
4. Click **Send SMS**.

Endpoint Context Servers

This section describes the following topics:

- Introduction
- Endpoint Context Servers Page
- Adding an Endpoint Context Server
- Importing an Endpoint Context Server
- Exporting All Endpoint Context Servers
- Modifying an Endpoint Context Server
- Polling an Endpoint Context Server
- Deleting an Endpoint Context Server

For related information, see:

- Configuring Endpoint Context Server Actions on page 590
- Adding Vendor-Specific Endpoint Context Servers on page 595
- Endpoint Information Collectors on page 436

Introduction

ClearPass Policy Manager provides the ability to collect endpoint profile information from different types of Aruba IAPs (Instant Access Points) and RAPs (Remote Access Points) via Aruba Activate.

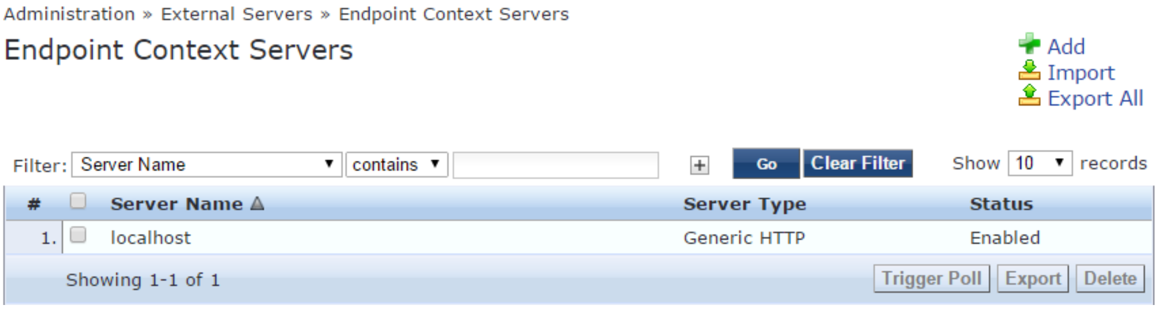
The mobile device management (MDM) platforms run on MDM servers. These servers provision mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Endpoint Context Servers Page

1. To access the Endpoint Context Servers page, navigate to **Administration > External Servers > Endpoint Context Servers**.

   The **Endpoint Context Servers** page appears:

Figure 575: *Endpoint Context Servers Page*



Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

Add
Import
Export All

Filter: Server Name ▾ contains ▾ Go Clear Filter Show 10 ▾ records

#	□	Server Name △	Server Type	Status
1.	□	localhost	Generic HTTP	Enabled

Showing 1-1 of 1 Trigger Poll Export Delete

The following table describes the **Endpoint Context Servers** categories:

Table 315: *Endpoint Context Server Categories*

Parameter	Description
Server Name	Displays the name of the endpoint context server.
Server Type	Displays the type of the endpoint context server.
Status	Displays the status of the endpoint context server: **Enabled** or **Disabled**. For non-MDM servers, the status is always displayed as **Disabled**.

Adding an Endpoint Context Server

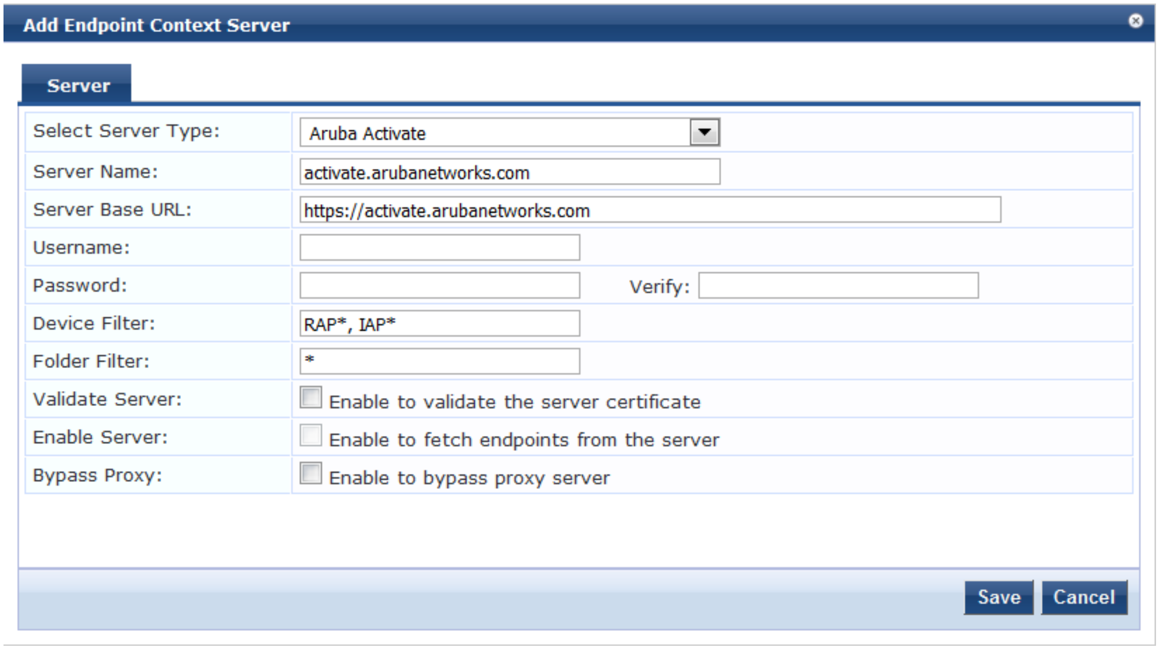
To add an endpoint context server:

1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.
2. Click the **Add** link at the top right section of the page.

   The **Add Endpoint Context Server** dialog opens.

   The fields and parameters that are displayed in the **Add Endpoint Context Server** dialog vary depending on which **Server Type** you select (see **Select Server Type** in Table 316).

Figure 576: *Adding an Endpoint Context Server*



Select Server Type:	Aruba Activate
Server Name:	activate.arubanetworks.com
Server Base URL:	https://activate.arubanetworks.com
Username:	
Password:	Verify:
Device Filter:	RAP*, IAP*
Folder Filter:	*
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

3. In the **Add Endpoint Context Server** dialog, specify the parameters as described in Table 316.
4. Click **Save**.

Table 316 describes the **Add Endpoint Context Servers** parameters:

Table 316: *Add Endpoint Context Server Parameters*

Parameter	Description
Select Server Type	1. Choose one of the Server Types (endpoint context server vendors) from the following options. The Server Type you select determines the configuration parameters. ■ AirWatch ■ Aruba Activate ■ AirWave ■ Google Admin Console ■ Generic HTTP ■ JAMF ■ Juniper SRX ■ 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.
Server Name	2. Enter the name of the server or host.
Server Base URL	3. 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	4. Enter the username.
Password	5. Enter the password of the server or host, then verify the password.
API Key	6. Enter the API key that was provided by the vendor, then verify the API key. This field is not displayed for all endpoint context servers.

Table 316: *Add Endpoint Context Server Parameters (Continued)*

Parameter	Description
Validate Server	7. Select the **Enable to validate the server certificate** check box to validate. By default, this field is disabled. **NOTE:** Checking this option enables the **Certificate** tab.
Enable Server	8. Select the **Enable to fetch endpoints from the server** check box to enable the endpoint context server. By default, this field is disabled. **NOTE:** The **Bypass Proxy** field is enabled only if you enable this field. Checking this option enables the **Poll Status** tab.
Bypass Proxy	9. Select the **Enable to bypass proxy server** check box to bypass the proxy server. By default, this field is disabled. You must enable the **Enable Server** parameter to enable this field. You 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 bypasses the proxy server for functions such MDM API, Endpoint Context Server Actions, and Generic HTTP outbound enforcement. **NOTE:** 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.

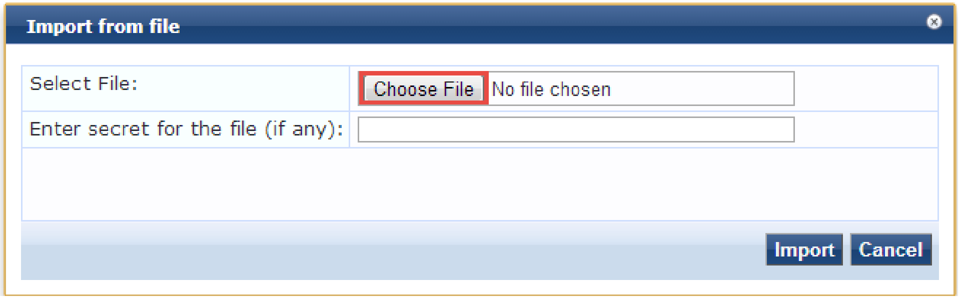
Importing an Endpoint Context Server

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.
3. Enter the parameters based on Table 317.
4. Click **Import**.

Figure 577 displays the **Import from File** dialog:

Figure 577: *Import from File Dialog*



Import from file

Select File: Choose File No file chosen

Enter secret for the file (if any):

The following table describes the **Import from file** parameters:

Table 317: *Import from File Dialog 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.

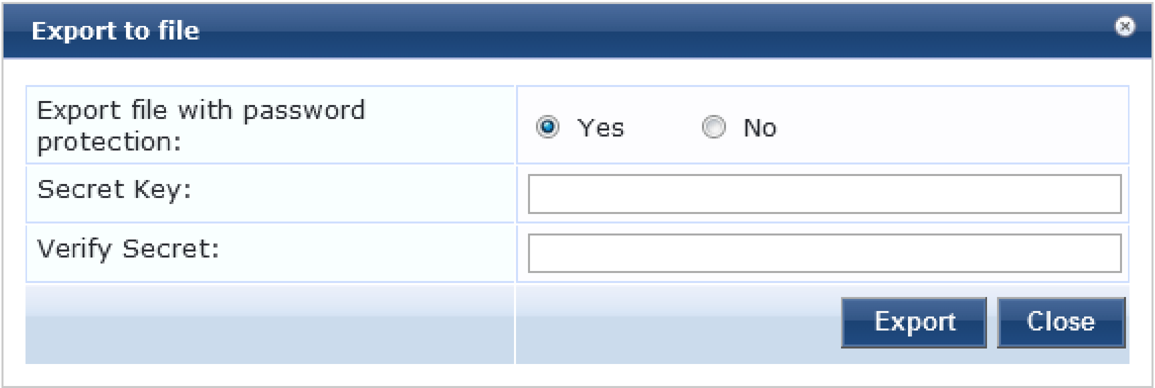
Exporting All Endpoint Context Servers

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.

   The **Export to File** dialog opens.

Figure 578: *Export to File Dialog*



Export to file

Export file with password protection: ● Yes ○ No

Secret Key:

Verify Secret:

3. Enter the parameters as described in Table 318.
4. Click **Export**.
5. Enter the XML file name in the **Save As** dialog box.
6. Click **Save**.

Table 318 describes the **Export to file** parameters:

Table 318: *Export to File Dialog Parameters*

Parameter	Action/Description
Export file with password protection	1. To export the file with password protection, choose **Yes**.
Secret Key	2. Enter the secret key.
Verify Secret	3. 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** dialog, enter the details based on specific **Server Type** (vendor link) listed in Table 316, "Add Endpoint Context Server Parameters."
4. Click **Update**.

NOTE

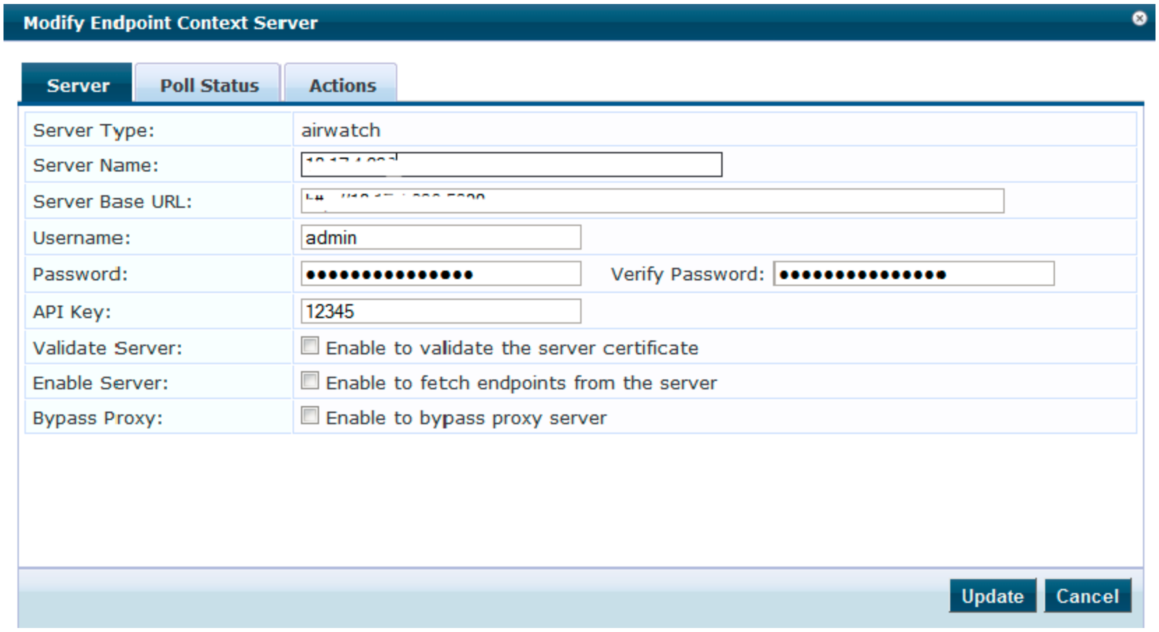
The tabs that appear when you add or modify an endpoint context server vary depending on the type (vendor) of endpoint context server selected.

Server Tab

Use the **Server** tab to modify the server name, server base URL, and API key.

You can also use this dialog to validate the server certificate and to bypass proxy servers. The following figure displays the **Modify Endpoint Context Server** > **Server** dialog:

Figure 579: *Modify Endpoint Context Server > Server Dialog*



Modify Endpoint Context Server

Server Type:	airwatch
Server Name:	[redacted]
Server Base URL:	[redacted]
Username:	admin
Password:	●●●●●●●●●●●●●●● Verify Password: ●●●●●●●●●●●●●●●
API Key:	12345
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

The following table describes the **Modify Endpoint Context Server** > **Server** parameters:

Table 319: *Modify Endpoint Context Server > Server Parameters*

Parameter	Action Description
Server Type	The **Server Type** cannot be modified.
Server Name	1. Enter the name of the server or host.
Server Base URL	2. 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	3. Enter the username of the server or host.
Password	4. Enter the password of the server or host, then verify the password.
Validate Server	5. Enable this check box to validate the server certificate. By default, this field is disabled. **NOTE:** Checking this option enables the **Certificate** tab.
Bypass Proxy	6. Select the **Enable to bypass proxy server** check box to bypass the proxy server. By default, this field is disabled. You must enable the **Enable Server** parameter to enable this field. You 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 bypasses the proxy server for functions such MDM API, Endpoint Context Server Actions, and Generic HTTP outbound enforcement. **NOTE:** 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.

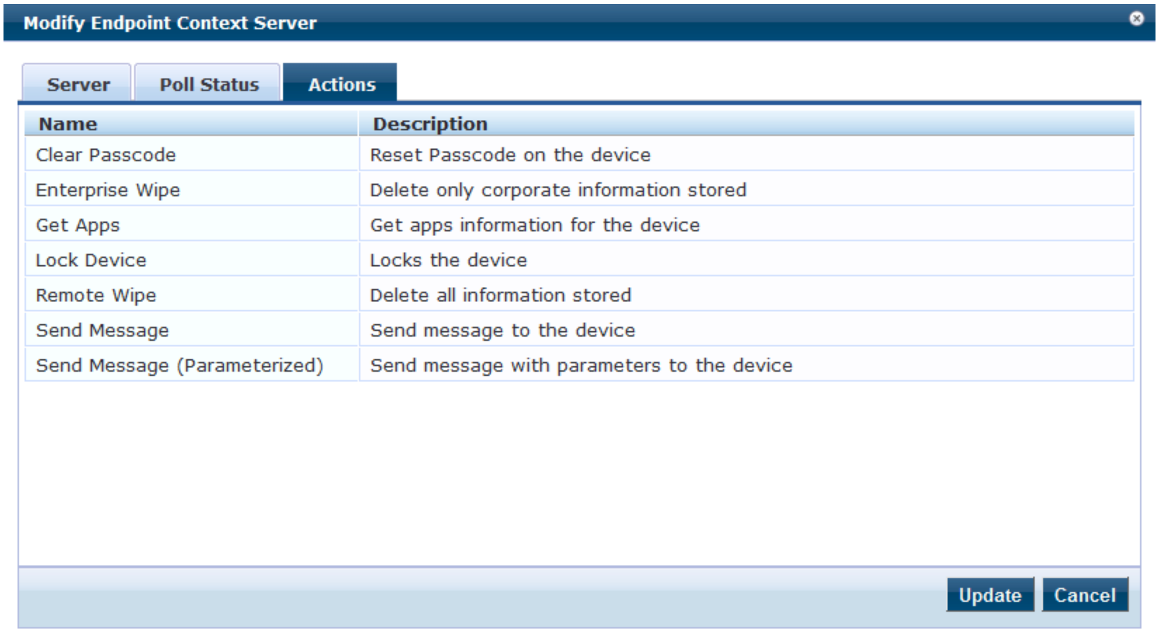
Actions Tab

Use the **Actions** tab to view the server action that is performed on endpoints and their description. The fields and parameters that are displayed in the **Actions** dialog vary depending on which **Server Type** you select (see the **Select Server Type** vendor links listed in Table 316, "Add Endpoint Context Server Parameters").

For more information about endpoint context server actions configuration, see Configuring Endpoint Context Server Actions on page 590.

The following figure displays an example of the **Modify Endpoint Context Server > Actions** tab:

Figure 580: *Modify Endpoint Context Server > Actions Tab*



Name	Description
Clear Passcode	Reset Passcode on the device
Enterprise Wipe	Delete only corporate information stored
Get Apps	Get apps information for the device
Lock Device	Locks the device
Remote Wipe	Delete all information stored
Send Message	Send message to the device
Send Message (Parameterized)	Send message with parameters to the device

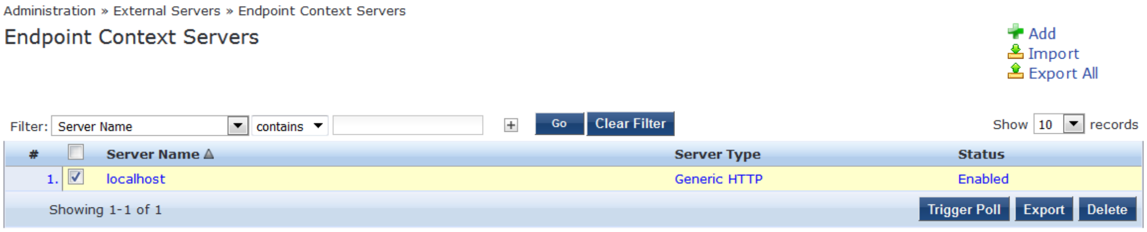
Polling an Endpoint Context Server

To poll an endpoint context server:

> NOTE
>
> You can poll only one server at a time. You cannot poll multiple server entries. Also, you can only poll MDM-type servers.

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.

Figure 581: *Selecting the Trigger Poll Option*



#	□	Server Name ▲	Server Type	Status
1.	☑	localhost	Generic HTTP	Enabled

3. Click **Trigger Poll**.

Deleting an Endpoint Context Server

Deleting an endpoint context server removes the configuration information from the Policy Manager server.

To save the endpoint context server configuration prior to deleting the server:

1. Before you delete the endpoint context server, export the server.
2. Save the configuration so that you can import it in future if necessary.

To delete an endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.
2. Select the check box next to the server name entry, then click **Delete**.
3. To confirm the delete operation, click **Yes**.

Configuring Endpoint Context Server Actions

This section contains the following information:

- Filtering an Endpoint Context Server Action Report
- Configuring Endpoint Context Server Actions
- Adding machine-os and host-type Endpoint Attributes

Filtering an Endpoint Context Server Action Report

Use the **Filter** controls to configure a search for a subset of Endpoint Context Server Action items.

To filter an endpoint context server action report:

1. Navigate to **Administration > Dictionaries > Context Server Actions.**

   The Endpoint Context Server Actions page appears (see Figure 582).
2. From the Filter drop-down, select a filter: **ServerType**, **Action Name**, or **HTTP method**.
3. To add up to four new search fields, click the **Plus** icon.
4. Select a search argument.

   The search arguments are limited to **contains** or **equals**.
5. Click **Go**.

Configuring 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.

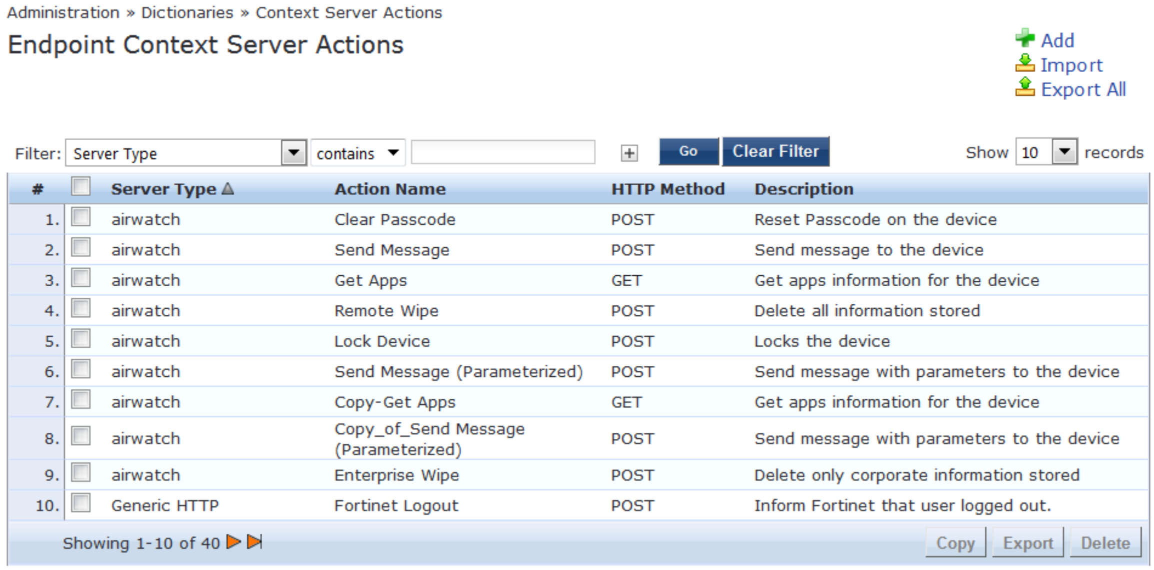
The **Context Server Actions** page displays the report that shows information about all configured Endpoint Context Server Actions.

To configure endpoint context server actions:

1. Navigate to **Administration > Dictionaries > Context Server Actions** > **Endpoint Context Server Actions** page.

   Figure 582 displays an example of the **Endpoint Context Server Actions** page:

Figure 582: *Endpoint Context Server Actions Page*



Administration » Dictionaries » Context Server Actions

Endpoint Context Server Actions

#		Server Type	Action Name	HTTP Method	Description
1.	□	airwatch	Clear Passcode	POST	Reset Passcode on the device
2.	□	airwatch	Send Message	POST	Send message to the device
3.	□	airwatch	Get Apps	GET	Get apps information for the device
4.	□	airwatch	Remote Wipe	POST	Delete all information stored
5.	□	airwatch	Lock Device	POST	Locks the device
6.	□	airwatch	Send Message (Parameterized)	POST	Send message with parameters to the device
7.	□	airwatch	Copy-Get Apps	GET	Get apps information for the device
8.	□	airwatch	Copy_of_Send Message (Parameterized)	POST	Send message with parameters to the device
9.	□	airwatch	Enterprise Wipe	POST	Delete only corporate information stored
10.	□	Generic HTTP	Fortinet Logout	POST	Inform Fortinet that user logged out.

Showing 1-10 of 40

Table 320 describes the **Endpoint Context Server Actions** settings:

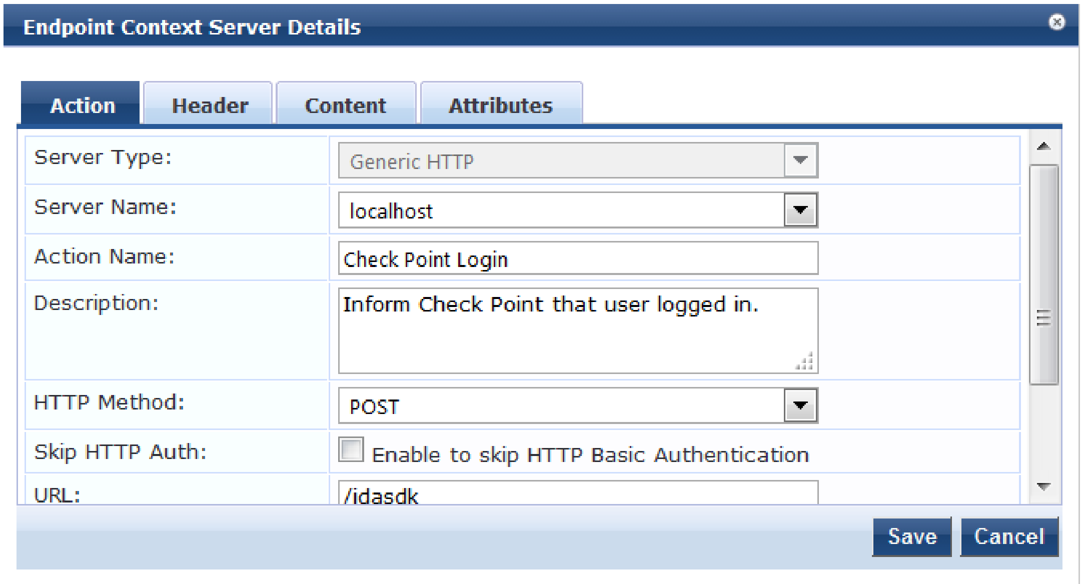
Table 320: *Endpoint Context Server Actions Page Settings*

Settings	Description
Server Type	Indicates the server type configured when the server action was configured.
Action Name	Indicates the name of the context server action. The available server actions vary depending on what Server Type is specified.
HTTP Method	Specifies the HTTP method selected when the server action was configured.
Description	Provides the description of the server action.

2. From the **Endpoint Context Server Actions** page, click a row in the report.

   The **Endpoint Content Server Details** dialog appears.

Figure 583: *Endpoint Context Server Details Dialog*



Server Type:	Generic HTTP
Server Name:	localhost
Action Name:	Check Point Login
Description:	Inform Check Point that user logged in.
HTTP Method:	POST
Skip HTTP Auth:	☐ Enable to skip HTTP Basic Authentication
URL:	/idasdk

3. Click a tab to view details about the selected Endpoint Context Server action.
4. Make any changes required, then click **Save**.

Action Tab Parameters

Use the **Action** tab to specify the server type, action name, HTTP method, and URL for the specified HTTP method.

Table 321 describes the the **Action** tab parameters.

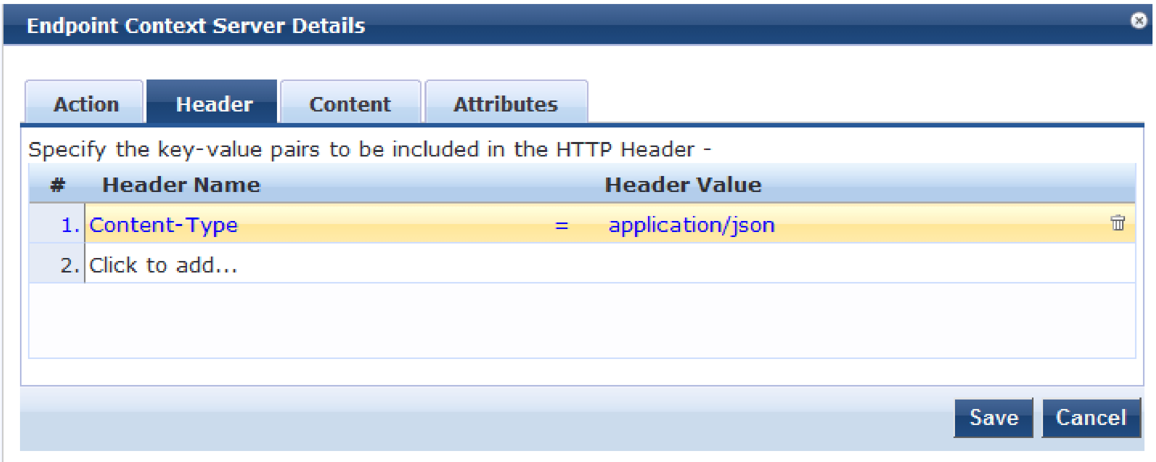
Table 321: *Action Parameters—Endpoint Context Server Details*

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 to be used in context server actions.
URL	Indicates the URL for the selected HTTP method.

Header Tab Parameters

Use the **Header** tab to specify the key-value pairs to be included in the HTTP header.

Figure 584: *Header Tab—Endpoint Context Server Details*



Endpoint Context Server Details

Specify the key-value pairs to be included in the HTTP Header -

#	Header Name		Header Value
1.	Content-Type	=	application/json
2.	Click to add...		

Table 322 describes the **Endpoint Context Server Details—Header** parameters:

Table 322: *Header Parameters—Endpoint Context Server Details*

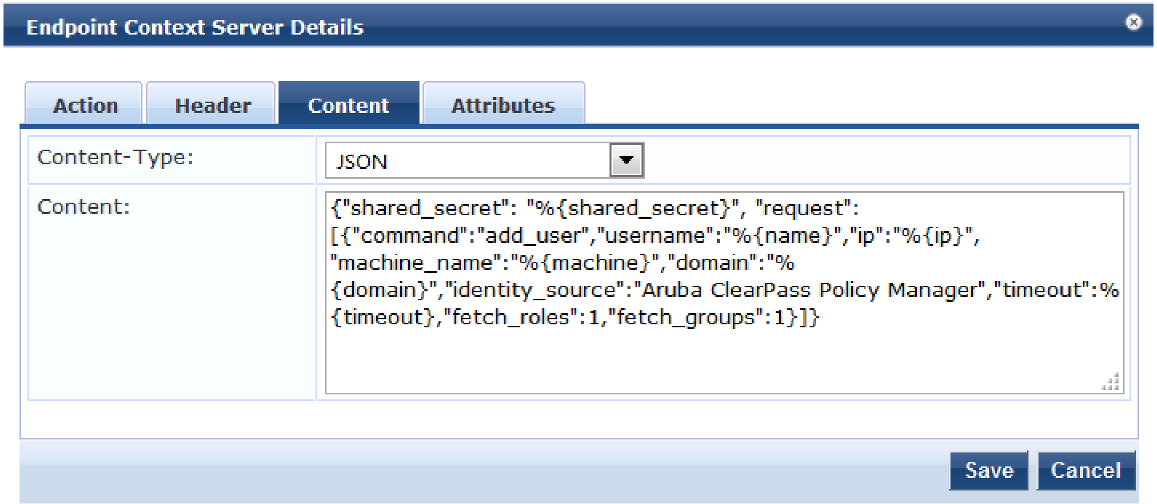
Parameter	Description
Header Name	Specify the name of the header to be included in the HTTP header.
Header Value	Specify the value of the header specific to the name to be included in the HTTP header.

Content Tab

Use the **Content** tab to specify a content type and add non-default context server attributes (see Figure 585).

The information in the Content window is the template of what will be posted to the server. The fields preceded by the % sign are replaced with their corresponding values.

Figure 585: *Content Tab—Endpoint Context Server Details*



Content-Type: JSON

Content:

```
{"shared_secret": "%{shared_secret}", "request":
[{"command":"add_user","username":"%{name}","ip":"%{ip}",
"machine_name":"%{machine}","domain":"%
{domain}","identity_source":"Aruba ClearPass Policy Manager","timeout":%
{timeout},"fetch_roles":1,"fetch_groups":1}]}
```

Table 323 describes the **Endpoint Context Server Details—Content** parameters:

Table 323: *Content Parameters—Endpoint Context Server Details*

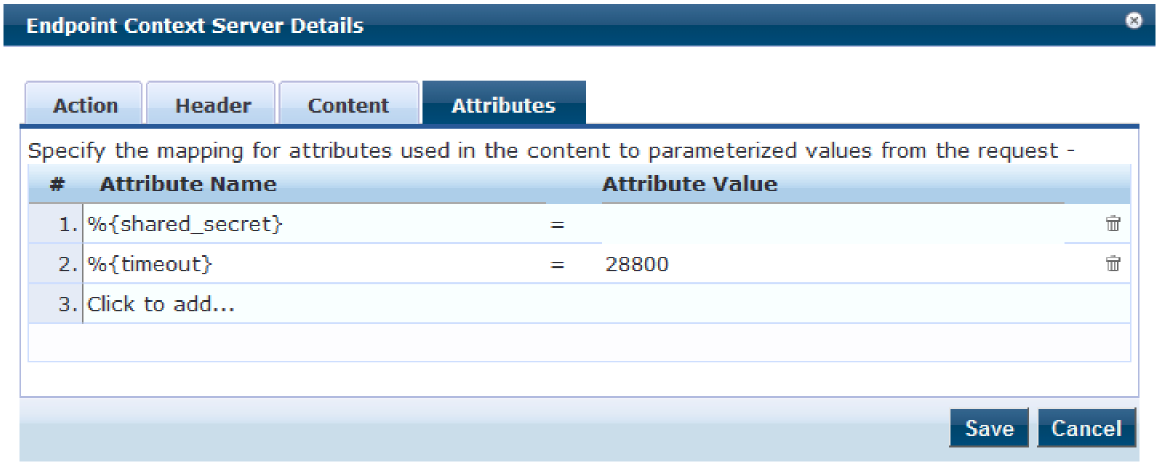
Parameter	Description
Content-Type	Specify the type of the content. Select from the following options: ● CUSTOM ● HTML ● JSON ● PLAIN ● XML
Content	Specify the content. For example, { "mac": "%{Connection:Client-Mac-Address-NoDelim} ","nmap": {"device": "%{DEVICECATEGORY}"}}.

For related information, see Adding machine-os and host-type Endpoint Attributes on page 594).

Attributes Tab Parameters

Use the **Attributes** tab to specify the mapping for attributes used in the content to parameterized values from the request.

Figure 586: *Attributes Tab—Endpoint Context Server Details*



Specify the mapping for attributes used in the content to parameterized values from the request -

#	Attribute Name		Attribute Value
1.	%{shared_secret}	=	
2.	%{timeout}	=	28800
3.	Click to add...		

Table 324 describes the **Endpoint Context Server Details—Attributes** parameters:

Table 324: *Attributes Parameters—Endpoint Context Server Details*

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.

Adding machine-os and host-type Endpoint Attributes

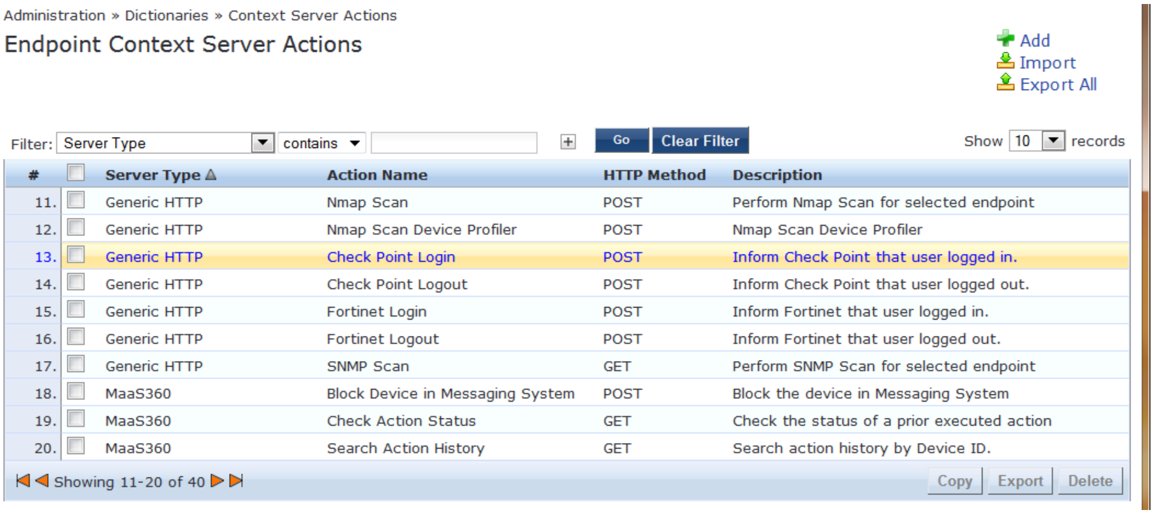
To be able to indicate the entire OS family (Android, Windows, Linux, etc.) and the type of device (iPad, iPhone, etc.), you can add the **machine-os** Device Family attribute and the **host-type** Device Type attribute to the default set of endpoint context attributes provided in the Content window:

To add the **machine-os** and **host-type** endpoint context attributes:

1. Navigate to **Administration** > **Dictionaries** > **Context Server Actions**.

   The **Endpoint Context Server Actions** page appears.
2. Scroll to and select the **Generic HTTP/Check Point Login** server action.

Figure 587: *Selecting the Check Point Login Server Action*

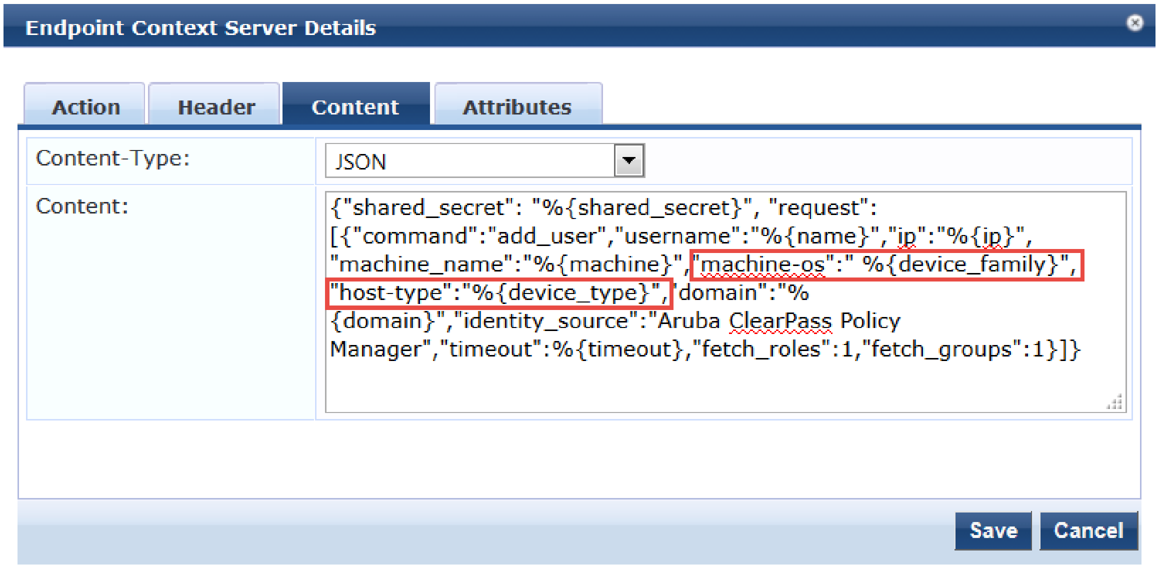

Administration » Dictionaries » Context Server Actions
Endpoint Context Server Actions
Add
Import
Export All
Filter: Server Type
contains
Go
Clear Filter
Show 10 records

#	☐	Server Type	Action Name	HTTP Method	Description
11.	☐	Generic HTTP	Nmap Scan	POST	Perform Nmap Scan for selected endpoint
12.	☐	Generic HTTP	Nmap Scan Device Profiler	POST	Nmap Scan Device Profiler
13.	☐	Generic HTTP	Check Point Login	POST	Inform Check Point that user logged in.
14.	☐	Generic HTTP	Check Point Logout	POST	Inform Check Point that user logged out.
15.	☐	Generic HTTP	Fortinet Login	POST	Inform Fortinet that user logged in.
16.	☐	Generic HTTP	Fortinet Logout	POST	Inform Fortinet that user logged out.
17.	☐	Generic HTTP	SNMP Scan	GET	Perform SNMP Scan for selected endpoint
18.	☐	MaaS360	Block Device in Messaging System	POST	Block the device in Messaging System
19.	☐	MaaS360	Check Action Status	GET	Check the status of a prior executed action
20.	☐	MaaS360	Search Action History	GET	Search action history by Device ID.

The **Endpoint Context Server Details** dialog appears.

3. Select the **Content** tab (see Figure 588).
4. In the **Content** field, add the following attributes (see Figure 588):
   - "machine-os":" %{device_family}"
   - "host-type":"%{device_type}"

Figure 588: *Adding Endpoint Context Server Attributes*



Content-Type: JSON

Content:

```
{"shared_secret": "%{shared_secret}", "request":
[{"command":"add_user","username":"%{name}","ip":"%{ip}",
"machine_name":"%{machine}","machine-os":" %{device_family}",
"host-type":"%{device_type}","domain":"%
{domain}","identity_source":"Aruba ClearPass Policy
Manager","timeout":%{timeout},"fetch_roles":1,"fetch_groups":1}]}
```

5. Click **Save**.

   You receive the following message:

   Context Server Action "Check Point Login (Generic HTTP)" updated successfully

Adding Vendor-Specific Endpoint Context Servers

This section provides information on the following topics:

- Adding an AirWatch Endpoint Context Server
- Adding an AirWave Endpoint Context Server

- Adding an Aruba Activate Endpoint Context Server
- Adding a ClearPass Cloud Proxy Endpoint Context Server
- Adding a Generic HTTP Endpoint Context Server
- Adding a Google Admin Console Endpoint Context Server
- Integrating ClearPass with Infoblox
- Adding a JAMF Endpoint Context Server
- Integrating ClearPass with Juniper Networks SRX
- Adding a MaaS360 Endpoint Context Server
- Adding a MobileIron Endpoint Context Server
- Adding a Palo Alto Networks Firewall Endpoint Context Server
- Adding a Palo Alto Networks Panorama Endpoint Context Server
- Adding an SAP Afaria Endpoint Context Server
- Adding a SOTI Endpoint Context Server
- Adding a XenMobile Endpoint Context Server

Adding an AirWatch Endpoint Context Server

Consult Airwatch's documentation for information about the parameters that you must enter to configure this endpoint.

To add an Airwatch Endpoint Context Server:

1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.

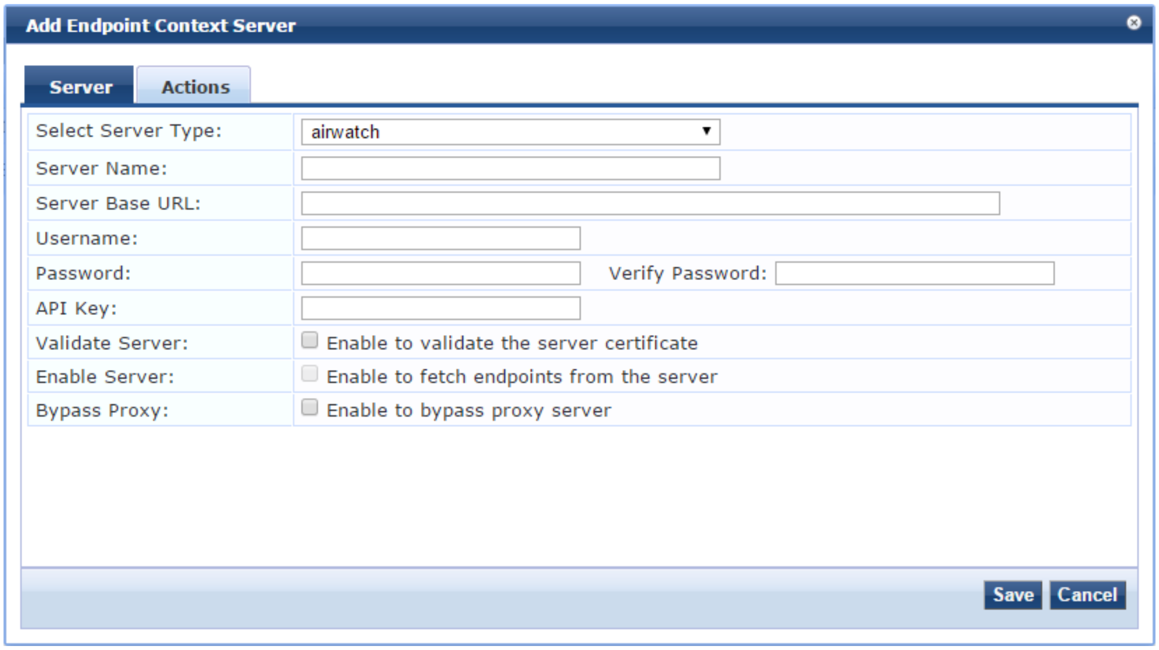
   The **Endpoint Context Servers** page appears.
2. Click **Add**.

   The **Add Endpoint Context Server** dialog appears. This dialog opens in the **Server** tab.
3. From the **Select Server Type** drop-down, select **airwatch**.

Server Tab

The following figure displays the **Airwatch Add Endpoint Context Server - Server** dialog:

Figure 589: *Adding an Airwatch Endpoint Context Server - Server Dialog*



Add Endpoint Context Server

Select Server Type:	airwatch
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
API Key:	
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

NOTE

You can add more than one endpoint context server of the same type.

The following table displays the **Add Endpoint Context Server - Server** (AirWatch) tab parameters:

Table 325: *Adding an Airwatch Endpoint Context Server - Server 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 user name.
Password	Enter and verify the password.
Verify Password	
API Key	Enter the API key that is provided by the vendor.

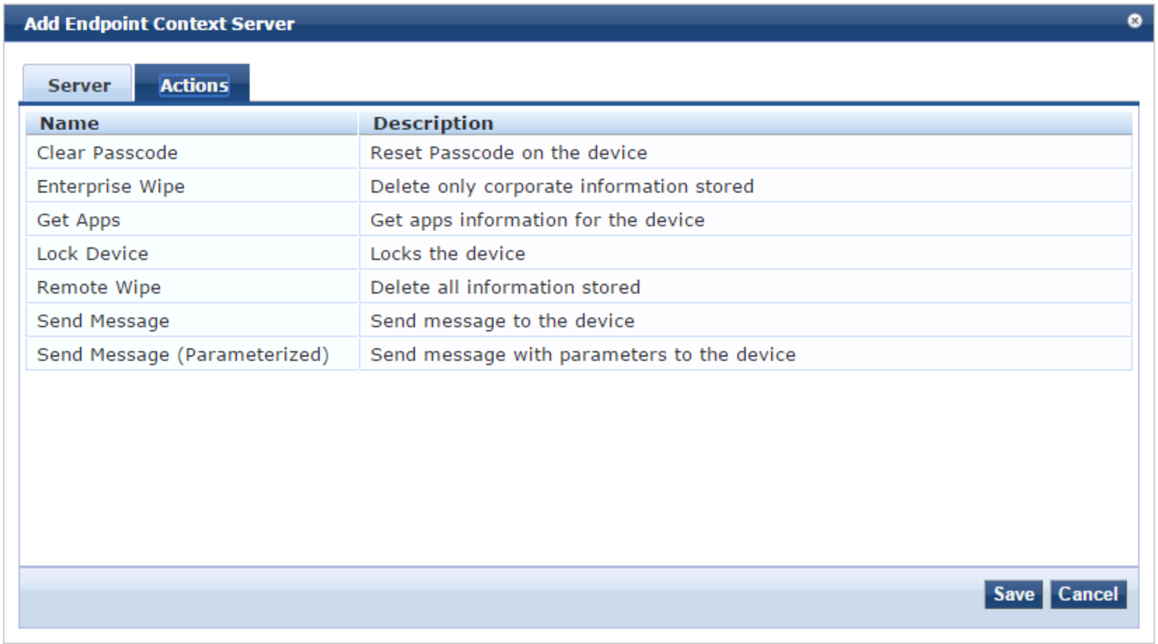
Table 325: *Adding an Airwatch Endpoint Context Server - Server Tab Parameters (Continued)*

Parameter	Description
Validate Server	Enable to validate the server certificate. Checking this option activates 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 table displays the **Airwatch Add Endpoint Context Server - Server** dialog parameters:

Figure 590: *Adding an Airwatch Endpoint Context Server - Actions Dialog*



Name	Description
Clear Passcode	Reset Passcode on the device
Enterprise Wipe	Delete only corporate information stored
Get Apps	Get apps information for the device
Lock Device	Locks the device
Remote Wipe	Delete all information stored
Send Message	Send message to the device
Send Message (Parameterized)	Send message with parameters to the device

The following table describes the **Airwatch Add Endpoint Context Server - Actions** dialog parameters:

Table 326: *Adding an Airwatch Endpoint Context Server - Actions 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 AirWave Endpoint Context Server

For more information about AirWave, refer to Aruba AirWave documentation.

To add an AirWave Endpoint Context Server:

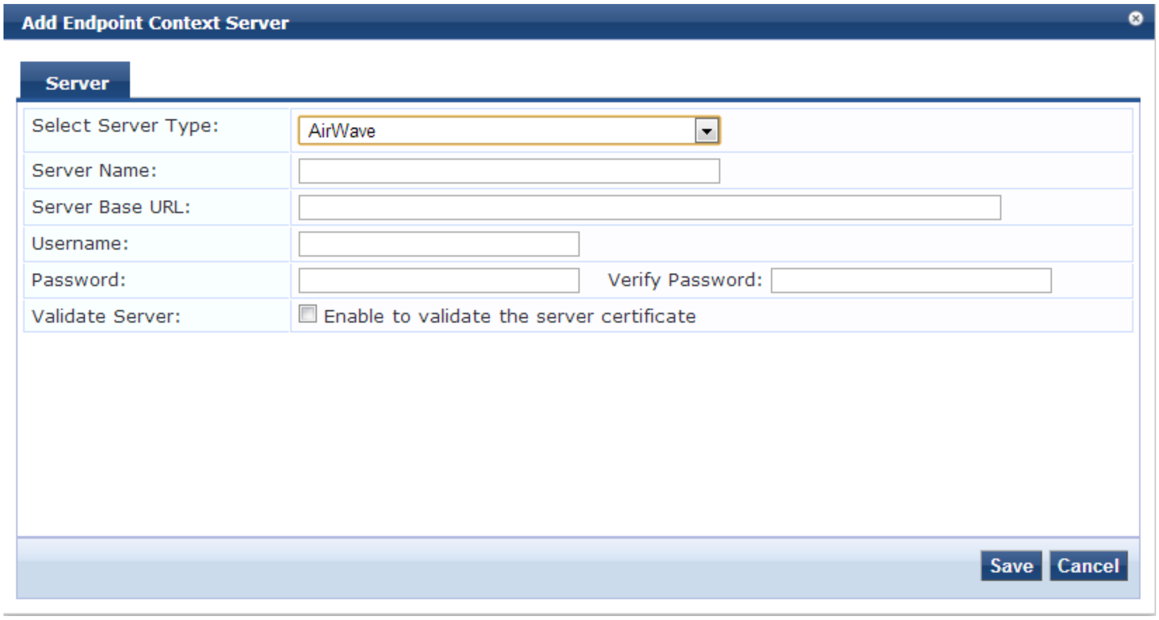
1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.

   The **Endpoint Context Servers** page opens.
2. Click **Add**.

   The **Add Endpoint Context Server** dialog opens.
3. From the **Select Server Type** drop-down, select **AirWave**.

   The following dialog is displayed:

Figure 591: *Add an AirWave Endpoint Context Server > Server Dialog*



Select Server Type: AirWave

Server Name:

Server Base URL:

Username:

Password: Verify Password:

Validate Server: □ Enable to validate the server certificate

NOTE

You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the AirWave Add Endpoint Context Server parameters described in Table 327.
5. When satisfied with the settings, click **Save**.

Table 327: *Adding an AirWave Endpoint Context Server > Server Parameters*

Parameter	Action/Description
Select Server Type	1. Choose **AirWave** from the **Select Server Type** drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or hostname.
Server Base URL	3. Enter the full URL for the AirWave server. You can append a custom port, such as for an MDM server: *https://yourserver.yourcompany.com:customerportnumber*
Username	4. Enter the username for the AirWave server.
Password	5. Enter the password for the server, then verify the password.
Verify Password	
Validate Server	6. Enable **Validate Server** to validate the server certificate. Checking this option enables the **Certificate** tab.
Bypass Proxy	7. Enable **Bypass Proxy** to bypass the proxy server.

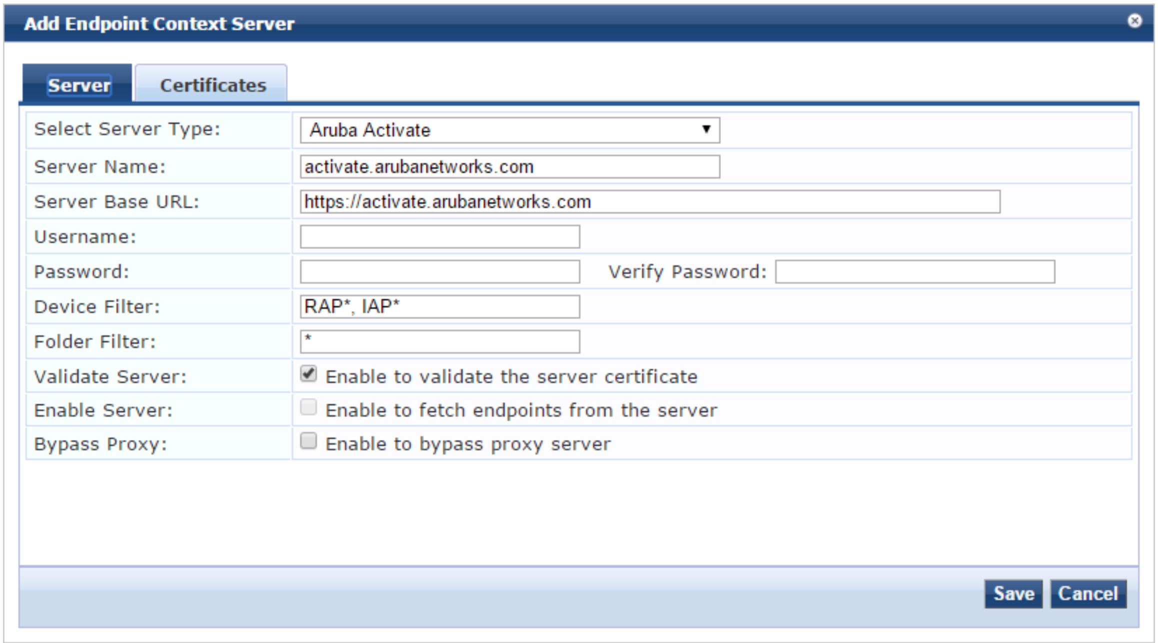
Adding an Aruba Activate Endpoint Context Server

For more information about Activate, refer to Aruba Activate documentation.

Server Tab

The following figure displays the **Aruba Activate Add Endpoint Context Server > Server** tab:

Figure 592: *Adding an Aruba Activate Endpoint Context Server*



Add Endpoint Context Server

Select Server Type:	Aruba Activate
Server Name:	activate.arubanetworks.com
Server Base URL:	https://activate.arubanetworks.com
Username:	
Password:	Verify Password:
Device Filter:	RAP*, IAP*
Folder Filter:	*
Validate Server:	☑ Enable to validate the server certificate
Enable Server:	☐ Enable to fetch endpoints from the server
Bypass Proxy:	☐ Enable to bypass proxy server

The following table describes the **Aruba Activate Add Endpoint Context Server > Server** parameters:

Table 328: *Adding an Aruba Activate Endpoint Context Server > Server Parameters*

Parameter	Action/Description
Select Server Type	1. Choose **Aruba Activate** from the **Select Server Type** drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	3. Enter the complete URL for the Aruba Activate server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber
Username	4. Enter the username for the Aruba Activate server.
Password	5. Enter the password, then verify the password.
Verify Password	
Device Filter	The **Device Filter** field is populated with a default regular expression to retrieve only the Remote AP (RAP) and Instant AP (IAP) information.
Folder Filter	The **Folder Filter** field is set to "*" by default.

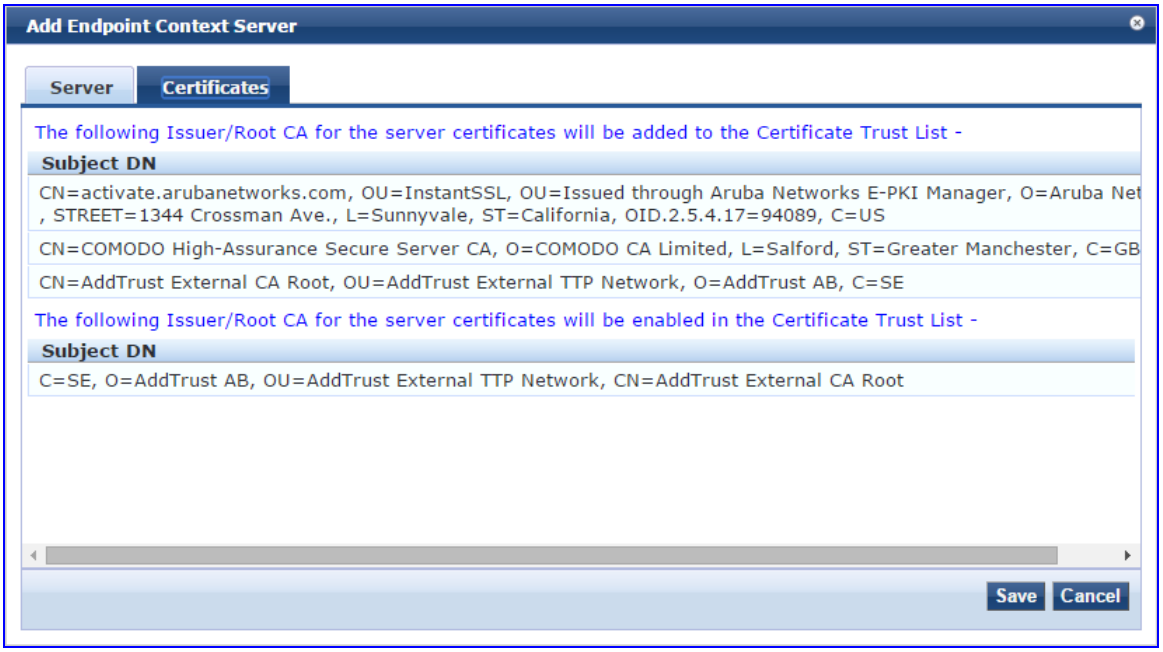
Table 328: *Adding an Aruba Activate Endpoint Context Server > Server Parameters (Continued)*

Parameter	Action/Description
Disable Stale Enpoints	6. To disable stale endpoints in the Endpoint database, enable this option.
Validate Server	7. Enable **Validate Server** to validate the server certificate. Checking this option enables the **Certificate** tab. For information on certificate configuration, see Certificates Tab on page 602.
Enable Server	8. Enable **Enable Server** to fetch endpoints from the server.
Bypass Proxy	9. Enable **Bypass Proxy** to bypass the proxy server.
	10. To save your configuration changes, click **Save**.

Certificates Tab

The following figure displays the **Aruba Activate Add Endpoint Context Server > Certificates** tab:

Figure 593: *Adding an Aruba Activate Endpoint Context Server > Certificates*



The following Issuer/Root CA for the server certificates will be added to the Certificate Trust List -

Subject DN
CN=activate.arubanetworks.com, OU=InstantSSL, OU=Issued through Aruba Networks E-PKI Manager, O=Aruba Net , STREET=1344 Crossman Ave., L=Sunnyvale, ST=California, OID.2.5.4.17=94089, C=US
CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE

The following Issuer/Root CA for the server certificates will be enabled in the Certificate Trust List -

Subject DN
C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root

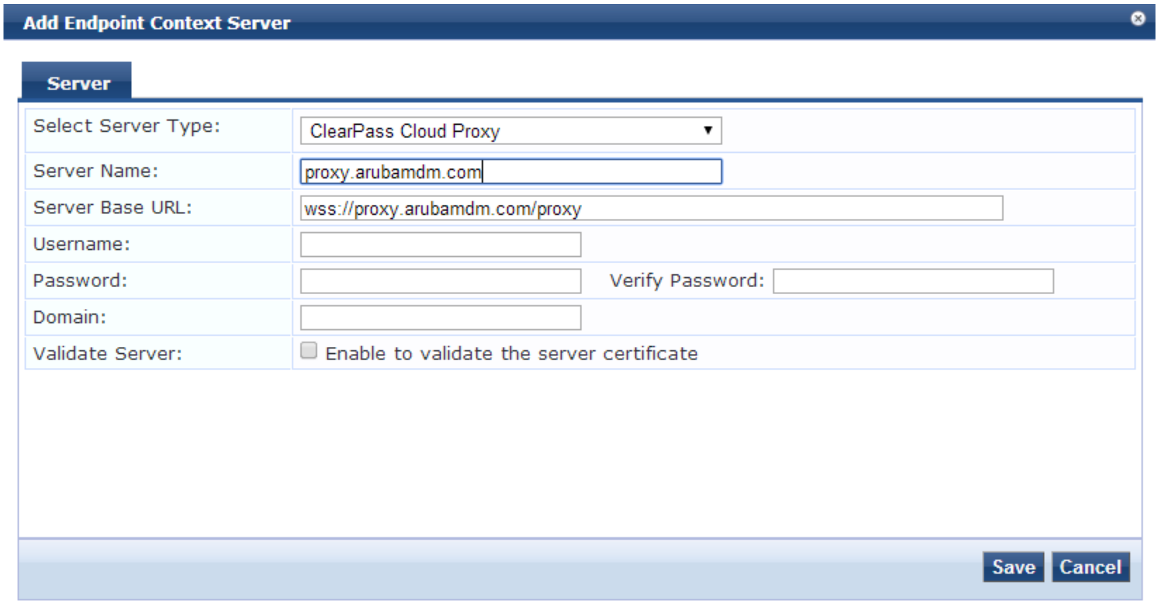
Adding a ClearPass Cloud Proxy Endpoint Context Server

The Cloud Proxy is a virtual instance configured in the cloud. This multi-tenant and single instance serves multiple customers having many ClearPass server nodes.

Once configured, the ClearPass Policy Manager server establishes a Cloud Tunnel to the Cloud Proxy instance given the credentials and Domain. The Domain is required as an identifier to indicate which Cloud Tunnel is applicable for which customer.

You can select individual ClearPass nodes in the cluster to establish the Cloud Tunnel, rather than all nodes in the ClearPass cluster.

Figure 594: *Add ClearPass Cloud Proxy Endpoint Context Server Dialog*



Select Server Type:	ClearPass Cloud Proxy
Server Name:	proxy.arubamdm.com
Server Base URL:	wss://proxy.arubamdm.com/proxy
Username:	
Password:	Verify Password:
Domain:	
Validate Server:	□ Enable to validate the server certificate

Specify the ClearPass Cloud Proxy Endpoint parameters as described in the following table:

Table 329: *Add ClearPass Cloud Proxy Endpoint Context Server Parameters*

Parameter	Action/Description
Select Server Type	Select **ClearPass Cloud Proxy**.
Server Name	Enter the host name of the cloud instance that will proxy all requests directed to the ClearPass server in the enterprise.
Server Base URL	Enter the full URL for the server. The default URL is the name you entered above with *https://* prepended. You can append a custom port, such as for an MDM (Mobile Device Management) server: *https://yourserver.yourcompany.com:customerportnumber*
Username	Enter the username. Username/Password-based authentication is used when you set up a cloud tunnel from the ClearPass server to the Cloud Proxy instance.
Password Verify Password	Enter the password, then verify it.
Domain	Specify a domain identifier used to determine the specific Cloud Tunnel to which the request must be sent by the Cloud Proxy.
Validate Server	Click the **Validate Server** check box to enable validation of the server certificate.

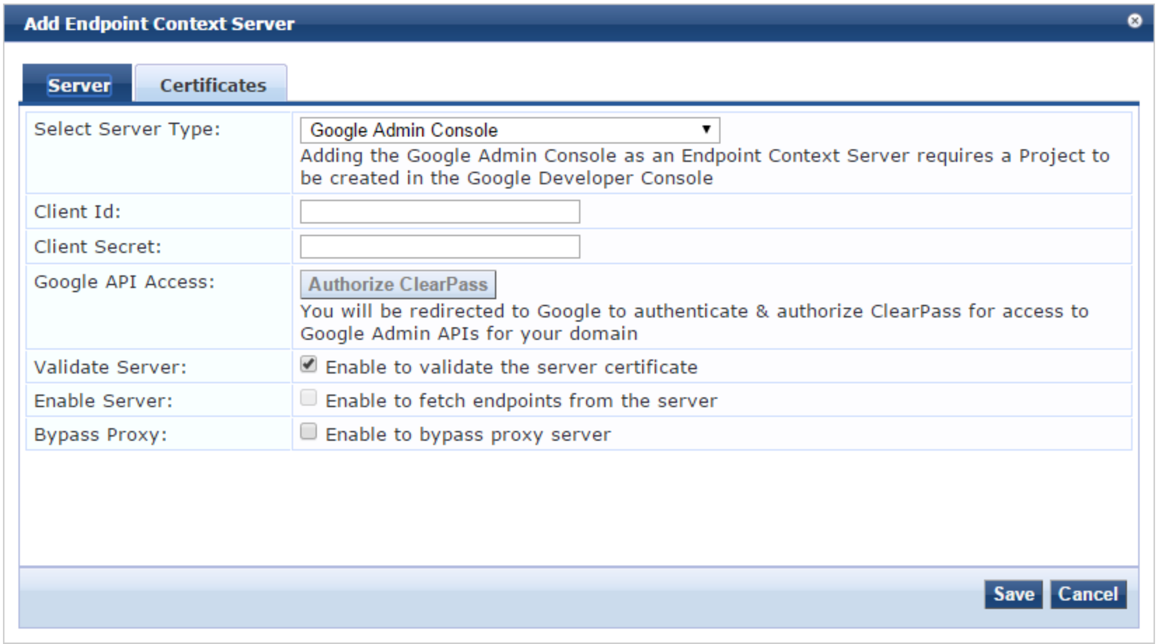
Adding a Google Admin Console Endpoint Context Server

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 595: *Add Endpoint Context Server - Server (Google Admin Console) Tab*



Add Endpoint Context Server

Select Server Type: Google Admin Console
Adding the Google Admin Console as an Endpoint Context Server requires a Project to be created in the Google Developer Console

Client Id:

Client Secret:

Google API Access: Authorize ClearPass
You will be redirected to Google to authenticate & authorize ClearPass for access to Google Admin APIs for your domain

Validate Server: ☑ Enable to validate the server certificate

Enable Server: ☐ Enable to fetch endpoints from the server

Bypass Proxy: ☐ Enable to bypass proxy server

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 330: *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.

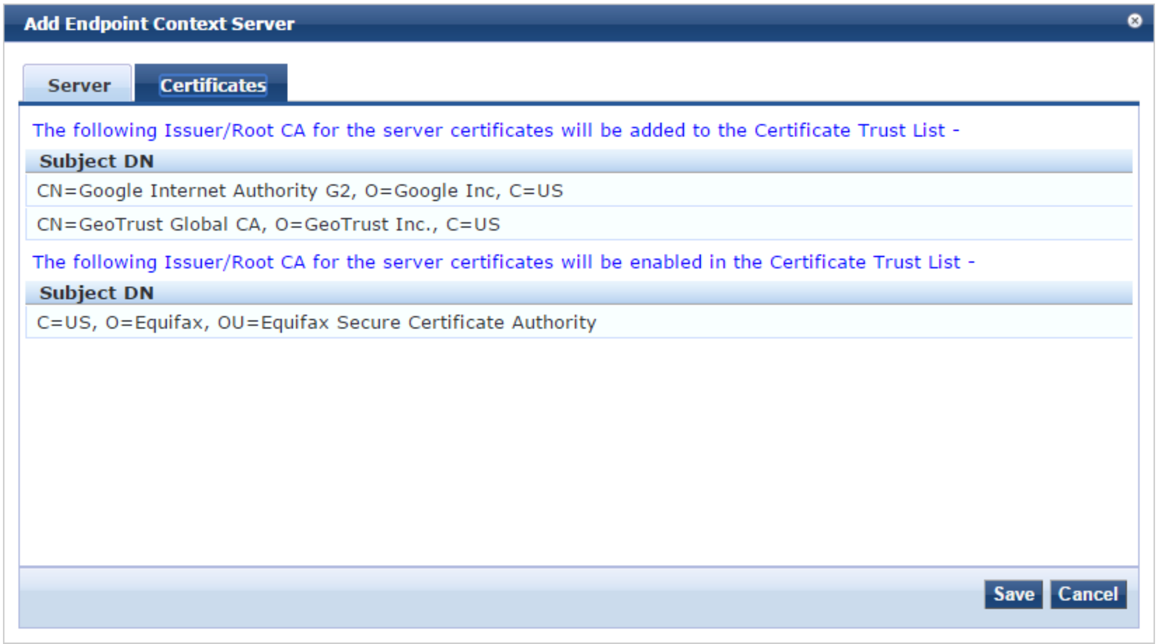
Table 330: *Add Endpoint Context Server - Server (Google Admin Console) Tab Parameters (Continued)*

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 605.
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 596: *Add Endpoint Context Server - Certificates (Google Admin Console) Tab*



The following Issuer/Root CA for the server certificates will be added to the Certificate Trust List -

Subject DN
CN=Google Internet Authority G2, O=Google Inc, C=US
CN=GeoTrust Global CA, O=GeoTrust Inc., C=US

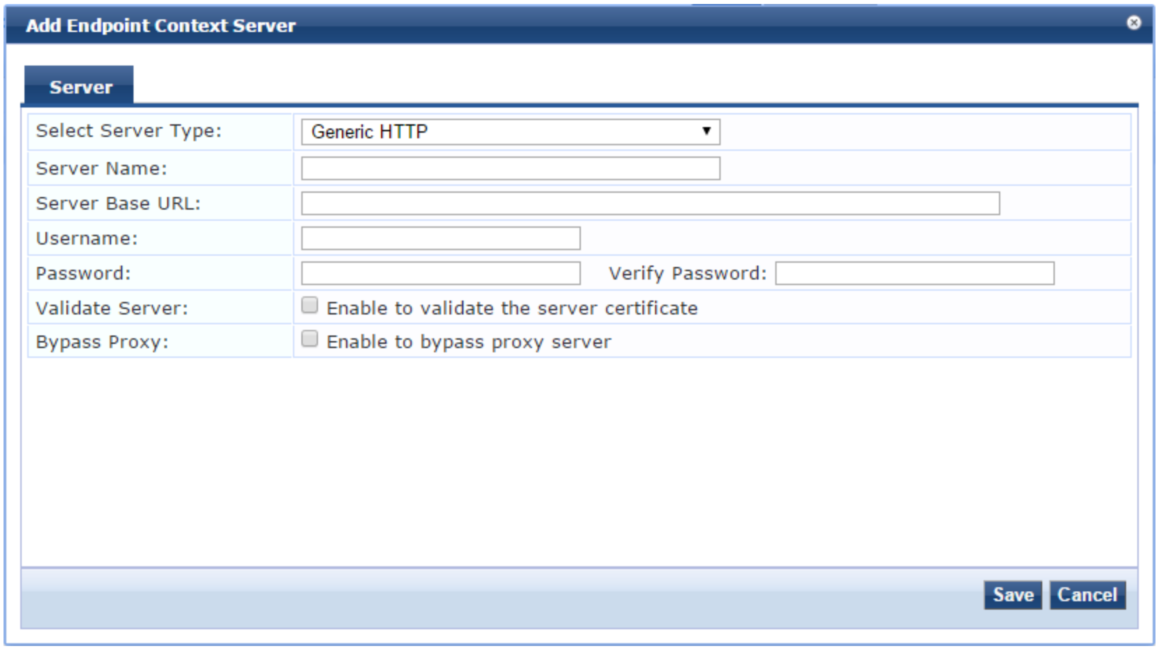
The following Issuer/Root CA for the server certificates will be enabled in the Certificate Trust List -

Subject DN
C=US, O=Equifax, OU=Equifax Secure Certificate Authority

Adding a Generic HTTP Endpoint Context Server

The following figure displays the **Generic HTTP Add Endpoint Context Server > Server** tab:

Figure 597: *Adding a Generic HTTP Endpoint Context Server*



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 **Generic HTTP Add Endpoint Context Server > Server** parameters:

Table 331: *Add Endpoint Context Server - Server (Generic HTTP) Tab Parameters*

Parameter	Action/Description
Select Server Type	1. Choose **Generic HTTP** from the Select Server Type drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	3. Enter the complete URL for the server. You can append a custom port, such as for an MDM server: *https://yourserver.yourcompany.com:customerportnumber*
Username	4. Enter the username for the server.
Password	5. Enter the password, then verify the password.
Verify Password	

Table 331: *Add Endpoint Context Server - Server (Generic HTTP) Tab Parameters (Continued)*

Parameter	Action/Description
Validate Server	6. Enable **Validate Server** to validate the server certificate. Checking this option enables the **Certificate** tab.
Bypass Proxy	7. Enable **Bypass Proxy** to bypass the proxy server.
	8. Click **Save** to save your changes.

Integrating ClearPass with Infoblox

This section provides the following information:

- Adding an Infoblox Endpoint Context Server
- Adding a Context Server Action to the Infoblox Server
- Creating an Infoblox Enforcement Profile
- Configuring an Infoblox RADIUS Enforcement Profile
- Creating an Infoblox Enforcement Policy
- Defining an Infoblox Service
- Authenticating External Devices Against the Infoblox Service
- Creating a Filter to Accept Information from the ClearPass Server

Infoblox is a server that provides a host of services, such as DNS, DHCP, and IPAM (IP address management). Infoblox provides a DHCP management system that issues IP addresses to externally authenticated devices and also maintains a MAC address context associated with the newly allocated IP address.

Integrating ClearPass with Infoblox typically tags the username context, as well as the external device being authenticated, along with its respective MAC address, which further simplifies IP address management on the Infoblox side.

This section describes the configurations that you must make on the ClearPass server in order for the ClearPass server to send data to an Infoblox server.

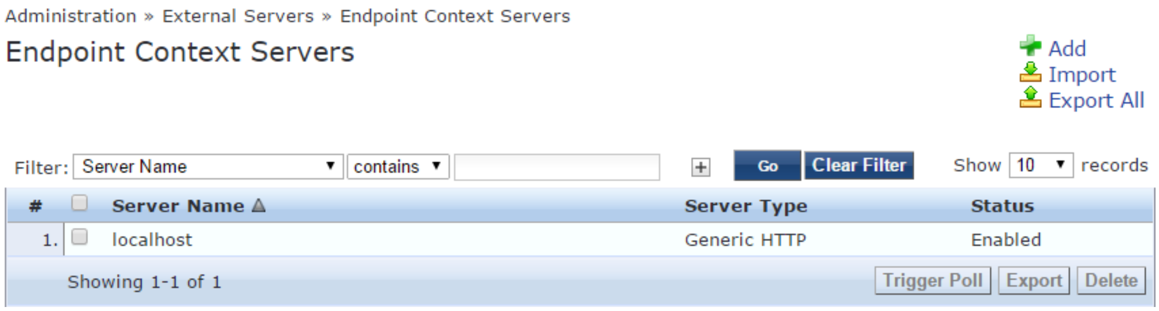
Adding an Infoblox Endpoint Context Server

To add an Infloblox endpoint context server:

1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.

   The **Endpoint Context Servers** page opens.

Figure 598: *Endpoint Context Servers Page*



Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

Filter: Server Name contains

Show 10 records

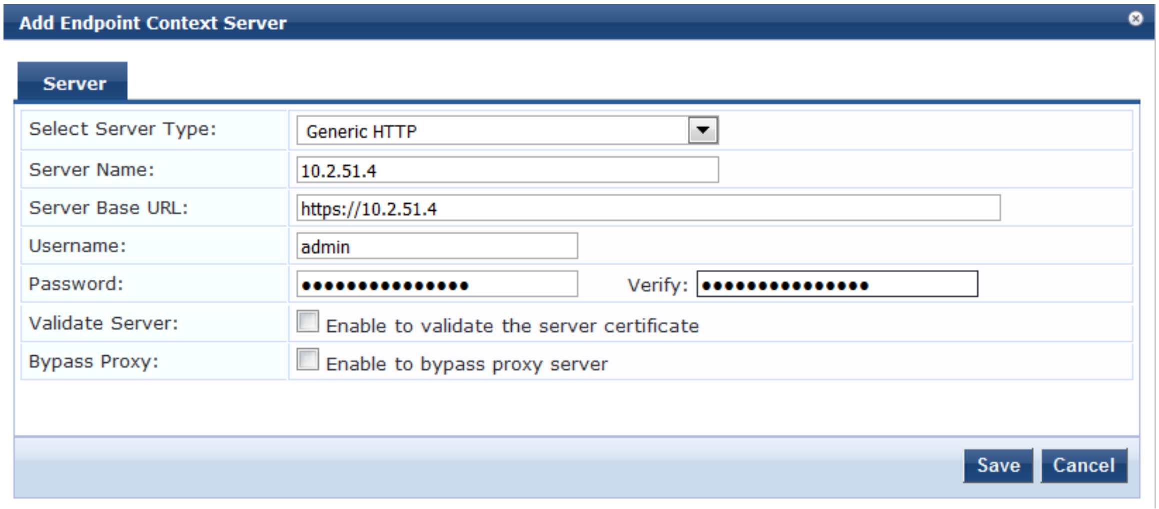
#	□	Server Name	Server Type	Status
1.	□	localhost	Generic HTTP	Enabled

Showing 1-1 of 1

2. Click **Add**.

The **Add Endpoint Context Server** dialog opens. This dialog opens in the **Server** page.

Figure 599: *Adding an Infoblox Endpoint Context Server*



Add Endpoint Context Server

Server

Select Server Type:	Generic HTTP
Server Name:	10.2.51.4
Server Base URL:	https://10.2.51.4
Username:	admin
Password:	●●●●●●●●●●●●●●● Verify: ●●●●●●●●●●●●●●●
Validate Server:	□ Enable to validate the server certificate
Bypass Proxy:	□ Enable to bypass proxy server

3. Enter the following information:
   a. **Select Server Type**: From the drop-down list, select **Generic HTTP**.
   b. **Server Name**: Enter the IP address of the Infoblox server.
   c. **Server Base URL**: As you enter the IP address in the **Server Name** field, the **Server Base URL** is populated automatically with the same IP address.
   d. **Password**: Enter the password for this server, then verify the password.
4. When finished defining the parameters in the **Server** page, click **Save**.

   You return to the **Endpoint Context Servers** page, where the endpoint context server you added is now listed.

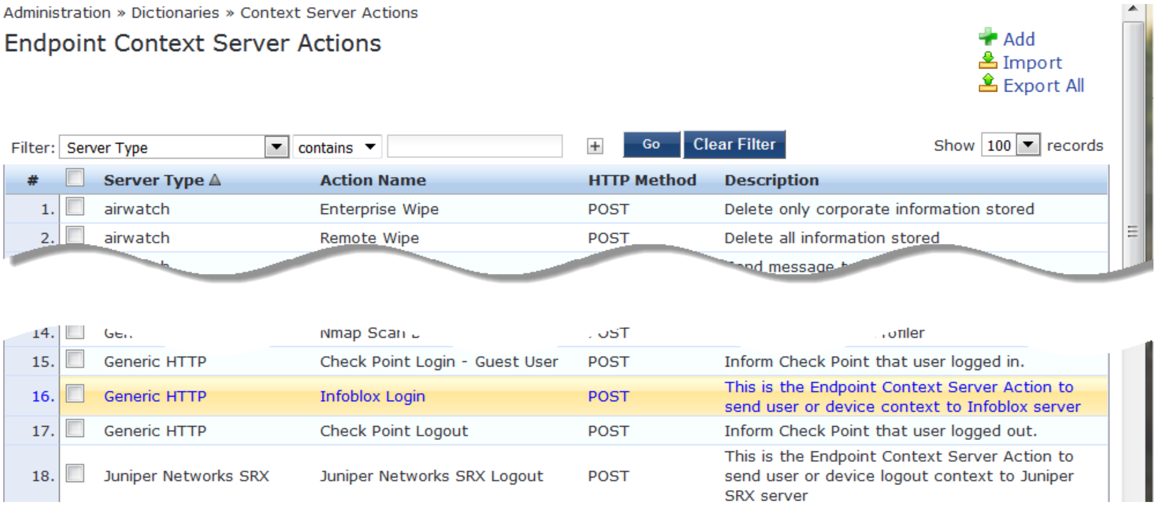
Adding a Context Server Action to the Infoblox Server

This section describes how to define an Infoblox Login action and specify the URL to post content from the ClearPass Policy Manager server to the Infoblox server.

To add a context server action to the Infoblox server:

1. Navigate to **Administration** > **Dictionaries** > **Context Server Actions**.

   The **Endpoint Context Server Actions** page appears.



Administration » Dictionaries » Context Server Actions

Endpoint Context Server Actions

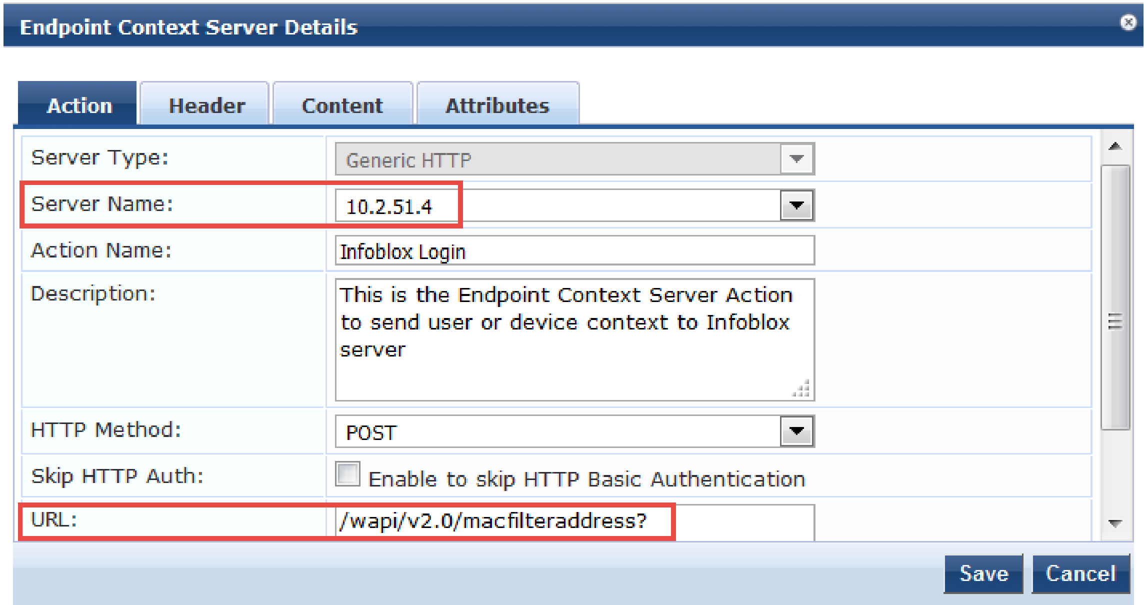
#	□	Server Type ▵	Action Name	HTTP Method	Description
1.	□	airwatch	Enterprise Wipe	POST	Delete only corporate information stored
2.	□	airwatch	Remote Wipe	POST	Delete all information stored
					...nd message t...
14.	□	Ge...	Nmap Scan ...	...OST	...rofiler
15.	□	Generic HTTP	Check Point Login - Guest User	POST	Inform Check Point that user logged in.
16.	□	Generic HTTP	Infoblox Login	POST	This is the Endpoint Context Server Action to send user or device context to Infoblox server
17.	□	Generic HTTP	Check Point Logout	POST	Inform Check Point that user logged out.
18.	□	Juniper Networks SRX	Juniper Networks SRX Logout	POST	This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server

2. Select the **Infoblox Login** endpoint context server action.

   The **Endpoint Context Server Details** dialog for the selected action is displayed.

   For descriptions of the parameters in the **Endpoint Context Servers Details** tabs, refer to Configuring Endpoint Context Server Actions on page 590.

Figure 600: *Selecting the Infoblox Server for the Endpoint Context Server Action*



Endpoint Context Server Details

Server Type: Generic HTTP

Server Name: 10.2.51.4

Action Name: Infoblox Login

Description: This is the Endpoint Context Server Action to send user or device context to Infoblox server

HTTP Method: POST

Skip HTTP Auth: □ Enable to skip HTTP Basic Authentication

URL: /wapi/v2.0/macfilteraddress?

3. **Server Name**: Select the IP address of the Infoblox server.
4. **URL**: Note the URL for posting content from the ClearPass server to the Infoblox server:

   /wapi/v2.0/macfilteraddress?
5. Click **Save**.

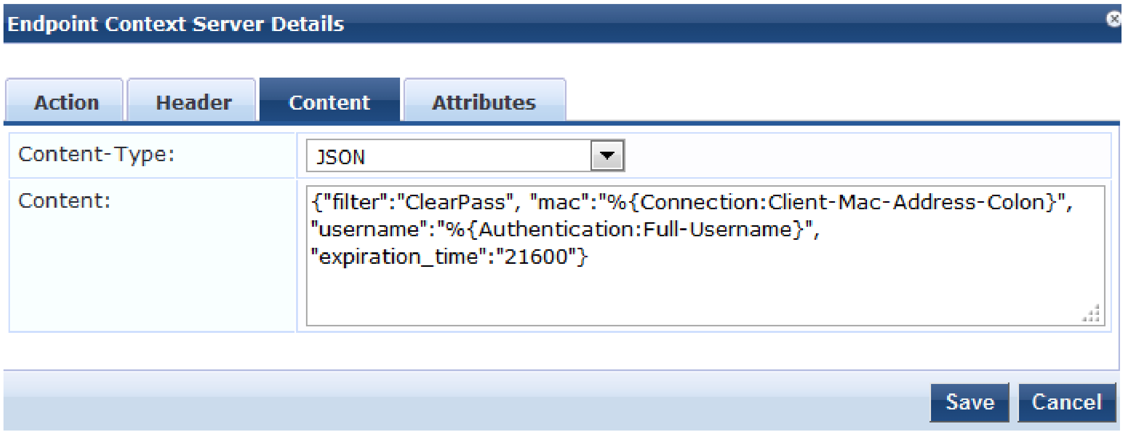
Attributes Sent to the Infoblox Server

6. To view the attributes that will be sent to the Infoblox server, click the **Content** tab.

   As shown in Figure 601, the following attributes are sent in JSON format to the Infoblox server:

   - Filter name **"ClearPass"**
   - Username and MAC addresses of the authenticated devices

Figure 601: *Attributes Sent to Infoblox Server*



Endpoint Context Server Details

Content-Type: JSON

Content:

```
{"filter":"ClearPass", "mac":"%{Connection:Client-Mac-Address-Colon}",
"username":"%{Authentication:Full-Username}",
"expiration_time":"21600"}
```

7. Click **Cancel**.

Creating an Infoblox Enforcement Profile

This section describes how to create a a simple HTTP-based enforcement profile named "*Infoblox Notify*" that acts against the Infoblox Login action.

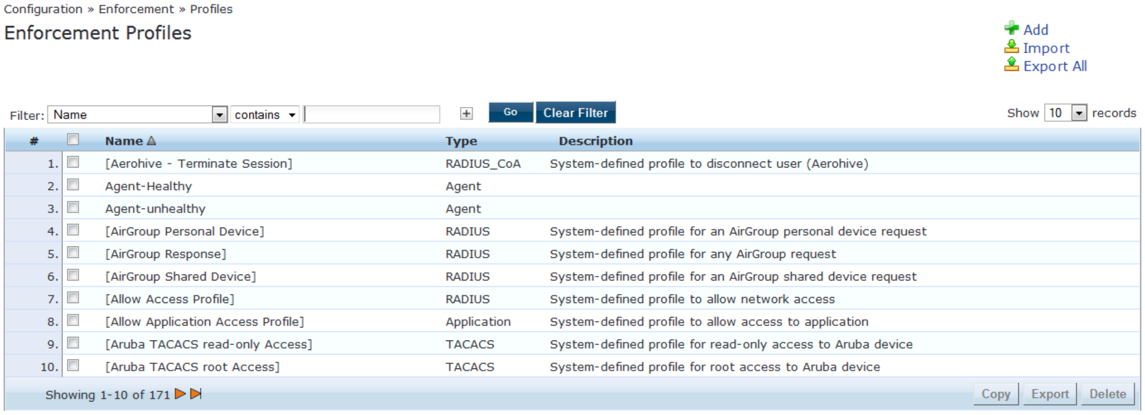
For details on configuring enforcement profiles, see Configuring Enforcement Profiles on page 357.

To create an Infoblox enforcement profile:

1. Navigate to **Configuration** > **Enforcement** > **Profiles**.

   The **Enforcement Profiles** page opens.

Figure 602: *Enforcement Profiles Page*



Configuration » Enforcement » Profiles

Enforcement Profiles

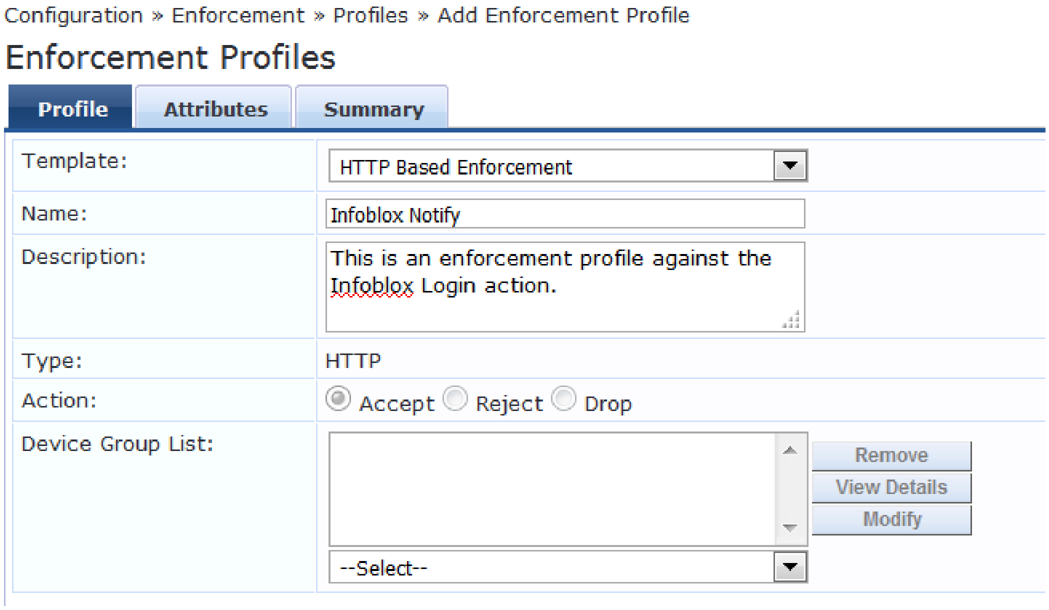
#	□	Name	Type	Description
1.	□	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	□	Agent-Healthy	Agent	
3.	□	Agent-unhealthy	Agent	
4.	□	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
5.	□	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
6.	□	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
7.	□	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
8.	□	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
9.	□	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
10.	□	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device

Showing 1-10 of 171

2. Click **Add**.

   The **Add Enforcement Profiles** dialog appears.

Figure 603: *Adding the Infoblox Enforcement Profile*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	HTTP Based Enforcement
Name:	Infoblox Notify
Description:	This is an enforcement profile against the Infoblox Login action.
Type:	HTTP
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

3. Configure the **Add Enforcement Profile** page as follows:

   a. **Template:** Select **HTTP Based Enforcement**.

      For details on configuring HTTP-based enforcement profiles, see HTTP Based Enforcement Profile on page 390.

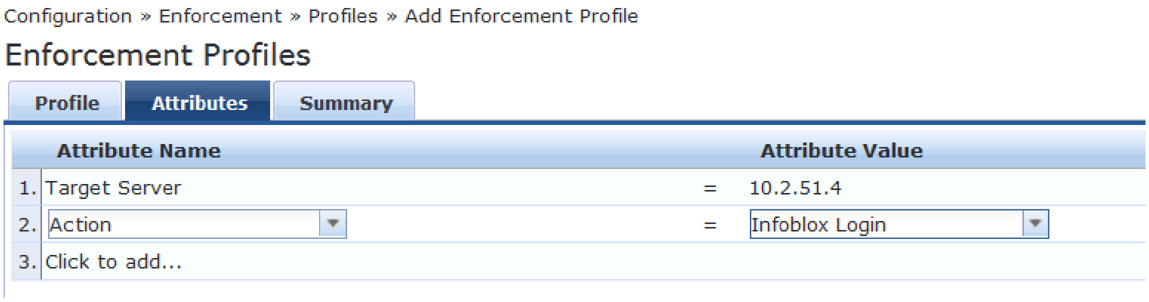
   b. **Name:** Enter **Infoblox Notify**.

   c. **Description**: Optionally, enter a description of this enforcement profile.

d. Click **Next**.

The **Enforcement Profiles Attributes** page appears.

Figure 604: *Specifying the Target Server and Enforcement Action*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Attribute Name		Attribute Value
1.	Target Server	=	10.2.51.4
2.	Action	=	Infoblox Login
3.	Click to add...		

4. Configure the **Enforcement Profile Attributes** page as follows:

   a. **Target Server:** Select the IP address of the Infoblox server.

   b. **Action:** Select **Infoblox Login**.

   c. Click **Save**.

   You return to the **Enforcement Profiles** page, where the Infoblox Notify enforcement profile is now listed.

Configuring an Infoblox RADIUS Enforcement Profile

This section describes how to define a RADIUS Enforcement type profile for Infoblox. This profile configures parameters to define tunnel parameters, VLAN ID, and the termination action.

> NOTE
>
> This configuration is specific to the lab environments in which this feature has been tested. The RADIUS: IETF attributes can take any values, depending on the lab environment.

For details on configuring a RADIUS-based enforcement policy, see RADIUS Based Enforcement Profile on page 391.

To define a RADIUS Enforcement profile:

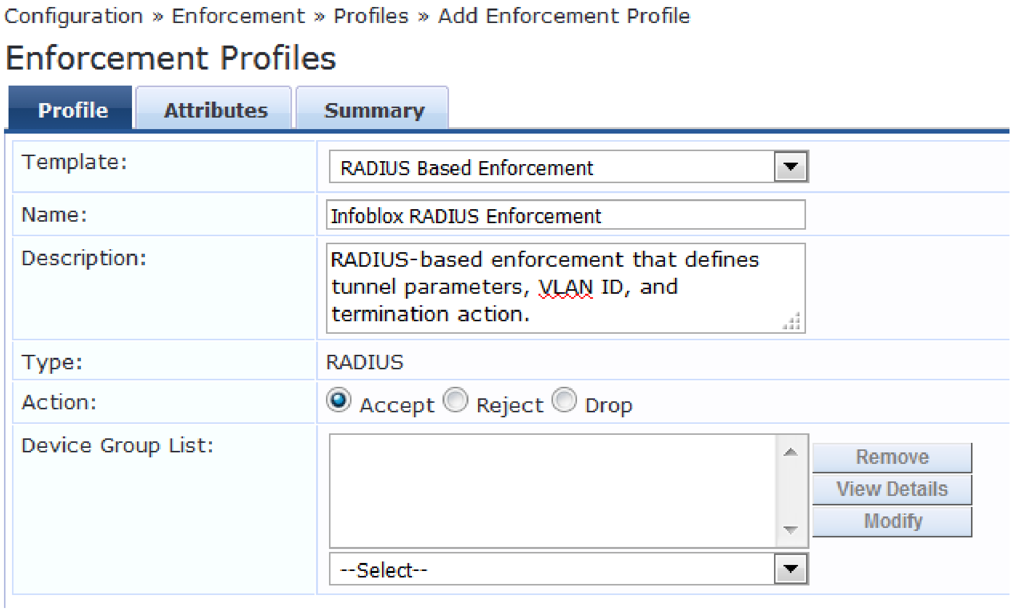
1. Navigate to **Configuration** > **Enforcement** > **Profiles**.

   The **Enforcement Profiles** page appears.

2. Click **Add**.

   The **Add Enforcement Profiles** dialog appears.

Figure 605: *Adding a RADIUS-Based Enforcement Profile*



Configuration » Enforcement » Profiles » Add Enforcement Profile

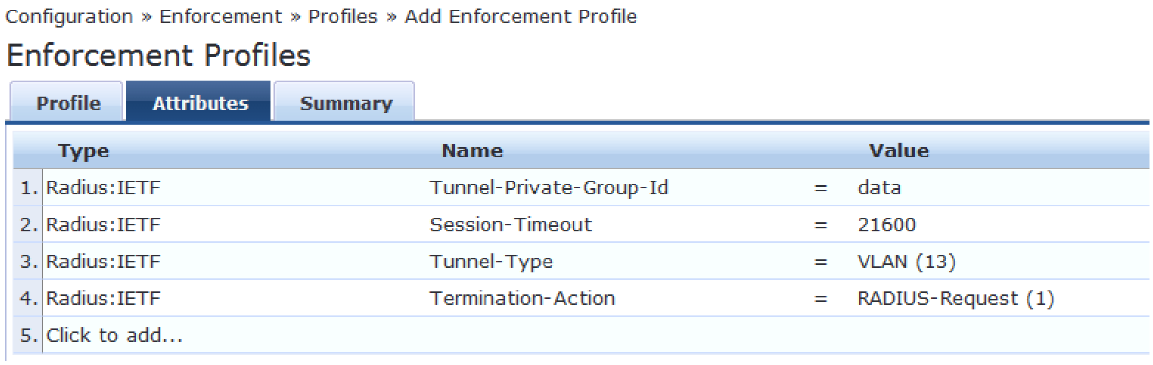
Enforcement Profiles

Template:	RADIUS Based Enforcement
Name:	Infoblox RADIUS Enforcement
Description:	RADIUS-based enforcement that defines tunnel parameters, VLAN ID, and termination action.
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

3. Enter the following information:
   a. **Template**: Select **RADIUS Based Enforcement**.
   b. **Name**: Enter **Infoblox RADIUS Enforcement**.
   c. **Description**: Optionally, enter a description of this profile.
   d. Click **Next**.

   The Enforcement Profiles **Attributes** page opens. In the following steps, you will add the four RADIUS Enforcement attributes illustrated in Figure 606.

Figure 606: *Adding Attributes to the RADIUS Enforcement Profile*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Type	Name		Value
1.	Radius:IETF	Tunnel-Private-Group-Id	=	data
2.	Radius:IETF	Session-Timeout	=	21600
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
5.	Click to add...			

Tunnel-Private_Group-Id

4. Click **Click to add...**.
   a. **Type:** Select **Radius:IETF**.
   b. **Name**: Select **Tunnel-Private_Group-Id**.
   c. **Value:** Enter the value configured for the **Tunnel-Private_Group-Id** attribute on the controller.

Session-Timeout

5. Click **Click to add...**.
   a. **Type**: Select **Radius:IETF**.
   b. **Name**: Select **Session-Timeout**.

c. **Value**: Enter **21600** (which equals six hours in seconds).

Tunnel-Type

6. Click **Click to add...**.
   a. **Type:** Select **Radius:IETF**.
   b. **Name:** Select **Tunnel-Type**.
   c. **Value**: Select **VLAN**.

Termination-Action

7. Click **Click to add...**.
   a. **Type:** Select **Radius:IETF**.
   b. **Name:** Select **Termination-Action**.
   c. **Value**: Select **RADIUS-Request**.
8. Click **Save**.

   You return to the Enforcement Profiles page. The following message is displayed:

   Enforcement profile "Infoblox RADIUS Enforcement" added

Creating an Infoblox Enforcement Policy

This section describes how to create an enforcement policy to act against the "Infoblox Notify" and "Infoblox RADIUS Enforcement" profiles so that external devices can authenticate against this policy.

For details on configuring enforcement policies, see Configuring Enforcement Policies on page 355.

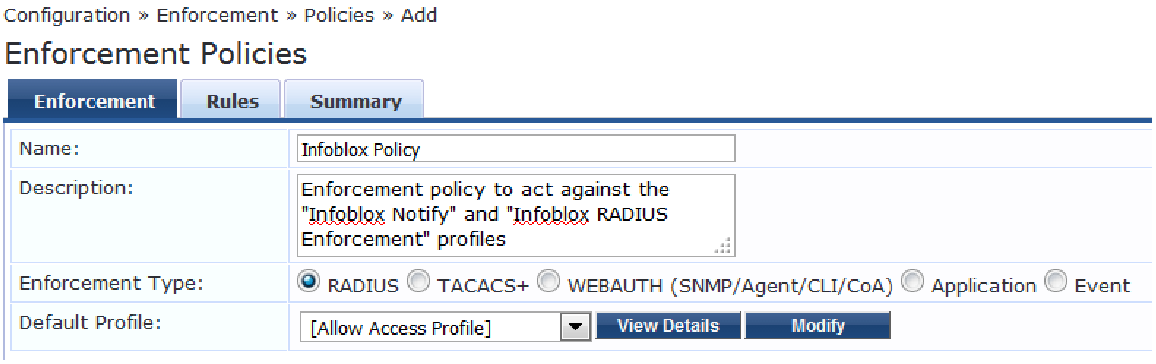
To create an Infoblox Enforcement Policy:

1. Navigate to **Configuration** > **Enforcement** > **Policies**.

   The **Enforcement Policies** page opens.
2. Click **Add**.

   The Add Enforcement Policies page appears.

Figure 607: *Adding the Infoblox Enforcement Policy*



Name: Infoblox Policy

Description: Enforcement policy to act against the "Infoblox Notify" and "Infoblox RADIUS Enforcement" profiles

Enforcement Type: ● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event

Default Profile: [Allow Access Profile]

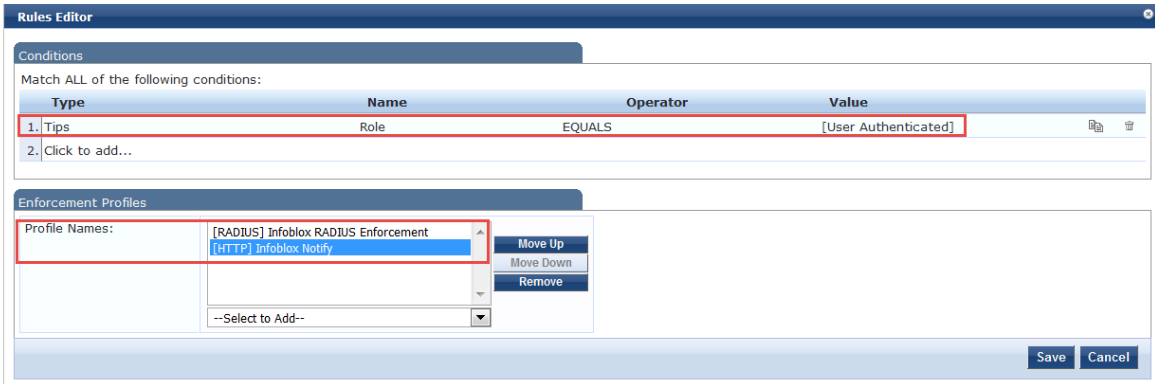
3. Enter the following information:
   a. **Name**: Enter **Infoblox Policy**.
   b. **Description**: Optionally, enter a description of this profile.
   c. **Enforcement Type**: Set by default to **RADIUS**.
   d. Default Profile: Select **Allow Access Profile**.
   e. Click **Next**.

      The **Rules** page appears.

4. Click **Add Rule**.

   The Rules Editor dialog appears.

Figure 608: *Configuring Infoblox Enforcement Policy Rules*



Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	Role	EQUALS	[User Authenticated]
2.	Click to add...			

Enforcement Profiles

Profile Names: [RADIUS] Infoblox RADIUS Enforcement
[HTTP] Infoblox Notify

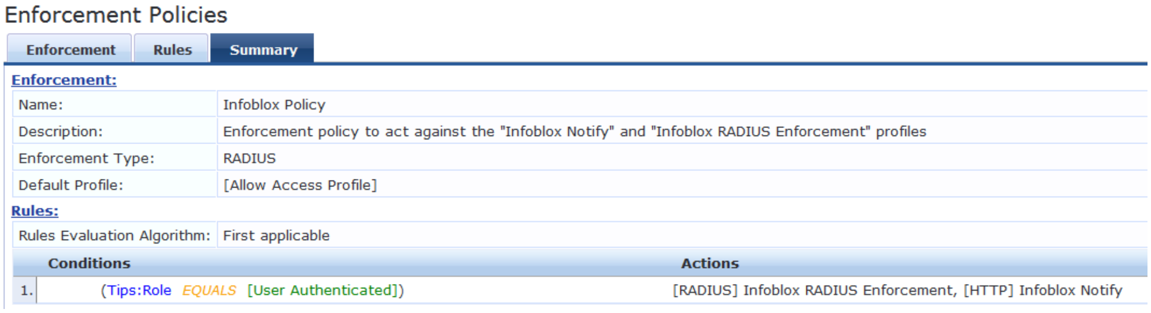
5. In the **Conditions** panel, click **Click to add**, then enter the following information:
   a. **Type**: Select **Tips**.
   b. **Name**: Select **Role**.
   c. **Operator**: Select **EQUALS**.
   d. **Value**: Select **User Authenticated**.
6. In the **Enforcement Profiles** panel:
   a. Click **Select to Add**.

NOTE

You must add the enforcement profies in the order specified here.

   b. Select **[RADIUS] Infoblox RADIUS Enforcement**.
   c. Click **Select to Add**.
   d. Select **[HTTP] Infoblox Notify**.
7. Click **Save**.
8. To view the Infoblox enforcement policy summary, click the **Summary** tab.

Figure 609: *Summary of the Infoblox Enforcement Policy*



Enforcement Policies

Enforcement:

Name:	Infoblox Policy
Description:	Enforcement policy to act against the "Infoblox Notify" and "Infoblox RADIUS Enforcement" profiles
Enforcement Type:	RADIUS
Default Profile:	[Allow Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [User Authenticated])	[RADIUS] Infoblox RADIUS Enforcement, [HTTP] Infoblox Notify

9. Check the summary information to make sure the policy is correct, make any changes if necessary, then click **Save**.

   You return to the Enforcement Policies page where the new **Infoblox Policy** is now listed.

Defining an Infoblox Service

This section describes how to create a Generic RADIUS Enforcement wireless service named "Infoblox Service" for the policy "Infoblox Policy."

To create the wireless service:

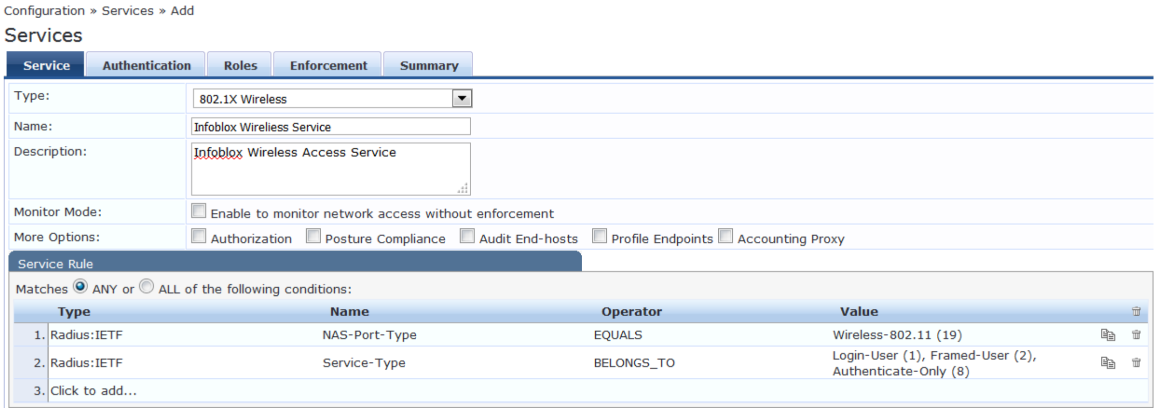
1. Navigate to **Configuration** > **Services**.

   The **Services** page opens.

2. Click **Add**.

   The **Add Services** page opens.

Figure 610: *Adding an Infoblox Wireless Service*



Configuration » Services » Add

Services

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

Service Rule

Matches ● ANY or ○ ALL of the following conditions:

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

3. Enter the following information:

   a. **Type**: Select **802.1X Wireless**.

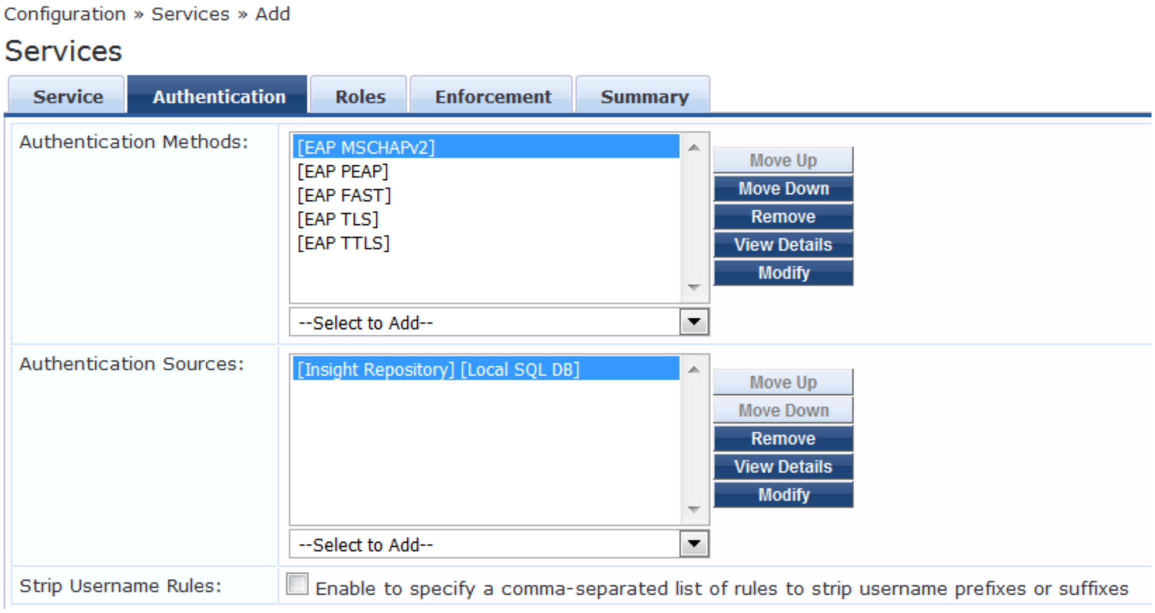
   b. **Name**: Enter **Infoblox Wireless Service**.

   c. **Description**: Optionally, enter a description of this service.

   d. In the **Service Rule** panel, set **Matches** to **ANY**, then click **Next**.

      The **Authentication** page appears.

Figure 611: *Specifying Wireless Service Authentication Settings*



Configuration » Services » Add

Services

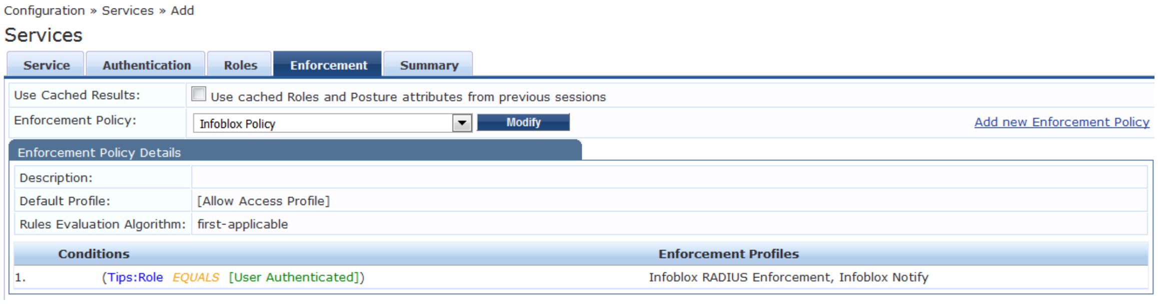
Authentication Methods:	[EAP MSCHAPv2] [EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS] --Select to Add--
Authentication Sources:	[Insight Repository] [Local SQL DB] --Select to Add--
Strip Username Rules:	□ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

4. Enter the following information:
   a. **Authentication Methods**: Select the authentication method.

      This example uses **EAP MSCHAPv2**.
   b. **Authentication Sources**: Select the authentication source(s).

      This example uses **Local SQL DB**.
5. Select the **Enforcement** tab.

Figure 612: *Specifying the Enforcement Policy for the Service*



Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Infoblox Policy

Enforcement Policy Details

Description:

Default Profile: [Allow Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* [User Authenticated])	Infoblox RADIUS Enforcement, Infoblox Notify

6. From the **Enforcement Policy** drop down, select **Infoblox Policy**, then click **Next**.

   The **Infoblox Wireless Service Summary** page is displayed.
7. Check the summary information to make sure the service is correct, make any changes if necessary, then click **Save**.

   You return to the **Services** page where the new **Infoblox Wireless Service** is now listed.

Authenticating External Devices Against the Infoblox Service

This section defines the configuration on the Infoblox server to receive the MAC address and username context from ClearPass.

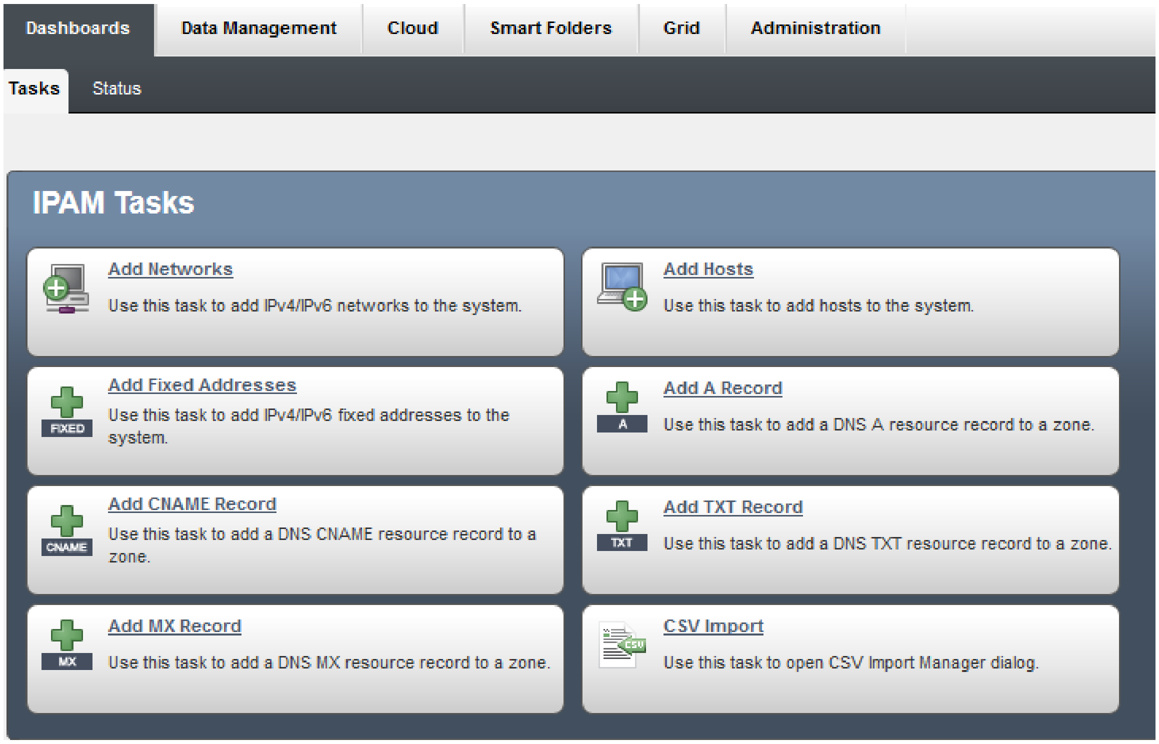
The following procedure adds an IPv4 network that is used as a DHCP pool to assign IP addresses to the external devices that must be authenticated.

To configure an Infoblox server to authenticate external devices:

1. Log into the Infoblox server.

   The **Infoblox IPAM Tasks** page opens.

Figure 613: *Infoblox Server Initial Page*



IPAM Tasks

Add Networks
Use this task to add IPv4/IPv6 networks to the system.

Add Hosts
Use this task to add hosts to the system.

Add Fixed Addresses
Use this task to add IPv4/IPv6 fixed addresses to the system.

Add A Record
Use this task to add a DNS A resource record to a zone.

Add CNAME Record
Use this task to add a DNS CNAME resource record to a zone.

Add TXT Record
Use this task to add a DNS TXT resource record to a zone.

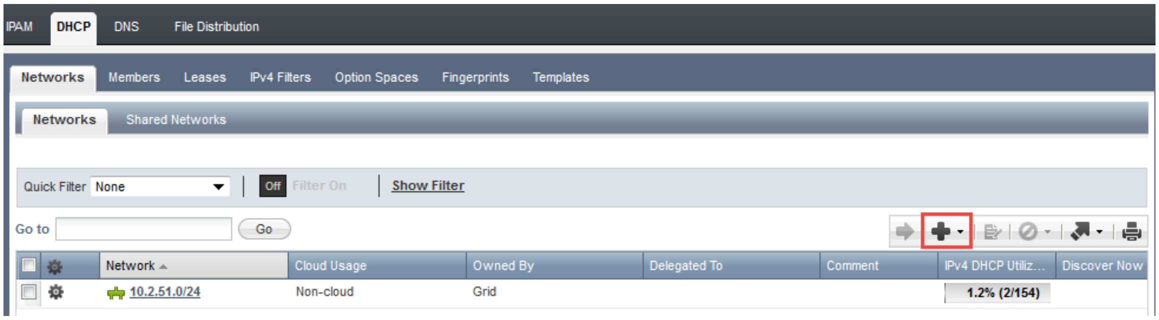
Add MX Record
Use this task to add a DNS MX resource record to a zone.

CSV Import
Use this task to open CSV Import Manager dialog.

2. Select the **Data Management** tab, then select the **DHCP** tab.

   The **DHCP Networks** page appears.

Figure 614: *Adding an IPv4 Network*

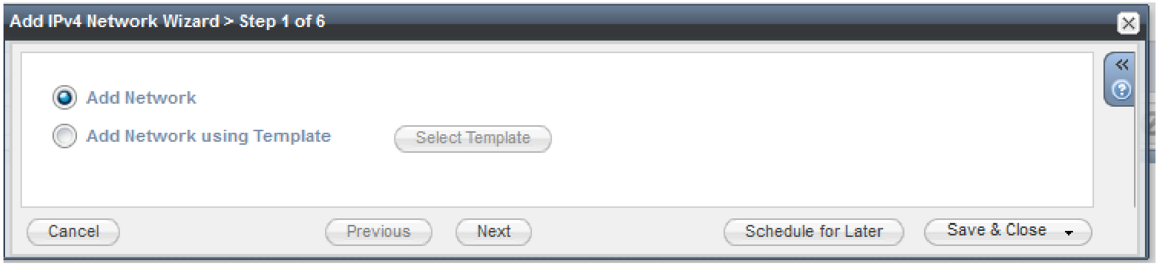


		Network ▲	Cloud Usage	Owned By	Delegated To	Comment	IPv4 DHCP Utiliz...	Discover Now
□	⚙	10.2.51.0/24	Non-cloud	Grid			1.2% (2/154)	

3. To add a new network, click the **Plus** icon.

   The **Add IPv4 Network Wizard** begins.

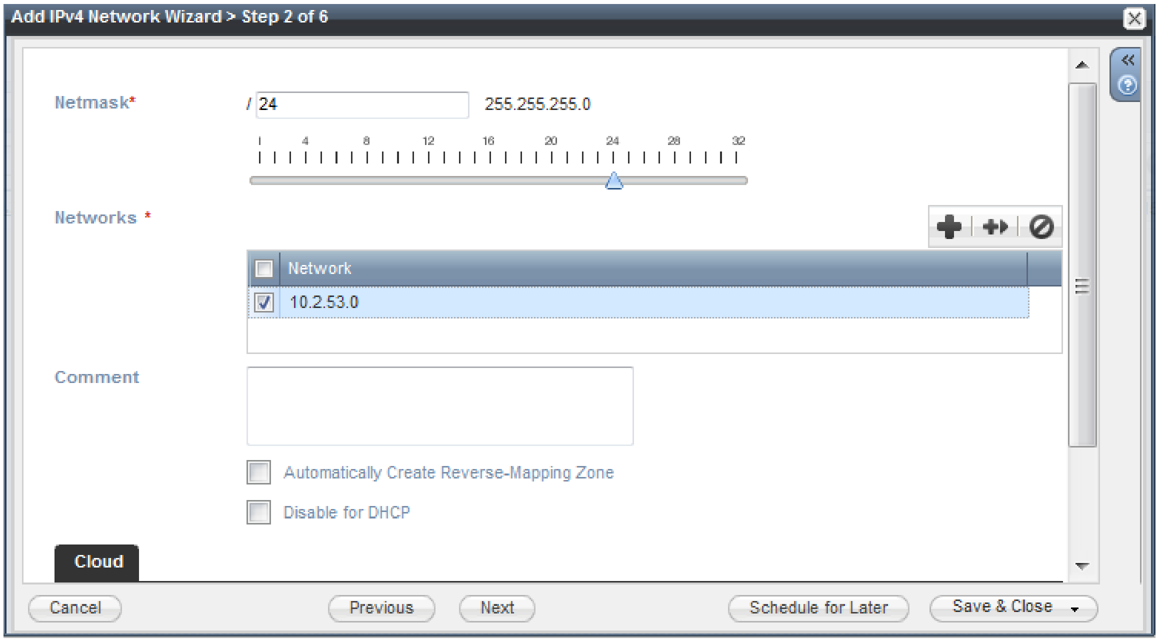
Figure 615: *Adding an IPv4 Network*



4. With **Add Network** selected by default, click **Next**.

   The following screen appears.

Figure 616: *Specifying the Netmask*



Add IPv4 Network Wizard > Step 2 of 6

Netmask* / 24 255.255.255.0

Networks *

□	Network
☑	10.2.53.0

Comment

□ Automatically Create Reverse-Mapping Zone

□ Disable for DHCP

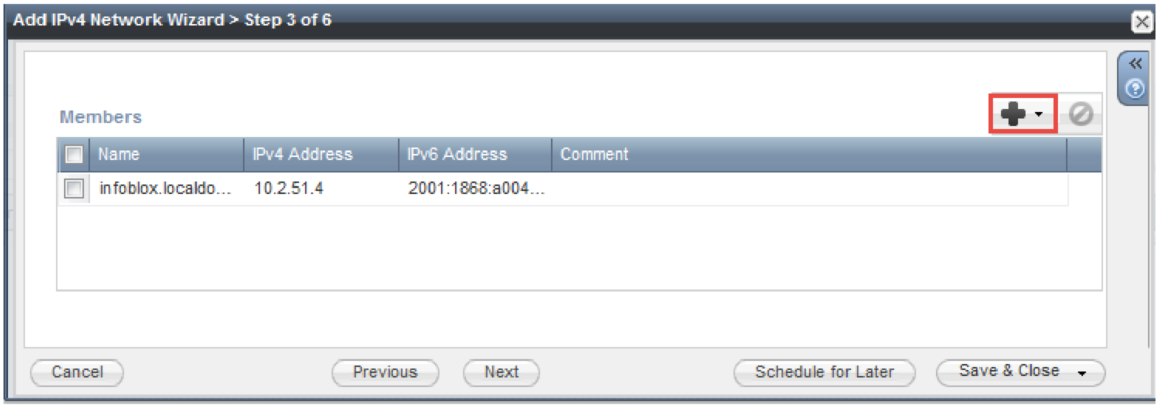
5. In the **Netmask** field, specify the netmask for the new network.

   The netmask is set by default to **/24** (that is, a Class C IP address), but you can set the netmask to any appropriate netmask value for your network.

6. To add an IPv4 network, in the **Networks** panel, click the **Plus** sign (see Figure 616).
7. In the **Networks** field, enter the IP address of the network, then click **Next**.

   The **Members** screen appears.

Figure 617: *Adding Members*



Add IPv4 Network Wizard > Step 3 of 6

Members

□	Name	IPv4 Address	IPv6 Address	Comment
□	infoblox.localdo...	10.2.51.4	2001:1868:a004...	

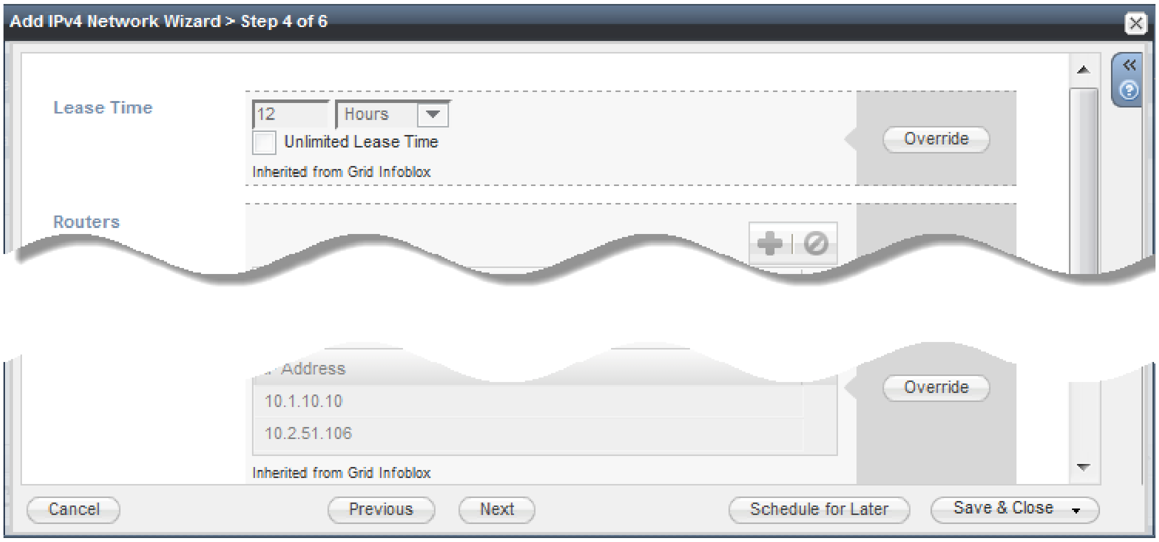
8. Click the **Plus** sign.

   While adding members for the DHCP pool, the members group from **Data Management** > **DHCP** > **Members** is populated automatically.

9. Click **Next**.

   The following screen appears.

Figure 618: *Specifying the Lease Time (Session-Timeout Value)*



Add IPv4 Network Wizard > Step 4 of 6

Lease Time: 12 Hours

□ Unlimited Lease Time

Inherited from Grid Infoblox

Routers

Address

10.1.10.10

10.2.51.106

Inherited from Grid Infoblox

10. In the **Lease Time Override** panel, click **Override**.
11. In the **Lease Time** field, enter **21600**; from the drop-down, select **Seconds**. Then click **Next**.

NOTE

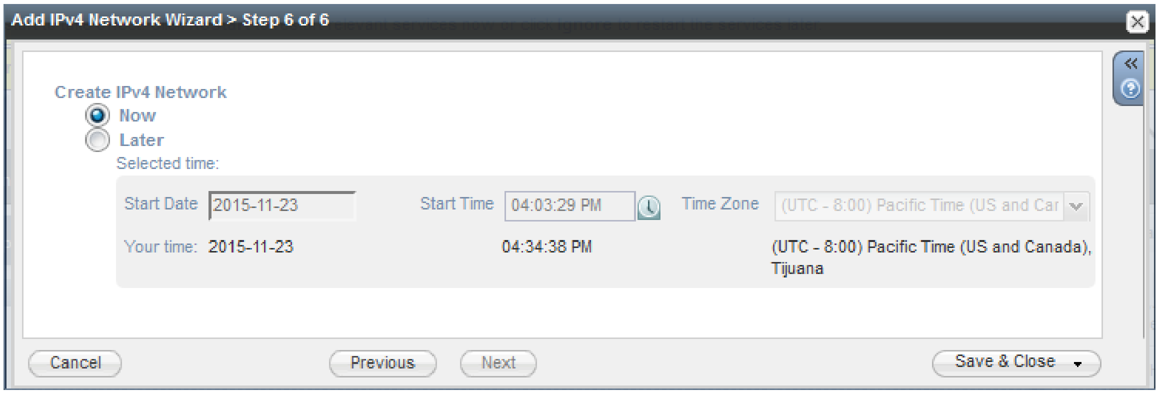
The Lease Time value you enter here must correspond to the **Session-Timeout** value defined under Infoblox RADIUS Enforcement (see Figure 606).

The **Extension Attributes** screen opens. No changes are required here.

12. Click **Next**.

The **Create IPv4 Network** screen opens. You can choose to create the network now or schedule it for a later day and time.

Figure 619: *Scheduling Date and Time for Creating the IPv4 Network*



Add IPv4 Network Wizard > Step 6 of 6

Create IPv4 Network

● Now

○ Later

Selected time:

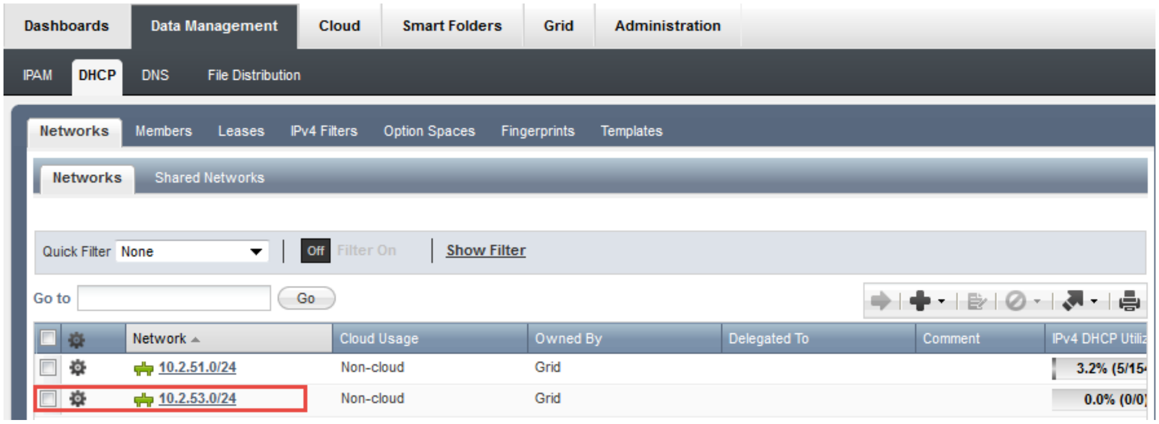
Start Date: 2015-11-23 Start Time: 04:03:29 PM Time Zone: (UTC - 8:00) Pacific Time (US and Car

Your time: 2015-11-23 04:34:38 PM (UTC - 8:00) Pacific Time (US and Canada), Tijuana

13. Specify when you choose to create the IPv4 network, then click **Save & Close**.

The new network is created.

Figure 620: *New IPv4 Network Created*



Quick Filter: None

Network ▲	Cloud Usage	Owned By	Delegated To	Comment	IPv4 DHCP Utiliz
10.2.51.0/24	Non-cloud	Grid			3.2% (5/15
10.2.53.0/24	Non-cloud	Grid			0.0% (0/0)

Creating a Filter to Accept Information from the ClearPass Server

To create a filter to accept information from the ClearPass server:

1. From the **Data Management** > **DHCP** tab, select the newly created network.

   The **Networks** page opens.

2. Select the **IPv4 Filters** tab.
3. To add a filter, click the **Plus** sign.

   The **Add IPv4 MAC Address Filter** dialog opens.

4. In the **Name** field, enter **ClearPass.**

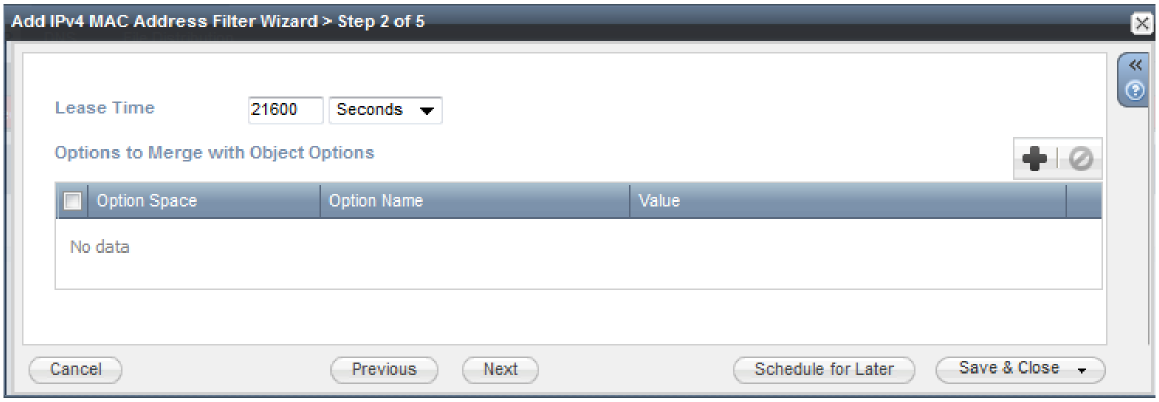
Note. the name of the filter must correspond to the filter value in the Endpoint Context Server Content page (see Attributes Sent to the Infoblox Server on page 609).

5. Optionally, enter a comment to describe this filter, then click **Next**.

   Step 2 of the **Add IPv4 MAC Address Filter** wizard appears.

6. In the **Lease Time** fields, enter **21600 Seconds**, then click **Next**.

Figure 621: *Specifying Lease Time in the IPv4 MAC Address Filter*


Add IPv4 MAC Address Filter Wizard > Step 2 of 5
Options to Merge with Object Options
Cancel
Previous
Next
Schedule for Later
Save & Close

Lease Time: 21600 Seconds

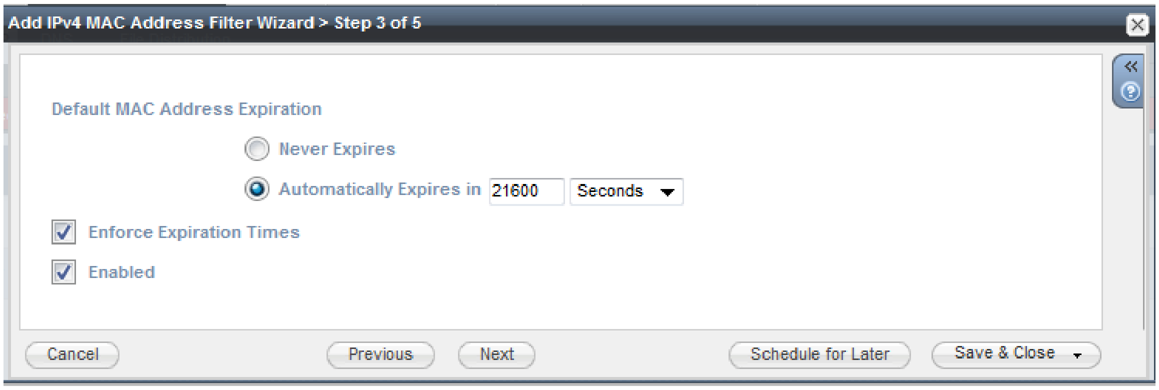
□ Option Space	Option Name	Value
No data		

NOTE

The **Lease Time** value entered here must correspond to the **Session-Timeout** value defined under Infoblox RADIUS Enforcement Profile (see Session-Timeout on page 612).

Step 3 of the IPv4 MAC Address Filter wizard appears.

Figure 622: *Specifying the MAC Address Expiration in the IPv4 MAC Address Filter*



Add IPv4 MAC Address Filter Wizard > Step 3 of 5

Default MAC Address Expiration

○ Never Expires

● Automatically Expires in 21600 Seconds

☑ Enforce Expiration Times

☑ Enabled

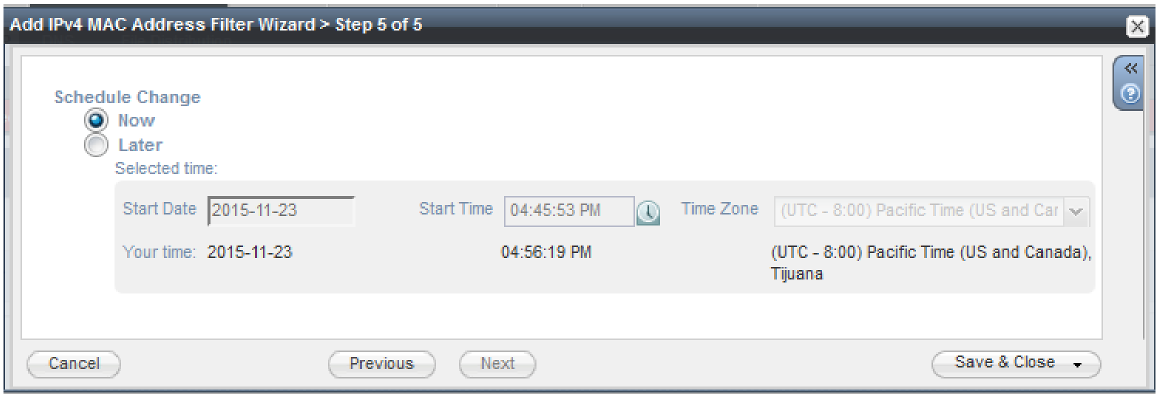
7. For the **Default MAC Address Expiration** setting:
   a. Select the **Automatically Expires in** button.
   b. Specify **21600 Seconds**.
   c. Then click **Next**.

   The Extensible attributes screen appears.

8 No changes are required for this step, so click **Next**.

In Step 5, the **Schedule Change** dialog appears.

Figure 623:



Add IPv4 MAC Address Filter Wizard > Step 5 of 5

Schedule Change

● Now

○ Later

Selected time:

Start Date 2015-11-23 Start Time 04:45:53 PM Time Zone (UTC - 8:00) Pacific Time (US and Car

Your time: 2015-11-23 04:56:19 PM (UTC - 8:00) Pacific Time (US and Canada), Tijuana

8. Specify the Schedule Change settings:
   a. If you wish to run the MAC address filter now, select **Now**.
   b. If you wish to schedule the MAC address filter for later, select **Later** and specify the **Start Date** and **Start Time**.
   c. When finished with the **Schedule Change** settings, click **Save & Close**.

Integrating ClearPass with Juniper Networks SRX

This section provides the following information:

- Adding a Juniper Networks SRX Endpoint Context Server
- Adding a Context Server Action to the Juniper SRX Server
- Viewing or Modifying Juniper Networks SRX Endpoint Context Server Actions
- Creating a Juniper SRX Enforcement Profile
- Creating a Juniper SRX Enforcement Policy

- Defining a Juniper SRX Wireless Service

For more information about the parameters that you must enter to configure this endpoint context server, consult Juniper Network's documentation.

Integrating ClearPass with Juniper Networks SRX typically tags the username context, as well as the external devices being authenticated, along with its respective MAC address, which further simplifies IP address management on the Juniper SRX server side.

This section describes the configurations that you must make on the ClearPass server in order for the ClearPass server to send data to a Juniper Networks SRX server.

Adding a Juniper Networks SRX Endpoint Context Server

To add a Juniper Networks SRX Endpoint Context Server:

1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.

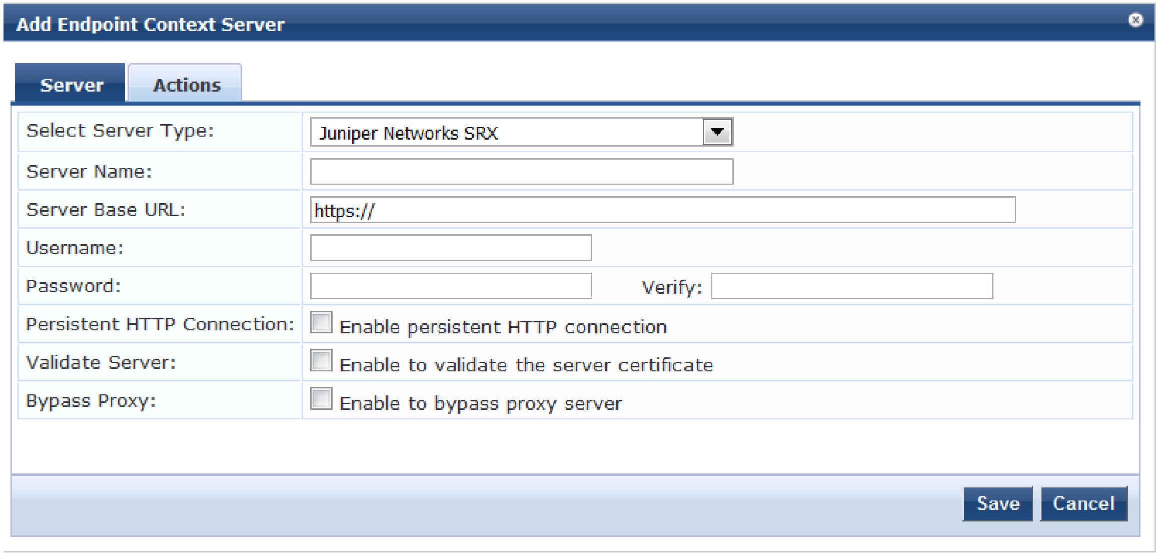
   The **Endpoint Context Servers** page appears.
2. Click **Add**.

   The **Add Endpoint Context Server** dialog appears. This dialog opens in the **Server** page.
3. From the **Select Server Type** drop-down, select **Juniper Networks SRX**.

Server Page

The following dialog is displayed (see Figure 624).

Figure 624: *Adding a Juniper Networks SRX Endpoint Context Server > Server Dialog*



Select Server Type:	Juniper Networks SRX
Server Name:	
Server Base URL:	https://
Username:	
Password:	Verify:
Persistent HTTP Connection:	□ Enable persistent HTTP connection
Validate Server:	□ Enable to validate the server certificate
Bypass Proxy:	□ Enable to bypass proxy server

NOTE

You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the Juniper Networks SRX Add Endpoint Context Server parameters described in Table 332.
5. When satisfied with the settings, click **Save**.

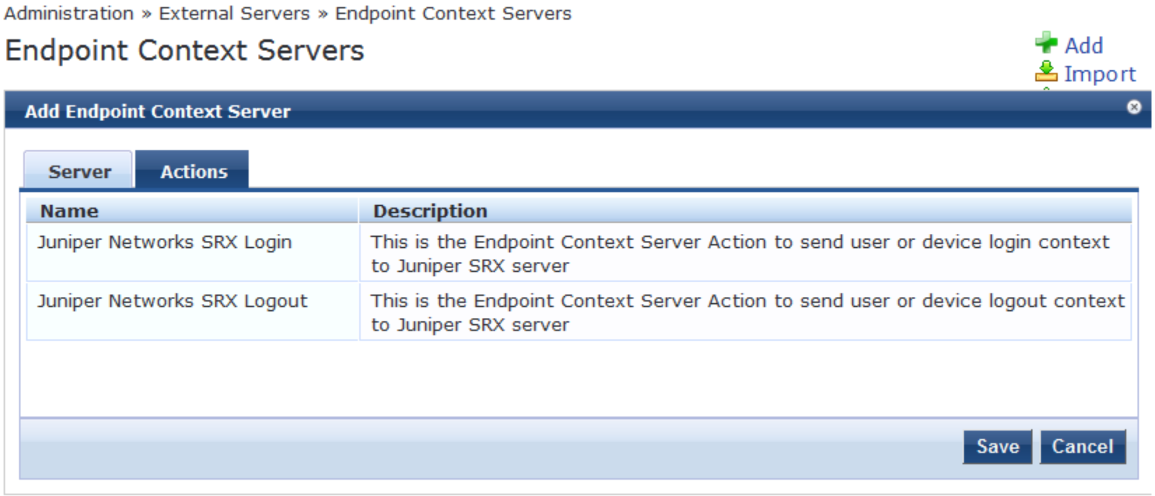
Table 332: *Specifying Juniper Networks SRX Endpoint Context Server - Server Page Parameters*

Parameter	Action/Description
Select Server Type	Choose **Juniper Networks SRX**.
Server Name	Enter a valid server name. You can enter an IP address or a host name.
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 user name.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable the **Validate Server** check box to validate the server certificate. Enabling this option activates the **Certificate** tab.
Enable Server	Enable this option to fetch endpoints from the server. Enabling this option activates the **Poll Status** tab.
Bypass Proxy	Enable this option to bypass the proxy server.

Adding a Context Server Action to the Juniper SRX Server

Figure 625 displays the **Juniper Network SRX Add Endpoint Context Server > Actions** page:

Figure 625: *Adding a Juniper Networks SRX Endpoint Context Server > Actions Page*


Administration » External Servers » Endpoint Context Servers
Endpoint Context Servers
Add
Import
Add Endpoint Context Server
Server
Actions
Save
Cancel

Name	Description
Juniper Networks SRX Login	This is the Endpoint Context Server Action to send user or device login context to Juniper SRX server
Juniper Networks SRX Logout	This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server

Table 333 describes the Endpoint Context Server Actions that are available:

Table 333: *Juniper Networks SRX Endpoint Context Server Actions*

Action	Description
Juniper Networks SRX Login	Endpoint Context Server action to send a user or device login context to a Juniper SRX server.
Juniper Networks SRX Logout	Endpoint Context Server action to send a user or device logout context to a Juniper SRX server.

Viewing or Modifying Juniper Networks SRX Endpoint Context Server Actions

To view or modify the Juniper Networks SRX endpoint context server actions:

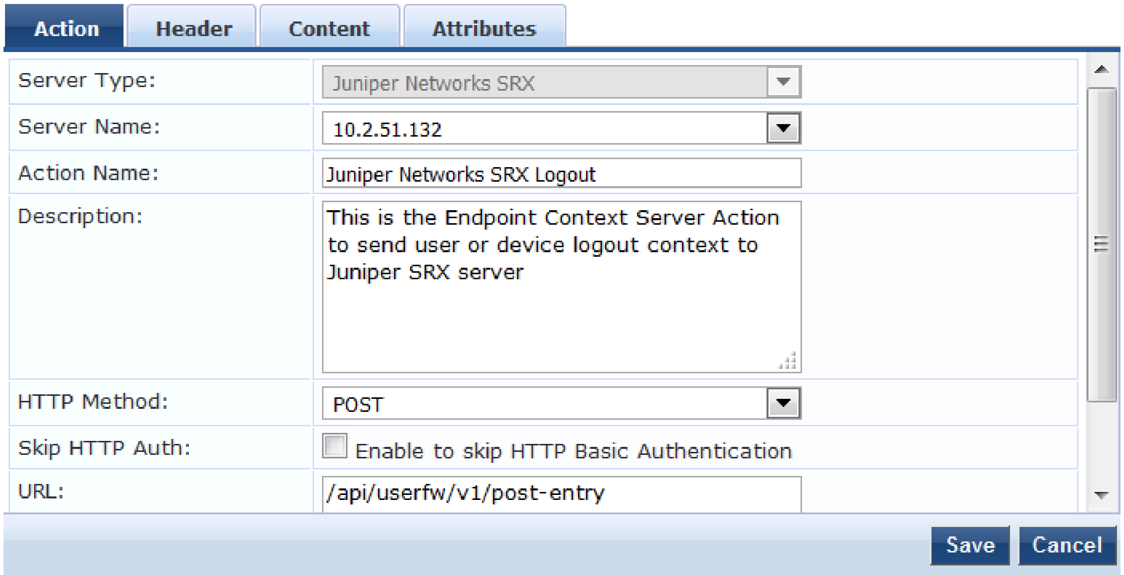
1. Navigate to **Administration** > **Dictionaries** > **Context Server Actions**.

   The **Endpoint Context Server Actions** page appears.

2. Select the Juniper Networks SRX endpoint context server action of interest.

   The **Endpoint Context Server Details** dialog for the selected action is displayed.

Figure 626: *Endpoint Context Server Details for the Juniper SRX Action*



Server Type: Juniper Networks SRX

Server Name: 10.2.51.132

Action Name: Juniper Networks SRX Logout

Description: This is the Endpoint Context Server Action to send user or device logout context to Juniper SRX server

HTTP Method: POST

Skip HTTP Auth: □ Enable to skip HTTP Basic Authentication

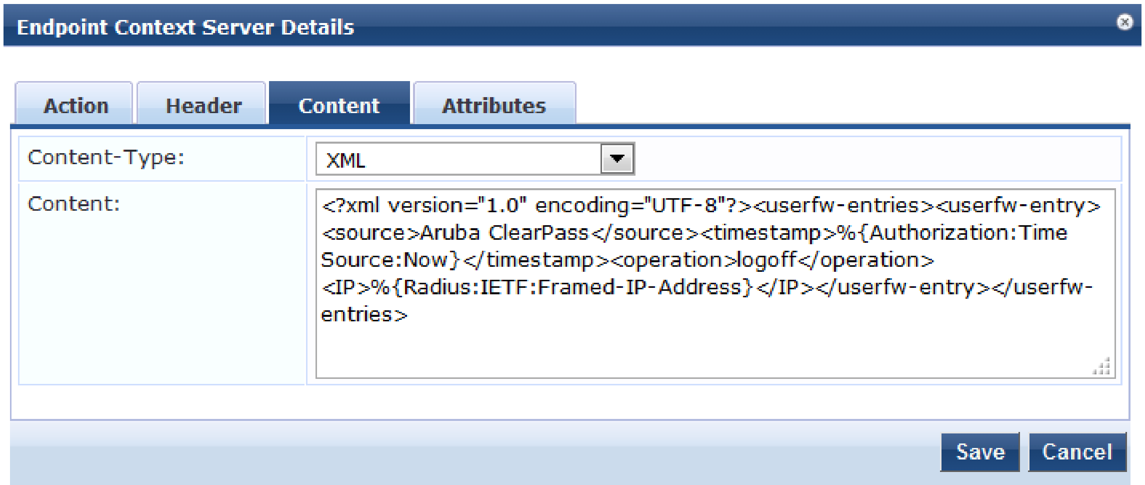
URL: /api/userfw/v1/post-entry

For descriptions of the parameters in the **Endpoint Context Servers Details** pages, refer to Configuring Endpoint Context Server Actions on page 590.

3. If necessary, modify the parameters in the **Action** page, then click **Save**.
4. To specify a content type and add non-default context server attributes, select the **Content** tab.

   Figure 627 shows the content of the Juniper Networks SRX Login action:

Figure 627: *Content for the Juniper Networks SRX Login Action*



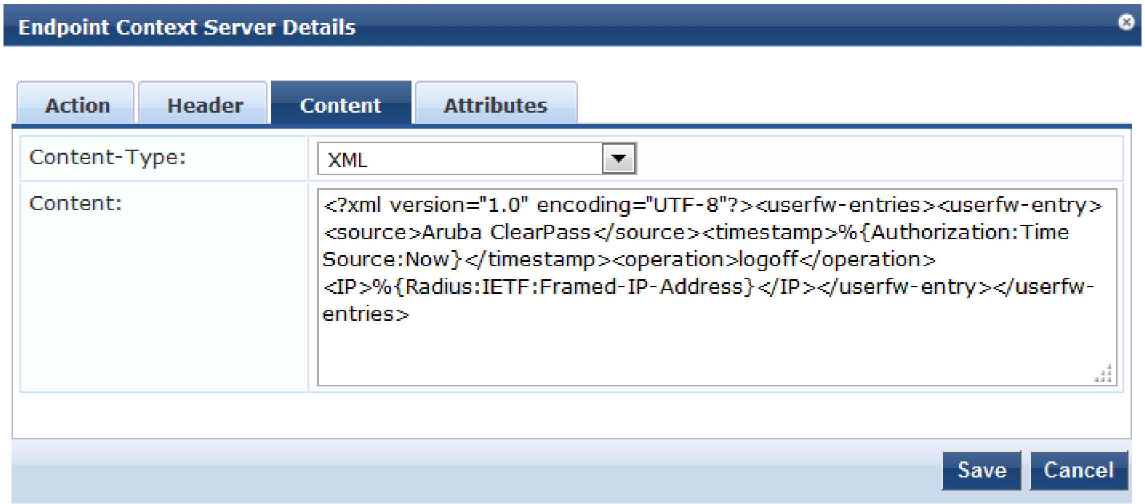
Content-Type: XML

Content:

```
<?xml version="1.0" encoding="UTF-8"?><userfw-entries><userfw-entry><source>Aruba ClearPass</source><timestamp>%{Authorization:Time Source:Now}</timestamp><operation>logoff</operation><IP>%{Radius:IETF:Framed-IP-Address}</IP></userfw-entry></userfw-entries>
```

Figure 628 shows the content of the Juniper Networks SRX Logout action:

Figure 628: *Content for the Juniper Networks SRX Logout Action*



Content-Type: XML

Content:

```
<?xml version="1.0" encoding="UTF-8"?><userfw-entries><userfw-entry>
<source>Aruba ClearPass</source><timestamp>%{Authorization:Time
Source:Now}</timestamp><operation>logoff</operation>
<IP>%{Radius:IETF:Framed-IP-Address}</IP></userfw-entry></userfw-
entries>
```

5. Make any necessary changes to the **Content** page, then click **Save**.

   You return to the **Endpoint Context Servers** page, where the endpoint context server you added is now listed.

Creating a Juniper SRX Enforcement Profile

This section describes how to create a a session-notification enforcement profile named "**Juniper SRX Notify**" that acts against the Juniper SRX Login action.

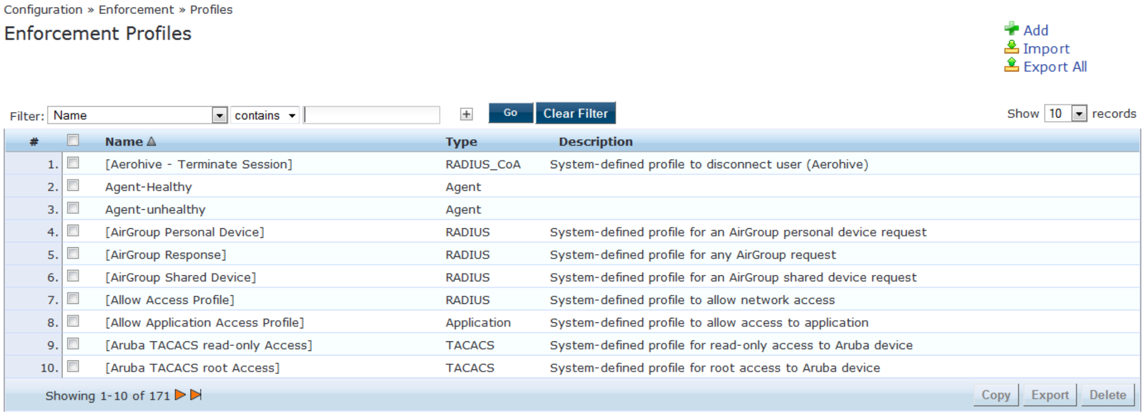
For details on configuring enforcement profiles, see Configuring Enforcement Profiles on page 357.

To create a Juniper SRX enforcement profile:

1. Navigate to **Configuration** > **Enforcement** > **Profiles**.

   The **Enforcement Profiles** page appears.

Figure 629: *Enforcement Profiles Page*

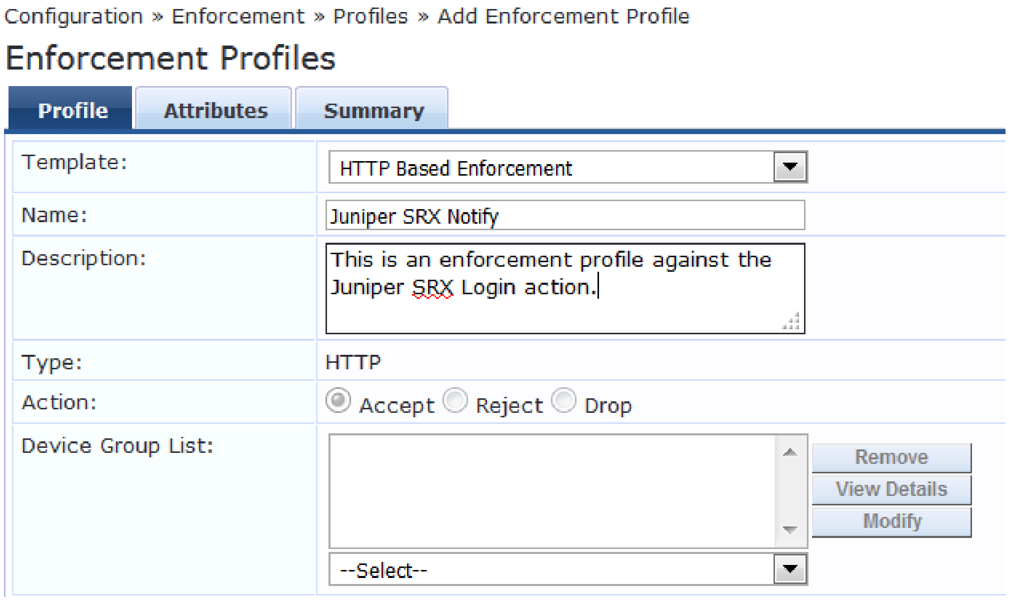


#	□	Name ▲	Type	Description
1.	□	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	□	Agent-Healthy	Agent	
3.	□	Agent-unhealthy	Agent	
4.	□	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
5.	□	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
6.	□	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
7.	□	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
8.	□	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
9.	□	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
10.	□	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device

2. Click **Add**.

   The **Add Enforcement Profiles** dialog appears.

Figure 630: *Adding the Juniper SRX Enforcement Profile*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	HTTP Based Enforcement
Name:	Juniper SRX Notify
Description:	This is an enforcement profile against the Juniper SRX Login action.
Type:	HTTP
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

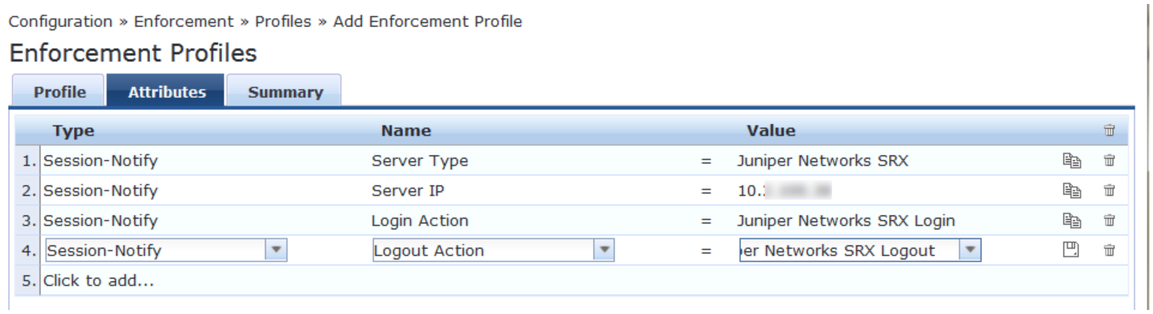
3. Configure the **Add Enforcement Profile** page as follows:
   a. **Template:** Select **Session Notification Enforcement**.

      For details on configuring session notification enforcement profiles, see Session Notification Enforcement Profile on page 395

   b. **Name:** Enter **Juniper SRX Notify**.
   c. **Description**: Optionally, enter a description of this enforcement profile.
   d. Click **Next**.

      The **Enforcement Profiles Attributes** page appears. In the following steps, you will add the four Session Notify Enforcement attributes illustrated in Figure 631.

Figure 631: *Adding Attributes to the Enforcement Profile*



Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Type	Name		Value
1.	Session-Notify	Server Type	=	Juniper Networks SRX
2.	Session-Notify	Server IP	=	10.[redacted]
3.	Session-Notify	Login Action	=	Juniper Networks SRX Login
4.	Session-Notify	Logout Action	=	er Networks SRX Logout
5.	Click to add...			

Server Type

4. Click **Click to add...**.
   a. **Type:** Select **Session-Notify**.
   b. **Name**: Select **Server Type**.
   c. **Value:** Select **Juniper Networks SRX**.

Server IP

5. Click **Click to add...**.
   a. **Type:** Select **Session-Notify**.
   b. **Name**: Select **Server IP**.

c. **Value:** Select the IP address of the Juniper SRX server.

Login Action

6. Click **Click to add...**.
   a. **Type:** Select **Session-Notify**.
   b. **Name**: Select **Login Action**.
   c. **Value:** Select **Juniper Networks SRX Login**.

Logout Action

7. Click **Click to add...**.
   a. **Type:** Select **Session-Notify**.
   b. **Name**: Select **Logout Action**.
   c. **Value:** Select **Juniper Networks SRX Logout**.
8. Click **Save**.

   You return to the **Enforcement Profiles** page, where the Juniper Networks SRX Notify enforcement profile is now listed.

Creating a Juniper SRX Enforcement Policy

This section describes how to create an enforcement policy to act against the "**Juniper SRX Notify**" profile so that external devices can authenticate against this policy.

For details on configuring enforcement policies, see Configuring Enforcement Policies on page 355.

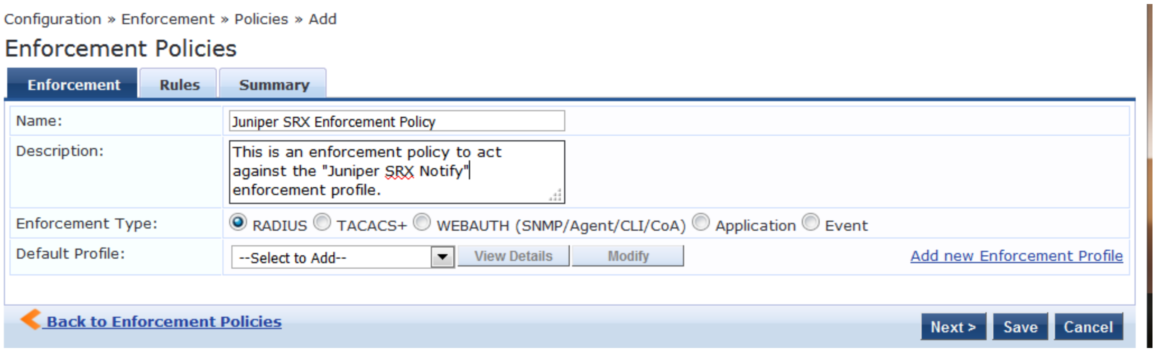
To create a Juniper SRX Enforcement Policy:

1. Navigate to **Configuration** > **Enforcement** > **Policies**.

   The **Enforcement Policies** page appears.
2. Click **Add**.

   The **Add Enforcement Policies** dialog appears.

Figure 632: *Adding the Juniper SRX Enforcement Policy*


Configuration » Enforcement » Policies » Add
Enforcement Policies
Enforcement
Rules
Summary
Back to Enforcement Policies
Next >
Save
Cancel

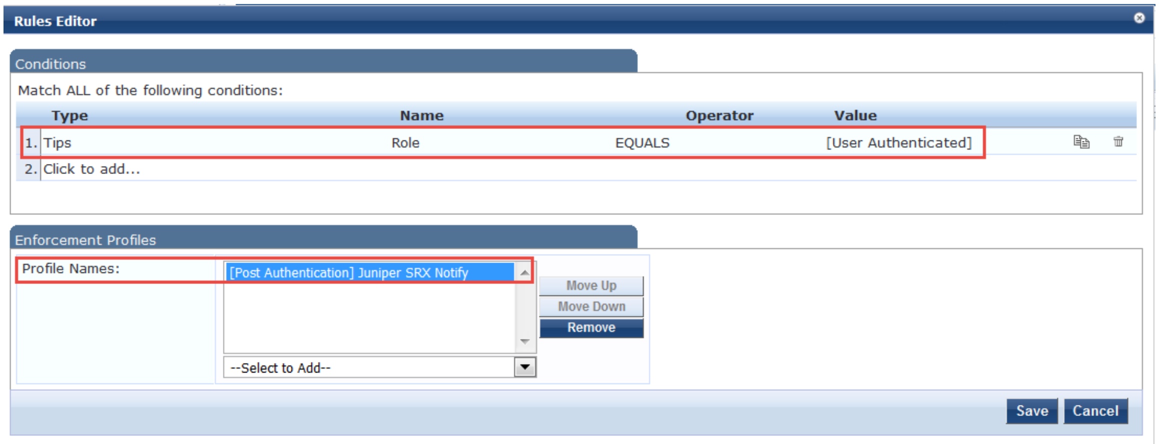
Name:	Juniper SRX Enforcement Policy
Description:	This is an enforcement policy to act against the "Juniper SRX Notify" enforcement profile.
Enforcement Type:	● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event
Default Profile:	--Select to Add-- View Details Modify Add new Enforcement Profile

3. Enter the following information:
   a. **Name**: Enter **Juniper SRX Enforcement Policy**.
   b. **Description**: Optionally, enter a description of this profile.
   c. **Enforcement Type**: Set by default to **RADIUS**.
   d. Default Profile: Select **Allow Access Profile**.
   e. Click **Next**.

      The **Rules** page opens.
4. Click **Add Rule**.

The Rules Editor dialog opens.

Figure 633: *Configuring Juniper SRX Enforcement Policy Rules*



Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	Role	EQUALS	[User Authenticated]
2.	Click to add...			

Enforcement Profiles

Profile Names: [Post Authentication] Juniper SRX Notify

--Select to Add--

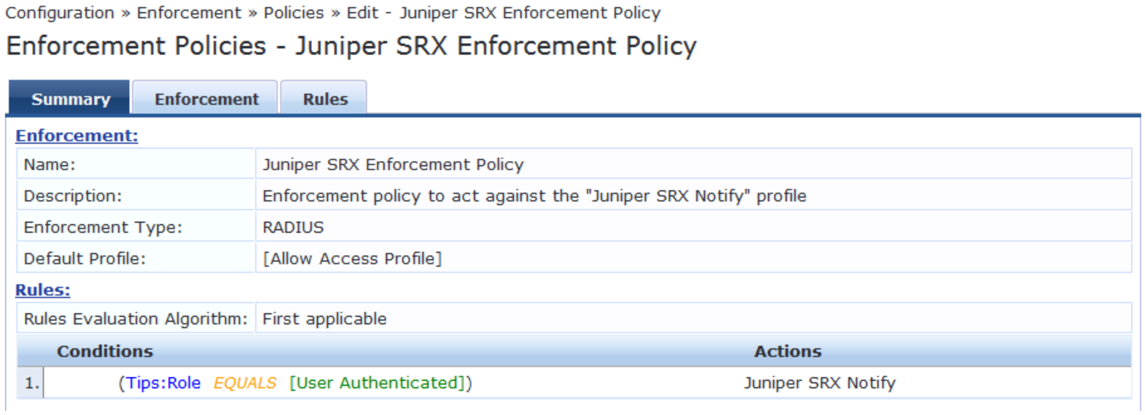
Specify Conditions

5. In the **Conditions** panel, click **Click to add**, then enter the following information:
   a. **Type**: Select **Tips**.
   b. **Name**: Select **Role**.
   c. **Operator**: Select **EQUALS**.
   d. **Value**: Select **User Authenticated**.

Specify the Enforcement Profile

6. In the **Enforcement Profiles** panel:
   a. Click **Select to Add**.
   b. Select **[Post Authentication] Juniper SRX Notify**.
7. Click **Save**.
8. To view the Juniper SRX enforcement policy summary, click the **Summary** tab.

Figure 634: *Summary of the Juniper SRX Enforcement Policy*



Configuration » Enforcement » Policies » Edit - Juniper SRX Enforcement Policy

Enforcement Policies - Juniper SRX Enforcement Policy

Enforcement:

Name:	Juniper SRX Enforcement Policy
Description:	Enforcement policy to act against the "Juniper SRX Notify" profile
Enforcement Type:	RADIUS
Default Profile:	[Allow Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [User Authenticated])	Juniper SRX Notify

9. Check the summary information to make sure the enforcement policy is correct, make any changes if necessary, then click **Save**.

   You return to the Enforcement Policies page where the new **Juniper SRX Policy** is now listed.

Defining a Juniper SRX Wireless Service

This section describes how to create a n 802.1X wireless service named "Juniper SRX Wireless Service" to be applied to the policy "Juniper SRX Policy."

To create the Juniper SRX wireless service:

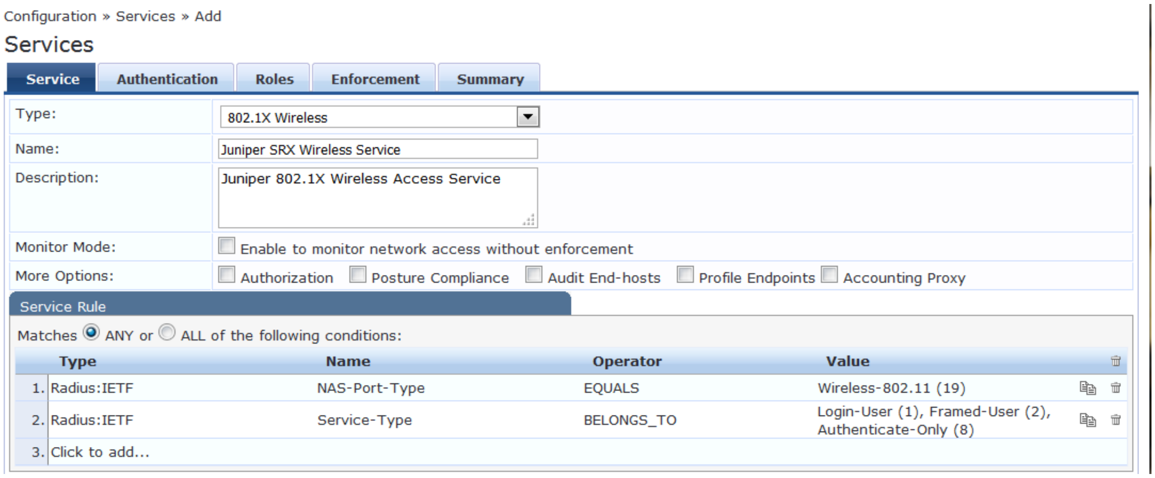
1. Navigate to **Configuration** > **Services**.

   The Services page appears.

2. Click **Add**.

   The Add Services page appears.

Figure 635: *Adding a Juniper SRX Wireless Service*



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

Service Rule

Matches ● ANY or ○ ALL of the following conditions:

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

3. Specify the following information:

   a. **Type**: Select **802.1X Wireless**.

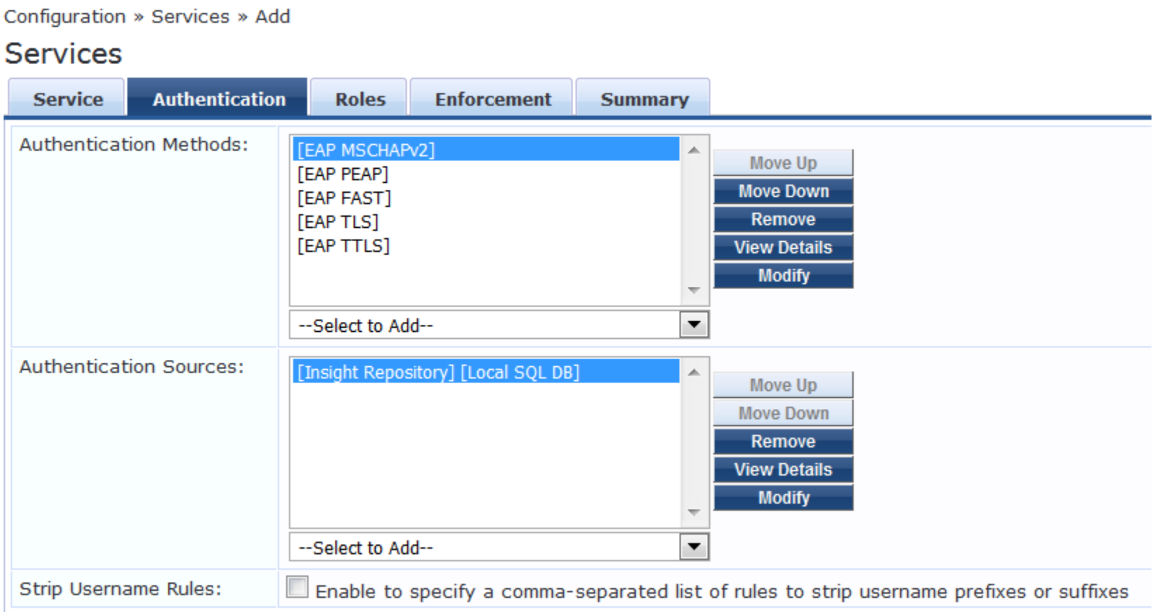
   b. **Name**: Enter **Juniper SRX Wireless Service**.

   c. **Description**: Optionally, enter a description of this service.

   d. In the **Service Rule** panel, set **Matches** to **ANY**, then click **Next**.

      The **Authentication** page appears.

Figure 636: *Specifying the Wireless Service Authentication Settings*



Authentication Methods: [EAP MSCHAPv2]
[EAP PEAP]
[EAP FAST]
[EAP TLS]
[EAP TTLS]
--Select to Add--

Authentication Sources: [Insight Repository] [Local SQL DB]
--Select to Add--

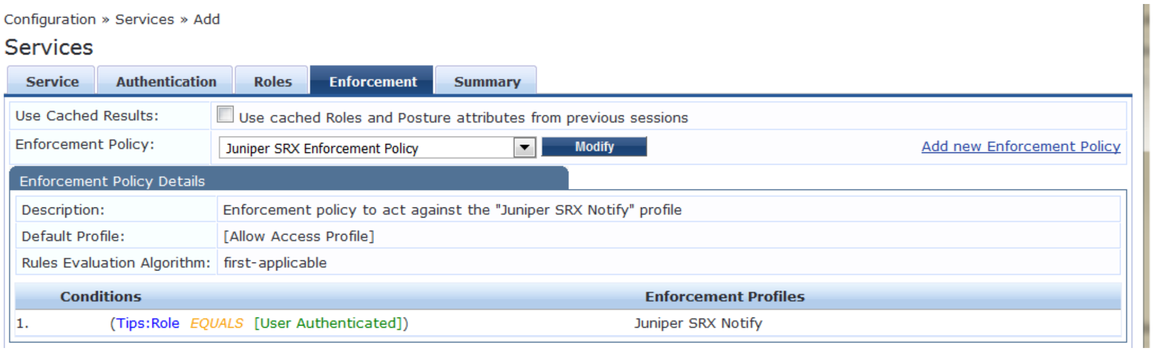
Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

4. Specify the following information:
   a. **Authentication Methods**: Select the authentication method.

      This example uses **EAP MSCHAPv2** as the authentication method.
   b. **Authentication Sources**: Select the authentication source(s).

      This example uses **[Local User Repository] [Local SQL DB]**.as the authentication source.
5. Select the **Enforcement** tab.

Figure 637: *Specifying the Enforcement Policy for the Juniper SRX Wireless Service*


Configuration » Services » Add
Services
Service
Authentication
Roles
Enforcement
Summary
Modify
Add new Enforcement Policy
Enforcement Policy Details

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Juniper SRX Enforcement Policy

Description: Enforcement policy to act against the "Juniper SRX Notify" profile

Default Profile: [Allow Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS [User Authenticated])	Juniper SRX Notify

6. From the **Enforcement Policy** drop-down, select **Juniper SRX Policy**, then click **Next**.

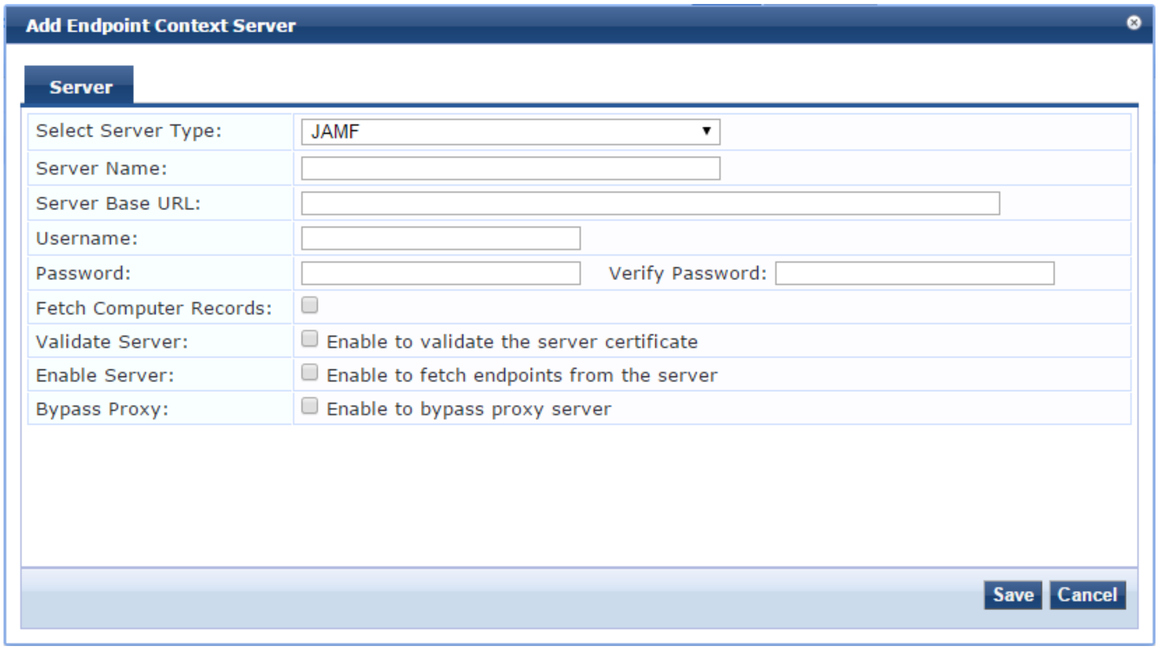
   The **Juniper SRX Wireless Service Summary** is displayed.
7. Check the service summary information to make sure the service is correct, make any changes if necessary, then click **Save**.

   You return to the **Services** page where the new **Juniper SRX Wireless Service** is now listed.

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 638: *Add Endpoint Context Server - Server (JAMF) Tab*



Add Endpoint Context Server

Server

Select Server Type:	JAMF ▾
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Fetch Computer Records:	□
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

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 334: *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 334: *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.

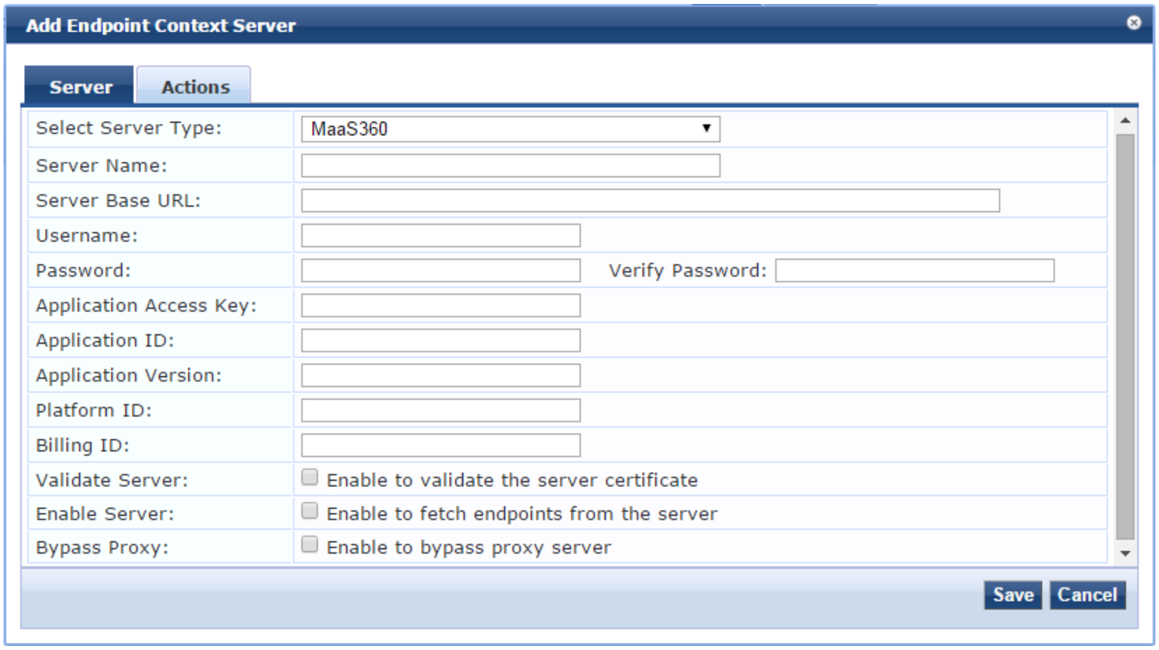
Adding a MaaS360 Endpoint Context Server

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 639: *Add Endpoint Context Server - Server (MaaS360) Tab*



Select Server Type:	MaaS360
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Application Access Key:	
Application ID:	
Application Version:	
Platform ID:	
Billing ID:	
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

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:

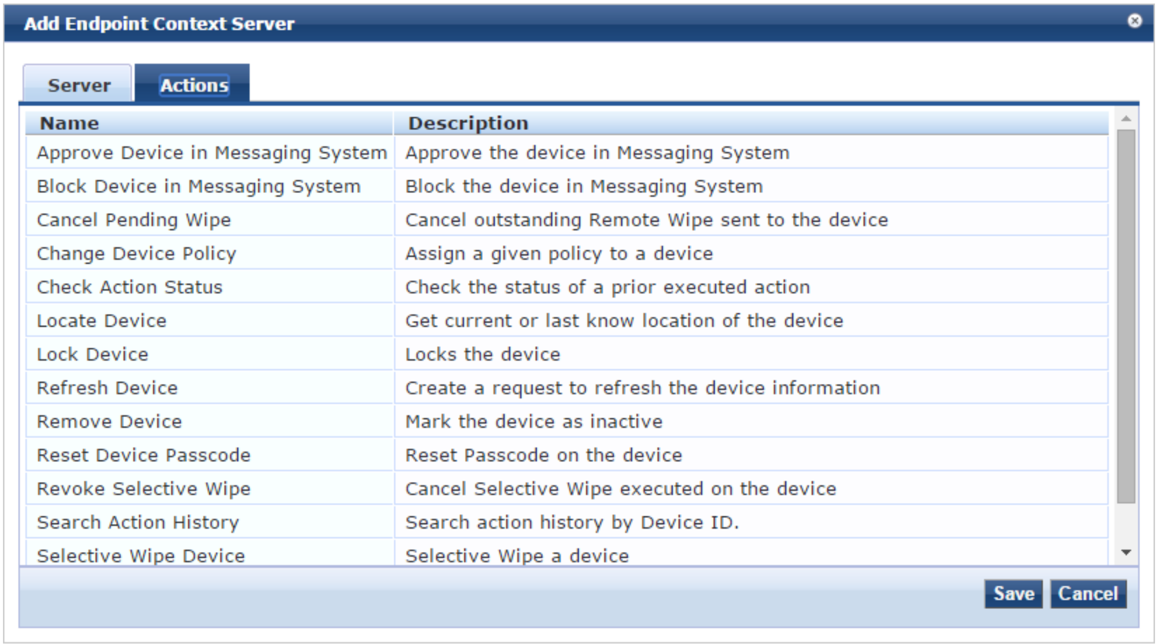
Table 335: *Add Endpoint Context Server - Server (MaaS360) Tab Parameters*

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 640: *Add Endpoint Context Server - Actions (MaaS360) Tab*



Name	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	Locks the device
Refresh Device	Create a request to refresh the device information
Remove Device	Mark the device as inactive
Reset Device Passcode	Reset Passcode on the device
Revoke Selective Wipe	Cancel Selective Wipe executed on the device
Search Action History	Search action history by Device ID.
Selective Wipe Device	Selective Wipe a device

The following table describes the **Add Endpoint Context Server - Actions** (MaaS360) tab parameters:

Table 336: *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 336: *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 MobileIron's documentation for more information about the parameters that you must enter to configure this endpoint context server.

To add a MobileIron Endpoint Context Server:

1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.

   The **Endpoint Context Servers** page appears.

2. Click **Add**.

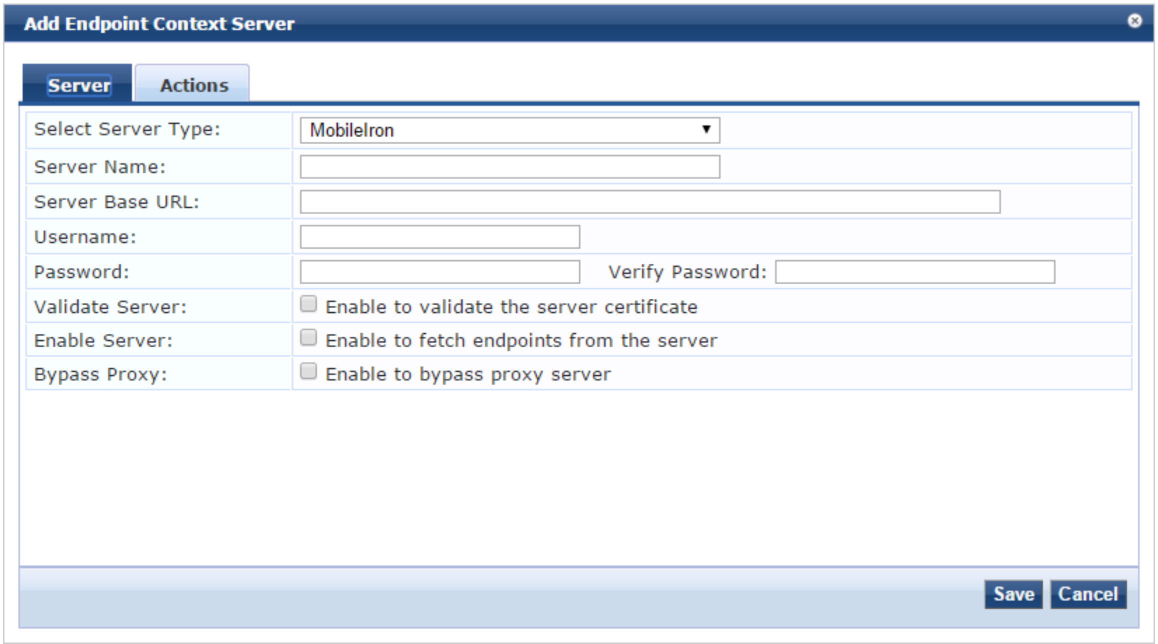
   The **Add Endpoint Context Server** dialog appears. This dialog opens in the **Server** tab.

3. From the **Select Server Type** drop-down, select **MobileIron**.

Server Page

The following figure displays the **Add Endpoint Context Server - Server** (MobileIron) dialog:

Figure 641: *Adding a MobileIron Endpoint Context Server - Server Page*



Select Server Type:	MobileIron ▾
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

NOTE

You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the MobileIron Add Endpoint Context Server parameters described in Table 337.
5. When satisfied with the settings, click **Save**.

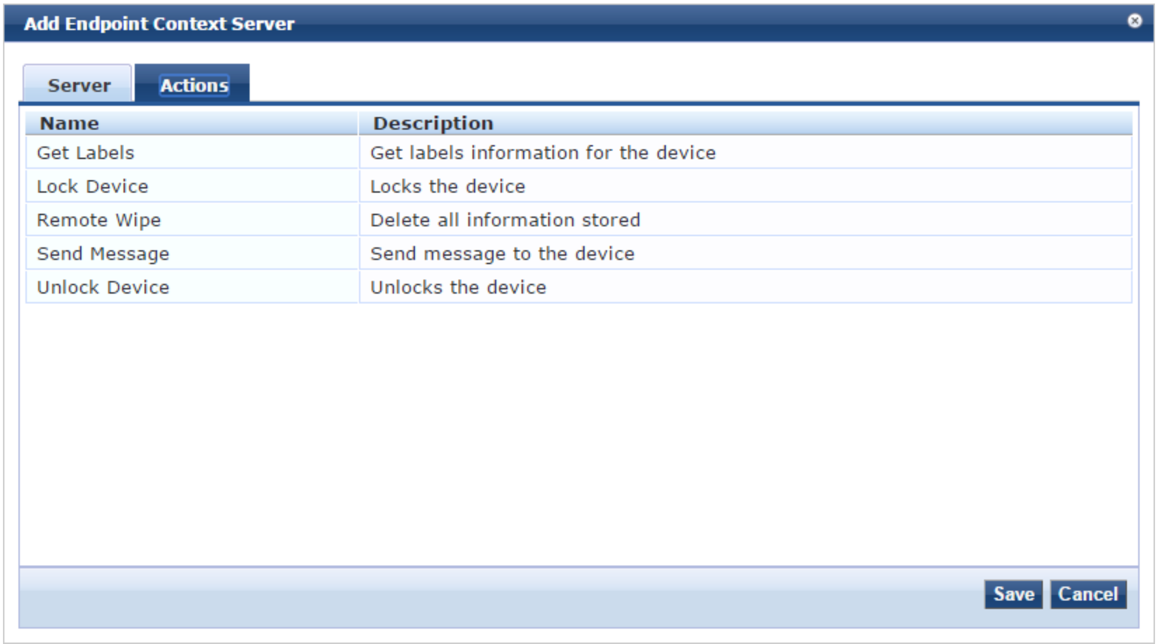
Table 337: *Adding a MobileIron Endpoint Context Server - Server Page Parameters*

Parameter	Description
Select Server Type	1. Choose **MobileIron** from the drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or host name.
Server Base URL	3. 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	4. Enter the username.
Password	5. Enter and verify the password.
Verify Password	
Validate Server	6. Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	7. Enable to fetch endpoints from the server.
Bypass Proxy	8. Enable to bypass the proxy server.

Actions Page

The following figure displays the **Add Endpoint Context Server - Actions** (MobileIron) page:

Figure 642: *Adding a MobileIron Endpoint Context Server - Actions Page*



Name	Description
Get Labels	Get labels information for the device
Lock Device	Locks the device
Remote Wipe	Delete all information stored
Send Message	Send message to the device
Unlock Device	Unlocks the device

Table 338 describes the Endpoint Context Server Actions that are available:

Table 338: *Adding a MobileIron Endpoint Context Server - Actions Page 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.

9. When satisfied with the **Action** settings, click **Save**.

Adding a Palo Alto Networks Firewall Endpoint Context Server

Consult Palo Alto Networks' documentation for more information about the parameters that you must enter to configure this endpoint context server.

To add a Palo Alto Networks Firewall endpoint context server:

1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.

   The **Endpoint Context Servers** page opens.

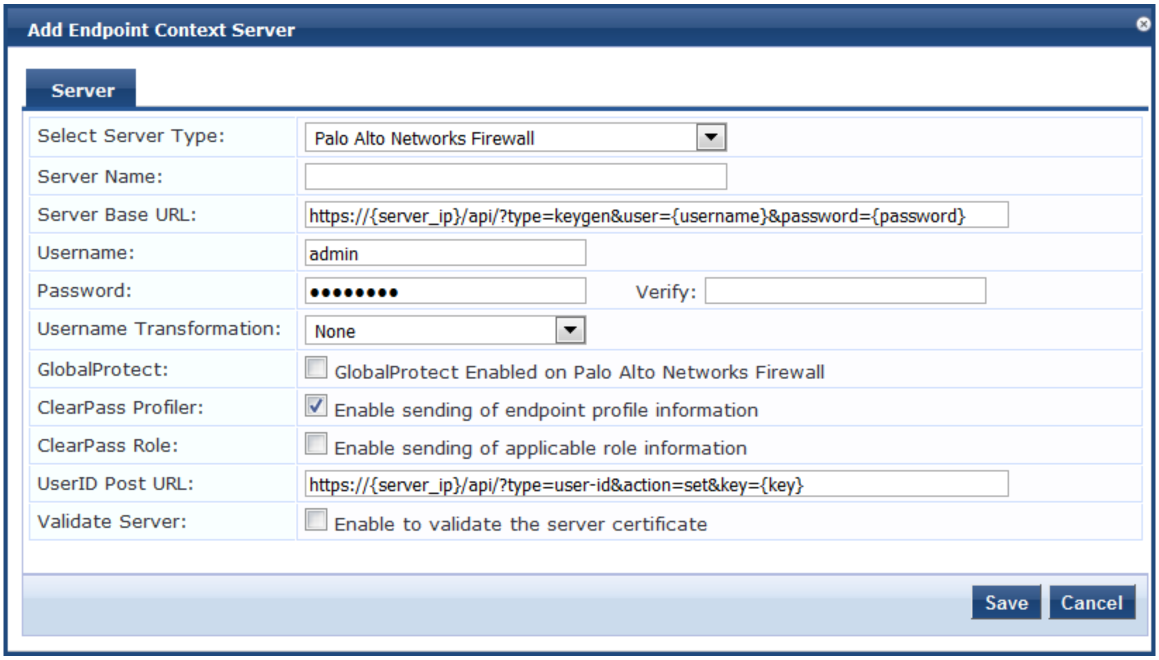
2. Click **Add**.

   The **Add Endpoint Context Server** dialog opens.

3. From the **Select Server Type** drop-down, select **Palo Alto Networks Firewall**.

   The following dialog is displayed (see Figure 643).

Figure 643: *Add Endpoint Context Server > Palo Alto Networks Firewall Dialog*



Select Server Type:	Palo Alto Networks Firewall
Server Name:	
Server Base URL:	https://{server_ip}/api/?type=keygen&user={username}&password={password}
Username:	admin
Password:	•••••••• Verify:
Username Transformation:	None
GlobalProtect:	□ GlobalProtect Enabled on Palo Alto Networks Firewall
ClearPass Profiler:	☑ Enable sending of endpoint profile information
ClearPass Role:	□ Enable sending of applicable role information
UserID Post URL:	https://{server_ip}/api/?type=user-id&action=set&key={key}
Validate Server:	□ Enable to validate the server certificate

NOTE

You can add multiple endpoint context servers of the same type.

4. Enter the appropriate values for each of the **Palo Alto Networks Firewall** > **Add Endpoint Context Server** parameters described in Table 339.
5. When satisfied with the settings, click **Save**.

Table 339: *Add Endpoint Context Server > Palo Alto Networks Firewall Parameters*

Parameter	Action/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 a 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**: Use the Prefix NetBIOS name in UID updates. ● **Use Full Username**: Use the full username in UID updates.
GlobalProtect	Enable this option to send an HIP (Host Information Profiles) report to the firewall. You must enable the GlobalProtect license on the firewall for this to work.
ClearPass Profiler	Select this check box to enable sending of endpoint profile information.
ClearPass Role	Select this check box to enable sending of the applicable role information.
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.

Using the ClearPass Configuration API to Load Endpoint Context Servers

If you use the ClearPass Configuration API to load Palo Alto Networks endpoint context servers, you should include the following attributes in the XML file:

- PA_Panorama_RegisterDevice
- PA_Panorama_SendRoles

Adding a Palo Alto Networks Panorama Endpoint Context Server

Consult Palo Alto Networks' documentation for more information about the parameters that you must enter to configure this endpoint context server.

To add a Palo Alto Networks Panorama endpoint context server:

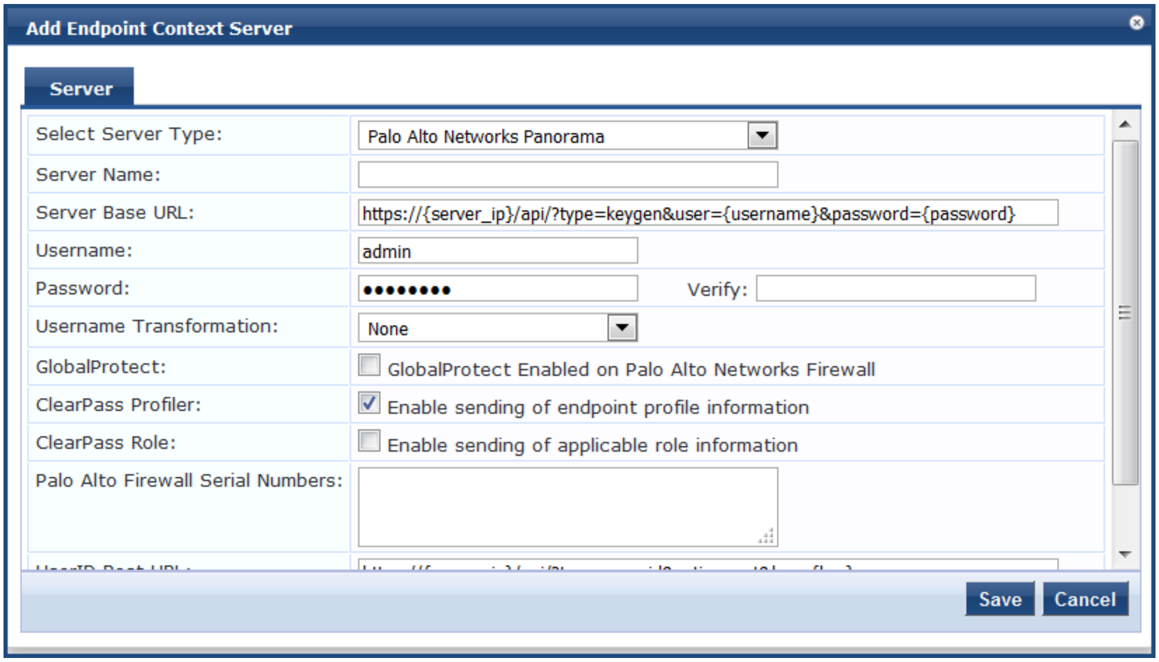
1. Navigate to **Administration** > **External Servers** > **Endpoint Context Servers**.

   The **Endpoint Context Servers** page opens.
2. Click **Add**.

   The **Add Endpoint Context Server** dialog opens.
3. From the **Select Server Type** drop-down, select **Palo Alto Networks Panorama**.

   The following dialog is displayed:

Figure 644: *Add Endpoint Context Server > Palo Alto Networks Panorama Dialog*



Select Server Type:	Palo Alto Networks Panorama
Server Name:	
Server Base URL:	https://{server_ip}/api/?type=keygen&user={username}&password={password}
Username:	admin
Password:	•••••••• Verify:
Username Transformation:	None
GlobalProtect:	□ GlobalProtect Enabled on Palo Alto Networks Firewall
ClearPass Profiler:	☑ Enable sending of endpoint profile information
ClearPass Role:	□ Enable sending of applicable role information
Palo Alto Firewall Serial Numbers:	

You can add more than one endpoint context server of the same type. For example, you can add more than one Palo Alto Networks endpoint context server.

4. Enter the appropriate values for each of the **Palo Alto Networks Panorama** > **Add Endpoint Context Server** parameters described in Table 340.
5. When satisfied with the settings, click **Save**.

Table 340: *Add Endpoint Context Server > Palo Alto Networks Panorama 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}

Table 340: *Add Endpoint Context Server > Palo Alto Networks Panorama Parameters (Continued)*

Parameter	Description
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.
ClearPass Profiler	Select this check box to enable sending of endpoint profile information. This parameter is enabled by default.
ClearPass Role	Select this check box to enable sending of the applicable role information.
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.

Using the ClearPass Configuration API to Load Endpoint Context Servers

If you use the ClearPass Configuration API to load Palo Alto Networks endpoint context servers, you should include the following attributes in the XML file:

- PA_Panorama_RegisterDevice
- PA_Panorama_SendRoles

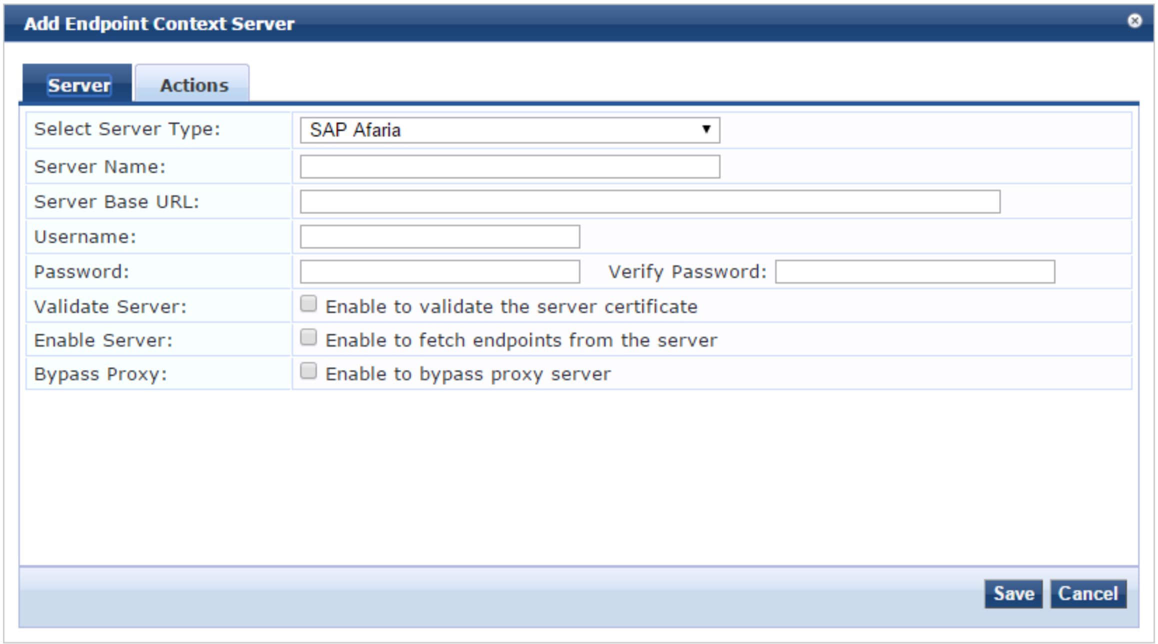
Adding an SAP Afaria Endpoint Context Server

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 645: *Add Endpoint Context Server - Server (SAP Afaria) Tab*



Add Endpoint Context Server

Server | Actions

Select Server Type:	SAP Afaria ▾
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

Save Cancel

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:

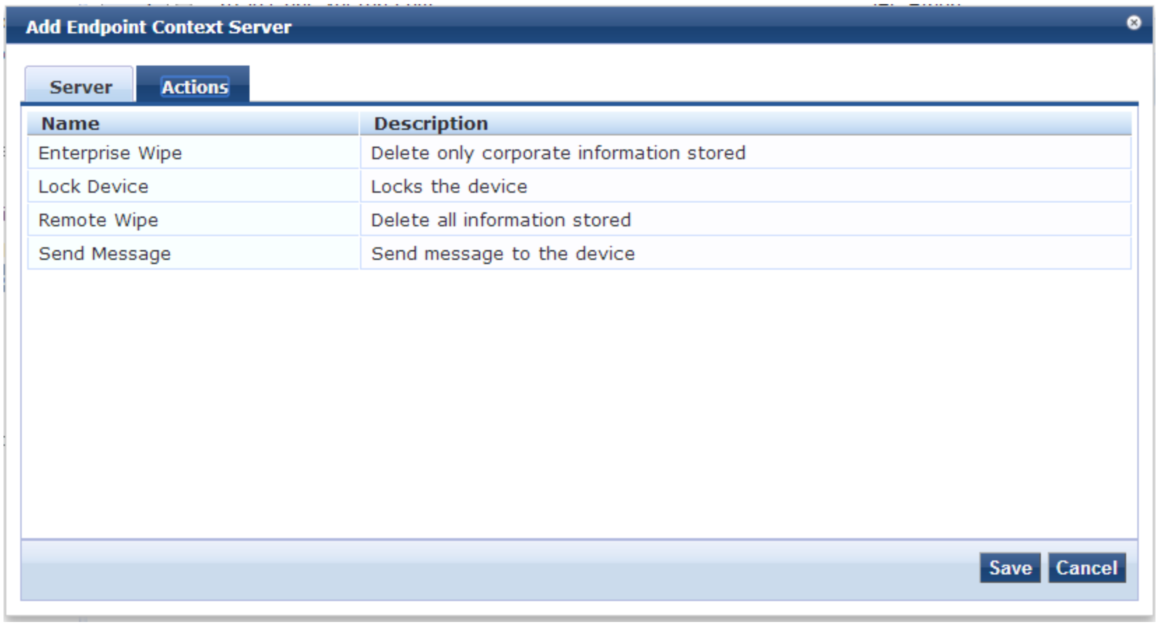
Table 341: *Add Endpoint Context Server - Server (SAP Afaria) Tab Parameters*

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 646: *Add Endpoint Context Server - Actions (SAP Afaria) Tab*



Name	Description
Enterprise Wipe	Delete only corporate information stored
Lock Device	Locks the device
Remote Wipe	Delete all information stored
Send Message	Send message to the device

The following table describes the **Add Endpoint Context Server - Actions** (SAP Afaria) tab parameters:

Table 342: *Add Endpoint Context Server - Actions (SAP Afaria) Tab Parameters*

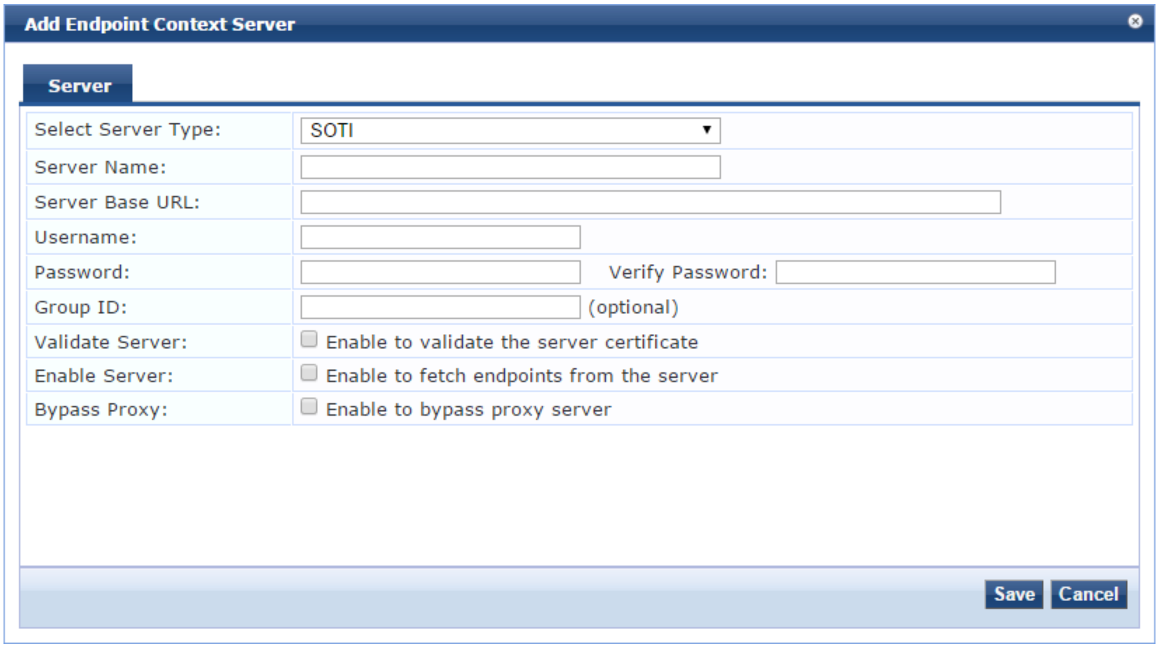
Parameter	Description
Enterprise Wipe	Delete corporate information related data.
Lock Device	Lock the associated device.
Remote Wipe	Delete all stored information.
Send Message	Send message to the device.

Adding a 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 **SOTI Add Endpoint Context Server > Server** dialog:

Figure 647: *Adding a SOTI Endpoint Context Server > Server (SOTI) Dialog*



Select Server Type:	SOTI ▾
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Group ID:	(optional)
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

NOTE

You can add more than one endpoint context server of the same type.

The following table describes the **SOTI Add Endpoint Context Server > Server** parameters:

Table 343: *Adding a SOTI Endpoint Context Server > Server Parameters*

Parameter	Action/Description
Select Server Type	1. Choose **SOTI** from the **Select Server Type** drop-down list.
Server Name	2. Enter a valid server name. You can enter an IP address or a hostname.
Server Base URL	3. Enter the complete URL for the SOTI server. You can append a custom port, such as for an MDM server: https://yourserver.yourcompany.com:customerportnumber
Username	4. Enter the username for the SOTI server.
Password	5. Enter the password, then verify it.
Verify Password	
Group ID	6. Enter the group ID. This parameter is optional.
Validate Server	7. Enable **Validate Server** to validate the server certificate. Enabling this option enables the **Certificate** tab.

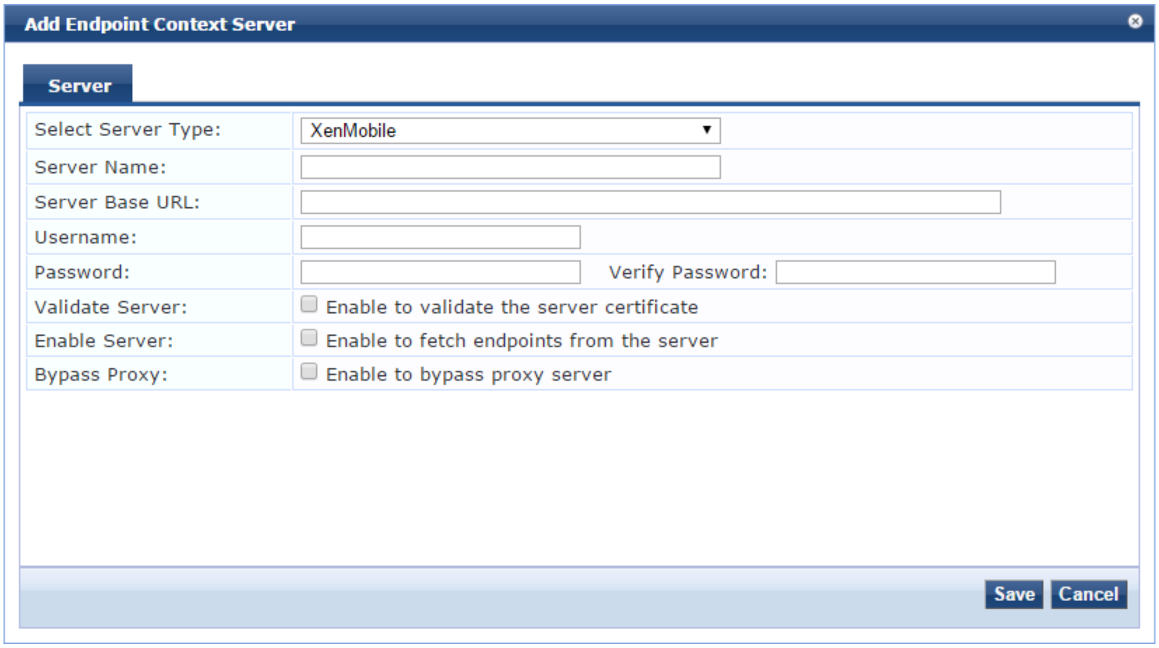
Table 343: *Adding a SOTI Endpoint Context Server > Server Parameters (Continued)*

Parameter	Action/Description
Enable Server	8. Enable **Enable Server** to fetch endpoints from the server.
Bypass Proxy	9. Enable **Bypass Proxy** to bypass the proxy server.
	10. To save your changes, click **Save**.

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 648: *Add Endpoint Context Server - Server (XenMobile) Tab*



Select Server Type:	XenMobile ▾
Server Name:	
Server Base URL:	
Username:	
Password:	Verify Password:
Validate Server:	□ Enable to validate the server certificate
Enable Server:	□ Enable to fetch endpoints from the server
Bypass Proxy:	□ Enable to bypass proxy server

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 344: *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}

Table 344: *Add Endpoint Context Server - Server (XenMobile) Tab Parameters (Continued)*

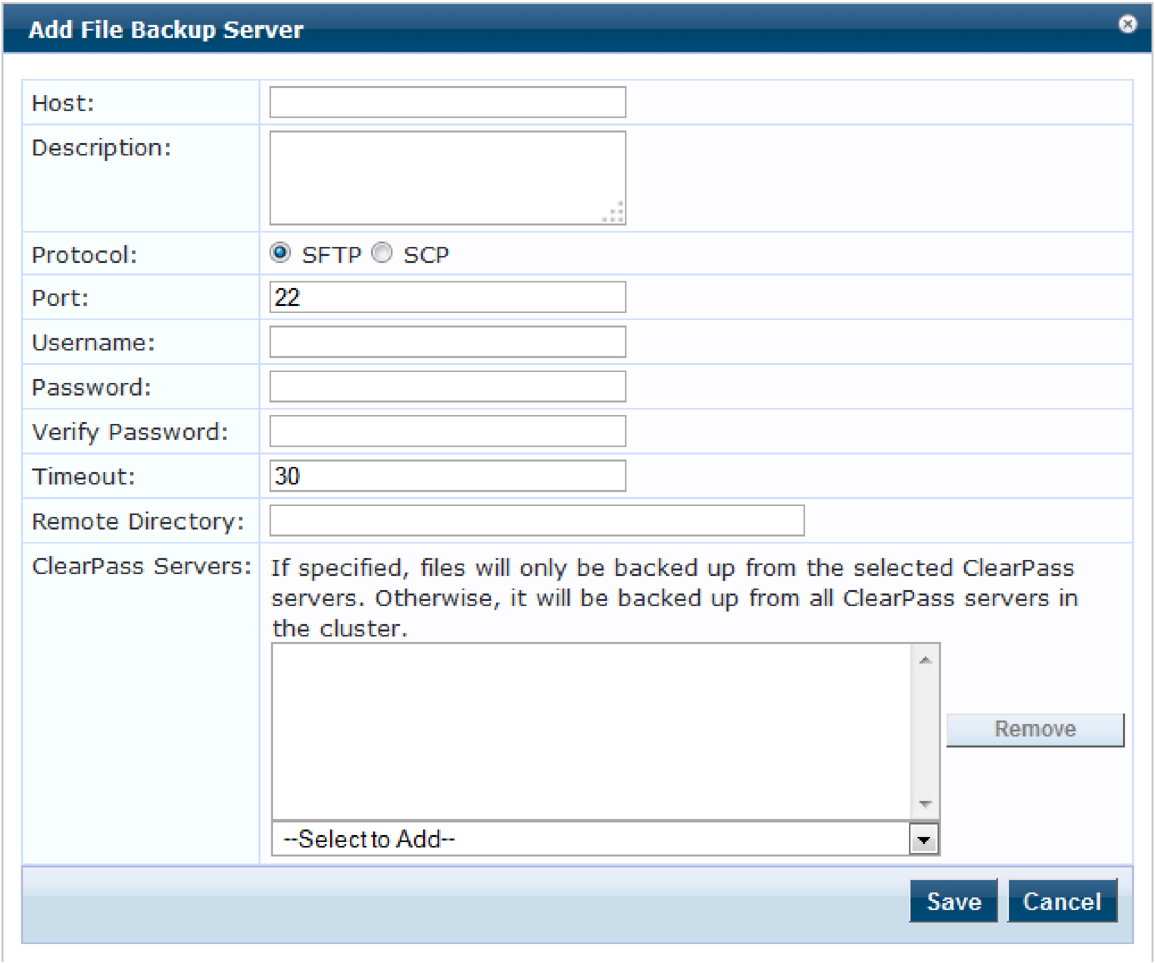
Parameter	Description
	/api/?type=keygen&user={username}&password={password}
Username	Enter the username.
Password	Enter and verify the password.
Verify Password	
Validate Server	Enable to validate the server certificate. Checking this option enables the **Certificate** tab.
Enable Server	Enable to fetch endpoints from the server.
Bypass Proxy	Enable to bypass proxy server.

File Backup Servers

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 649: *File Backup Servers - Add File Backup Server Page*



Add File Backup Server

Host:	
Description:	
Protocol:	● SFTP ○ SCP
Port:	22
Username:	
Password:	
Verify Password:	
Timeout:	30
Remote Directory:	
ClearPass Servers:	If 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. --Select to Add--

The following table describes the **Add File Backup Server** page parameters:

Table 345: *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)
Port	Specify the port number. The default port is 22.
Username	Enter the user name and password of the host server.

Table 345: *Add File Backup Server Page Parameters (Continued)*

Parameter	Description
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 Certificates

This section describes the following topics:

- Server Certificate Page on page 648
- Server Certificate Type on page 649
- Creating and Installing a Self-Signed Certificate on page 653
- Importing a Server Certificate on page 658
- Exporting a Server Certificate on page 659

Server Certificate Page

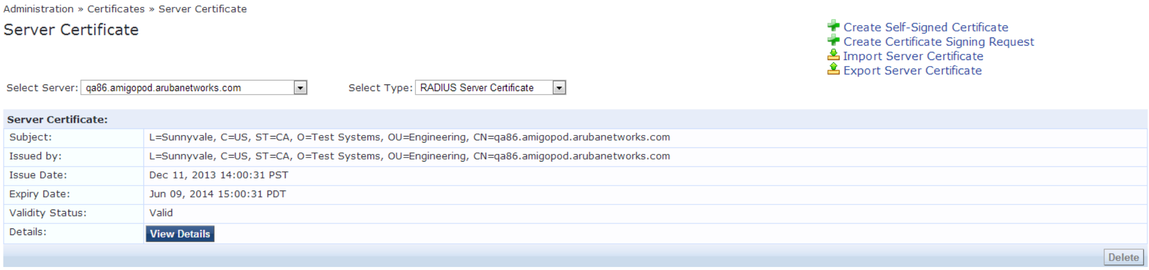
The information provided on the **Server Certificate** page depends on whether the *RADIUS Server Certificate* type or the *HTTPS Service Certificate* type is assigned to the selected server.

To configure the server certificate:

1. Navigate to **Administration** > **Certificates** > **Server Certificate**.

   The following figure displays the **Server Certificate** page:

Figure 650: *Server Certificate Page*


Administration » Certificates » Server Certificate
Server Certificate
Create Self-Signed Certificate
Create Certificate Signing Request
Import Server Certificate
Export Server Certificate
View Details
Delete

Select Server: qa86.amigopod.arubanetworks.com

Select Type: RADIUS Server Certificate

Server Certificate:	
Subject:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issued by:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issue Date:	Dec 11, 2013 14:00:31 PST
Expiry Date:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Details:	View Details

2. Specify the **Server Certificate** parameters as described in the following table:

Table 346: *Server Certificate Parameters*

Parameter	Action/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 and Installing a Self-Signed Certificate on page 653.
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 651.
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 658.
Export Server Certificate	On clicking this link, the self-signed certificate is downloaded. For more information, see Exporting a Server Certificate on page 659.
Select Server	Select a server in the cluster for server certificate operations.
Select Type	Select a certificate type. The options are: ● **RADIUS Server Certificate** ● **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

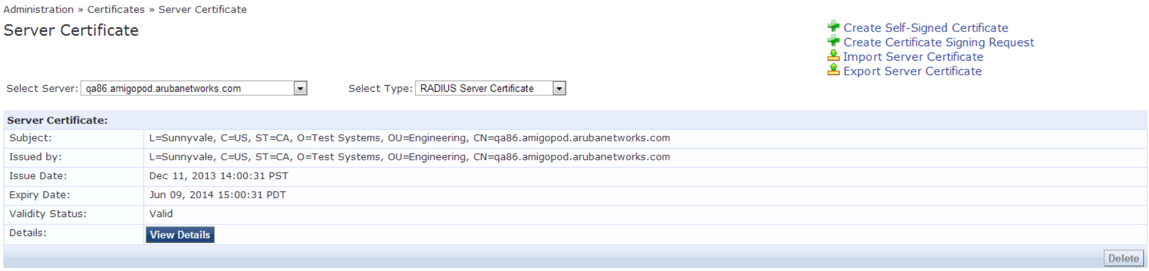
ClearPass Policy Manager provides two types of server certificates.

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 651: *RADIUS Server Certificate Page*


Create Self-Signed Certificate
Create Certificate Signing Request
Import Server Certificate
Export Server Certificate
View Details
Delete

Administration » Certificates » Server Certificate

Server Certificate

Select Server: qa86.amigopod.arubanetworks.com   Select Type: RADIUS Server Certificate

Server Certificate:	
Subject:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issued by:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issue Date:	Dec 11, 2013 14:00:31 PST
Expiry Date:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Details:	View Details

The following table describes the RADIUS **Server Certificate** parameters:

Table 347: *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

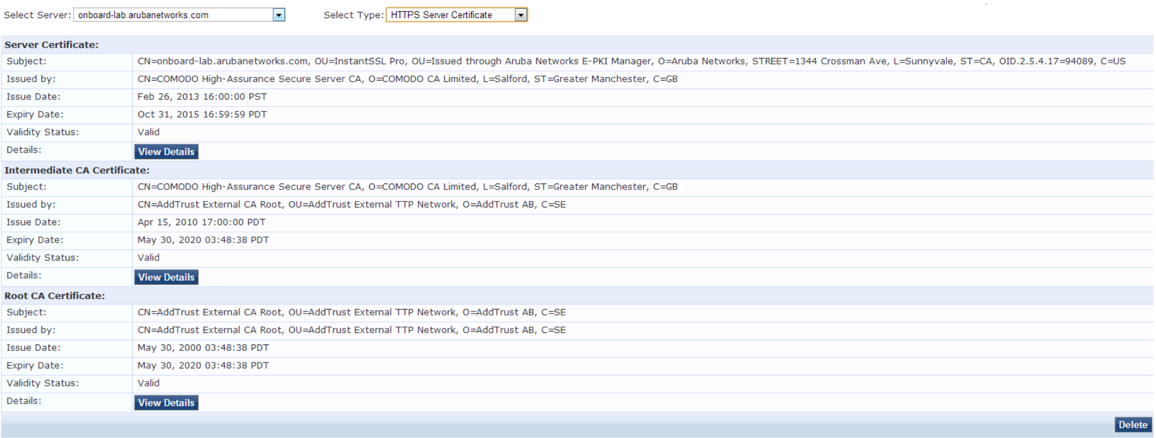
The page displays the parameters configured after a self-signed certificate with an HTTPS Server Certificate is created and installed.

The page contains data about the server certificate, Intermediate CA Certificate, and Root CA Certificate.

Tto see details about Signature Algorithm, Public Key Info, and more, click the **View Details** button.

The following figure displays the HTTPS **Server Certificate** page:

Figure 652: *HTTPS Server Certificate Page*



Select Server: onboard-lab.arubanetworks.com

Select Type: HTTPS Server Certificate

Server Certificate:	
Subject:	CN=onboard-lab.arubanetworks.com, OU=InstantSSL Pro, OU=Issued through Aruba Networks E-PKI Manager, O=Aruba Networks, STREET=1344 Crossman Ave, L=Sunnyvale, ST=CA, OID.2.5.4.17=94089, C=US
Issued by:	CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issue Date:	Feb 26, 2013 16:00:00 PST
Expiry Date:	Oct 31, 2015 16:59:59 PDT
Validity Status:	Valid
Details:	View Details
Intermediate CA Certificate:	
Subject:	CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issued by:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issue Date:	Apr 15, 2010 17:00:00 PDT
Expiry Date:	May 30, 2020 03:48:38 PDT
Validity Status:	Valid
Details:	View Details
Root CA Certificate:	
Subject:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issued by:	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issue Date:	May 30, 2000 03:48:38 PDT
Expiry Date:	May 30, 2020 03:48:38 PDT
Validity Status:	Valid
Details:	View Details

The following table describes the **HTTPS Server Certificate** information:

Table 348: *HTTPS Server Certificate Parameters*

Parameter	Action/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	To view details about the certificate, such as Signature Algorithm and Subject Public Key Info, click the **View Details** button.

Creating a Certificate Signing Request

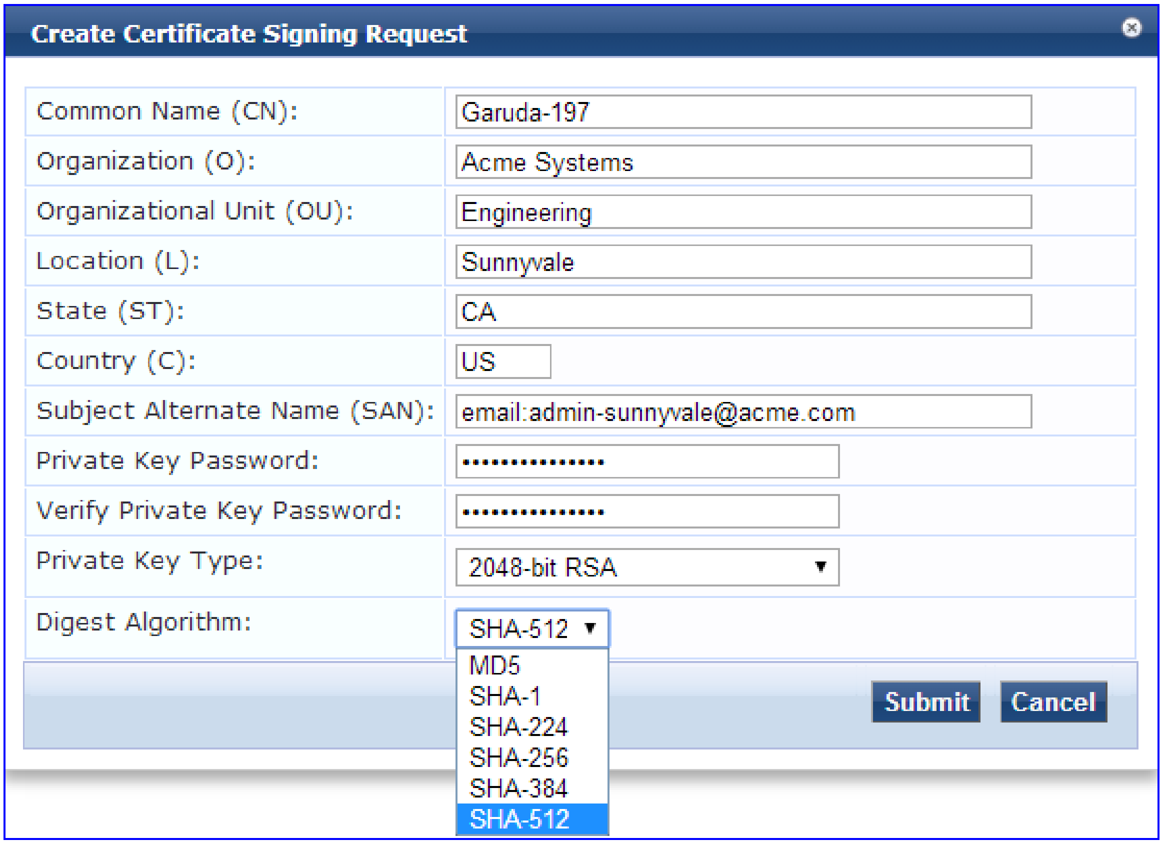
After you select a server and a certificate type, you can create a certificate signing request. This task creates a self-signed certificate to be signed by a CA (Certificate Authority).

To create a certificate signing request:

1. Navigate to **Administration** > **Certificates** > **Server Certificate**.
2. Select a server.
3. Click the **Create Certificate Signing Request** link.

   The **Create Certificate Signing Request** dialog opens:

Figure 653: *Create Certificate Signing Request Dialog*



Create Certificate Signing Request

Common Name (CN):	Garuda-197
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	Sunnyvale
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin-sunnyvale@acme.com
Private Key Password:	•••••••••••••••
Verify Private Key Password:	•••••••••••••••
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

4. Specify the **Create Certificate Signing Request** parameters as described in Table 349, then click **Submit**.

Table 349: *Create Certificate Signing Request Parameters*

Parameter	Action/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) State (ST) Country (C)	Optionally, enter the name of the location, state, country.
Subject Alternate Name (SAN)	Optionally, enter the alternative names for the specified Common Name in one of the following formats: ■ email: *email_address* ■ URI: *uri* ■ IP: *ip_address* ■ dns: *dns_name*

Table 349: *Create Certificate Signing Request Parameters (Continued)*

Parameter	Action/Description
	■ rid: *id*
Private Key Password Verify Private Key Password	Enter the private key password, then verify it.
Private Key Type	Select the length for the generated private key types from the following options: ■ 1024-bit RSA ■ **2048-bit RSA**. This is the default. ■ 4096-bit RSA ■ X9.62/SECG curve over a 256 bit prime field ■ NIST/SECG curve over a 384 bit prime field
Digest Algorithm	Select the message digest algorithm from the following options: ■ SHA-1 ■ SHA-224 ■ SHA-256 ■ SHA-384 ■ **SHA-512**. This is the default.

After you create a **Certificate Signing Request** form and click **Submit**, the generated certificate signing request is displayed.

5. Copy the certificate and paste it into the Web form as part of the enrollment process.
6. To save the Certificate Signing Request file and the private key password file, click **Download CSR and Private Key Files**.

Creating and Installing a Self-Signed Certificate

After you select a server and a certificate type, you can create and install a self-signed certificate.

NOTE

When Common Criteria mode is enabled, the **Create-Self Signed Certificate** option for both HTTPS and RADIUS certificates is not available from the **Administration** > **Certificates** > **Server Certificate** page (for more information, see Mode Parameters on page 536).

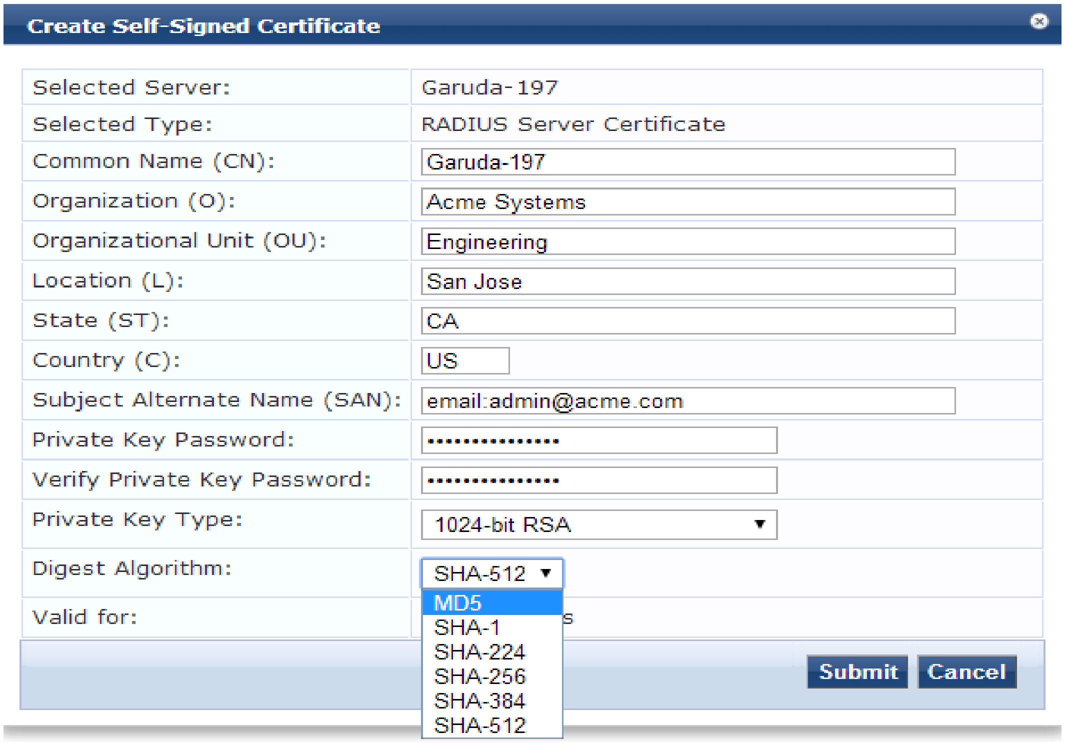
Creating a Self-Signed Certificate

To create a self-signed certificate:

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Select a server.
3. Click the **Create Self-Signed Certificate** link.

   The **Create Self-Signed Certificate** page opens.

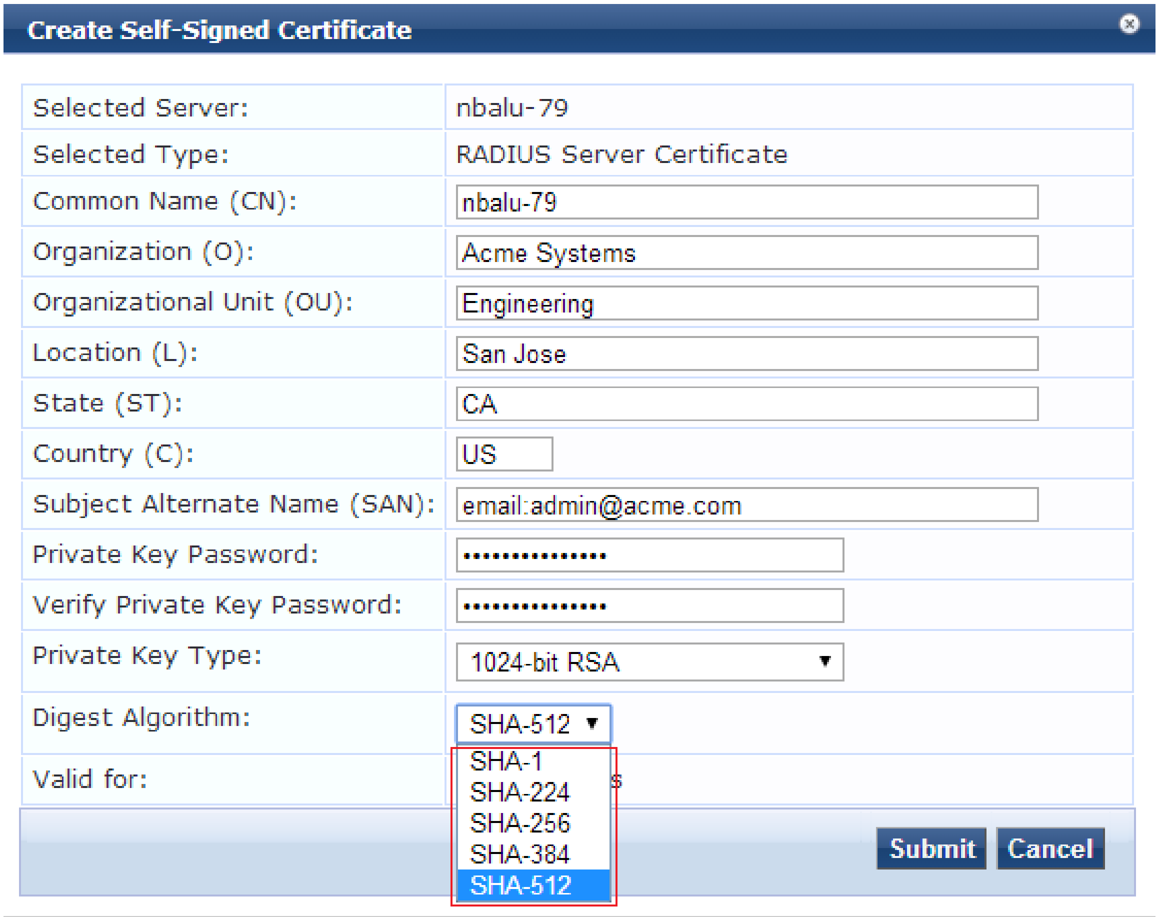
Figure 654: *Create Self-Signed Certificate Page*



Create Self-Signed Certificate

Selected Server:	Garuda-197
Selected Type:	RADIUS Server Certificate
Common Name (CN):	Garuda-197
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	San Jose
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin@acme.com
Private Key Password:	•••••••••••••••
Verify Private Key Password:	•••••••••••••••
Private Key Type:	1024-bit RSA
Digest Algorithm:	SHA-512
Valid for:	s

Figure 655: *Create Self-Signed Certificate Page - FIPS Mode Page*



Create Self-Signed Certificate

Selected Server:	nbalu-79
Selected Type:	RADIUS Server Certificate
Common Name (CN):	nbalu-79
Organization (O):	Acme Systems
Organizational Unit (OU):	Engineering
Location (L):	San Jose
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	email:admin@acme.com
Private Key Password:	•••••••••••••••
Verify Private Key Password:	•••••••••••••••
Private Key Type:	1024-bit RSA
Digest Algorithm:	SHA-512
Valid for:	s

4. Configure the **Create Self-Signed Certificate** parameters as described in Table 350, then click **Submit**.

Table 350: *Create Self-Signed Certificate Parameters*

Parameter	Action/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.
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 name for the specified Common Name. **NOTE:** Enter the Subject Alternate Name in one of 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 reenter the Private Key password.
Verify Private Key Password	

Table 350: *Create Self-Signed Certificate Parameters (Continued)*

Parameter	Action/Description
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 **FIPS** mode.
Valid for	Enter the certificate duration in number of days. The default is **180** days.

Installing a Self-Signed Certificate

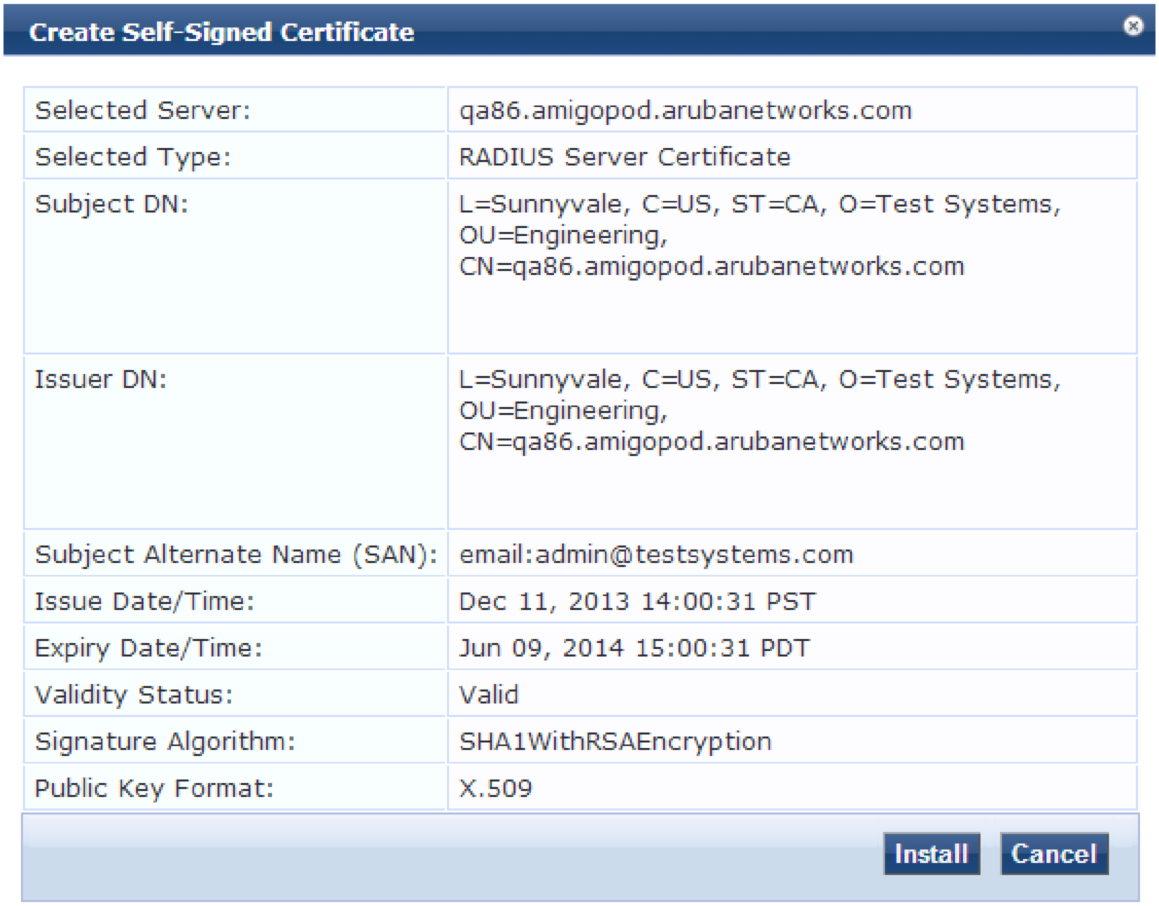
Once you click **Submit**, you are prompted to install the self-signed certificate.

This page displays a summary of the values selected in the **Create Self-Signed Certificate** page.

1. To install the self-signed certificate, click **Install**.

   The **Create Self-Signed Certificate** dialog opens.

Figure 656: *Create Self-Signed Certificate Page*



Create Self-Signed Certificate

Selected Server:	qa86.amigopod.arubanetworks.com
Selected Type:	RADIUS Server Certificate
Subject DN:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Issuer DN:	L=Sunnyvale, C=US, ST=CA, O=Test Systems, OU=Engineering, CN=qa86.amigopod.arubanetworks.com
Subject Alternate Name (SAN):	email:admin@testsystems.com
Issue Date/Time:	Dec 11, 2013 14:00:31 PST
Expiry Date/Time:	Jun 09, 2014 15:00:31 PDT
Validity Status:	Valid
Signature Algorithm:	SHA1WithRSAEncryption
Public Key Format:	X.509

The following table describes the **Create Self-Signed Certificate** parameters configured:

Table 351: *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 351: *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.

After you click **Install**, Policy Manager generates a message about the status of the certificate installation.

If the installation is successful the page displays "*Server Certificate updated successfully. Please login again to continue...*"

Because all services are restarted after a successful certificate installation, you must click **Logout**, then log in to the ClearPass client to continue.

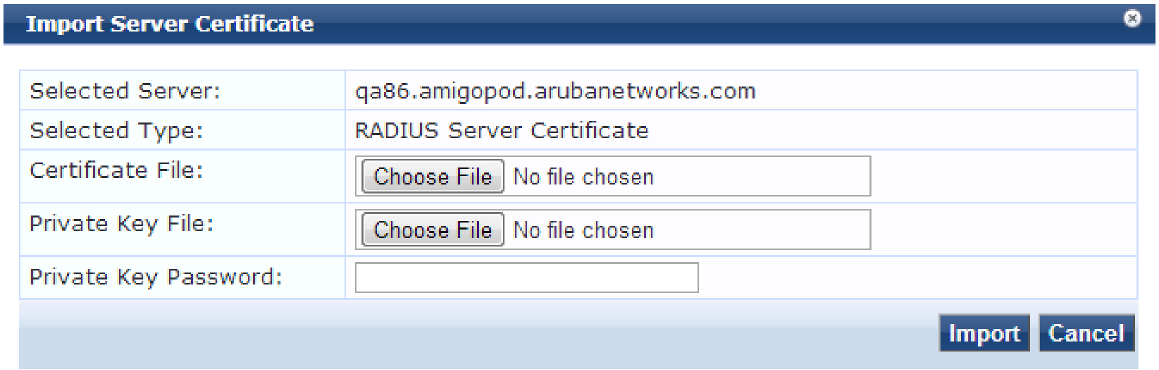
Importing a Server Certificate

To import a server certificate into the current ClearPass server:

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Click the **Import Server Certificate** link.

   The **Import Server Certificate** dialog opens:

Figure 657: *Import Server Certificate Dialog*



Import Server Certificate

Selected Server:	qa86.amigopod.arubanetworks.com
Selected Type:	RADIUS Server Certificate
Certificate File:	Choose File No file chosen
Private Key File:	Choose File No file chosen
Private Key Password:	

NOTE

For security reasons, certificates signed using SHA1RSA is not recommended. It is recommended to import certificates signed with stronger keys such as RSA with a length more than 1024 bits.

3. Specify the **Import Server Certificate** parameters as described in the following table, then click **Import**:

Table 352: *Import Server Certificate Parameters*

Parameter	Action/Description
Selected Server	Displays the name of the selected server.
Selected Type	Displays the selected certificate type of server certificate.
Certificate File	Browse to the certificate file to be imported.
Private Key File	Browse to the private key file to be imported.
Private Key Password	Enter the private key password that was entered when the server certificate was configured.

Exporting a Server Certificate

To export a server certificate from the current ClearPass server:

1. Navigate to **Administration > Certificates > Server Certificate**.
2. Click the **Export Server Certificate** link.

   The Open RADIUSServerCertificate.zip dialog opens.
3. Open or save the file as necessary.

   The default location for a server certificate to be exported is:

- C:/ <user>/Downloads/<HTTPSServerCertificate.zip>
- or <RADIUSServerCertificate.zip>.

  The zip file has the server certificate (.crt file) and the private key (.pvk) file.

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:

- Certificate Trust List Main Page on page 660
- Adding a Certificate on page 660
- Viewing a Certificate Detail on page 661
- Deleting a Certificate on page 661

NOTE

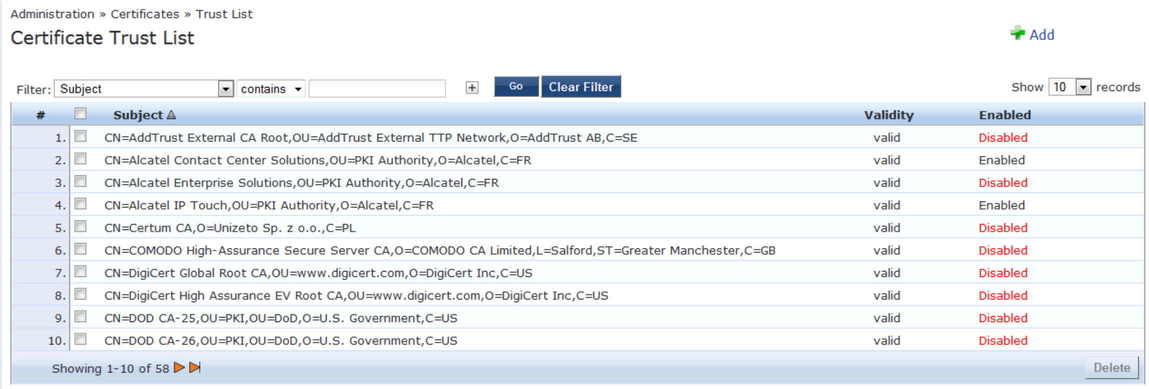
You cannot import the certificates that are created with the **MD5** digest algorithm to the **Certificate Trust List** in the **FIPS** mode.

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 658: *Certificate Trust List Main Page*



Administration » Certificates » Trust List

Certificate Trust List

#	□	Subject	Validity	Enabled
1.	□	CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddTrust AB,C=SE	valid	Disabled
2.	□	CN=Alcatel Contact Center Solutions,OU=PKI Authority,O=Alcatel,C=FR	valid	Enabled
3.	□	CN=Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR	valid	Disabled
4.	□	CN=Alcatel IP Touch,OU=PKI Authority,O=Alcatel,C=FR	valid	Enabled
5.	□	CN=Certum CA,O=Unizeto Sp. z o.o.,C=PL	valid	Disabled
6.	□	CN=COMODO High-Assurance Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	valid	Disabled
7.	□	CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US	valid	Disabled
8.	□	CN=DigiCert High Assurance EV Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US	valid	Disabled
9.	□	CN=DOD CA-25,OU=PKI,OU=DoD,O=U.S. Government,C=US	valid	Disabled
10.	□	CN=DOD CA-26,OU=PKI,OU=DoD,O=U.S. Government,C=US	valid	Disabled

Showing 1-10 of 58

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 353: *Certificate Trust List Parameters*

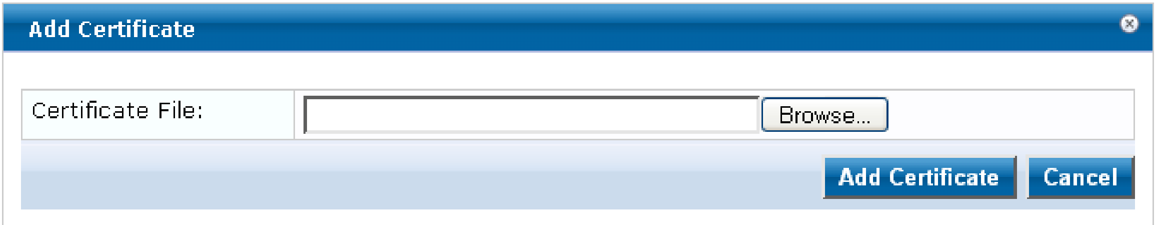
Parameter	Description
Subject	Displays the Distinguished Name (DN) of the subject field in the certificate.
Validity	Indicates whether the CA certificate is valid or expired.
Enabled	Indicates whether the CA certificate is enabled or disabled.

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 659: *Add Certificate Pop-up*



The following table describes the **Add Certificate** parameters:

Table 354: *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

This section provides the following information:

- About Certificate Revocation Lists
- Updating All Certificate Revocation Lists
- Adding a Certificate Revocation List
- Deleting a Certificate Revocation List

About Certificate Revocation Lists

A certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.

Certificate revocation lists are a type of blacklist and they are used by various endpoints, including Web browsers, to verify whether a certificate is valid and trustworthy.

Digital certificates are used in the encryption process to secure communications, most often by using the Transport Layer Security (TLS) or the Secure Sockets Layer (SSL) protocols. The certificate, which is signed by the issuing certificate authority, also provides proof of the identity of the certificate owner.

Updating All Certificate Revocation Lists

When certificates are revoked by an external certificate authority, there is a need to be able to verify that Policy Manager's authentication of that certificate fails, which requires an up-to-date certificate revocation list on the ClearPass server if the Online Certificate Status Protocol (OCSP) is not in use.

You can poll all configured CRLs for an immediate update regardless of the schedule for each CRL.

To immediately update all certificate revocation lists:

1. Navigate to **Administration > Certificates > Revocation Lists**.

   The **Certificate Revocation Lists** page opens.

2. Click the **Check Now** button.

   All the updated CRLs are displayed immediately. The information in the **Last Checked Time** column is also updated for each newly-checked CRL.

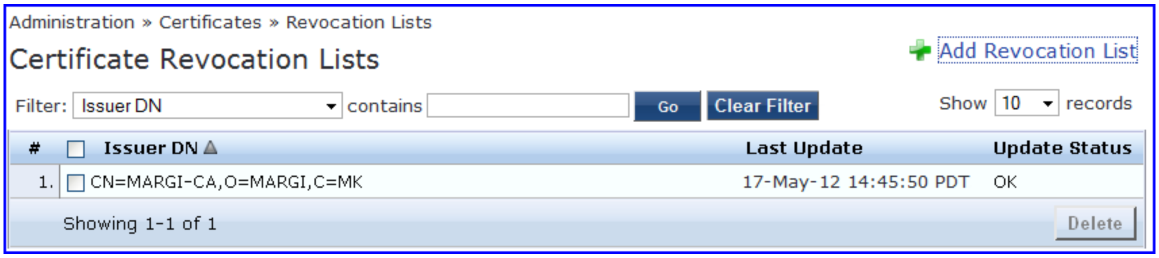
Adding a Certificate Revocation List

To add a certificate revocation list:

1. Navigate to **Administration > Certificates > Revocation Lists**.

   The **Certificate Revocation Lists** page opens:

Figure 660: *Certificate Revocation Lists Page*



Administration » Certificates » Revocation Lists

Certificate Revocation Lists

Filter: Issuer DN contains

Show 10 records

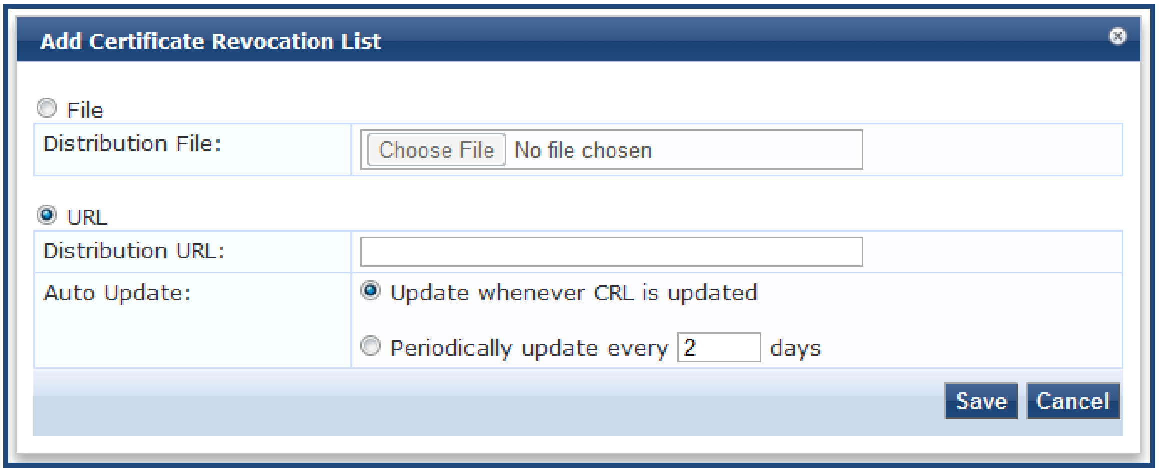
#	□ Issuer DN	Last Update	Update Status
1.	□ CN=MARGI-CA,O=MARGI,C=MK	17-May-12 14:45:50 PDT	OK

Showing 1-1 of 1

2. Click the **Add** link on the top-right section of the page.

   The **Add Certificate Revocation List** dialog opens:

Figure 661: *Add Certificate Revocation List Dialog*



Add Certificate Revocation List

○ File

Distribution File:	Choose File No file chosen

● URL

Distribution URL:	
Auto Update:	● Update whenever CRL is updated ○ Periodically update every 2 days

3. Configure the **Add Certificate Revocation List** parameters as described in Table 355, then click **Save**.

Table 355: *Add Certificate Revocation List Parameters*

Parameter	Action/Description
File	Enable the **File** button to use a distribution file as the Certificate Revocation List distribution point. **File** is enabled by default.
Distribution File	To select the distribution file to fetch the certificate revocation list, click **Browse** and select the CRL distribution file.
URL	Enable the **URL** button to use a URL as the CRL distribution point. Selecting **URL** enables the **Distribution URL** option.
Distribution URL	Specify the distribution URL to fetch the certificate revocation list.
Auto Update	- To update the CRL at intervals specified in the list, select **Update whenever CRL is updated**. - To check periodically and at the specified frequency (in hours), select **Periodically update every ______ hour(s)**.
Bypass Proxy	To bypass the proxy server, click the **Enable to bypass proxy server** option.

Deleting a Certificate Revocation List

To delete a certificate revocation list:

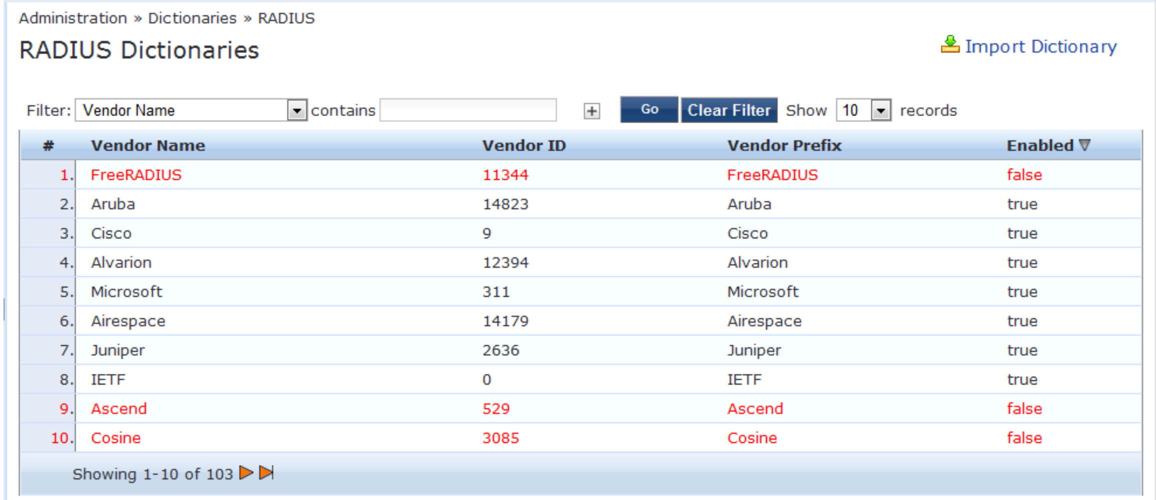
1. Navigate to **Administration > Certificates > Revocation Lists**.
2. Select the check box to the left of the certificate revocation list.
3. Click **Delete.**

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 662: *RADIUS Dictionaries*



Administration » Dictionaries » RADIUS

RADIUS Dictionaries

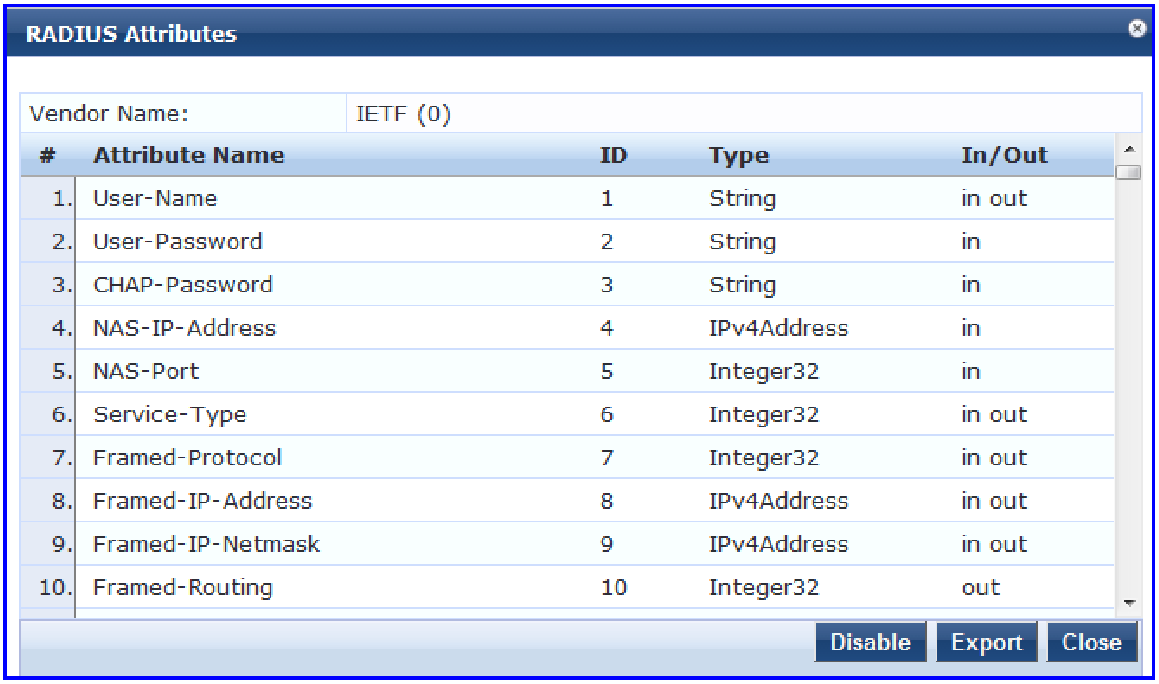
Filter: Vendor Name contains Go Clear Filter Show 10 records

#	Vendor Name	Vendor ID	Vendor Prefix	Enabled ▽
1.	FreeRADIUS	11344	FreeRADIUS	false
2.	Aruba	14823	Aruba	true
3.	Cisco	9	Cisco	true
4.	Alvarion	12394	Alvarion	true
5.	Microsoft	311	Microsoft	true
6.	Airespace	14179	Airespace	true
7.	Juniper	2636	Juniper	true
8.	IETF	0	IETF	true
9.	Ascend	529	Ascend	false
10.	Cosine	3085	Cosine	false

Showing 1-10 of 103

Click on a row view the dictionary attributes, to enable or disable the dictionary, and to export the dictionary. For example, click on vendor IETF to see all IETF attributes and their data type. The following figure displays the RADIUS IETF dictionary attributes pop-up:

Figure 663: *RADIUS Attributes Pop-up*



RADIUS Attributes

Vendor Name: IETF (0)

#	Attribute Name	ID	Type	In/Out
1.	User-Name	1	String	in out
2.	User-Password	2	String	in
3.	CHAP-Password	3	String	in
4.	NAS-IP-Address	4	IPv4Address	in
5.	NAS-Port	5	Integer32	in
6.	Service-Type	6	Integer32	in out
7.	Framed-Protocol	7	Integer32	in out
8.	Framed-IP-Address	8	IPv4Address	in out
9.	Framed-IP-Netmask	9	IPv4Address	in out
10.	Framed-Routing	10	Integer32	out

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

Table 356: *RADIUS Dictionary Attributes Parameters*

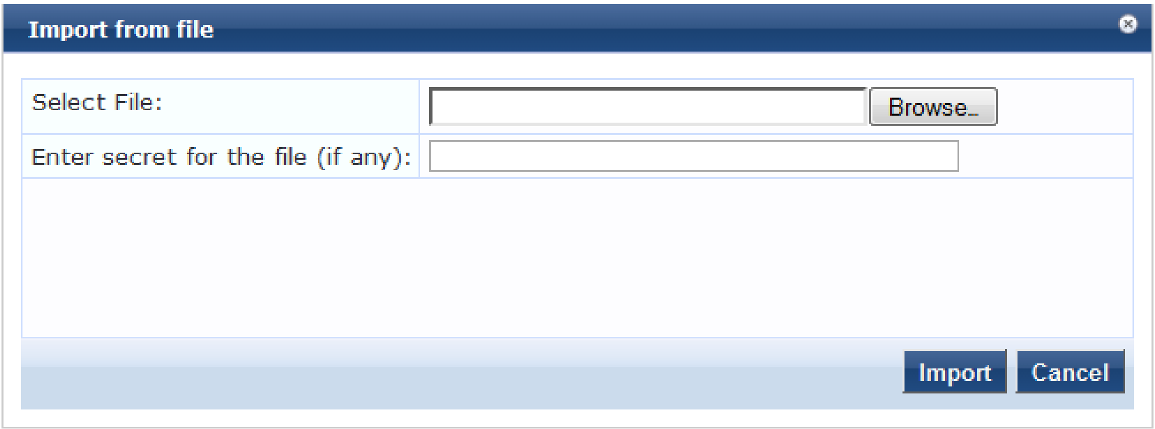
Parameter	Description
Export	Click to save the dictionary file in XML format. You can make modifications to the dictionary and import the file back into Policy Manager.
Enable/Disable	Enable or disable this dictionary. Enabling a dictionary makes it appear in the Policy Manager rules editors (Service 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 664: *Import RADIUS Dictionary Pop-up*


Import from file

Select File:

Enter secret for the file (if any):

The following table describes the **Import from file** parameters:

Table 357: *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.

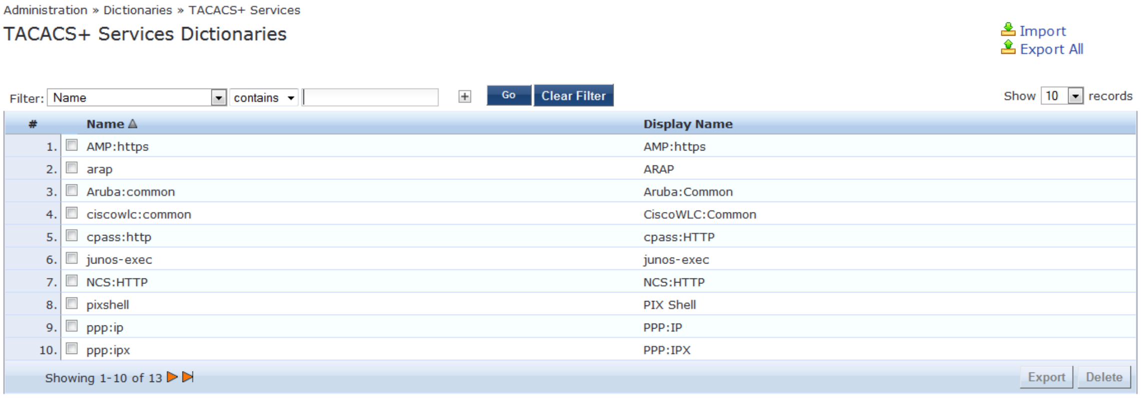
TACACS+ Services Dictionary

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 665: *TACACS+ Services Dictionaries Page*



Administration » Dictionaries » TACACS+ Services

TACACS+ Services Dictionaries

Filter: Name contains

Show 10 records

#	Name	Display Name
1.	AMP:https	AMP:https
2.	arap	ARAP
3.	Aruba:common	Aruba:Common
4.	ciscowlc:common	CiscoWLC:Common
5.	cpass:http	cpass:HTTP
6.	junos-exec	junos-exec
7.	NCS:HTTP	NCS:HTTP
8.	pixshell	PIX Shell
9.	ppp:ip	PPP:IP
10.	ppp:ipx	PPP:IPX

Showing 1-10 of 13

The following table describes the **TACACS+ Services Dictionaries** parameters:

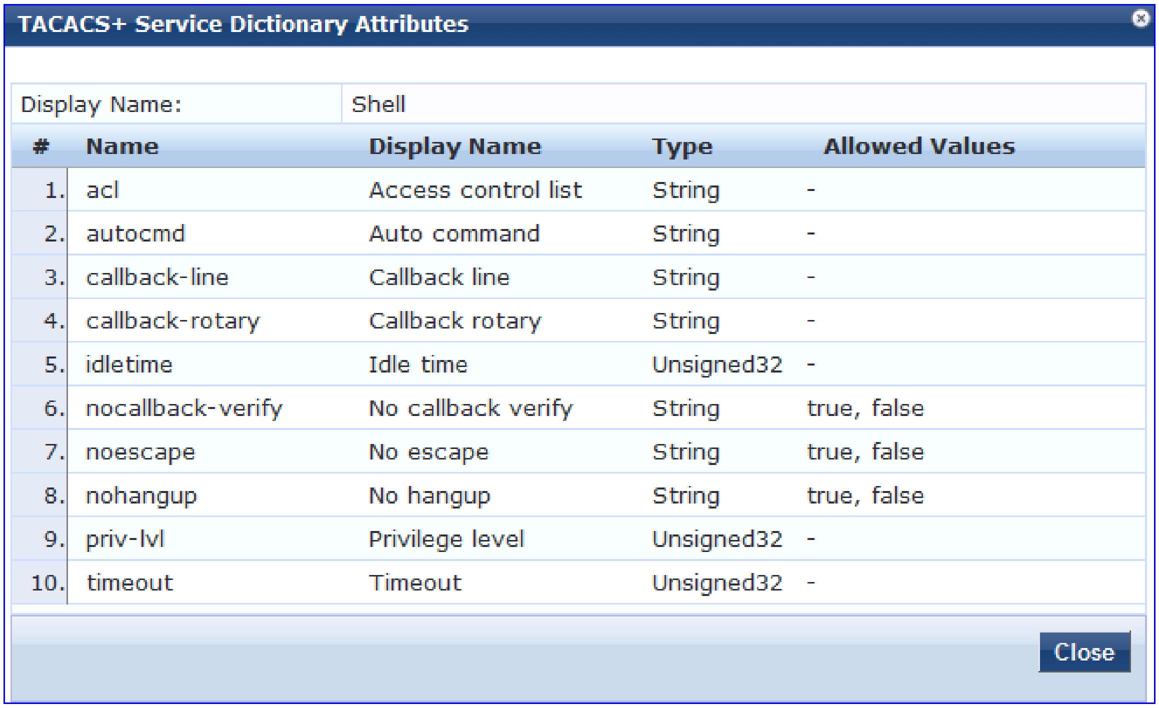
Table 358: *TACACS+ Services Dictionaries Parameters*

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 666: *TACACS+ Service Dictionary Attributes Pop-up*



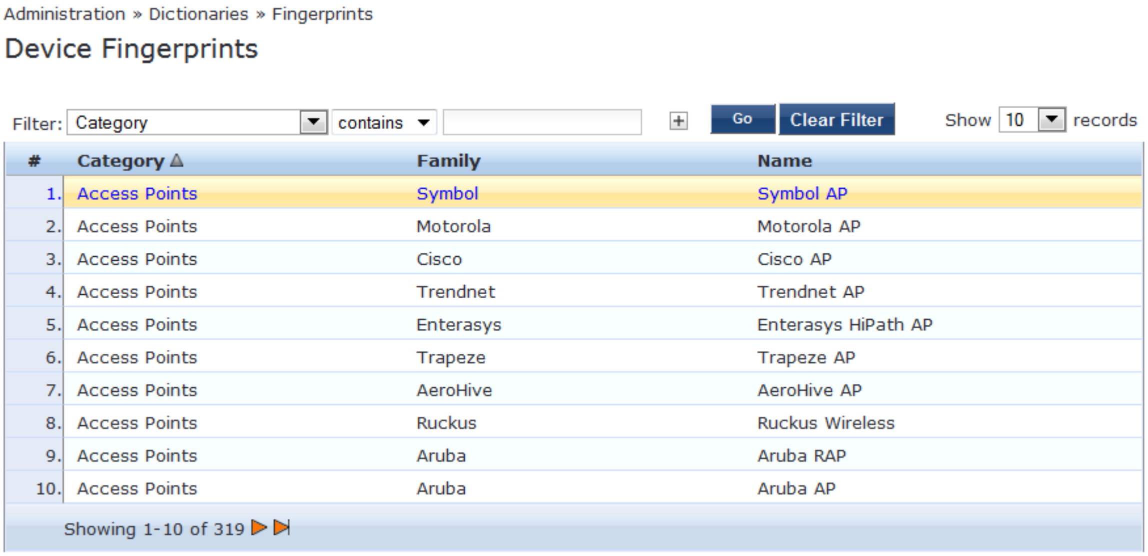
TACACS+ Service Dictionary Attributes

Display Name:	Shell			
#	**Name**	**Display Name**	**Type**	**Allowed Values**
1.	acl	Access control list	String	-
2.	autocmd	Auto command	String	-
3.	callback-line	Callback line	String	-
4.	callback-rotary	Callback rotary	String	-
5.	idletime	Idle time	Unsigned32	-
6.	nocallback-verify	No callback verify	String	true, false
7.	noescape	No escape	String	true, false
8.	nohangup	No hangup	String	true, false
9.	priv-lvl	Privilege level	Unsigned32	-
10.	timeout	Timeout	Unsigned32	-

Fingerprints Dictionary

The **Device Fingerprints** page shows a listing of all the device fingerprints recognized by the Profile module. These fingerprints are updated from the Aruba ClearPass Update Portal (see Updating Policy Manager Software on page 673 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 667: *Device Fingerprints Page*



Administration » Dictionaries » Fingerprints

Device Fingerprints

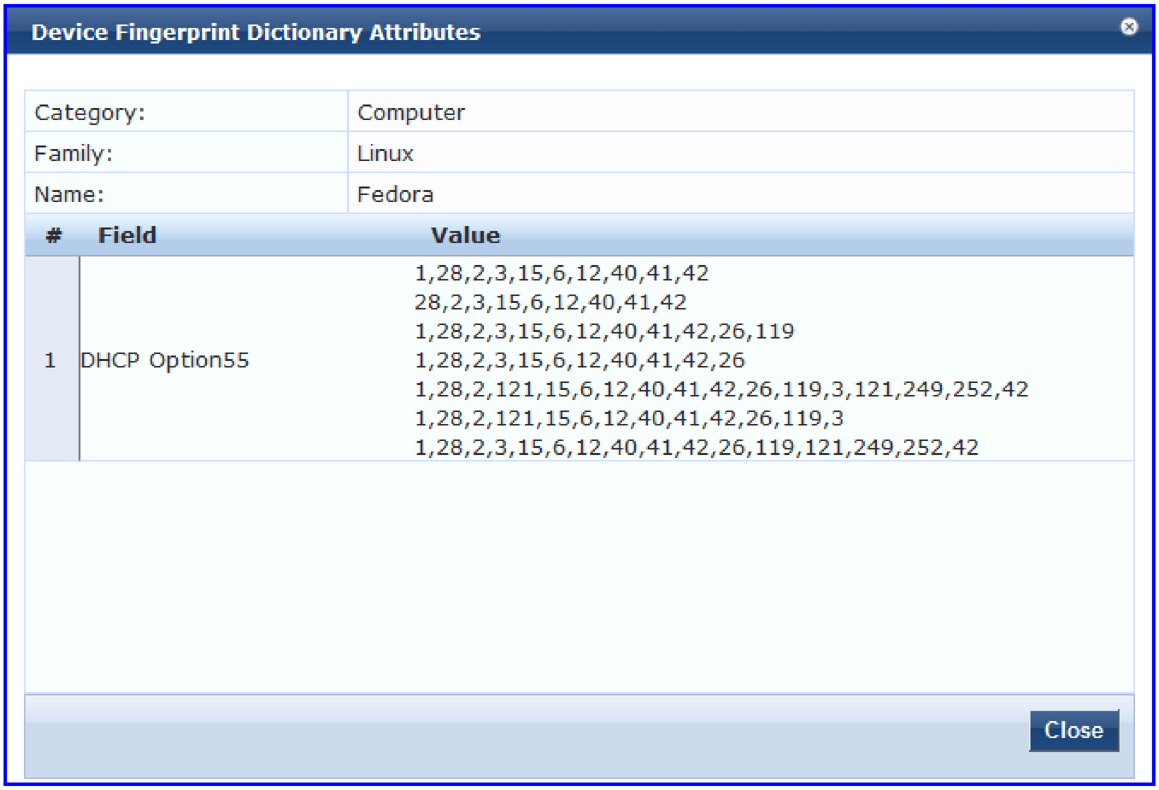
Filter: Category contains

#	Category	Family	Name
1.	Access Points	Symbol	Symbol AP
2.	Access Points	Motorola	Motorola AP
3.	Access Points	Cisco	Cisco AP
4.	Access Points	Trendnet	Trendnet AP
5.	Access Points	Enterasys	Enterasys HiPath AP
6.	Access Points	Trapeze	Trapeze AP
7.	Access Points	AeroHive	AeroHive AP
8.	Access Points	Ruckus	Ruckus Wireless
9.	Access Points	Aruba	Aruba RAP
10.	Access Points	Aruba	Aruba AP

Showing 1-10 of 319

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 668: *Device Fingerprint Dictionary Attributes Pop-up*



Device Fingerprint Dictionary Attributes

Category:	Computer
Family:	Linux
Name:	Fedora

#	Field	Value
1	DHCP Option55	1,28,2,3,15,6,12,40,41,42 28,2,3,15,6,12,40,41,42 1,28,2,3,15,6,12,40,41,42,26,119 1,28,2,3,15,6,12,40,41,42,26 1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42 1,28,2,121,15,6,12,40,41,42,26,119,3 1,28,2,3,15,6,12,40,41,42,26,119,121,249,252,42

Dictionary Attributes

This section contains the following information:

- Introduction
- Adding a Dictionary Attribute
- Modifying Dictionary Attributes
- Importing Dictionary Attributes
- Exporting All Dictionary Attributes
- Exporting Selected Dictionary Attributes

Introduction

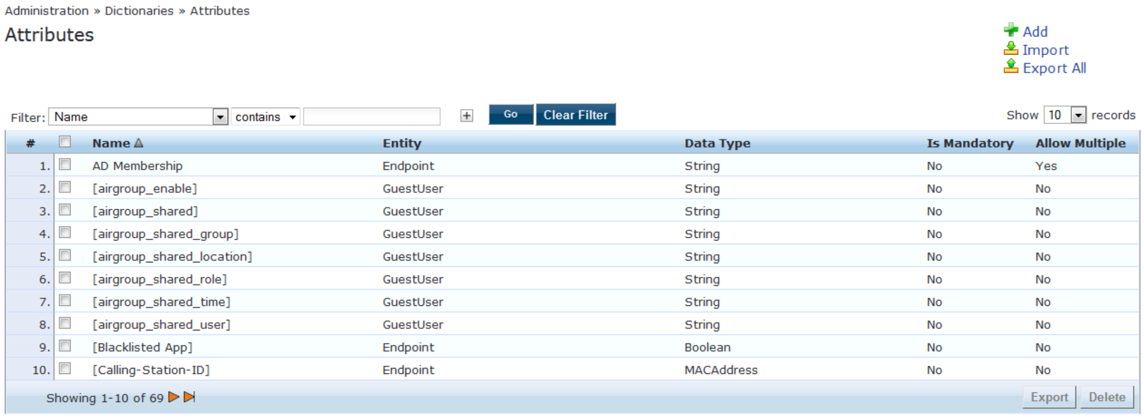
The **Attributes** dictionary page allows you to specify unique sets of criteria for local users, guest users, endpoints, and devices. This information can then be used with role-based device policies for enabling appropriate network access.

To view the contents of the attributes dictionary:

1. Navigate to **Administration** > **Dictionaries** > **Attributes**.

   The dictionary **Attributes** page opens:

Figure 669: *Dictionary Attributes Page*



#	☐	Name	Entity	Data Type	Is Mandatory	Allow Multiple
1.	☐	AD Membership	Endpoint	String	No	Yes
2.	☐	[airgroup_enable]	GuestUser	String	No	No
3.	☐	[airgroup_shared]	GuestUser	String	No	No
4.	☐	[airgroup_shared_group]	GuestUser	String	No	No
5.	☐	[airgroup_shared_location]	GuestUser	String	No	No
6.	☐	[airgroup_shared_role]	GuestUser	String	No	No
7.	☐	[airgroup_shared_time]	GuestUser	String	No	No
8.	☐	[airgroup_shared_user]	GuestUser	String	No	No
9.	☐	[Blacklisted App]	Endpoint	Boolean	No	No
10.	☐	[Calling-Station-ID]	Endpoint	MACAddress	No	No

Table 359 describes the dictionary **Attributes** parameters:

Table 359: *Dictionary Attributes Parameters*

Parameter	Action/Description
Filter	Use the Filter drop-down list to create a search based on the **Name**, **Entity**, **Data Type**, **Is Mandatory**, or **Allow Multiple** settings.
Name	The name of the attribute.
Entity	Indicates whether the attribute applies to a Local User, Guest User, Device, or Endpoint.
Data Type	Indicates whether the data type is String, Integer, Boolean, List, Text, Date, MAC address, or IPv4 address.
Is Mandatory	Indicates whether the attribute is required for a specific entity.
Allow Multiple	Indicates whether multiple attributes are allowed for an entity.

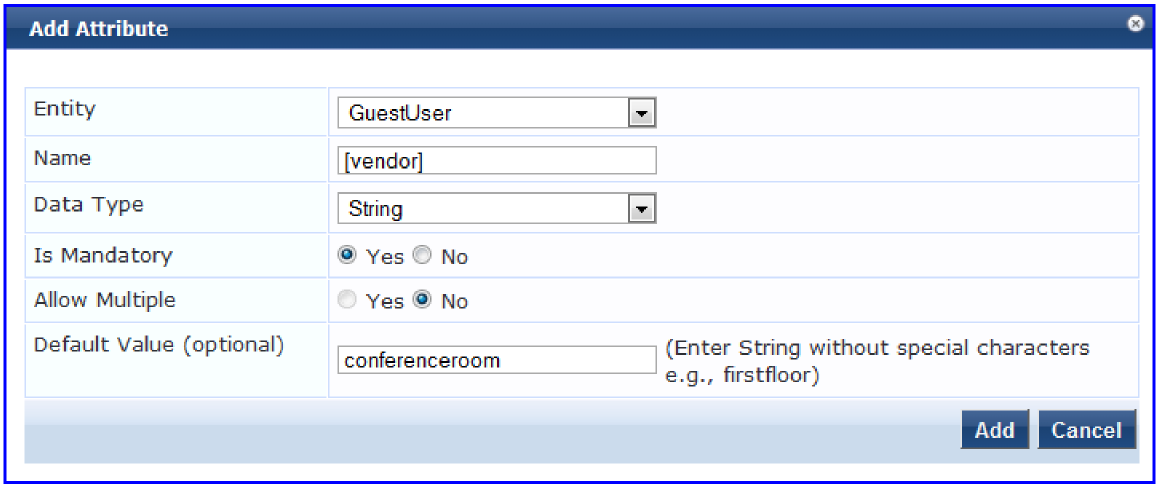
Adding a Dictionary Attribute

To add a dictionary attribute:

1. From the Attributes page, click **Add**.

   The **Add Attribute** dialog appears.

Figure 670: *Add Attribute Dialog*



Entity	GuestUser
Name	[vendor]
Data Type	String
Is Mandatory	● Yes ○ No
Allow Multiple	○ Yes ● No
Default Value (optional)	conferenceroom (Enter String without special characters e.g., firstfloor)

2. Specify the **Add Attribute** parameters as described in the following table, then click **Add**.

Table 360: *Attribute Setting Parameters*

Parameter	Action/Description
Entity	Specify whether the attribute applies to a Device, Endpoint, Guest User, Local User, or Onboard.
Name	Enter a unique ID for this dictionary attribute.
Data Type	From the drop-down, specify the data type.
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	Optionally, specify whether the default value is true or false.

Modifying Dictionary Attributes

To modify dictionary attributes in a service dictionary:

1. From the **Attributes** page, select the dictionary attribute.

   The **Edit Attribute** page opens.

2. Make any necessary changes, then click **Save**.

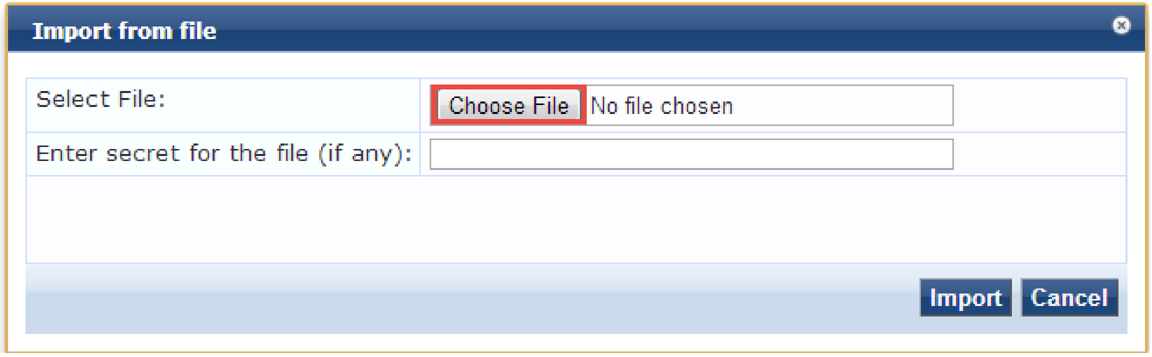
Importing Dictionary Attributes

To import attributes:

1. From the menu at the top right section of the page, click **Import**.

   The **Import from File** dialog opens.

Figure 671: *Importing Dictionary Attributes*



2. Enter the **Import from File** parameters as described in Table 361.

Table 361: *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.

3. When finished, click **Import**.

NOTE

The imported file is in XML format. To view a sample of this XML format, export a dictionary file and open it in an XML viewer.

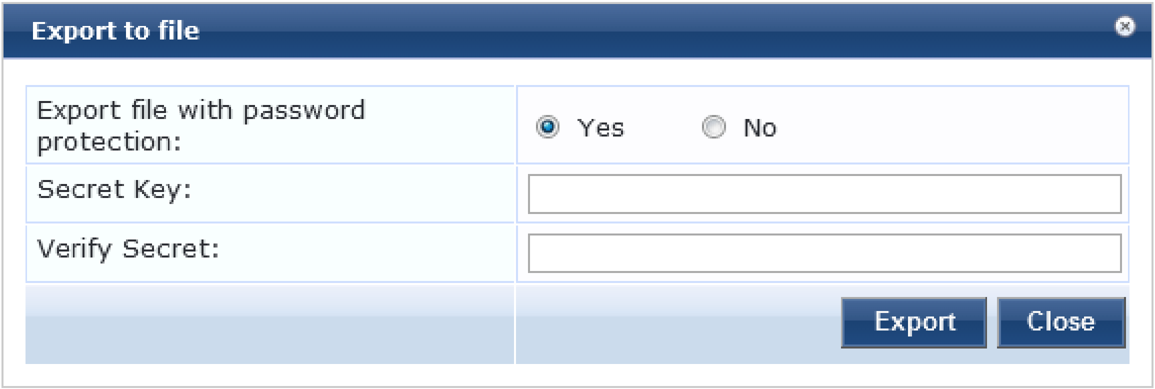
Exporting All Dictionary Attributes

To export all the dictionary attributes at once:

1. From the **Attributes** page, select **Export All**.

   The **Export to File** dialog opens.

Figure 672: *Exporting Dictionary Attributes*



Export file with password protection: ● Yes ○ No

2. Specify the **Export to File** parameters as described in Table 362.

Table 362: *Export to File Parameters*

Parameter	Action/Description
Export file with password protection	The **Yes** option is enabled by default. If you wish to disable password protection when exporting a file, select **No**.
Secret Key	If the file that you want to import is password protected, enter the secret here. Then verify the secret key.

3. When finished, click **Export**.

   The **TagDictionary.xml** file is created.

4. Download the file.

Exporting Selected Dictionary Attributes

To export selected dictionary attributes:

1. On the **Attributes** dictionary page, select one or more attribute entries.

   The **Export** and **Delete** buttons on the lower right are now enabled.

2. Click **Export**.

   The **Export to File** dialog opens.

3. Specify the **Export to File** parameters as described in Table 362.
4. When finished, click **Export**.

   The **TagDictionary.xml** file is created.

5. Download the file.

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.

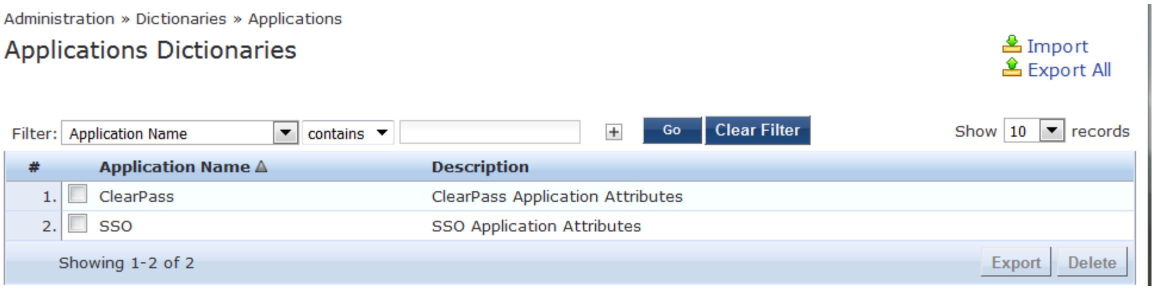
Viewing an Application Dictionary

To view the contents of the application dictionary:

1. Navigate to **Administration > Dictionaries > Applications**.

   The **Applications Dictionaries** page appears.

Figure 673: *Applications Dictionaries Page*



Administration » Dictionaries » Applications

Applications Dictionaries

Filter: Application Name contains

Show 10 records

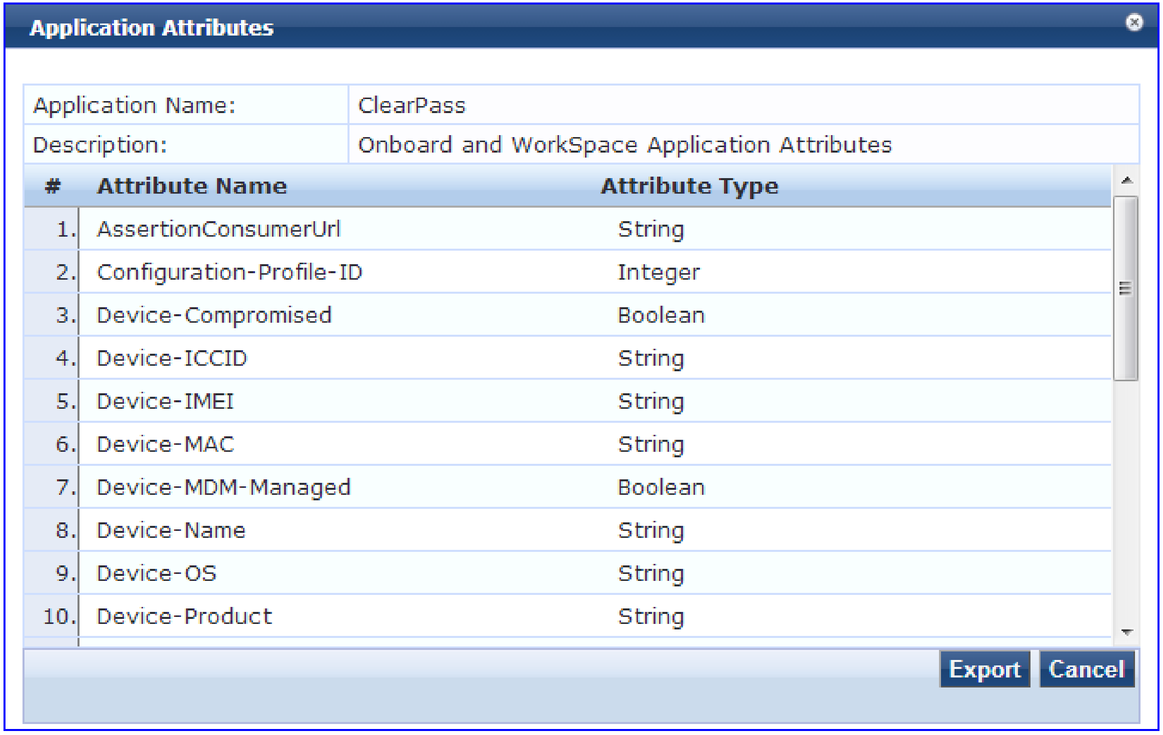
#	Application Name	Description
1.	ClearPass	ClearPass Application Attributes
2.	SSO	SSO Application Attributes

Showing 1-2 of 2

2. To see the application attributes, click the name of an application.

   The **Application Attributes** dialog box appears.

Figure 674: *Application Attributes Dialog*



Application Name:	ClearPass
Description:	Onboard and WorkSpace Application Attributes

#	Attribute Name	Attribute Type
1.	AssertionConsumerUrl	String
2.	Configuration-Profile-ID	Integer
3.	Device-Compromised	Boolean
4.	Device-ICCID	String
5.	Device-IMEI	String
6.	Device-MAC	String
7.	Device-MDM-Managed	Boolean
8.	Device-Name	String
9.	Device-OS	String
10.	Device-Product	String

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

Updating Policy Manager Software

This section provides the following information:

- Introduction
- Software Updates Page on page 674
- Install Update Dialog Box on page 676
- Reinstalling a Patch on page 678
- Uninstalling a Skin on page 678
- Updating the Software on page 1
- OnGuard Settings on page 679
- OnGuard Global Agent Settings on page 682

Introduction

This section describes the ClearPass Policy Manager server software update process.

Use the **Software Updates** page to register for and receive live updates for:

- Posture updates, including antivirus, antispyware, and Windows updates
- Profile data updates, including Fingerprints
- Software upgrades for the ClearPass family of products
  - Patch binaries, including Onboard, Guest plug-ins, and skins

You can also:

- Reinstall a patch in the event the previous installation attempt fails.
- Uninstall a skin.

The 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, 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.

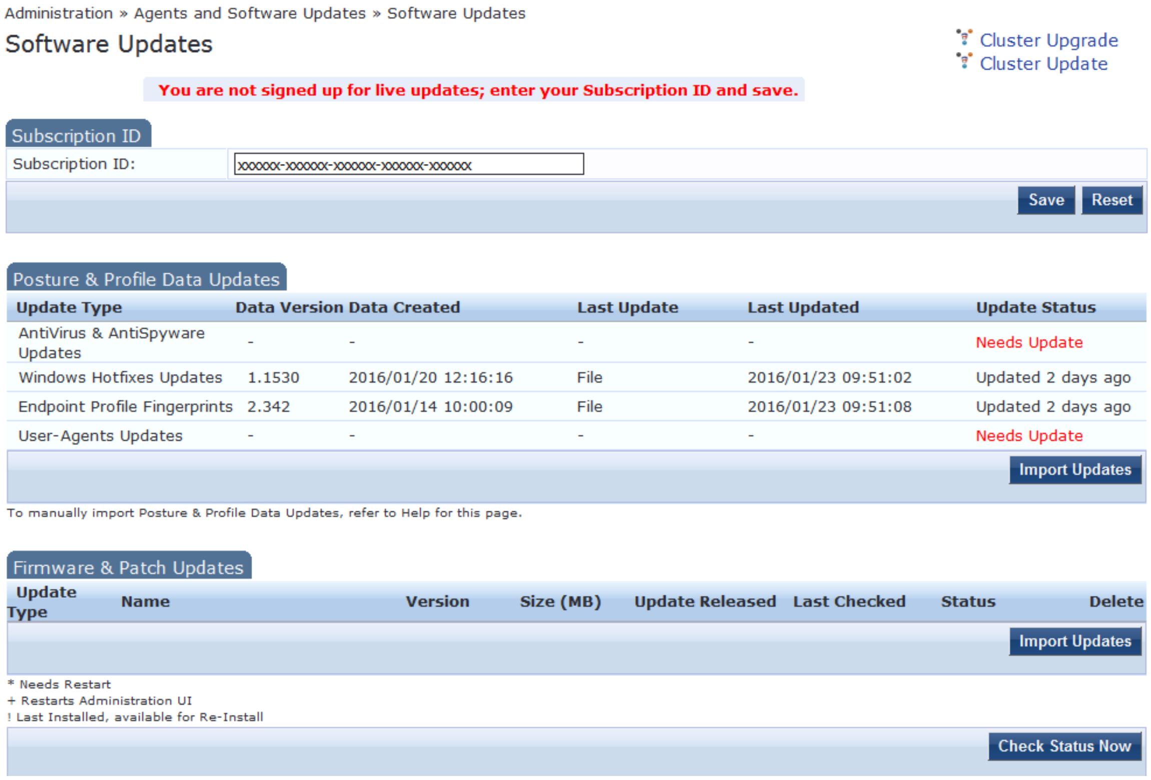
Software Updates Page

To update the software on the current ClearPass server:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.

   Figure 675 displays the **Software Updates** page:

Figure 675: *Software Updates Page*



Administration » Agents and Software Updates » Software Updates

Software Updates

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID

Subscription ID:	xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx

Posture & Profile Data Updates

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
AntiVirus & AntiSpyware Updates	-	-	-	-	Needs Update
Windows Hotfixes Updates	1.1530	2016/01/20 12:16:16	File	2016/01/23 09:51:02	Updated 2 days ago
Endpoint Profile Fingerprints	2.342	2016/01/14 10:00:09	File	2016/01/23 09:51:08	Updated 2 days ago
User-Agents Updates	-	-	-	-	Needs Update

To manually import Posture & Profile Data Updates, refer to Help for this page.

Firmware & Patch Updates

Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

Table 363 describes the **Software Updates** parameters:

Table 363: *Software Updates Parameters*

Parameter	Action/Description
Subscription ID	
Subscription ID	1. Enter the **Subscription ID** provided to you. This text box is enabled only on a Publisher node. You can opt out of automatic downloads at any time by saving an empty Subscription ID.
Save	2. To save the **Subscription ID**, click **Save**. This button is enabled only on a Publisher node.
Reset	Performs an "undo" of any unsaved changes you have made in the **Subscription ID** field. **NOTE:** Reset does not clear the text box.
Posture & Profile Data Updates	
Import Updates	If this 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. 3. You can download the data from the Webservice server by accessing the following URL: *https://clearpass.arubanetworks.com/cppm/appupdate/cppm_apps_updates.zip* 4. When prompted for authentication credentials, enter the provided Subscription ID for both the username and the password. **NOTE:** In a ClearPass cluster, the **Import Updates** option is available on the Publisher node only.
Firmware & Patch Updates	
Import Updates	5. 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 the **Install** button. When logged in as *appadmin*, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands: ■ **system update** (for patches) ■ **system upgrade** (for upgrades) If a patch requires a prerequisite patch, that patch's **Install** button will not be enabled until the prerequisite patch is installed.
Install	The **Install** button appears after the update has been downloaded. 6. Click **Install**. When you click **Install**, the installation of the update starts and the **Install Update** dialog box appears, showing the log messages that are generated.
Re-Install	7. 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.

Table 363: *Software Updates Parameters (Continued)*

Parameter	Action/Description
Uninstall	8. To uninstall a skin, click **Uninstall** (for details, see Uninstalling a Skin). **NOTE:** You cannot uninstall cumulative or point patch updates.
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.
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

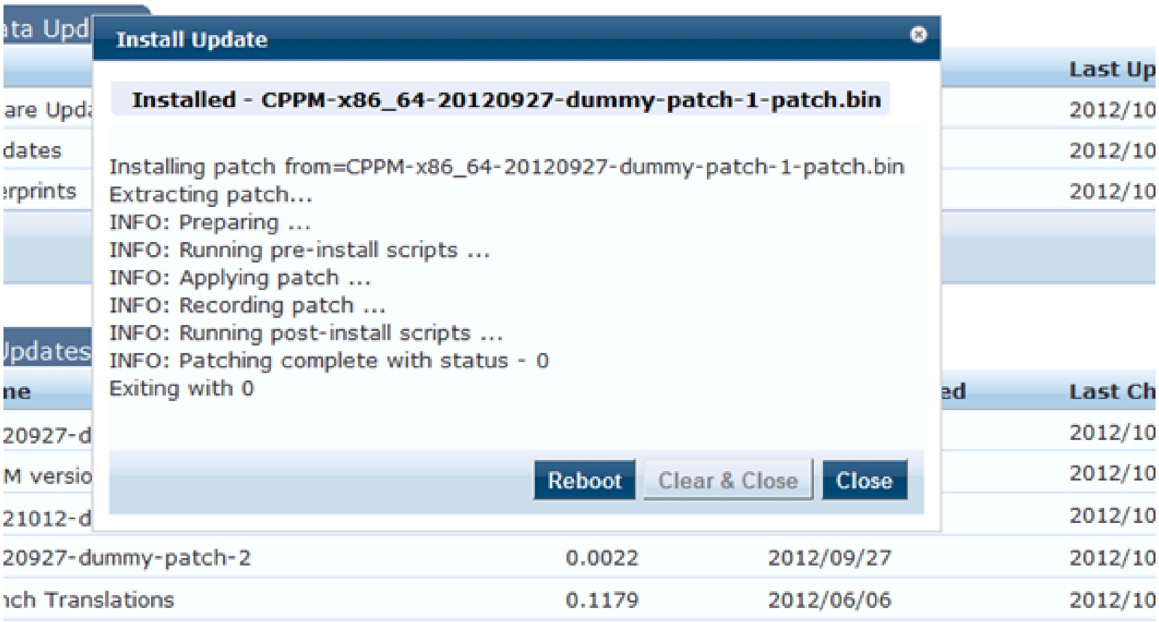
The **Install Update** dialog box shows the log messages generated during the installation of an update. This dialog appears when you click the **Install** button.

If the dialog is closed, you can bring it up again by any one of the three following methods:

- Clicking the **Install in progress...** link while the installation is in progress.
- Clicking the **Installed**, **Install Error** link.
- Clicking the **Needs Restart** link when the installation is completed.

The following figure displays the **Install Update** dialog box:

Figure 676: *Install Update Dialog Box*



Installed - CPPM-x86_64-20120927-dummy-patch-1-patch.bin

```
Installing patch from=CPPM-x86_64-20120927-dummy-patch-1-patch.bin
Extracting patch...
INFO: Preparing ...
INFO: Running pre-install scripts ...
INFO: Applying patch ...
INFO: Recording patch ...
INFO: Running post-install scripts ...
INFO: Patching complete with status - 0
Exiting with 0
```

The following table describes the **Install Update** parameters:

Table 364: *Install Update Parameters*

Parameter	Action/Description
Reboot	1. To initiate a reboot of the server, click **Reboot**. The **Reboot** button appears only for updates that require a reboot to complete the installation.
Clear & Close	2. To delete the log messages and close the dialog, click **Clear & Close**. **Clear & Close** also removes the corresponding row from the Firmware & Patch Updates table. To delete the log messages from a failed installation, click **Clear & Close**. 3. After the log messages are cleared, attempt the installation again.
Close	4. To close the dialog box, click **Close**.

Webservice Operations

System Events (as seen on the **Monitoring > Event Viewer** page) show records for events, such as communication failures with Webservice, successful or failed download of updates, and successful or failed installation of updates.

The ClearPass Policy Manager server contacts the Webservice server every hour in the background to download any newly available Posture & Profile Data updates. 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 user interface 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 node 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, click the **Installed**, **Install Error**, or **Needs Restart** link.
3. To reinstall the patch or software update, click **Re-Install**.

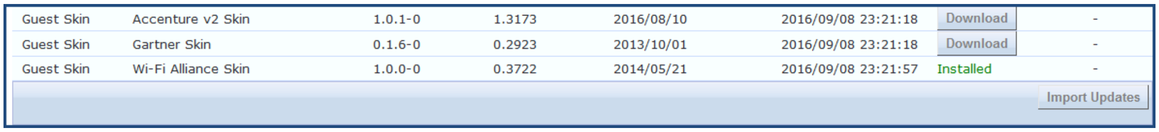
   The **Install Update** screen closes and the reinstallation process begins. A window displays, showing the installation progress via log messages.

Uninstalling a Skin

To uninstall a skin:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware & Patch Updates** section,select the installed skin that you want to uninstall.

Figure 677: *Viewing the Installed Link for a Skin*

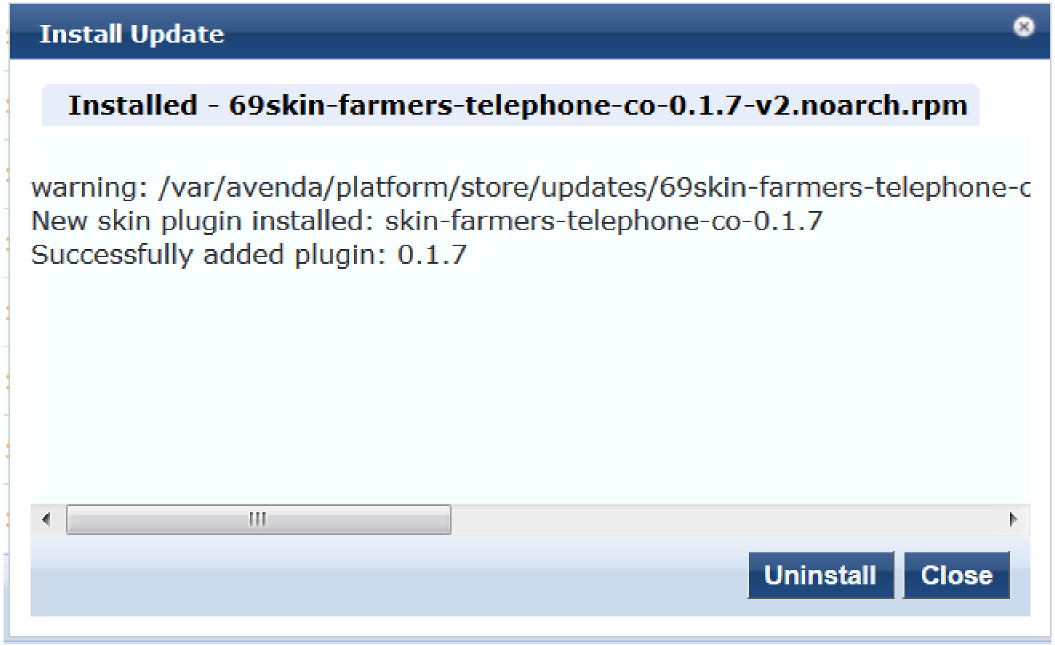


Guest Skin	Accenture v2 Skin	1.0.1-0	1.3173	2016/08/10	2016/09/08 23:21:18	Download	-
Guest Skin	Gartner Skin	0.1.6-0	0.2923	2013/10/01	2016/09/08 23:21:18	Download	-
Guest Skin	Wi-Fi Alliance Skin	1.0.0-0	0.3722	2014/05/21	2016/09/08 23:21:57	Installed	-

3. Click the **Installed** link.

   The **Install Update** dialog opens.

Figure 678: *Install Update Dialog*



Installed - 69skin-farmers-telephone-co-0.1.7-v2.noarch.rpm

```
warning: /var/avenda/platform/store/updates/69skin-farmers-telephone-c
New skin plugin installed: skin-farmers-telephone-co-0.1.7
Successfully added plugin: 0.1.7
```

4. To uninstall the skin, click **Uninstall**.

   The **Install Update** screen closes and the software is uninstalled.

OnGuard Settings

This section provides the following information:

- Introduction
- Accessing OnGuard Agent Support Charts
- Configuring OnGuard Settings

Introduction

Use the **OnGuard Settings** page to configure the agent deployment packages.

When you save the OnGuard configuration, ClearPass creates agent deployment packages for the Windows and Macintosh OS X operating systems and provides the packages at a fixed URL on the ClearPass Policy Manager hardware or virtual appliance.

You can then publish this URL to the user community. You can also download the agent deployment packages to another location.

Accessing OnGuard Agent Support Charts

For information about the OnGuard Agent Support Charts that are included with ClearPass Policy Manager, navigate to **Administration** > **Support** > **Documentation** > **OnGuard Agent Support Charts**.

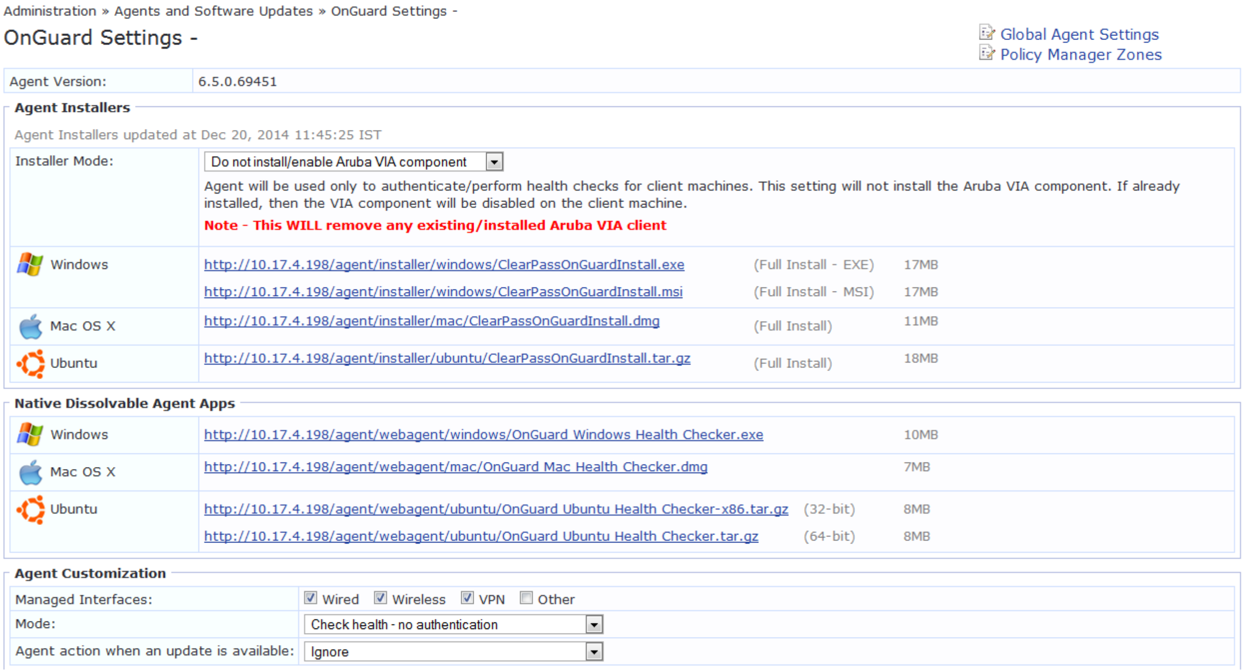
Configuring OnGuard Settings

To configure the OnGuard settings:

1. Navigate to **Administration** > **Agents and Software Updates** > **OnGuard Settings**.

   The OnGuard Settings main page appears:

Figure 679: *OnGuard Settings Main Page*



Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings -

Global Agent Settings
Policy Manager Zones

Agent Version:	6.5.0.69451

Agent Installers

Agent Installers updated at Dec 20, 2014 11:45:25 IST

Installer Mode:	Do not install/enable Aruba VIA component Agent will be used only to authenticate/perform health checks for client machines. This setting will not install the Aruba VIA component. If already installed, then the VIA component will be disabled on the client machine. **Note - This WILL remove any existing/installed Aruba VIA client**		
Windows	http://10.17.4.198/agent/installer/windows/ClearPassOnGuardInstall.exe	(Full Install - EXE)	17MB
	http://10.17.4.198/agent/installer/windows/ClearPassOnGuardInstall.msi	(Full Install - MSI)	17MB
Mac OS X	http://10.17.4.198/agent/installer/mac/ClearPassOnGuardInstall.dmg	(Full Install)	11MB
Ubuntu	http://10.17.4.198/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz	(Full Install)	18MB

Native Dissolvable Agent Apps

Windows	http://10.17.4.198/agent/webagent/windows/OnGuard Windows Health Checker.exe		10MB
Mac OS X	http://10.17.4.198/agent/webagent/mac/OnGuard Mac Health Checker.dmg		7MB
Ubuntu	http://10.17.4.198/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker-x86.tar.gz	(32-bit)	8MB
	http://10.17.4.198/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker.tar.gz	(64-bit)	8MB

Agent Customization

Managed Interfaces:	☑ Wired ☑ Wireless ☑ VPN □ Other
Mode:	Check health - no authentication
Agent action when an update is available:	Ignore

2. Configure the OnGuard Settings parameters as described in Table 365, then click **Save**.

Table 365: *OnGuard Settings Parameters*

Parameter	Action/Description
Global Agent Settings	1. Configure the global agent settings parameters for OnGuard agents. For more information, see OnGuard Global Agent Settings on page 682.
Policy Manager Zones	2. Configure the network (subnet) for a Policy Manager Zone. For more information on configuring Policy Manager zones, see Managing Policy Manager Zones on page 522.
Agent Version	Indicates the current version of the OnGuard agent.
Agent Installers	
Installer Mode	3. Specify the action to be taken from the following options when the Aruba VIA component is used to provide VPN-based access: ■ **Do not install/enable Aruba VIA component** ■ **Install and enable Aruba VIA component**
Windows	4. Use the download link to download OnGuard Agent for Windows. This binary file is provided in .exe and .msi formats.
Mac OS X	5. Use the download link to download OnGuard Agent for Mac OS X. This binary file is in .DMG format.
Ubuntu	6. Use the download link to download Ubuntu Agent for Linux. This binary file is in .tar.gz format.

Table 365: *OnGuard Settings Parameters (Continued)*

Parameter	Action/Description
Native Dissolvable Agent Apps	
Windows	7. Click the URL to download Native Dissolvable Agent for Windows.
Mac OS X	8. Click the URL to download Native Dissolvable Agent for Mac OS X.
Ubuntu	9. 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	10. Select the type(s) of interfaces that OnGuard will manage on the endpoint. Select from the following options: ▪ **Wired** ▪ **Wireless** ▪ **VPN** ▪ **Other**
Mode	11. 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 and Password fields 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	The label for the **Password** field on the OnGuard agent. This setting is not valid for the **Check health - no authentication** mode.

Table 365: *OnGuard Settings Parameters (Continued)*

Parameter	Action/Description
Agent action when an update is available	Determines what the agent does when an update is available. 12. Select one of the following options: - **Ignore**: ClearPass Policy Manager ignores the available update. - **Notify User**: ClearPass Policy Manager notifies the user that an update is available. - **Download and Install**: ClearPass Policy Manager automatically downloads and installs an update when it is available.
Native Dissolvable Agent Customization	
Managed Interfaces	This feature ensures that, if both wired and wireless interfaces are connected, the OnGuard Agent will send health requests through the correct interface. 13. Select the type(s) of managed interfaces that are supported for the Native Dissolvable Agent. The Native Dissolvable Agent performs health checks for one of the selected interfaces. Select from the following options: - **Wired** - **Wireless** - **VPN** - **Other**

OnGuard Global Agent Settings

This section provides the following information:

- About Global Agent Settings
- Global Settings Parameters for OnGuard Agents
- Global Agent Settings: Run OnGuard As Parameter

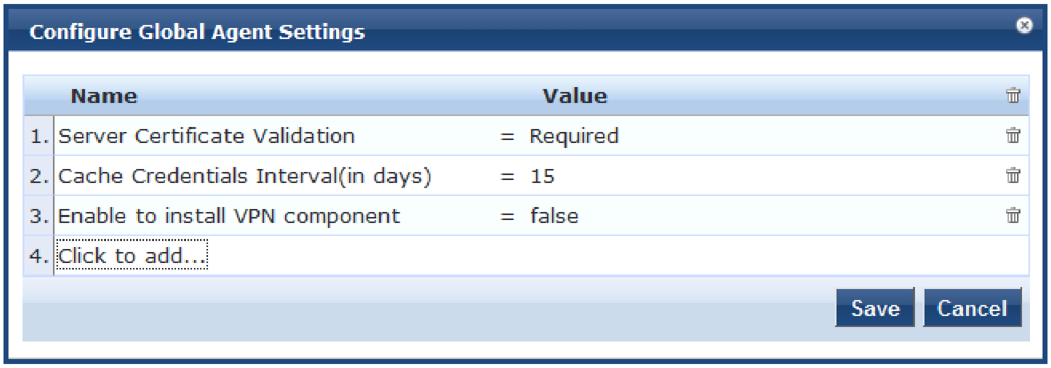
About Global Agent Settings

Use the **Global Agent Settings** page to configure the global parameters for OnGuard agents.

1. Navigate to the **Administration** > **Agents and Software Updates** > **OnGuard Settings** page.
2. Click the **Global Agent Settings** link at the top-right corner.

   The **Configure Global Agent Settings** page opens.

Figure 680: *Configure Global Agent Settings Page*



Configure Global Agent Settings

	Name		Value
1.	Server Certificate Validation	=	Required
2.	Cache Credentials Interval(in days)	=	15
3.	Enable to install VPN component	=	false
4.	Click to add...		

3. To add additional Global Agent Settings parameters, click **Click to add...**.
4. **Name**: Select the desired Global Agent Setting (see Table 366).
5. **Value**: Specify the appropriate value.
6. Repeat these steps as necessary for each additional setting, then click **Save**.

Global Settings Parameters for OnGuard Agents

Table 366 describes the Global Settings parameters for OnGuard agents:

Table 366: *Configure Global Settings Parameters*

Parameter	Action/Description
Name	**Allowed Subnets for Wired access:** Add a comma-separated list of IP addresses or subnet addresses.
	Allowed Subnets for Wireless access: Add a comma-separated list of IP addresses or subnet addresses.
	Cache Credentials Interval (in days): Select the number of days the user credentials should be cached on OnGuard agents.
	Delay to bounce after Logout (in minutes): Specify the number of minutes that should elapse before OnGuard bounces the interface if OnGuard remains disconnected.
	Enable OnGuard requests load-balancing: Enable this option to balance the load of OnGuard authentication requests across ClearPass Policy Manager servers in a cluster.
	Enable access over Remote Desktop Session: Enable this option to allow OnGuard access through a Remote Desktop session.
	Enable to hide Logout button: Enable this option to hide the **Logout** button on OnGuard agent.
	Enable to install VPN component: Enable this option to install the OnGuard VPN component.
	Enable to use Windows Single-Sign On: Enable this option to allow use of a user's Windows credentials for authentication.
	Keep-alive Interval (in seconds): Specify a keep-alive interval for OnGuard agents. The connected OnGuard Agents periodically send heart-beat (Keep-Alive) messages to ClearPass Policy Manager. This interval is defined by the **Keep-alive Interval (in seconds)** parameter. The default value is **60** seconds. ClearPass uses Keep-Alive messages to: ● Update the status of OnGuard Agents regarding OnGuard Activity. ● Issue CoA (Change of Authorization) for a Session Restrictions Enforcement Profile if OnGuard Agent is disconnected: ■ Session-Check > Agent-Connection = Down ■ Post-Auth-Check > Action = Disconnect For related information, see Session Restrictions Enforcement Profile on page 397.
	OnGuard Health Check Interval (in hours): Specify the number of hours that OnGuard will skip health checks for healthy clients.

Table 366: *Configure Global Settings Parameters (Continued)*

Parameter	Action/Description
	NOTE: Note the following information when you set the **OnGuard Health Check Interval** parameter: ■ You can set this parameter if OnGuard mode is set to health only. ■ This parameter is valid only for wired and wireless interface types. ■ This parameter is not applicable for the OnGuard Dissolvable Agent, VPN, and Other interface types. You can also specify the health check interval in the **Agent enforcement** (**Configuration** > **Agent enforcement** > **New attribute**) profile to create different Agent Enforcement Profiles for different users.
	Run OnGuard As: For details, see the next section, Global Agent Settings: Run OnGuard As Parameter.
	Server Certificate Validation: Enables the ClearPass OnGuard Unified Agent to validate the ClearPass Server Certificate when it sends a WebAuth health request to ClearPass.
	Support Team Email Address: Enter an email address that automatically populates the **To** field in the user's email client when they send logs.
Value	Enter the value for the parameters selected in the **Name** drop-down.

Global Agent Settings: Run OnGuard As Parameter

You can configure OnGuard to run health checks even if a user is not logged in.

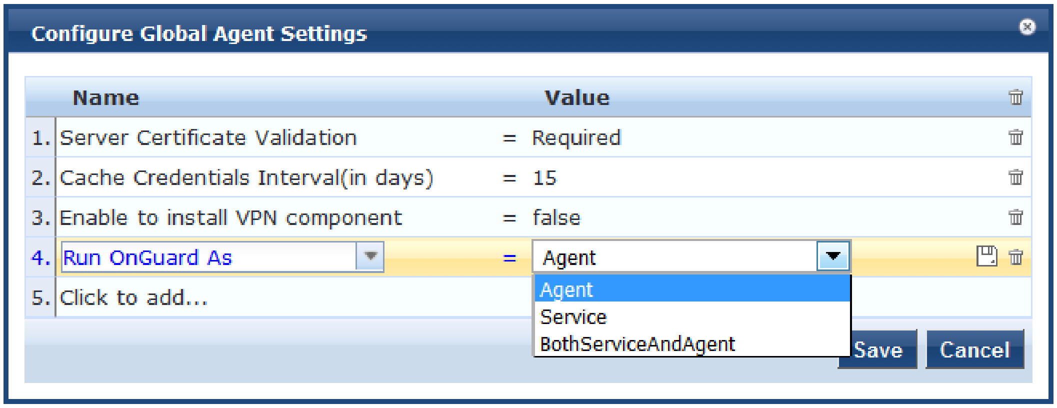
1. Navigate to **Administration** > **Agents and Software Updates** > **OnGuard Settings**.

   The OnGuard Settings page appears.

2. Click **Global Agent Settings**.

   The Global Agent Settings dialog appears.

Figure 681: *Global Agent Settings Dialog*



Configure Global Agent Settings

	Name		Value
1.	Server Certificate Validation	=	Required
2.	Cache Credentials Interval(in days)	=	15
3.	Enable to install VPN component	=	false
4.	Run OnGuard As	=	Agent
5.	Click to add...		

3. **Click Click to add...**.
4. **Name**: Select **Run OnGuard As**.
5. **Value:** Select the appropriate option as described in Table 367.

   Table 367 describes the available values for the **Run OnGuard As** parameter.

6. Click **Save**.

Table 367: *Global Agent Settings: Run OnGuard As Parameters*

Value	Description
Agent	Health checks are performed by the OnGuard Agent after the user logs in to the client.
Service	OnGuard Agent performs health checks as soon as the client boots up, that is, even before the user logs in to the client. When a user logs in to the client, the user can view the most recent health check results via the OnGuard Agent user interface. The user can perform health checks again by clicking the **Retry** button. For details, see the next section, Limitations for the Run OnGuard As Parameter.
BothService AndAgent	When the user is not logged in to the client, the ClearPass OnGuard Agent service performs health checks. As soon as the user logs in to the client, the ClearPass OnGuard Agent service stops health checks and the OnGuard Agent user interface initiates health checks.

Limitations for the Run OnGuard As Parameter

When **the Run OnGuard As** parameter is set to **Service**, the following limitations pertain:

1. In **Service** mode, OnGuard always runs in **Health Only** mode; that is, OnGuard always sends the client's MAC Address as User Name.
2. If a user is not logged in, some of the health checks and auto-remediation may fail in **Service** mode. These health checks are user-level checks, such as Registry Keys (HKCU), Processes, and Installed Applications (user applications).
3. When OnGuard Agent is running in **Service** mode, the OnGuard user interface is used only to display messages and provide the **Retry** button (to perform health checks).
4. The **Enable to Hide Quit Option** does not have any effect in **Service** mode as the **Quit** button is only for exiting the OnGuard user interface.

Using ClearPass Dictionaries

This section provides the following information:

- RADIUS Dictionary on page 664
- TACACS+ Services Dictionary on page 665
- Fingerprints Dictionary on page 667
- Dictionary Attributes on page 668
- Applications Dictionaries on page 672
- Configuring Endpoint Context Server Actions on page 590

Chapter 12
Cluster Upgrade/Update Tool

This chapter contains the following information:

- About the Cluster Update Tool
- About the Cluster Upgrade Tool

About the Cluster Update Tool

This section provides instructions for updating a ClearPass cluster with Patch and Skin releases using the Cluster Update feature.

The Cluster Update feature automates the process of updating your ClearPass cluster. The cluster Publisher is updated first. You can select one or more Subscriber nodes to be updated automatically after the Publisher update is complete.

After you initiate the Cluster Update, no manual actions are required until the Publisher and all the selected Subscriber nodes have been updated.

This section includes the following information:

- About the Cluster Update Feature
- Before Updating the Cluster
- Updating the Cluster
- Viewing Update Status

About the Cluster Update Feature

The Cluster Update feature performs the following actions:

- Copies the update image to the selected Subscriber nodes.

  Subscriber nodes copy the update image over a HTTPS connection to the Publisher.

  If you want to avoid the copy on one or more Subscriber nodes, log in to the subscriber and trigger a download of the update image in the Update portal or upload the update image through the Update Portal before initiating the cluster update.
- The Publisher is updated and rebooted (reboot is initiated only if it is mandatory).
- After the Publisher update completes, the Update utility will be accessible again to review progress and log messages.
- Update is now initiated on the selected Subscriber nodes; after completion, the Subscriber nodes are rebooted (reboot is initiated only if it is mandatory).
- Where possible, multiple Subscriber nodes are updated in parallel.
- After all selected Subscriber nodes have been updated, you may select and trigger Cluster Update for any additional Subscriber nodes.

The time required for subscriber update depends on multiple factors:

- Hardware or Virtual Appliance model. In the case of Virtual Machine installations, update times vary significantly based on the IOPS (I/O per second) performance of your Virtual Machine infrastructure.
- For Subscriber nodes, bandwidth and latency of the network link between subscriber and Publisher.

Before Updating the Cluster

- Confirm that Relevant Patch updates are available under software updates before starting the cluster update. Please download the patches either from Webservice or by uploading directly to Software Updates.
- Only patches listed under Software Updates will be shown in Cluster Update.
- Confirm that your Cluster sync and replications are fine before starting the Cluster Update.
- When a particular node's version information is set to "UNKNOWN", it means the Publisher is not able to contact the remote node. (If a Node has been disabled and gone out of sync, Cluster Update Interface might not detect the status until the patch failure has occurred, after which the failed/inaccessible node is marked as UNKNOWN).

  Please confirm the status of the cluster sync and service status of “Async network services” in such cases.
- In VM environments, ClearPass Policy Manager Virtual Machine host date/time settings should be in sync with that of the ESX or Hyper-V server, which is hosting the instance. Otherwise, you might see inconsistent data in "Time Taken" columns of the Update Interface.

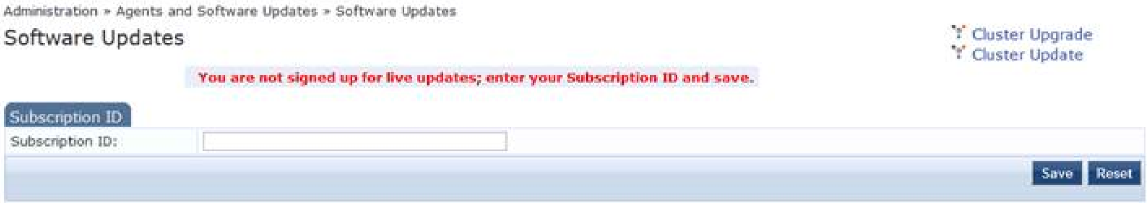
Updating the Cluster

Plan for sufficient downtime and review the Release Notes before starting the Cluster Update.

To update the cluster:

1. Navigate to **Administration > Agents and Software Updates > Software Updates > Cluster Update**.

Figure 682: *Navigate to Cluster Update*



Administration » Agents and Software Updates » Software Updates

Software Updates

You are not signed up for live updates; enter your Subscription ID and save.

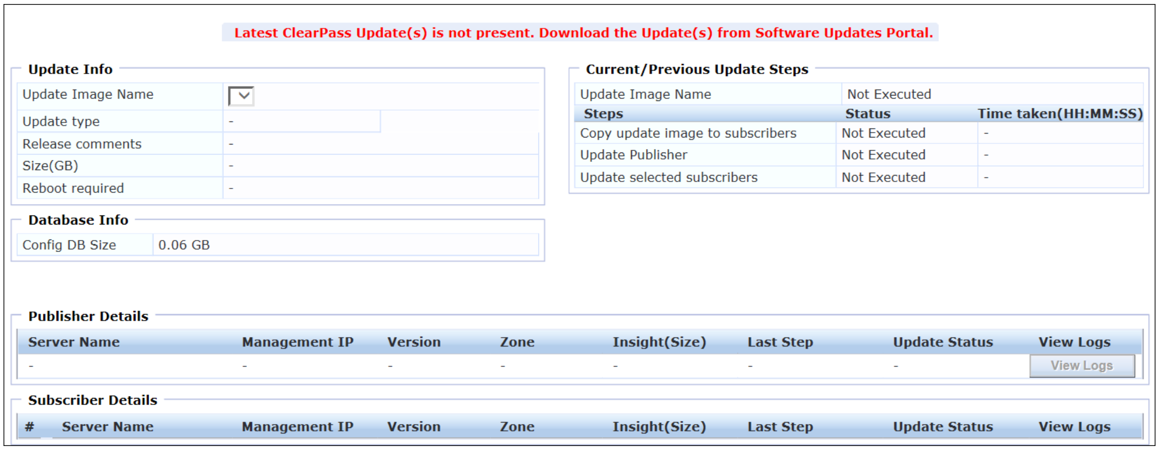
Subscription ID

Subscription ID:

2. Before you start the update, verify that the ClearPass update is downloaded and available in the Software Updates portal.

   If the update is not available, the Cluster Update page displays a message advising you to download it.

Figure 683: *The Message Advising that the Update Must Be Downloaded*



Latest ClearPass Update(s) is not present. Download the Update(s) from Software Updates Portal.

Update Info

Update Image Name	
Update type	-
Release comments	-
Size(GB)	-
Reboot required	-

Database Info

Config DB Size	0.06 GB

Current/Previous Update Steps

Update Image Name	Not Executed	
Steps	**Status**	**Time taken(HH:MM:SS)**
Copy update image to subscribers	Not Executed	-
Update Publisher	Not Executed	-
Update selected subscribers	Not Executed	-

Publisher Details

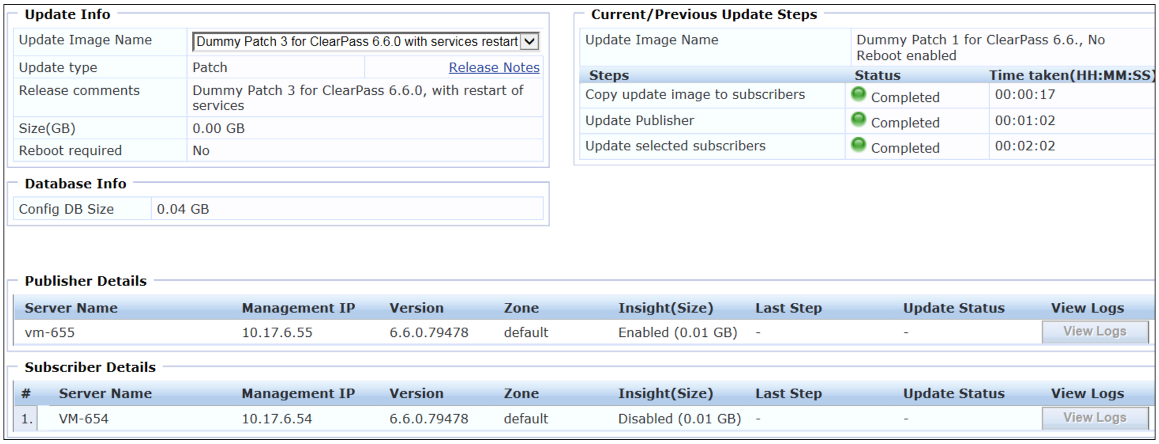
Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
-	-	-	-	-	-	-	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs

3. If you are prompted to log in, use your ClearPass Policy Manager administrator credentials. The Cluster Update page opens.

Figure 684: *Cluster Update Page*



Update Info

Update Image Name	Dummy Patch 3 for ClearPass 6.6.0 with services restart	
Update type	Patch	Release Notes
Release comments	Dummy Patch 3 for ClearPass 6.6.0, with restart of services	
Size(GB)	0.00 GB	
Reboot required	No	

Database Info

Config DB Size	0.04 GB

Current/Previous Update Steps

Update Image Name	Dummy Patch 1 for ClearPass 6.6., No Reboot enabled	
Steps	**Status**	**Time taken(HH:MM:SS)**
Copy update image to subscribers	● Completed	00:00:17
Update Publisher	● Completed	00:01:02
Update selected subscribers	● Completed	00:02:02

Publisher Details

Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
vm-655	10.17.6.55	6.6.0.79478	default	Enabled (0.01 GB)	-	-	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
1.	VM-654	10.17.6.54	6.6.0.79478	default	Disabled (0.01 GB)	-	-	View Logs

This page includes the information described below in Table 368.

Table 368: *Information on the Cluster Update Page*

Field	Description
Update Info	Describes the patch update details, provides a link to the Release Notes, includes release-specific comments, and specifies if a reboot is required for the patch.
Database Info	Shows the size of the Configuration database.
Publisher Details	Information for the Publisher and for all Subscriber nodes in the cluster. Information includes the management IP address, version number, zone, Insight database size, last update step completed, and update status.
Subscriber Details	
Update Steps	During the cluster update, this area shows the status of each stage in the process. As each stage completes, it shows how long it took to complete.
View Logs	In each Publisher and Subscriber row, this link provides detailed status and log messages for each update stage.

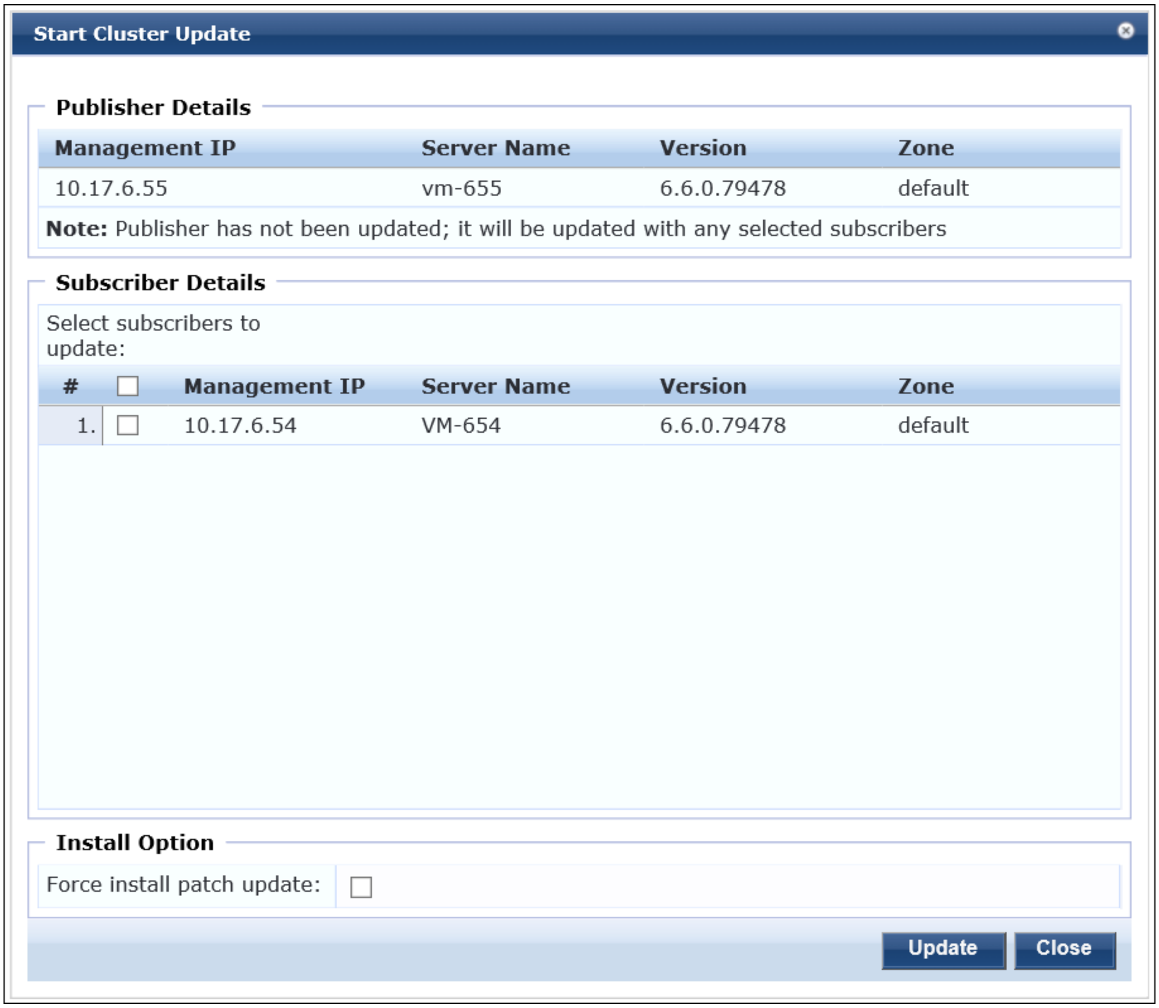
4. Select the **Update Image Name** from the drop-down list.

   When the update is available locally and all Subscriber nodes have been patched, the **Start Update** link is available in the upper-right corner.

5. Click **Start Update**.

   The **Start Cluster Update** window opens.

Figure 685: *The Start Cluster Update Window*



Start Cluster Update

Publisher Details

Management IP	Server Name	Version	Zone
10.17.6.55	vm-655	6.6.0.79478	default

Note: Publisher has not been updated; it will be updated with any selected subscribers

Subscriber Details

Select subscribers to update:

#	□	Management IP	Server Name	Version	Zone
1.	□	10.17.6.54	VM-654	6.6.0.79478	default

Install Option

Force install patch update: □

NOTE

You can update the entire cluster or just a subset of Subscriber nodes.

6. In the **Start Cluster Update** window, use the check boxes to select the Subscriber nodes to update.
7. To force the update, select **Force install patch update** under **Install Option**.
8. Click **Update**.

   This initiates the automated update process. No further manual steps are required until all selected Subscriber nodes have been updated. The Publisher is always updated and rebooted first.

   The Cluster Update page will not be available while the Publisher is rebooted. When the Publisher update is complete, you can use the Cluster Update page to monitor update progress.

Viewing Update Status

After the Publisher Update is complete, you can monitor the Update status of the Subscriber nodes at **Administration > Agents and Software Updates > Software Updates > Cluster Update**.

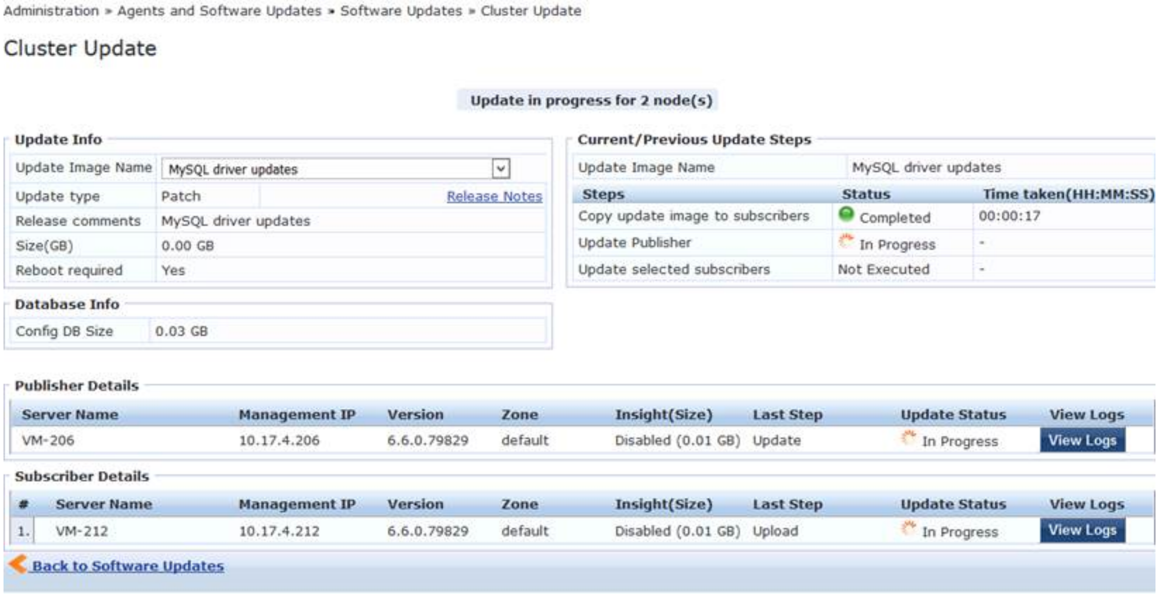
There are two ways to monitor the update's progress:

1. On the **Cluster Update** page, progress indicators in the **Update Steps** area show the status of some of the main steps.

Indicators in the **Publisher Details** and **Subscriber Details** areas also show when the Publisher or each subscriber is in progress or completed.

When the update is complete, these areas should show a successful update status for the Publisher and every subscriber.

Figure 686: *Status Indicators in the Update Steps Area*



Administration » Agents and Software Updates » Software Updates » Cluster Update

Cluster Update

Update in progress for 2 node(s)

Update Info

Update Image Name	MySQL driver updates	
Update type	Patch	Release Notes
Release comments	MySQL driver updates	
Size(GB)	0.00 GB	
Reboot required	Yes	

Database Info

Config DB Size	0.03 GB

Current/Previous Update Steps

Update Image Name	MySQL driver updates	
Steps	**Status**	**Time taken(HH:MM:SS)**
Copy update image to subscribers	● Completed	00:00:17
Update Publisher	In Progress	-
Update selected subscribers	Not Executed	-

Publisher Details

Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
VM-206	10.17.4.206	6.6.0.79829	default	Disabled (0.01 GB)	Update	In Progress	View Logs

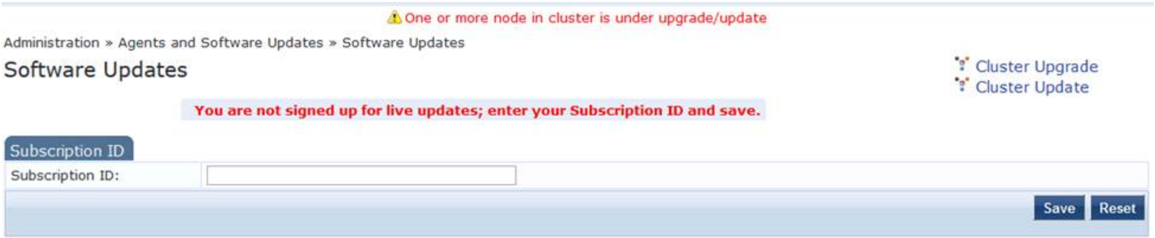
Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
1.	VM-212	10.17.4.212	6.6.0.79829	default	Disabled (0.01 GB)	Upload	In Progress	View Logs

Back to Software Updates

If you navigate to another page, and then navigate back to the Software Updates page, a status link will be provided.

Figure 687: *In Progress Status Link*



⚠ One or more node in cluster is under upgrade/update

Administration » Agents and Software Updates » Software Updates

Software Updates

Cluster Upgrade
Cluster Update

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID

Subscription ID:

Clicking the link takes you back to the **Cluster Update** page.

2. For detailed progress information, click the **View Logs** button in the Publisher's or subscriber's row.

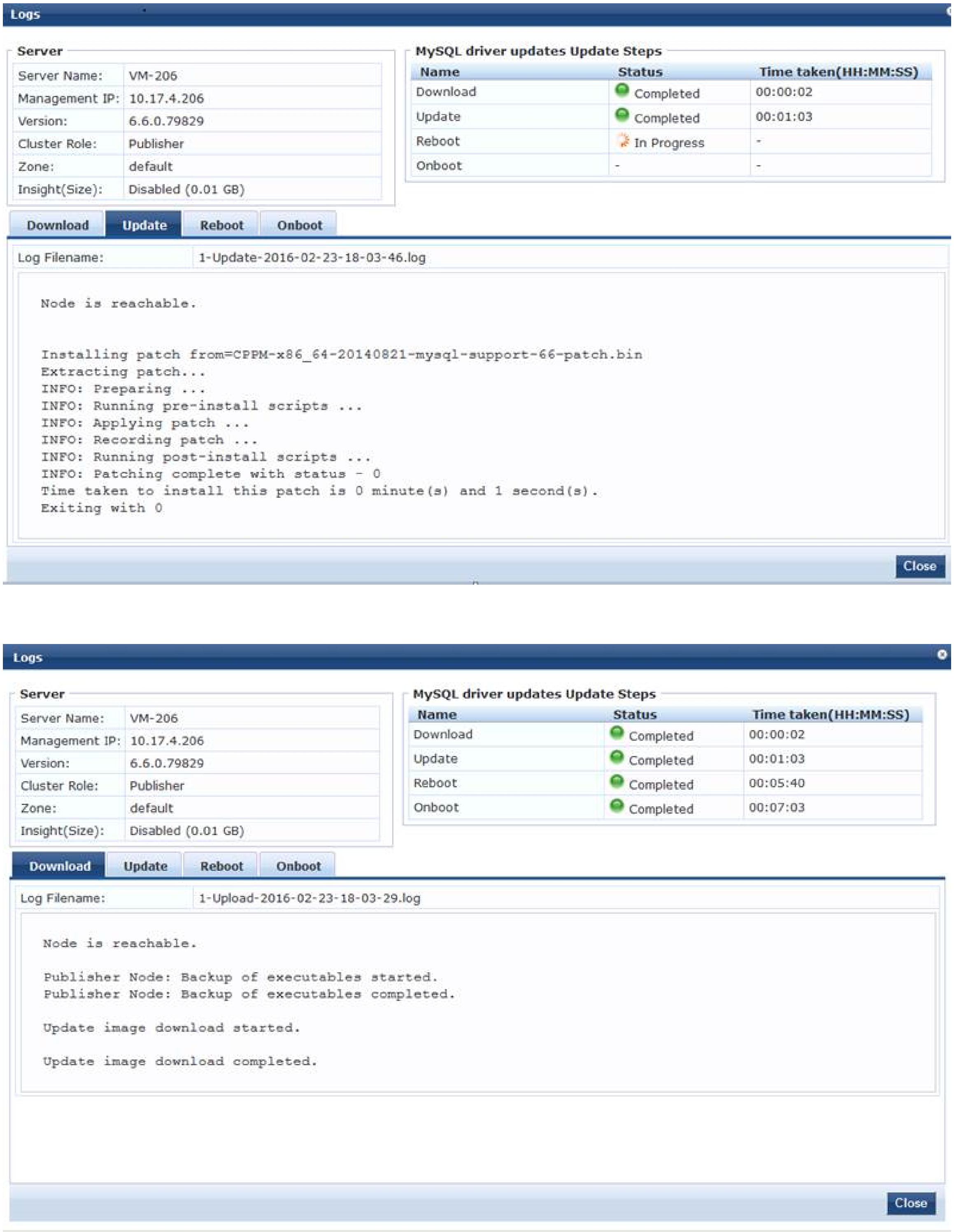
   The **Logs** window opens. This window includes tabs for the **Download**, **Upgrade**, **Reboot**, and **Onboot** logs.

   You can view detailed status in these logs during and after the update.

NOTE

This option is not available while the Publisher is rebooted and data migration is in progress. It is available again when the Publisher update is complete.

Figure 688: *Details Displayed on the Logs Window*



Server

Server Name:	VM-206
Management IP:	10.17.4.206
Version:	6.6.0.79829
Cluster Role:	Publisher
Zone:	default
Insight(Size):	Disabled (0.01 GB)

MySQL driver updates Update Steps

Name	Status	Time taken(HH:MM:SS)
Download	● Completed	00:00:02
Update	● Completed	00:01:03
Reboot	In Progress	-
Onboot	-	-

Log Filename: 1-Update-2016-02-23-18-03-46.log

```
Node is reachable.


Installing patch from=CPPM-x86_64-20140821-mysql-support-66-patch.bin
Extracting patch...
INFO: Preparing ...
INFO: Running pre-install scripts ...
INFO: Applying patch ...
INFO: Recording patch ...
INFO: Running post-install scripts ...
INFO: Patching complete with status - 0
Time taken to install this patch is 0 minute(s) and 1 second(s).
Exiting with 0
```

Logs

Server

Server Name:	VM-206
Management IP:	10.17.4.206
Version:	6.6.0.79829
Cluster Role:	Publisher
Zone:	default
Insight(Size):	Disabled (0.01 GB)

MySQL driver updates Update Steps

Name	Status	Time taken(HH:MM:SS)
Download	● Completed	00:00:02
Update	● Completed	00:01:03
Reboot	● Completed	00:05:40
Onboot	● Completed	00:07:03

Log Filename: 1-Upload-2016-02-23-18-03-29.log

```
Node is reachable.

Publisher Node: Backup of executables started.
Publisher Node: Backup of executables completed.

Update image download started.

Update image download completed.
```

About the Cluster Upgrade Tool

This section includes the following information:

- Cluster Upgrade Process Overview
- Before You Upgrade
- Installing the Cluster Upgrade Tool

- Launching the Cluster Upgrade Tool
- Upgrading the ClearPass Cluster
- Viewing Upgrade Status
- Steps in the Upgrade Tool's Automated Workflow
- Troubleshooting Tips

Introduction

This section provides instructions for upgrading a ClearPass cluster using the Cluster Upgrade Tool.

The Cluster Upgrade Tool is a simple user interface that automates the upgrade procedure for a ClearPass cluster. When the Upgrade is initiated, no manual actions are required until the publisher and all selected Subscribers have been upgraded.

This release of the tool can be used to upgrade ClearPass 6.3.6, 6.4.7, 6.5.x, and 6.6.x systems to ClearPass 6.6. It cannot be used to upgrade to an earlier version of the Cluster Upgrade Tool.

If you have an earlier version of the Cluster Upgrade Tool already installed, you can install this version directly over the earlier version of the tool; no cleanup steps are needed.

Cluster Upgrade Process Overview

These tasks summarize the Cluster Upgrade process:

1. Download the upgrade image to the **Software Updates Portal**.
2. Install the Cluster Upgrade Tool (see Installing the Cluster Upgrade Tool).
3. Launch the Cluster Upgrade Tool and specify the Subscriber nodes to be upgraded (see Launching the Cluster Upgrade Tool).
4. Initiate the Upgrade procedure (see Upgrading the ClearPass Cluster).

   The Cluster Upgrade tool automatically performs the upgrade.
5. After the upgrade, verify that the Publisher and all Subscriber nodes in the cluster are back in sync and all services are accessible (see Viewing Upgrade Status).

NOTE

Cloning a virtual machine to facilitate a ClearPass deployment is not recommended or supported.

Before You Upgrade

Before you begin the cluster upgrade process, ensure that the following tasks have been completed:

1. Review this section and the latest Release Notes for ClearPass 6.6.
2. Plan for adequate downtime for the upgrade.

   Use the upgrade time estimates in Sample Times Required for Upgrade on page 701 as a guide.
3. Install the Cluster Upgrade Tool on the Publisher node of your 6.3.6, 6.4.7, 6.5.x, and 6.6.x version.
4. Before installing the Cluster Upgrade Tool on the Publisher, verify that ClearPass services are up and running on both the Publisher and all Subscriber nodes. Verify again after installing the tool.
5. If the cluster password contains special characters, change it temporarily to only use alphanumeric characters (letters and numbers) before installing this patch.

   You can change the cluster password back to the old password after the cluster upgrade completes.
6. HTTP, HTTPS, and SSH port traffic must be allowed between the cluster nodes. This is required in order for the tool to be able to communicate between nodes.

   Verify that the following ports are in an open state between the cluster nodes:

- Port 80 (HTTP)
- Port 443 (HTTPS)
- Port 22 (SSH)

7. Confirm that the Publisher node and all Subscriber nodes in the cluster are in sync before starting the upgrade.
8. On the Publisher node, download the ClearPass 6.6 upgrade image from the **Software Updates** portal (see Updating Policy Manager Software on page 673).

   The Upgrade tool automates the process of copying over the upgrade image to the selected subscribers in the cluster.
9. If you are upgrading on a reverted system (retrying an upgrade), you will need to replace the contents of certain directories first before triggering the new upgrade. Please contact Support (see Contact Support on page 1), who will assist you with the following tasks:
   a. Copying the contents of the `/var/avenda/platform/store/updates/backup/*` directory to the `/var/avenda/platform/store/updates/` directory.
   b. Clearing the contents of the **`/var/avenda/tips/upgrade/db/*`** directory.
   c. Restarting the **cpass-admin-server** on the Publisher.
10. When a particular node's version information is set to "UNKNOWN," it means the publisher is not able to contact the remote node.

    If a node has been disabled and gone out of sync, the Cluster Upgrade Interface might not detect the status until the patch failure has occurred, after which the failed or inaccessible node is marked as UNKNOWN.

    In such cases, confirm the status of the cluster sync and service status of **Async network services**.
    d. In Virtual Machine environments, ClearPass Policy Manager virtual machine host date and time settings should be in sync with that of the ESX server or Hyper-V server, which is hosting the instance. Otherwise, you might see inconsistent data in "Time Taken" columns of the Upgrade interface.

Installing the Cluster Upgrade Tool

The Cluster Upgrade Tool is released as separate patches for each of the ClearPass 6.3.6, 6.4.7 and 6.5.* versions. It can be downloaded and installed either through Policy Manager’s Software Updates portal or from the Aruba Support Center.

NOTE

The Upgrade Tool can only be installed on the Publisher node.

To install the Upgrade Tool through the Software Updates Portal:

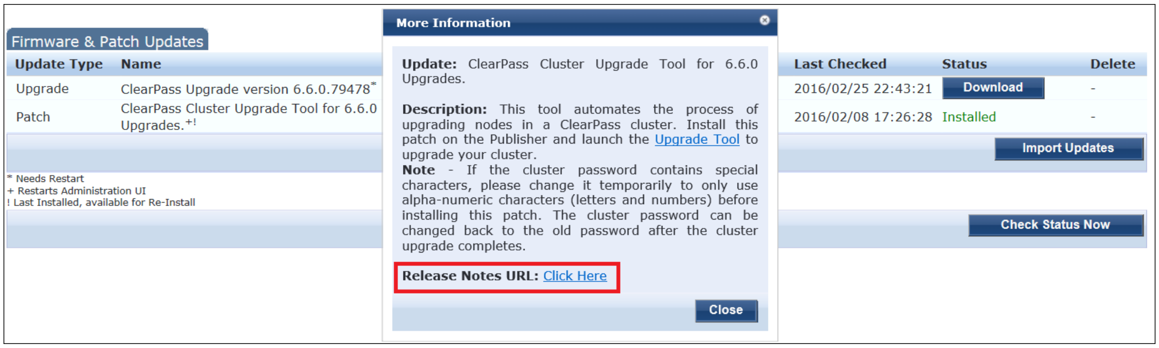
1. Log in to ClearPass Policy Manager on the Publisher and navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the row for the ClearPass Cluster Upgrade Tool patch, click the **Install** button.

   When the installation is complete, the Admin service will be restarted. You do not need to reboot.
3. To review the Release Notes for the tool, click the patch’s row.

   The **More Information** window opens.
4. Click the **Release Notes URL** link.

   The Support Center's **Release Notes** page opens in a new tab.

Figure 689: *The Link to the Cluster Upgrade Tool Release Notes*



Firmware & Patch Updates

Update Type	Name	Last Checked	Status	Delete
Upgrade	ClearPass Upgrade version 6.6.0.79478*	2016/02/25 22:43:21	Download	-
Patch	ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.+!	2016/02/08 17:26:28	Installed	-

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

More Information

Update: ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.

Description: This tool automates the process of upgrading nodes in a ClearPass cluster. Install this patch on the Publisher and launch the Upgrade Tool to upgrade your cluster.
Note - If the cluster password contains special characters, please change it temporarily to only use alpha-numeric characters (letters and numbers) before installing this patch. The cluster password can be changed back to the old password after the cluster upgrade completes.

Release Notes URL: Click Here

If the Publisher Is Not Set Up

To install the Upgrade Tool if the publisher is not set up to display available updates:

1. On the Aruba Support site (support.arubanetworks.com), manually download the Cluster Upgrade Tool.
2. On the Publisher's **Software Updates** portal, use the **Import Updates** link to upload it.
3. Install the Upgrade Tool as described above.

Launching the Cluster Upgrade Tool

After the Cluster Update Tool is installed, you can launch the Cluster Upgrade tool either from the Software Updates portal or through your Web browser.

To launch the Cluster Upgrade Tool from the Software Updates portal:

1. In ClearPass Policy Manager, navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the upper-right of the page, click **Cluster Upgrade**.

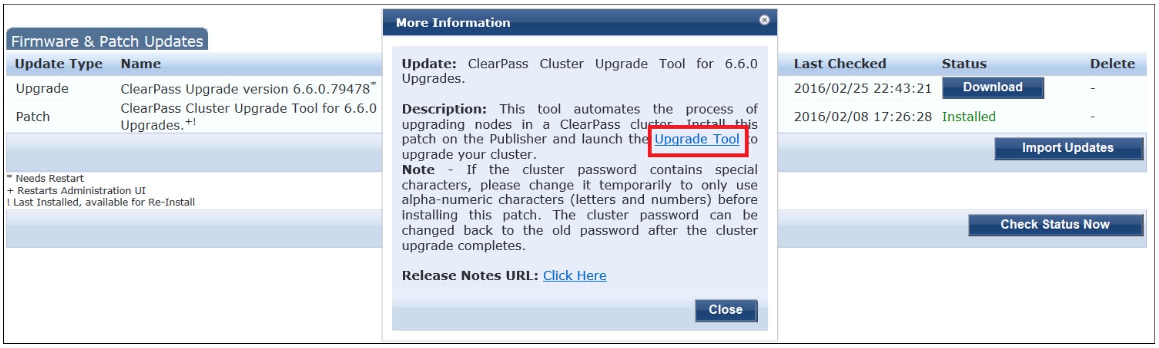
   The **Cluster Upgrade** page opens.

An Alternative Way to Open the Tool

An alternative way to open the tool is as follows:

1. In ClearPass Policy Manager, navigate to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware & Patch Updates** area, click the row of the ClearPass Cluster Upgrade Tool patch.
3. In the **More Information** window that opens, click the **Upgrade Tool** link.

Figure 690: *The Link to the Cluster Upgrade Tool*



Firmware & Patch Updates

Update Type	Name	Last Checked	Status	Delete
Upgrade	ClearPass Upgrade version 6.6.0.79478*	2016/02/25 22:43:21	Download	-
Patch	ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.+!	2016/02/08 17:26:28	Installed	-

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

More Information

Update: ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.

Description: This tool automates the process of upgrading nodes in a ClearPass cluster. Install this patch on the Publisher and launch the Upgrade Tool to upgrade your cluster.
Note - If the cluster password contains special characters, please change it temporarily to only use alpha-numeric characters (letters and numbers) before installing this patch. The cluster password can be changed back to the old password after the cluster upgrade completes.

Release Notes URL: Click Here

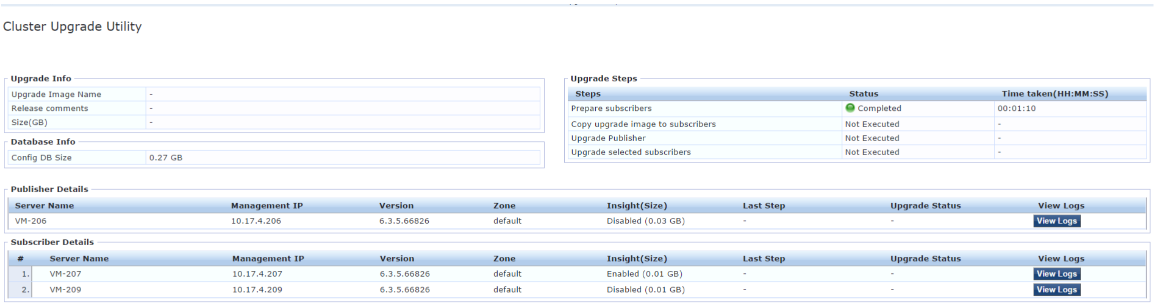
Opening the Tool Via Your Web Browser

To open the Cluster Upgrade Tool directly through your Web browser:

1. Enter **https://<*ClearPass-Publisher-IP*-address>/upgrade** in your browser's address bar.
2. If you are prompted to log in, use your ClearPass Policy Manager administrator credentials.

   The **Cluster Upgrade Utility** page opens.

Figure 691: *The Cluster Upgrade Utility Page*



Cluster Upgrade Utility

Upgrade Info

Upgrade Image Name	-
Release comments	-
Size(GB)	-

Database Info

Config DB Size	0.27 GB

Upgrade Steps

Steps	Status	Time taken(HH:MM:SS)
Prepare subscribers	● Completed	00:01:10
Copy upgrade image to subscribers	Not Executed	-
Upgrade Publisher	Not Executed	-
Upgrade selected subscribers	Not Executed	-

Publisher Details

Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
VM-206	10.17.4.206	6.3.5.66826	default	Disabled (0.03 GB)	-	-	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
1.	VM-207	10.17.4.207	6.3.5.66826	default	Enabled (0.01 GB)	-	-	View Logs
2.	VM-209	10.17.4.209	6.3.5.66826	default	Disabled (0.01 GB)	-	-	View Logs

This page includes the information described below in Table 369.

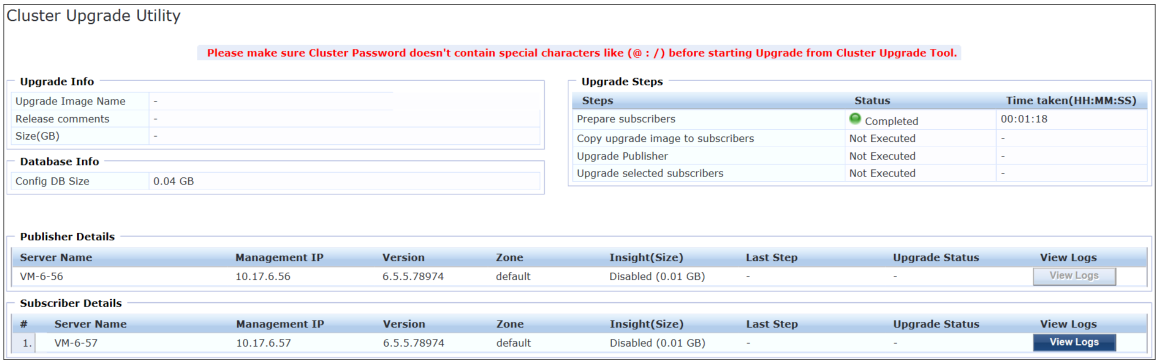
Table 369: *Information on the Cluster Upgrade Utility Page*

Field	Description
Upgrade Info	Describes the upgrade image's name and size, provides a link to the Cluster Upgrade Tool Release Notes, and includes release-specific comments.
Publisher Details	Information for the Publisher and for all Subscriber nodes in the cluster. Information includes the management IP address, version number, zone, Insight database size, last upgrade step completed, and upgrade status.
Subscriber Details	
Database Info	Shows the size of the Configuration database.
Upgrade Steps	During the cluster upgrade, this area shows the status of each stage in the process. As each stage completes, it shows how long it took to complete.
View Logs	In each Publisher and Subscriber row, this link provides detailed status and log messages for each upgrade stage.
Help	Briefly describes the actions performed by the tool.

3. If the cluster password contains special characters, change it temporarily to only use alphanumeric characters (letters and numbers) before installing this patch.

   The cluster password can be changed back to the old password after the cluster upgrade completes.

Figure 692: *Special Characters Note*



Cluster Upgrade Utility

Please make sure Cluster Password doesn't contain special characters like (@ : /) before starting Upgrade from Cluster Upgrade Tool.

Upgrade Info

Upgrade Image Name	-
Release comments	-
Size(GB)	-

Database Info

Config DB Size	0.04 GB

Upgrade Steps

Steps	Status	Time taken(HH:MM:SS)
Prepare subscribers	● Completed	00:01:18
Copy upgrade image to subscribers	Not Executed	-
Upgrade Publisher	Not Executed	-
Upgrade selected subscribers	Not Executed	-

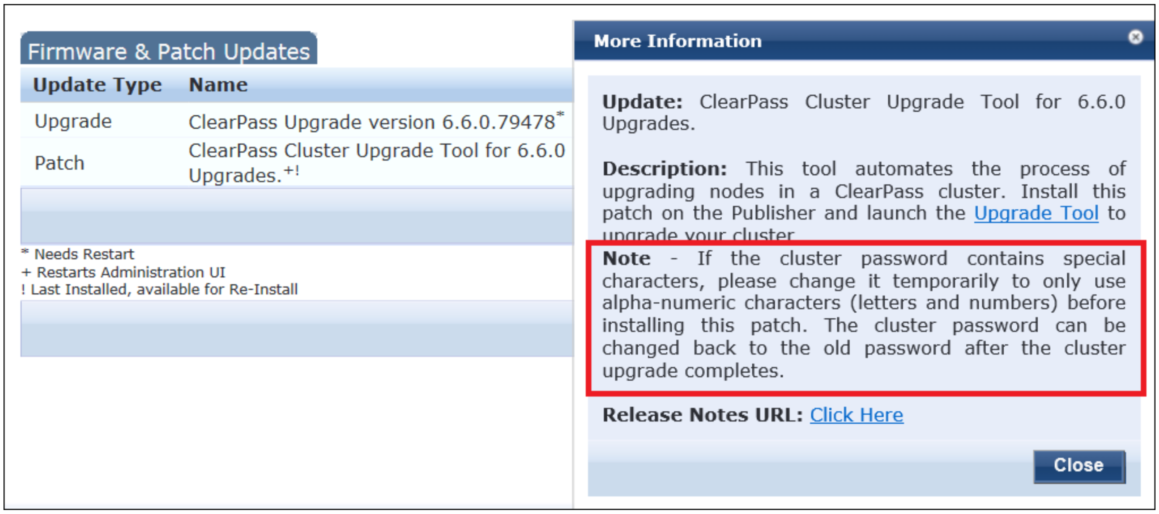
Publisher Details

Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
VM-6-56	10.17.6.56	6.5.5.78974	default	Disabled (0.01 GB)	-	-	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
1.	VM-6-57	10.17.6.57	6.5.5.78974	default	Disabled (0.01 GB)	-	-	View Logs

Figure 693: *More Information > Special Characters Note*



Firmware & Patch Updates

Update Type	Name
Upgrade	ClearPass Upgrade version 6.6.0.79478*
Patch	ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.+!

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

More Information

Update: ClearPass Cluster Upgrade Tool for 6.6.0 Upgrades.

Description: This tool automates the process of upgrading nodes in a ClearPass cluster. Install this patch on the Publisher and launch the Upgrade Tool to upgrade your cluster.

Note - If the cluster password contains special characters, please change it temporarily to only use alpha-numeric characters (letters and numbers) before installing this patch. The cluster password can be changed back to the old password after the cluster upgrade completes.

Release Notes URL: Click Here

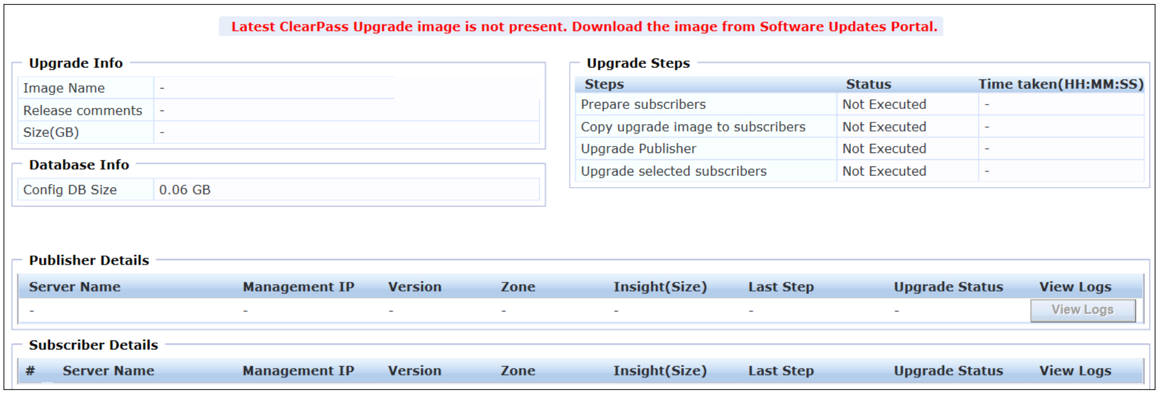
Upgrading the ClearPass Cluster

To upgrade the ClearPass cluster:

1. Navigate to **Administration > Agents and Software Updates > Software Updates > Cluster Upgrade**.
2. Before you start the upgrade, verify that the ClearPass 6.6 Upgrade Image is downloaded and available in the Software Updates portal.

   If the upgrade image is not available, the **Cluster Upgrad**e page displays a message advising you to download it.

Figure 694: *The Message Advising that the Upgrade Image Must Be Downloaded*



Latest ClearPass Upgrade image is not present. Download the image from Software Updates Portal.

Upgrade Info

Image Name	-
Release comments	-
Size(GB)	-

Database Info

Config DB Size	0.06 GB

Upgrade Steps

Steps	Status	Time taken(HH:MM:SS)
Prepare subscribers	Not Executed	-
Copy upgrade image to subscribers	Not Executed	-
Upgrade Publisher	Not Executed	-
Upgrade selected subscribers	Not Executed	-

Publisher Details

Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
-	-	-	-	-	-	-	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Upgrade Status	View Logs

3. When you open the Cluster Upgrade Tool, it immediately prepares the subscribers for upgrade by automatically installing the required additional API support.

   This is a background process and does not require any actions from the user. A progress indicator is shown during this stage.

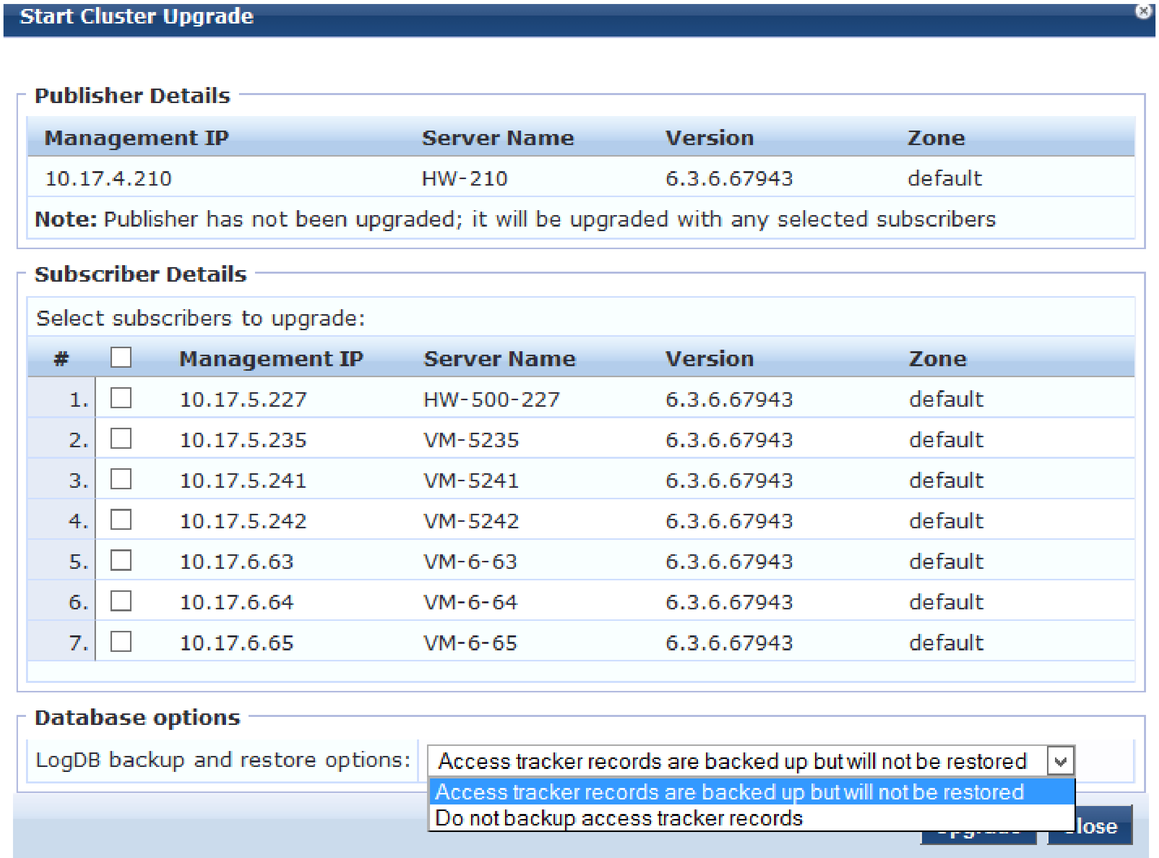
> NOTE
>
> To install the patch for API support on Subscriber nodes, these nodes must be able to access the Publisher over HTTP, or they must be able to access the publisher over HTTPS using its host name and validate the certificate that is presented (that is, trust the issuer and match the host name in the certificate Common Name (CN)).

   When the 6.6 upgrade image is available locally and all Subscriber nodes have been patched, the **Start Upgrade** link is available (in the upper-right corner).

4. Click **Start Upgrade**.

   The **Start Cluster Upgrade** window opens.

Figure 695: *The Start Cluster Upgrade Window*



Start Cluster Upgrade

Publisher Details

Management IP	Server Name	Version	Zone
10.17.4.210	HW-210	6.3.6.67943	default

Note: Publisher has not been upgraded; it will be upgraded with any selected subscribers

Subscriber Details

Select subscribers to upgrade:

#	☐	Management IP	Server Name	Version	Zone
1.	☐	10.17.5.227	HW-500-227	6.3.6.67943	default
2.	☐	10.17.5.235	VM-5235	6.3.6.67943	default
3.	☐	10.17.5.241	VM-5241	6.3.6.67943	default
4.	☐	10.17.5.242	VM-5242	6.3.6.67943	default
5.	☐	10.17.6.63	VM-6-63	6.3.6.67943	default
6.	☐	10.17.6.64	VM-6-64	6.3.6.67943	default
7.	☐	10.17.6.65	VM-6-65	6.3.6.67943	default

Database options

LogDB backup and restore options: Access tracker records are backed up but will not be restored

Access tracker records are backed up but will not be restored
Do not backup access tracker records
lose

You can upgrade the entire cluster or just a subset of Subscriber nodes.

5. In the **Start Cluster Upgrade** window, use the check boxes to select the Subscriber nodes to upgrade.
6. In the **LogDB backup and restore options** drop-down list:
   a. If you need a backup of the Access Tracker records to potentially restore after upgrade, select **Access tracker records are backed up but will not be restored**.

      This option will increase the overall upgrade time.

   b. If you do not need a backup of the Access Tracker records, select **Do not back up access tracker records.**
7. Click **Upgrade**.

   The Upgrade Tool begins the automated upgrade process.

No further manual steps are required until all selected subscribers have been upgraded. For information on the automated process, see Steps in the Upgrade Tool's Automated Workflow on page 700.

The Publisher is always upgraded and rebooted first. The Upgrade Tool will not be available while the publisher is rebooted and data migration is in progress.

8. When the Publisher upgrade is complete, navigate to the **Cluster Upgrade Utility** page to monitor upgrade progress, as described in Viewing Upgrade Status on page 699.
9. After a successful upgrade, confirm that all the Subscriber nodes in the cluster are back in sync and all the services are accessible.
10. Verify that any preexisting Standby Publisher settings are restored:

    Navigate to: **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters** link **> Standby Publisher** tab.

Viewing Upgrade Status

After the Publisher Upgrade is complete, you can monitor the Upgrade status of the Subscriber nodes at **Administration > Agents and Software Updates > Software Updates > Cluster Upgrade**.

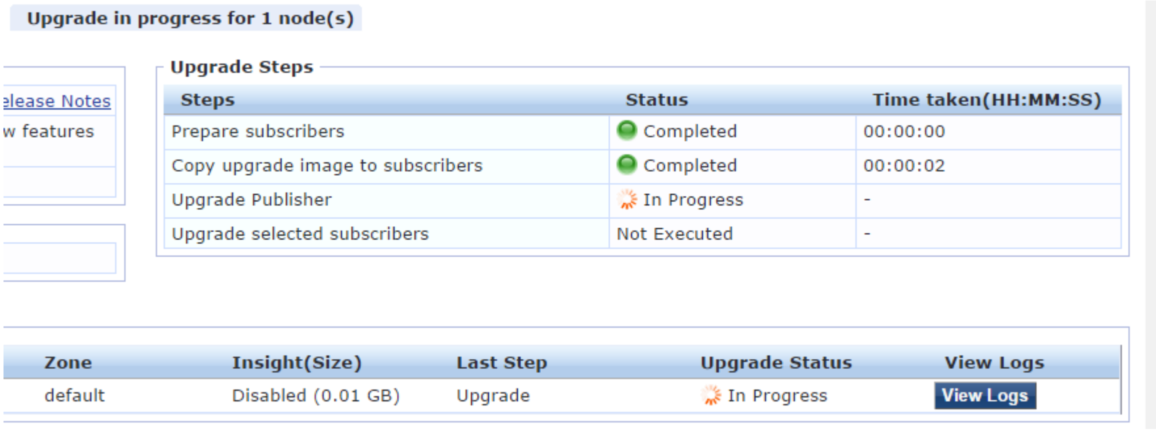
The tool provides two ways to monitor the upgrade's progress:

1. On the **Cluster Upgrade** page, progress indicators in the **Upgrade Steps** area show the status of some of the main steps.

   Indicators in the **Publisher Details** and **Subscriber Details** areas also show when the Publisher or each Subscriber node is in progress or completed.

   When the upgrade is complete, these areas should show a successful upgrade status for the Publisher and every Subscriber node.

Figure 696: *Status Indicators in the Upgrade Steps Area*



Upgrade in progress for 1 node(s)

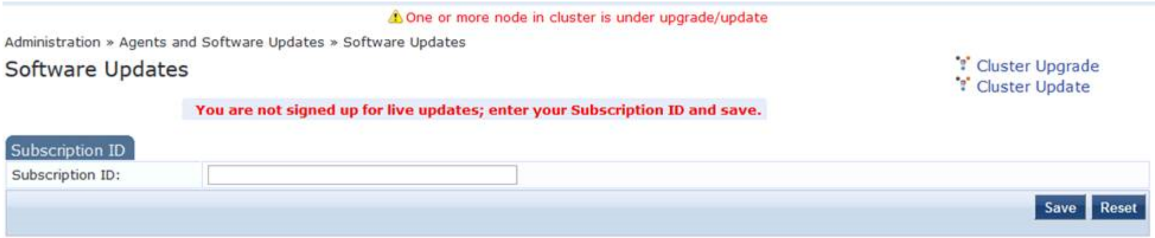
Upgrade Steps

Steps	Status	Time taken(HH:MM:SS)
Prepare subscribers	Completed	00:00:00
Copy upgrade image to subscribers	Completed	00:00:02
Upgrade Publisher	In Progress	-
Upgrade selected subscribers	Not Executed	-

Zone	Insight(Size)	Last Step	Upgrade Status	View Logs
default	Disabled (0.01 GB)	Upgrade	In Progress	View Logs

If you navigate to another page, and then navigate back to the Software Updates page, a status link will be provided.

Figure 697: *In Progress Status Link*



⚠ One or more node in cluster is under upgrade/update

Administration » Agents and Software Updates » Software Updates

Software Updates

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID

Subscription ID:

Clicking the link takes you back to the Cluster Upgrade page.

2. For detailed progress information, click the **View Logs** button in the Publisher's or Subscriber's row.

   The **Logs** window opens. This window includes tabs for the **Patch**, **Download**, **Upgrade**, **Reboot**, and **Onboot** logs.

   You can view detailed status in these logs during and after the upgrade.

NOTE

This option is not available while the Publisher is rebooted and data migration is in progress. It is available again when the Publisher upgrade is complete.

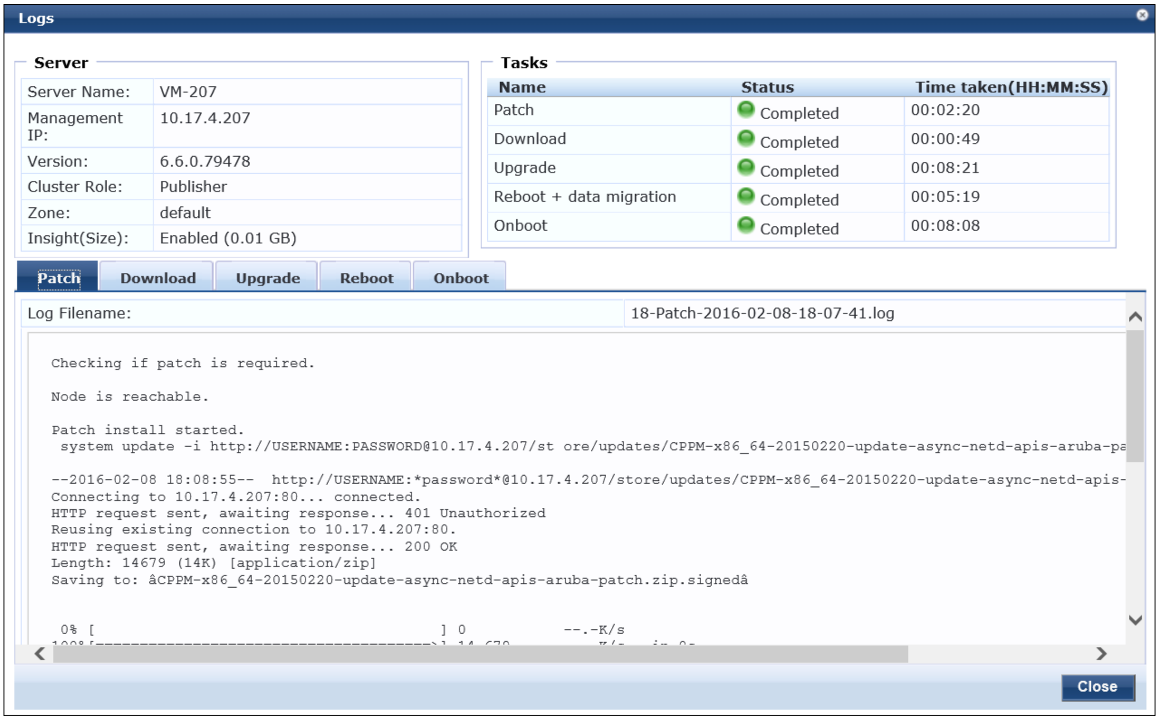


Figure 698: *Details Displayed on the Logs Window*

Server

Server Name:	VM-207
Management IP:	10.17.4.207
Version:	6.6.0.79478
Cluster Role:	Publisher
Zone:	default
Insight(Size):	Enabled (0.01 GB)

Tasks

Name	Status	Time taken(HH:MM:SS)
Patch	● Completed	00:02:20
Download	● Completed	00:00:49
Upgrade	● Completed	00:08:21
Reboot + data migration	● Completed	00:05:19
Onboot	● Completed	00:08:08

Log Filename: 18-Patch-2016-02-08-18-07-41.log

```
Checking if patch is required.

Node is reachable.

Patch install started.
 system update -i http://USERNAME:PASSWORD@10.17.4.207/st ore/updates/CPPM-x86_64-20150220-update-async-netd-apis-aruba-pa

--2016-02-08 18:08:55--  http://USERNAME:*password*@10.17.4.207/store/updates/CPPM-x86_64-20150220-update-async-netd-apis-
Connecting to 10.17.4.207:80... connected.
HTTP request sent, awaiting response... 401 Unauthorized
Reusing existing connection to 10.17.4.207:80.
HTTP request sent, awaiting response... 200 OK
Length: 14679 (14K) [application/zip]
Saving to: âCPPM-x86_64-20150220-update-async-netd-apis-aruba-patch.zip.signedâ


 0% [                                       ] 0           --.-K/s
```

Steps in the Upgrade Tool's Automated Workflow

This section describes the steps that are automatically completed by the Cluster Upgrade Tool.

1. To prepare the Subscriber nodes for upgrade, a patch that provides required API support is automatically installed by the Upgrade Tool on every Subscriber.

   The Cluster Upgrade Tool uses remote API calls to control and monitor upgrade progress on the subscribers.

NOTE

To install the patch for API support on the subscribers, subscribers must be able to access the publisher over HTTP, or they must be able to access the publisher over HTTPS using its hostname and validate the certificate that is presented (trust the issuer and match the hostname in the certificate CN).

2. After you select the Subscriber nodes and click **Upgrade**, the upgrade image is copied to the Subscribers you selected.

   The Subscriber nodes copy the upgrade image over an HTTPS connection to the Publisher.

   If the upgrade image is already present on a Subscriber node (you have downloaded it from the Software Updates portal, or uploaded it in the Software Updates portal), the existing upgrade image on the Subscriber node will be used for the upgrade.

3. If the Standby Publisher settings were configured, they are temporarily disabled. This setting is restored after all Subscriber nodes have been upgraded.

4. The Publisher is the first to be upgraded and rebooted. Configuration database and Insight database migration is performed on reboot.
5. When the Publisher upgrade is complete, you can use the **Cluster Upgrade Utility** page to review log messages.
6. When the Publisher upgrade is complete, upgrade is initiated on each selected Subscriber node. When possible, multiple Subscribers are upgraded in parallel. When each Subscriber node is complete, the Subscriber is rebooted.
7. During the parallel upgrade process, upgrade of the first Subscriber node begins five minutes after the Publisher upgrade is completed.
8. Upgrade of the second Subscriber node begins five minutes after the upgrade of the first Subscriber begins. This pattern continues sequentially for all Subscriber nodes in the cluster, with a five-minute delay between each start time.
9. When each Subscriber is rebooted, it is added back into the cluster. Insight data is migrated and restored.
10. When all selected Subscriber nodes have been upgraded, you can select and trigger the upgrade operation for any additional Subscribe nodes.
11. When all the Subscriber nodes in the cluster have been upgraded, the Standby Publisher settings are restored.

Detailed information for each of these steps is available in the Logs window during and after upgrade.

Sample Times Required for Upgrade

To help you estimate how much time the upgrade might take, Table 370 shows representative numbers for upgrade times under test conditions. Keep in mind that the figures here are only examples. The actual time required for your upgrade depends on several factors:

- Your hardware or virtual appliance model. In the case of virtual machine installations, upgrade times vary significantly based on the IOPS performance of your virtual machine infrastructure.
- The size of the configuration database to be migrated.
- For ClearPass Insight nodes, the size of the Insight database.
- For Subscriber nodes, the bandwidth and latency of the network link between the Subscriber and the Publisher.

Table 370: *Sample Times Required for Upgrade*

Hardware Model	Config DB Size	Insight DB Size	Publisher Upgrade Time	Subscriber Upgrade Time	Insight Restoration Time
CP-500	100 MB	5 GB	50 minutes	50 minutes	20 minutes
	200 MB	5 GB	60 minutes	60 minutes	20 minutes
CP-5K	100 MB	5 GB	50 minutes	50 minutes	15 minutes
	200 MB	5 GB	60 minutes	60 minutes	15 minutes
CP-25K	200 MB	5 GB	30 minutes	30 minutes	15 minutes
	500 MB	10 GB	40 minutes	40 minutes	20 minutes

Troubleshooting Tips

- If you encounter errors while upgrading a Subscriber, use a manual upgrade procedure to upgrade the Subscriber after the root cause for the upgrade failure has been fixed.
- If you need to revert to the previous version of ClearPass, you can do so manually from the CLI for individual Subscribers.

  Be aware that all status and progress information will be reset when the Publisher is reverted to a previous version. You can initiate the upgrade again from the Cluster Upgrade Tool.

Chapter 13
Configuring Processing for Ingress Events

This chapter includes the following information:

- Enabling Ingress Event Dictionaries
- Configuring the Ingress Event Sources
- Configuring an Event-Based Enforcement Service
- Configuring the Ingress Receiving Ports
- Enabling Ingress Events Processing

Overview

This chapter provides the procedures for configuring ClearPass Policy Manager to process ingress threat-related events.

The ClearPass Ingress Event Engine processes inbound threat-related events—which are Syslog events received from any third-party vendor device—and performs enforcements and actions based on defined policies.

Enabling Ingress Event Dictionaries

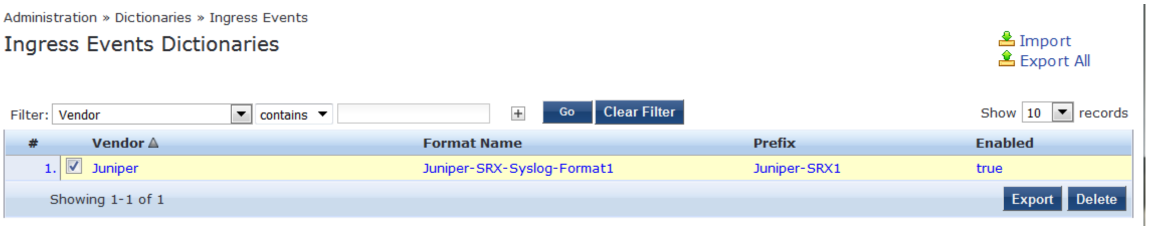
By default, a set of ingress event dictionaries are available and initially set to disabled. You must enable the ingress event dictionaries before you proceed.

To enable an ingress event dictionary:

1. Navigate to **Administration** > **Dictionaries** > **Ingress Events**.

   The Ingress **Events Dictionaries** page opens, where the set of ingress event dictionaries are displayed. By default, they are disabled.

Figure 699: *Viewing Ingress Event Dictionaries*



Administration » Dictionaries » Ingress Events

Ingress Events Dictionaries

Filter: Vendor contains

Show 10 records

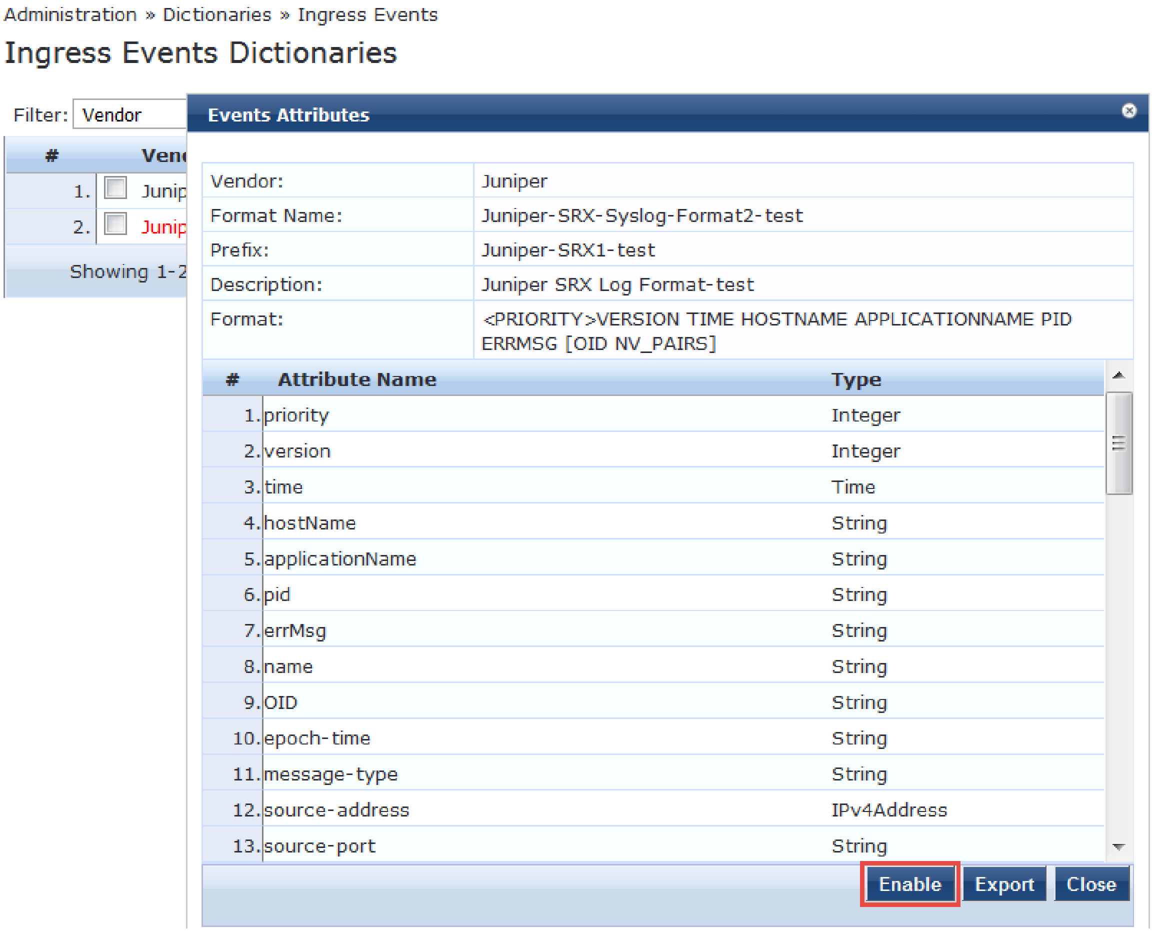
#		Vendor	Format Name	Prefix	Enabled
1.	☑	Juniper	Juniper-SRX-Syslog-Format1	Juniper-SRX1	true

Showing 1-1 of 1

2. To enable a dictionary, select the Ingress Events Dictionary for the appropriate vendor.

   The **Events Attributes** dialog opens.

Figure 700: *Enabling an Ingress Events Dictionary*



Vendor:	Juniper
Format Name:	Juniper-SRX-Syslog-Format2-test
Prefix:	Juniper-SRX1-test
Description:	Juniper SRX Log Format-test
Format:	<PRIORITY>VERSION TIME HOSTNAME APPLICATIONNAME PID ERRMSG [OID NV_PAIRS]

#	Attribute Name	Type
1.	priority	Integer
2.	version	Integer
3.	time	Time
4.	hostName	String
5.	applicationName	String
6.	pid	String
7.	errMsg	String
8.	name	String
9.	OID	String
10.	epoch-time	String
11.	message-type	String
12.	source-address	IPv4Address
13.	source-port	String

3. To enable the selected ingress events dictionary, click **Enable**.

   You return to the Ingress Events Dictionaries page. The dictionary information is no longer displayed in red and the **Status** column is set to **Enabled**.

Configuring the Ingress Event Sources

The Event Source is the device that sends Syslog events to ClearPass. Any events sent that are not from configured event sources are ignored.

To configure the Event Source (in this example, a Juniper Networks SRX gateway):

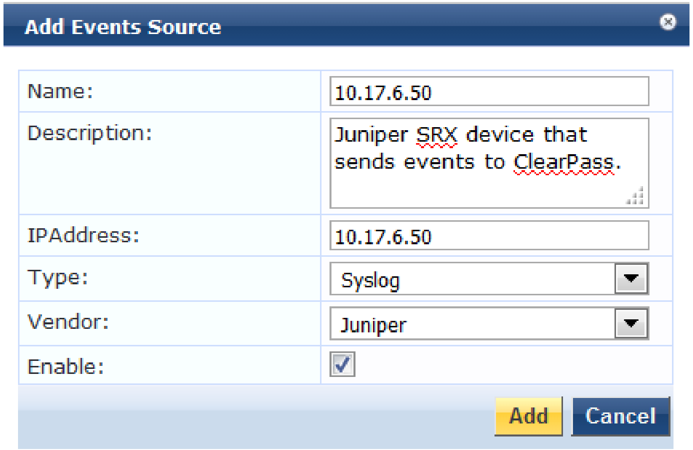
1. Navigate to **Configuration** > **Network** > **Event Sources**.

   The **Event Sources** page opens.

2. To add the Event Source for the desired vendor, click **Add**.

   The **Add Events Source** dialog opens.

Figure 701: *Adding an Event Source*



Add Events Source

Name:	10.17.6.50
Description:	Juniper SRX device that sends events to ClearPass.
IPAddress:	10.17.6.50
Type:	Syslog
Vendor:	Juniper
Enable:	☑

3. Specify the **Add Event Source** parameters as described in Table 371.

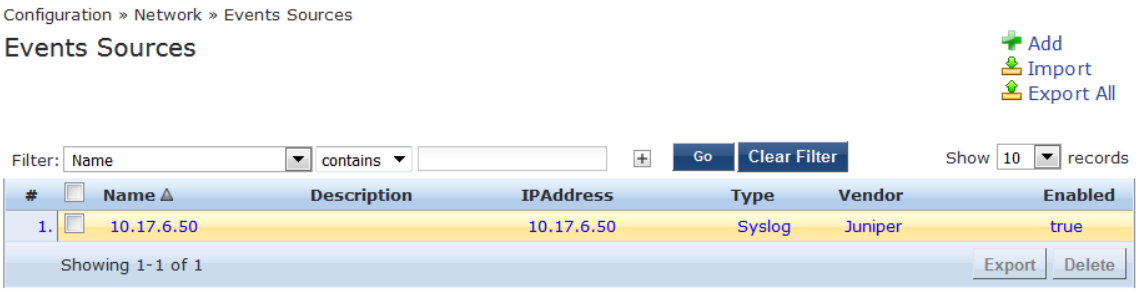
Table 371: *Configuring the Event Source Parameters*

Parameter	Action/Description
Name	1. Enter the IP address of the device that will send Syslog events to ClearPass.
Description	Optionally, enter a description of this Event Source.
IP Address	2. Enter the IP address of the device that will send Syslog events to ClearPass.
Type	3. From the drop-down, select the Event Source **Type**.
Vendor	4. From the drop-down, select the Event Source **Vendor**.
Enable	5. Select this check box to enable the device as an Event Source.

6. When finished, click **Add**.

   The **Event Sources** page now displays the new Event Sources (see Figure 702).

Figure 702: *Event Sources Page*



Configuration » Network » Events Sources

Events Sources

#	□	Name ▲	Description	IPAddress	Type	Vendor	Enabled
1.	□	10.17.6.50		10.17.6.50	Syslog	Juniper	true

Showing 1-1 of 1

The IP address displayed in Figure 702 is the IP address and host name of the Juniper SRX gateway that sends Syslog events to ClearPass.

Configuring the Ingress Receiving Ports

The ingress receiving ports are the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports on the ClearPass server where the events source sends threat-related events.

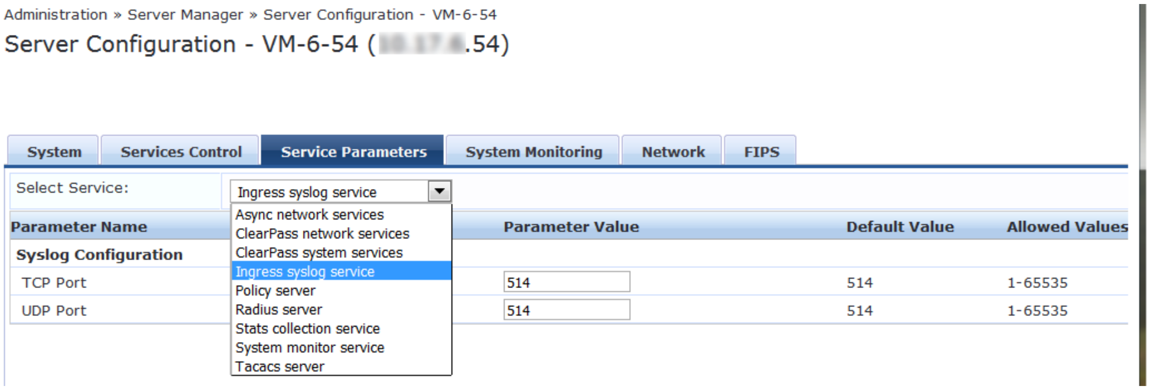
By default, the ingress receiving port is **514** for both TCP and UDP. You can modify the ingress receiving ports to a custom value as necessary.

To confirm or change the ingress receiving ports on the ClearPass server:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.
2. From the list of ClearPass servers, select the appropriate server.

   The Server Configuration page opens.
3. Select the **Service Parameters** tab.
4. From the **Select Service** drop-down, choose **Ingress syslog service** as shown in Figure 703.

Figure 703: *Selecting the Ingress Syslog Service*



Administration » Server Manager » Server Configuration - VM-6-54

Server Configuration - VM-6-54 ([redacted].54)

Select Service: Ingress syslog service

Parameter Name	Parameter Value	Default Value	Allowed Values
Syslog Configuration			
TCP Port	514	514	1-65535
UDP Port	514	514	1-65535

   As you can see in Figure 703, the parameter value for both the TCP and UDP receiving ports is set to the default value of **514**.
5. If you wish to modify the parameter values for one or both of the receiving ports, enter the new value(s).
6. When satisfied with the settings, click **Save**.

Configuring an Event-Based Enforcement Service

This section provides the following information:

- Introduction
- Adding an Event-Based Enforcement Service
- Associating the Enforcement Service with an Enforcement Policy

Introduction

This section describes how to add the **Event-Based Enforcement** service that manages enforcement actions in response to threat-event processing.

When there is a suspicious user, this user could represent a common DOS attack or some other threat. When a threat is detected, ClearPass performs enforcement operations as configured, for example, executing a change of authorization (COA) to disconnect a suspicious user from the network.

Adding an Event-Based Enforcement Service

To add an event-based enforcement service:

1. Navigate to **Configuration** > **Services**.

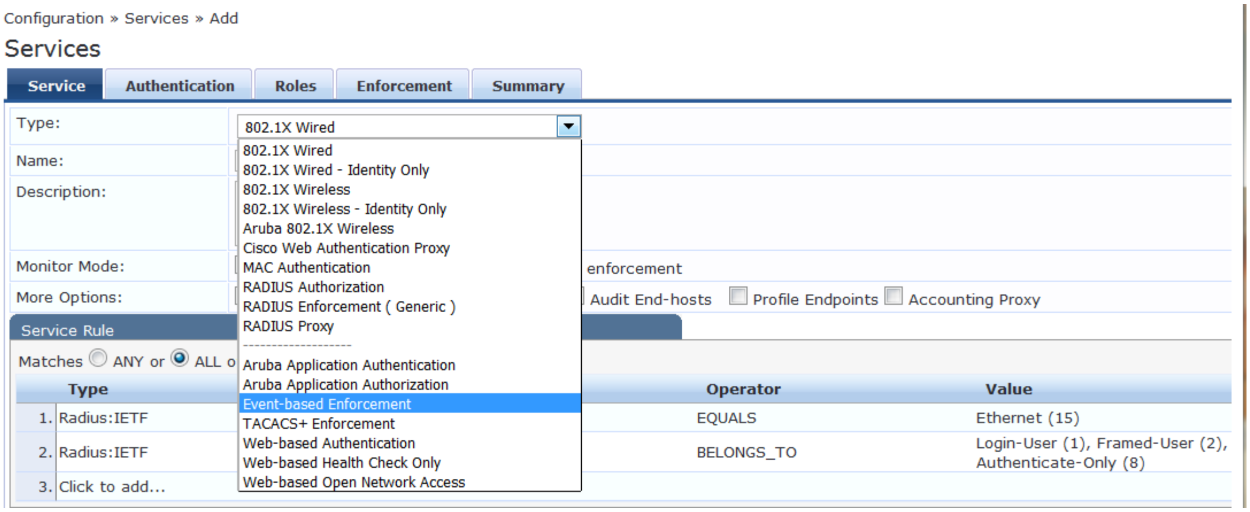
   The **Services** page opens. The **Services** page provides options to add, modify, and remove a service.

2. To add the event-based enforcement service, click **Add**.

   The **Add Services** dialog opens.

3. From the **Type** drop-down list, select **Event-based Enforcement** (see Figure 704).

Figure 704: *Specifying Event -Based Enforcement*



Configuration » Services » Add
Services
Service
Authentication
Roles
Enforcement
Summary
802.1X Wired
802.1X Wired - Identity Only
802.1X Wireless
802.1X Wireless - Identity Only
Aruba 802.1X Wireless
Cisco Web Authentication Proxy
MAC Authentication
RADIUS Authorization
RADIUS Enforcement (Generic)
RADIUS Proxy

Aruba Application Authentication
Aruba Application Authorization
Event-based Enforcement
TACACS+ Enforcement
Web-based Authentication
Web-based Health Check Only
Web-based Open Network Access
Service Rule

Type: 802.1X Wired

Name:

Description:

Monitor Mode: enforcement

More Options: Audit End-hosts □ Profile Endpoints □ Accounting Proxy

Matches ○ ANY or ● ALL o

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

For configuration information for each of the available service types, see Configuring Policy Manager Services on page 70.

4. Enter the name or label of the event-based enforcement service.

5. Enter the values for any other parameters, including service rules, required for this service.

   For a description of all the parameters in the **Service** page, see Adding Services on page 1.

6. Click **Next**.

   The **Add Services** > **Enforcement** tab opens.

Associating the Enforcement Service with an Enforcement Policy

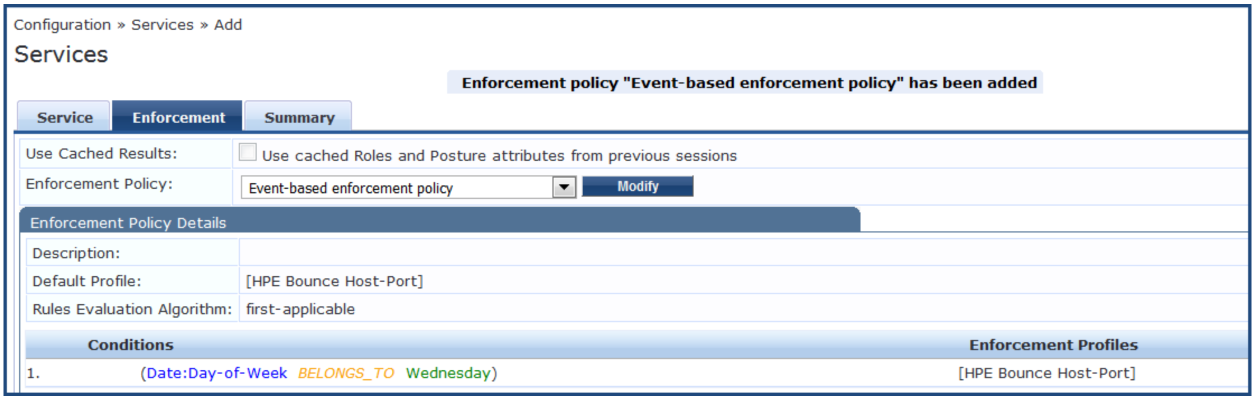
After you create the event-based enforcement service, you must associate the service with an enforcement policy.

To associate an event-based enforcement server with an enforcement policy:

1. When finished with the parameter settings on the **Add Services** > **Service** page, click **Next**.

   The **Add Services** > **Enforcement** page opens.

Figure 705: *Specifying the Event-Based Enforcement Policy*



Configuration » Services » Add

Services

Enforcement policy "Event-based enforcement policy" has been added

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Event-based enforcement policy ▾ Modify

Enforcement Policy Details

Description:	
Default Profile:	[HPE Bounce Host-Port]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Date:Day-of-Week BELONGS_TO Wednesday)	[HPE Bounce Host-Port]

From the **Add Services** > **Enforcement** page, you can either select an existing enforcement policy or create a new one.

2. From the **Enforcement Policy** drop-down list, select the appropriate Event Enforcement policy.
3. If you have not configured Event-type Enforcement policies, click **Add New Enforcement Policy** to create a new enforcement policy.
4. Specify the values for the remaining parameters as described in Table 372, then click **Save**.

Table 372: *Service Enforcement Page Parameters*

Parameter	Action/Description
Use Cached Results	1. Select this check box to use cached roles and posture attributes from previous sessions.
Enforcement Policy	2. From the drop-down list, select the preconfigured enforcement policy. This is mandatory.
Enforcement Policy Details	
Description	Displays additional information about the selected enforcement policy.
Default Profile	Displays a default profile applied by .
Rules Evaluation Algorithm	Shows first matched rule and return the role or select all matched rules and return a set of roles.

Enabling Ingress Events Processing

The final task is to enable ingress events processing.

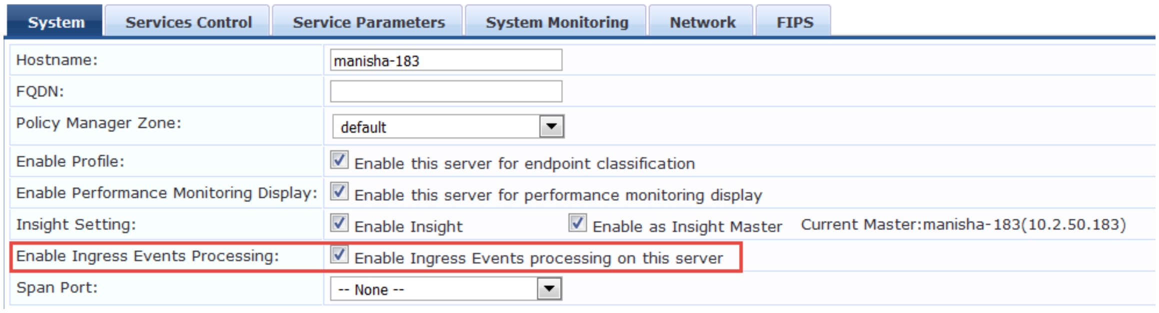
To enable ingress events processing on the ClearPass server:

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.
2. From the list of ClearPass servers, select the appropriate server.

   The **Server Configuration** page appears.
3. Select the appropriate server.

   The **Server Configuration** dialog appears.

Figure 706: *Enabling Ingress Event Processing*

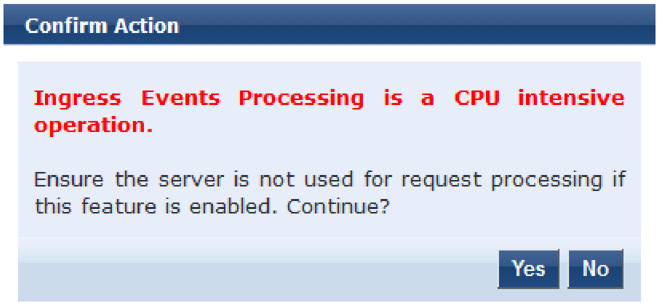


Hostname:	manisha-183
FQDN:	
Policy Manager Zone:	default
Enable Profile:	☑ Enable this server for endpoint classification
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	☑ Enable Insight ☑ Enable as Insight Master Current Master:manisha-183(10.2.50.183)
Enable Ingress Events Processing:	☑ Enable Ingress Events processing on this server
Span Port:	-- None --

4. Click the **Enable Ingress Events Processing** check box.

   The following warning dialog is displayed, alerting you to the impact on system performance that may occur when you enable ingress events processing.

Figure 707: *Warning Dialog for Enabling Ingress Events Processing*


Confirm Action

Ingress Events Processing is a CPU intensive operation.

Ensure the server is not used for request processing if this feature is enabled. Continue?

5. To proceed with ingress events processing on this server, click **Yes**.

   For details on the **Server Configuration** > **System Tab** parameters, see System Page on page 482.

ClearPass Insight Reports

This chapter describes how to use the ClearPass 6.6 Insight Reporting tool.

This chapter includes the following information:

- About ClearPass Insight
- About the Insight Dashboard
- Searching the Insight Database
- Creating Alerts
- Creating Reports
- Insight Report Categories Reference
- Administration Operations
- Managing Insight Admin Privileges

About ClearPass Insight

This section presents an overview of ClearPass Insight. It provides the following information:

- Introduction
- Enabling Insight and Specifying a Master Insight Node
- Launching Insight

Introduction

ClearPass Insight is an application for use with ClearPass Policy Manager that is capable of aggregating data from multiple Policy Manager appliances that contain archived network access logs.

You can access each application within the ClearPass suite with a single login. You need only sign in once for access to ClearPass Policy Manager, Insight, Onboard, and Guest. For more information, see Launching Insight below.

- Insight makes it easy to add many different types of report "widgets" that will produce reports that provide the specific kinds of information you need to monitor and understand what is occurring on the network. You can create customized reports to track detailed authentication records, audit trails, and details on network-access trends (see About the Insight Dashboard on page 713).
- The Insight Search feature allows you to search for clients, users, ClearPass servers, and network access devices (see Searching the Insight Database on page 724).
- This chapter illustrates how to generate customized reports that analyze authentication information, device profiling, client health and posture data, as well as guest and BYOD use cases (for details, see Creating Reports on page 732 and Insight Report Categories Reference on page 740).
- This chapter also describes how to configure alerts that allow you to receive near-real-time messages regarding anomalous network activity. Alerts can be delivered via SMS or email notification to multiple recipients.

  You can also set up a User Watchlist (a list of VIPs, executives or devices that warrant special tracking) that you can monitor for authentication failures or other key events (see Creating Alerts on page 725).
- Finally, this chapter provides information on how to configure operational elements about file transfers, as well as database and report data retention (see Administration Operations on page 755).

Browsers Supported

ClearPass Insight uses a Web-based management interface. The following browsers are supported:

- Apple Safari 6.2.x, 7.1.x, 8.0
- Google Chrome 47.x, 48.x
- Microsoft Edge 25.x
- Microsoft Internet Explorer 11.0
- Mozilla Firefox 43, 44

Enabling Insight and Specifying a Master Insight Node

Before you can use Insight, you must enable it on the current ClearPass server.

If multiple nodes in a cluster have Insight enabled, one node should be configured as an Insight Master.

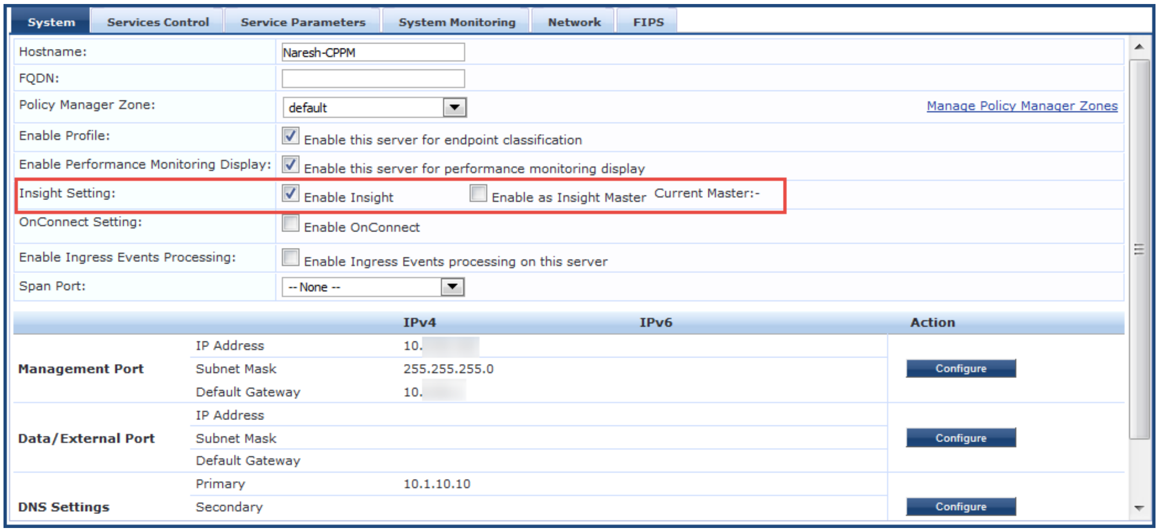
> NOTE
>
> Insight Reports, Alerts, and Administration settings can be configured on a Master Insight node only. To be able to generate a report, enabling the node as an Insight Master (even in a single-node cluster) is mandatory.

To enable Insight :

1. Navigate to **Administration** > **Server Manager** > **Server Configuration**.
2. From the list of ClearPass servers, click the server on which you want to enable Insight.

   The **Server Configuration** > **System** page opens.

Figure 708: *Server Configuration > System Page*



Hostname: Naresh-CPPM

FQDN:

Policy Manager Zone: default ▾ Manage Policy Manager Zones

Enable Profile: ☑ Enable this server for endpoint classification

Enable Performance Monitoring Display: ☑ Enable this server for performance monitoring display

Insight Setting: ☑ Enable Insight ☐ Enable as Insight Master Current Master:-

OnConnect Setting: ☐ Enable OnConnect

Enable Ingress Events Processing: ☐ Enable Ingress Events processing on this server

Span Port: -- None -- ▾

		IPv4	IPv6	Action
Management Port	IP Address	10.[redacted]		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	10.[redacted]		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
DNS Settings	Primary	10.1.10.10		Configure
	Secondary			

   a. **Enable Insight**: Select this check box to enable ClearPass Insight on the current server.

   b. **Enable as Insight Master**: Select this check box to specify this server as an Insight Master.

> NOTE
>
> To enable replication of Insight configurations across a cluster, you must configure one ClearPass server in the cluster as an Insight Master node.

3. Click **Save**.

Launching Insight

To launch ClearPass Insight:

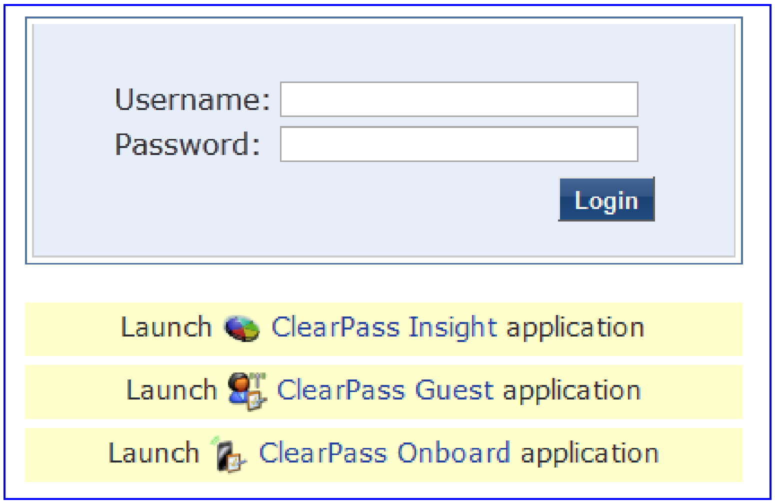
1. Use one of the following methods to launch ClearPass Insight.

- Log in to Policy Manager, and then select **Insight** in the **Dashboard > Applications** widget. This opens Insight in a new tab.
- Access Policy Manager by pointing the browser to https://<ClearPass-host-name>/tips, then select the **ClearPass Insight** link (see Figure 709).
- Point the browser to https://<ClearPass-host-name>/insight.

2. Enter the default username and password, then click **Login** to launch Insight.

   Figure 709 displays the ClearPass Access page:

Figure 709: *ClearPass Access Page*


Username:
Password:
Login
Launch ClearPass Insight application
Launch ClearPass Guest application
Launch ClearPass Onboard application

About the Insight Dashboard

This section provides the following information:

- Dashboard Overview
- Adding a Report Widget to the Dashboard Landing Page
- Removing a Report Widget from the Dashboard Landing Page
- Creating a Report or Alert From the Dashboard
- Specifying the Date Range for Data Collection
- Authentication Dashboard
- Endpoints Dashboard
- Guest Dashboard
- Network Dashboard
- Posture Dashboard
- System Dashboard
- System Monitor Dashboard

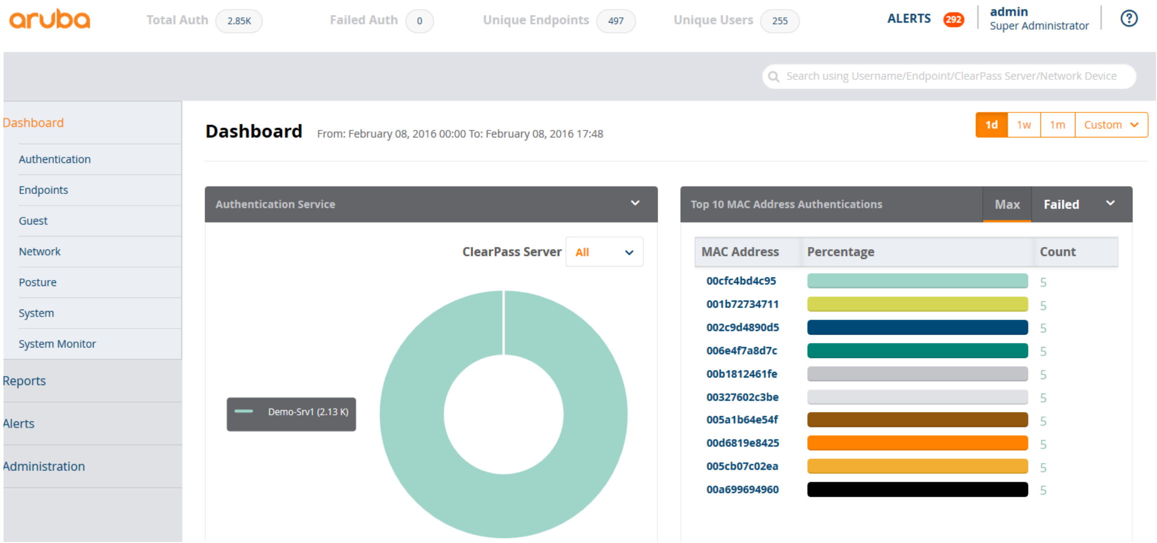
Dashboard Overview

The **Dashboard Landing Page** opens immediately when you successfully log in to ClearPass Insight. The Dashboard includes report widgets that provide a summarized and graphical view of your network analytics.

- You can customize the Dashboard to display the report widgets that you use most often by adding widgets to the Dashboard Landing Page; you can also remove any report widget from the Dashboard Landing Page as needed.

- You can create reports and alerts from any of the Dashboard pages.

Figure 710: *Insight Dashboard Landing Page*



Dashboard From: February 08, 2016 00:00 To: February 08, 2016 17:48

MAC Address	Percentage	Count
00cfc4bd4c95	▇	5
001b72734711	▇	5
002c9d4890d5	▇	5
006e4f7a8d7c	▇	5
00b1812461fe	▇	5
00327602c3be	▇	5
005a1b64e54f	▇	5
00d6819e8425	▇	5
005cb07c02ea	▇	5
00a699694960	▇	5

The following report widgets are included by default on the **Dashboard Landing** page:

- Authentication Trend
- Authentication Distribution
- Authentication Service
- Top 10 MAC Address Authentications

Adding a Report Widget to the Dashboard Landing Page

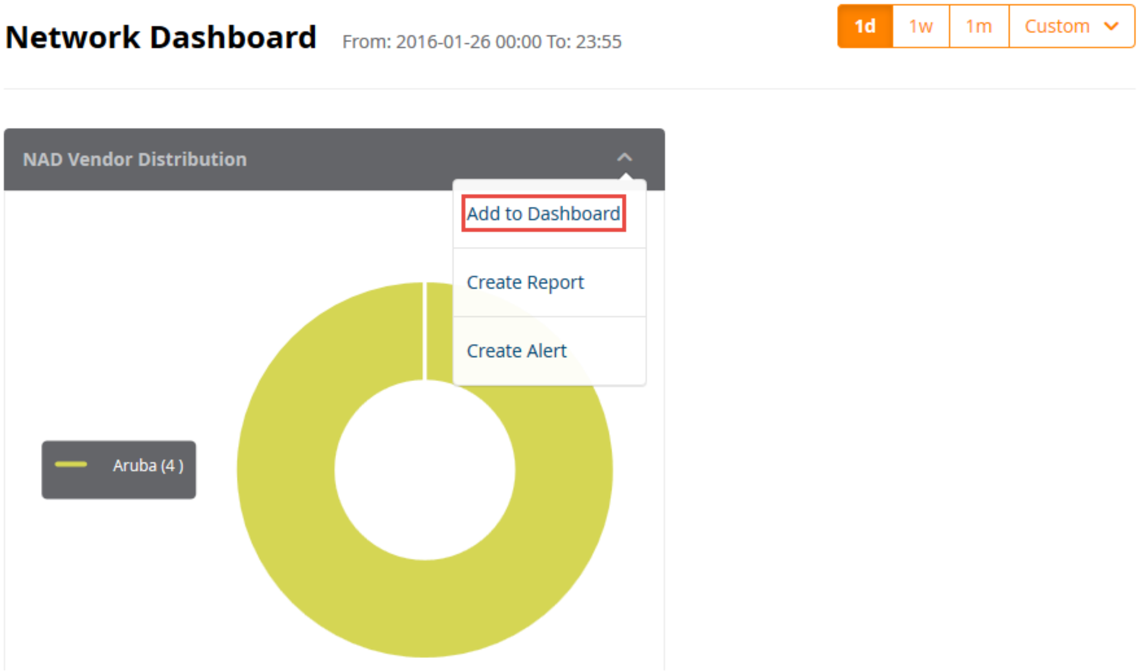
When you add a report widget to the Dashboard Landing page, that widget will appear in the Landing page, and the widget will also continue to be available on its Dashboard category page (for example, if you added the **Top 10 Restarted Services** widget from the System Dashboard, the **Top 10 Restarted Services** widget would be present in both the Dashboard Landing page and the System Dashboard).

To add a report widget to the Dashboard Landing page:

1. From any of the Dashboard category pages, click the arrow icon in the right corner of the widget title bar.
2. Select **Add to Dashboard** (see Figure 711).

   That report widget will appear when you return to the Dashboard Landing page.

Figure 711: *Adding a Widget to the Dashboard Landing Page*



3. To view the newly-added widget, return to the Dashboard Landing page.

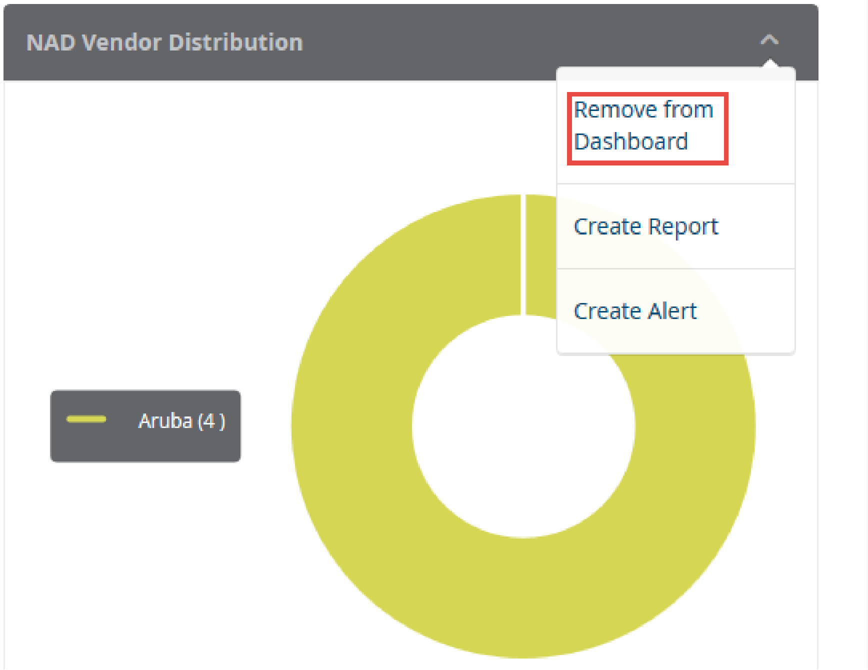
Removing a Report Widget from the Dashboard Landing Page

You can only remove a report widget from the **Dashboard Landing Page**. Report widgets cannot be deleted from Dashboard category pages (for example, if you choose to remove the Top 10 MAC Address Authentications widget from the Landing page, it will remain in the set of report widgets provided in the Authentication Dashboard).

To remove a report widget from the Dashboard Landing page:

1. From the **Dashboard Landing Page**, locate the widget you want to remove.
2. Click the arrow icon in the right corner of the widget title bar.
3. From the menu, select **Remove from Dashboard** (see Figure 712).

Figure 712: *Removing a Widget From the Dashboard*



When you refresh the page, that widget will disappear from the Dashboard.

Creating a Report or Alert From the Dashboard

The widgets on the **Dashboard** include links to the **Creat Reports** and **Create Alerts** pages.

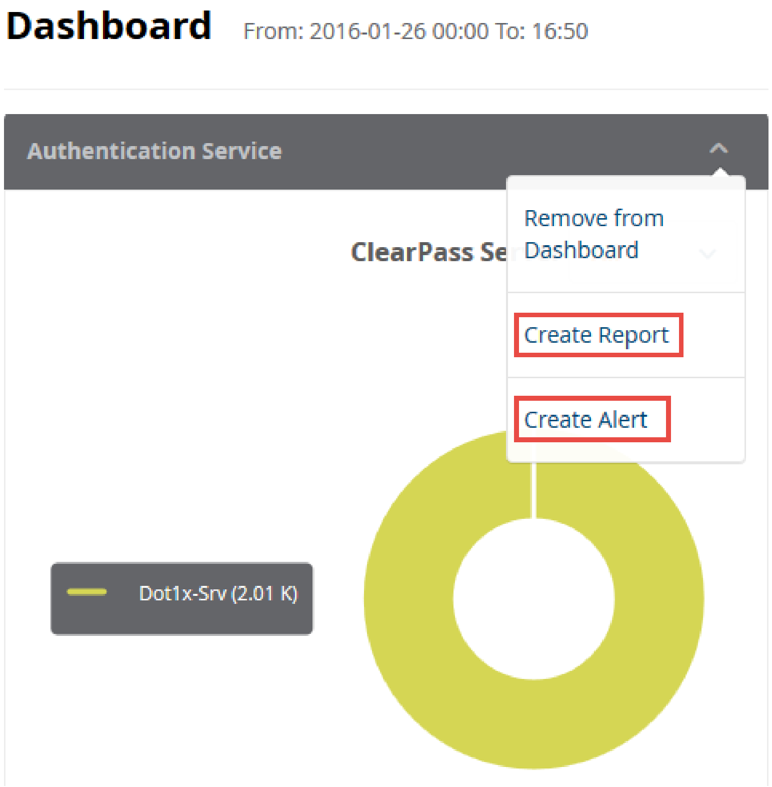
To define and to receive a regular report of data for that Dashboard:

- To open the **Create Reports** wizard from the Dashboard, click the down-arrow icon in the widget title bar and select **Create Report**.

To define and to receive alerts when customized thresholds are reached:

- To open the **Creat Alerts** wizard from the Dashboard, click the down-arrow icon in the widget title bar and select **Create Alert**.

Figure 713: *Opening the Reports or Alerts Wizard from the Dashboard*



For detailed procedures to create reports and alerts, see Creating Reports on page 732 and Creating Alerts on page 725.

Specifying the Date Range for Data Collection

By default, the Insight widgets, including those on the **Dashboard** page as well as all the other Insight widgets, such as Endpoints, Guest, Posture, and so on, display information collected over the previous seven days. The **System Monitor** widget is an exception as it displays data for the previous two hours.

You can modify the Authentication, Endpoints, Guest, Posture, and System widgets to display widget data for today, one week, one month, or a custom date and time range.

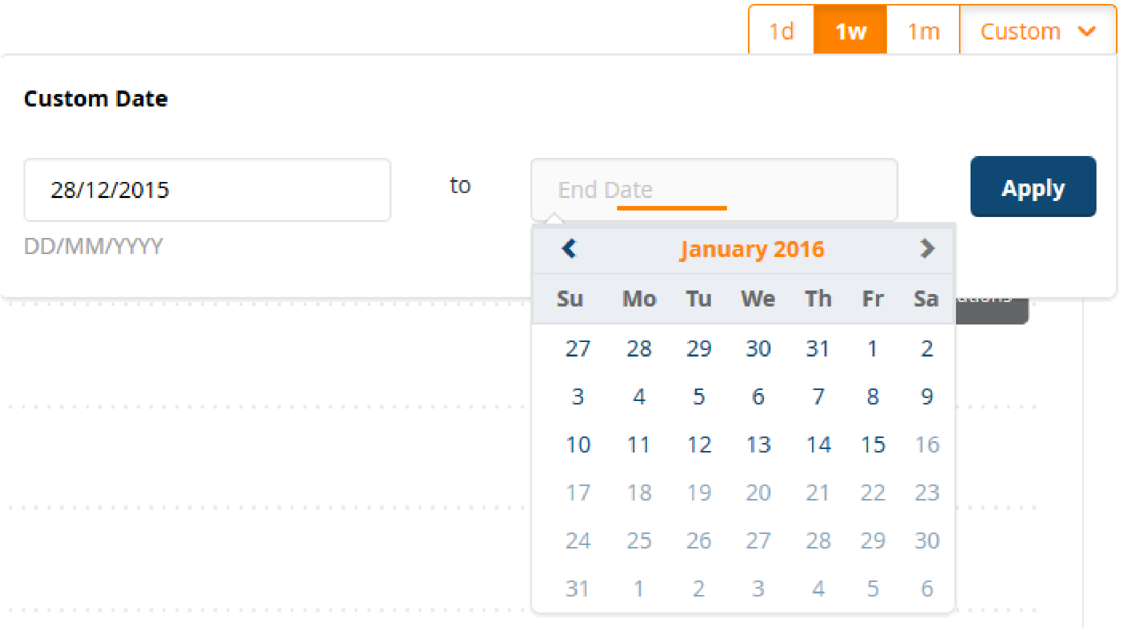
To specify the date range to have data collected for a Dashboard widget:

1. To specify data collection for today, one week, or one month, from the upper right corner of the Dashboard, select **Today**, **1w** (for one week), or **1m** (for one month) as desired.

   The Dashboard widgets then display the information for the specified number of days.
2. To specify a customized period for Insight data collection, click the **Custom** button.

   You are prompted to specify the start and end dates for your date range, as shown in Figure 714.

Figure 714: *Specifying a Custom Date Range*



28/12/2015

3. Select the **Start Date** and **End Date** from the calendar, then click **Apply**.

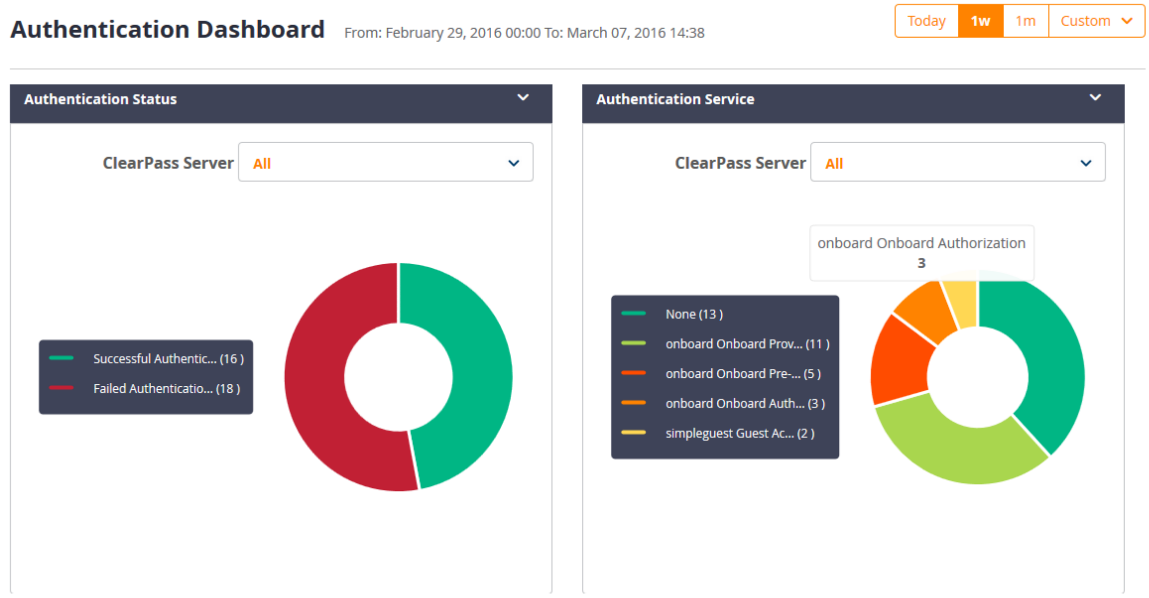
   The Dashboard widgets then display the information for the specified range of dates.

Authentication Dashboard

Authentication Dashboard widgets focus on authentication analytics and include widgets on trends, distribution, status, service, alerts, and statistics.

To access the Authentication Dashboard, navigate to **Dashboard** > **Authentication**.

Figure 715: *Authentication Dashboard*


Authentication Dashboard
From: February 29, 2016 00:00 To: March 07, 2016 14:38
Today
1w
1m
Custom
Authentication Status
ClearPass Server
All
Successful Authentic... (16)
Failed Authenticatio... (18)
Authentication Service
ClearPass Server
All
onboard Onboard Authorization
3
None (13)
onboard Onboard Prov... (11)
onboard Onboard Pre-... (5)
onboard Onboard Auth... (3)
simpleguest Guest Ac... (2)

The following widgets are included by default on the **Authentication Dashboard:**

- Authentication Trend
- Authentication Distribution

- Authentication Service
- Authentication Status
- Top 10 MAC Address Authentications
- Top 20 NAD Authentications
- Top 10 Authentication Errors
- Latest 10 Authentication Alerts

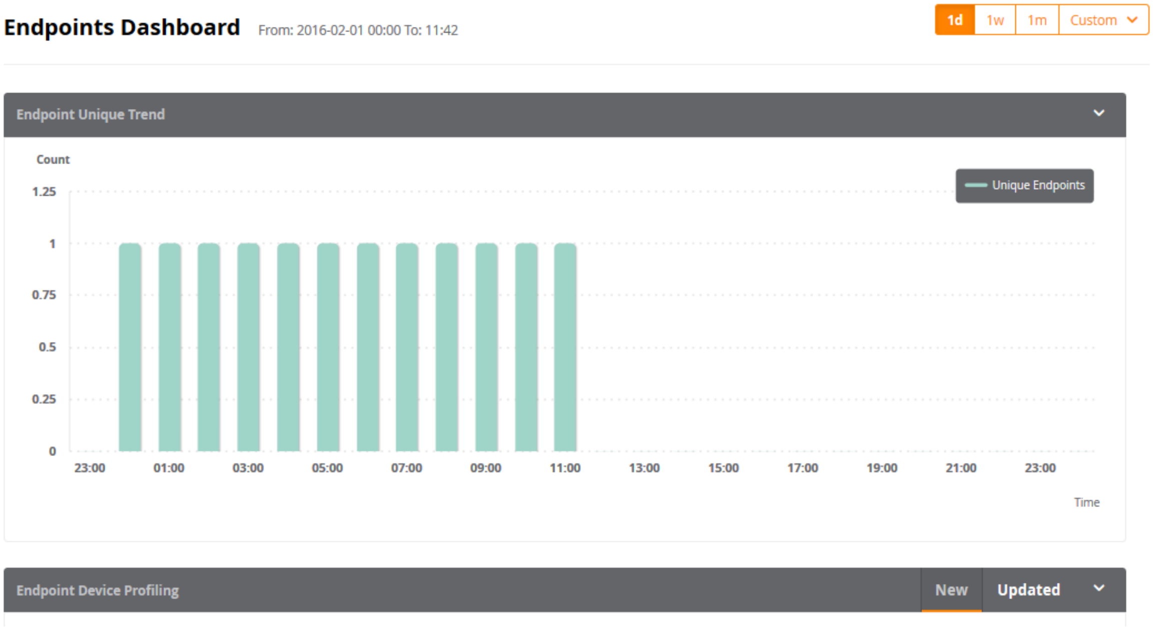
For more information about the Authentication reports and the widgets provided for each report, see Authentication Category Reports on page 740.

Endpoints Dashboard

The Endpoints Dashboard widgets provide analytics that focus on Endpoint trends, distribution, device profile, and bandwidth usage.

To access the Authentication Dashboard, navigate to **Dashboard** > **Endpoints**.

Figure 716: *Endpoints Dashboard*



The following widgets are included by default on the **Endpoints Dashboard:**

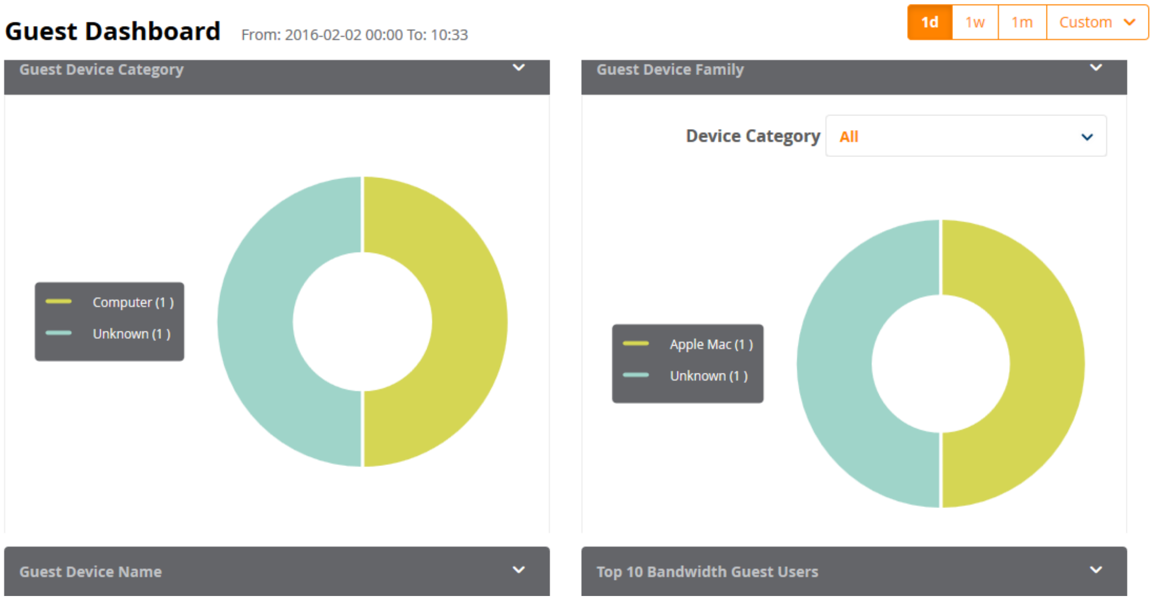
- Authentication Trend
- Authentication Distribution
- Authentication Service
- Top 10 MAC Address Authentications

For more information about the Authentication reports and the widgets provided for each report, see Authentication Category Reports on page 740.

Guest Dashboard

To access the Guest Dashboard, navigate to **Dashboard** > **Guest**.

Figure 717: *Guest Dashboard*



Guest Dashboard From: 2016-02-02 00:00 To: 10:33

The following widgets are included by default on the **Guest Dashboard**:

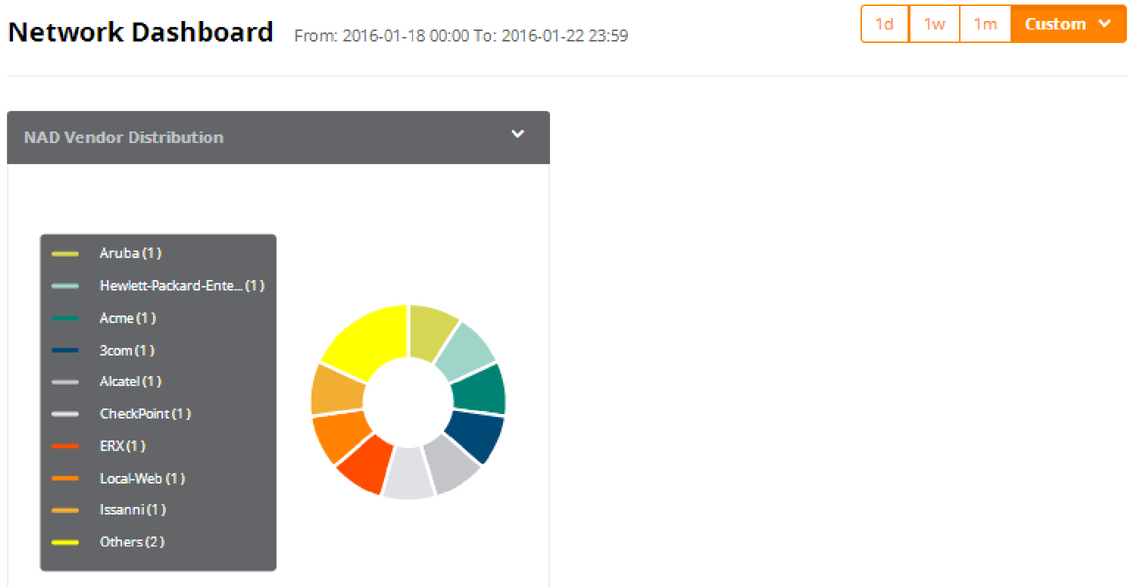
- Guests Authentication Trend
- Unique Guest Authentication
- Guests Provisioned
- Guest Device Category
- Guest Device Family
- Guest Device Name
- Top 20 Bandwidth Guest Users

For more information about the Guest reports and the widgets provided for each report, see Guest Authentication Category Reports on page 744.

Network Dashboard

To access the Network Dashboard, navigate to **Dashboard** > **Network**.

Figure 718: *Network Dashboard: NAD Vendor Distribution*



Network Dashboard From: 2016-01-18 00:00 To: 2016-01-22 23:59

The following widget is included on the **Network Dashboard**:

- NAD Vendor Distribution

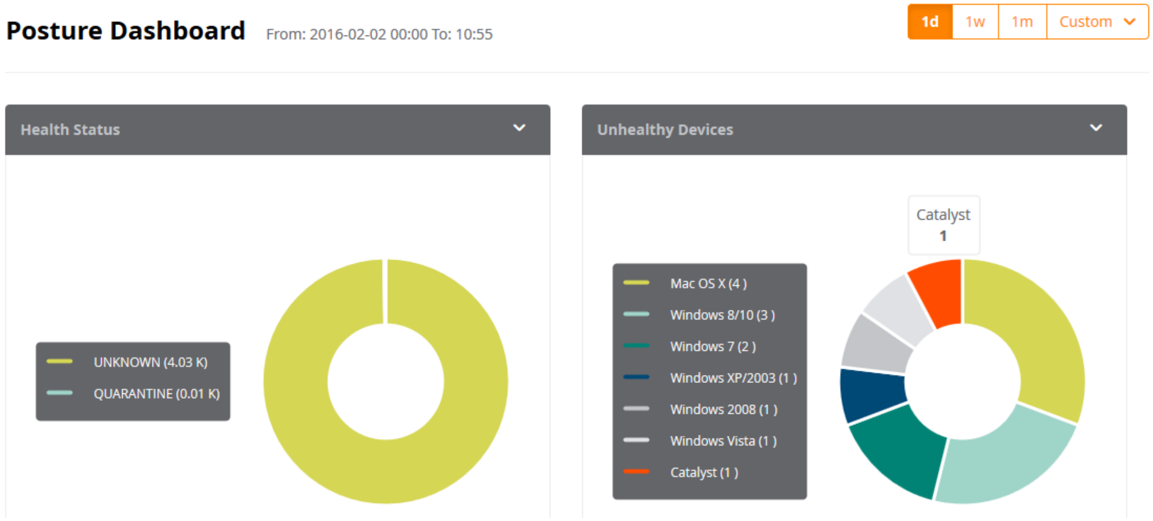
  This widget displays the list of all the NAD (Network Access Device) vendors, including the number of NADs by each vendor. Each vendor is associated with a unique color, and those colors are reflected in the circle graph that displays the distribution percentage each NAD vendor represents.

For more information about the Network reports, see Network Category Reports on page 746.

Posture Dashboard

The Posture Dashboard widgets focus on device health status and device profiles. To access the Posture Dashboard, navigate to **Dashboard** > **Posture**.

Figure 719: *Posture Dashboard*



Posture Dashboard From: 2016-02-02 00:00 To: 10:55

The following widgets are included by default on the **Posture Dashboard**:

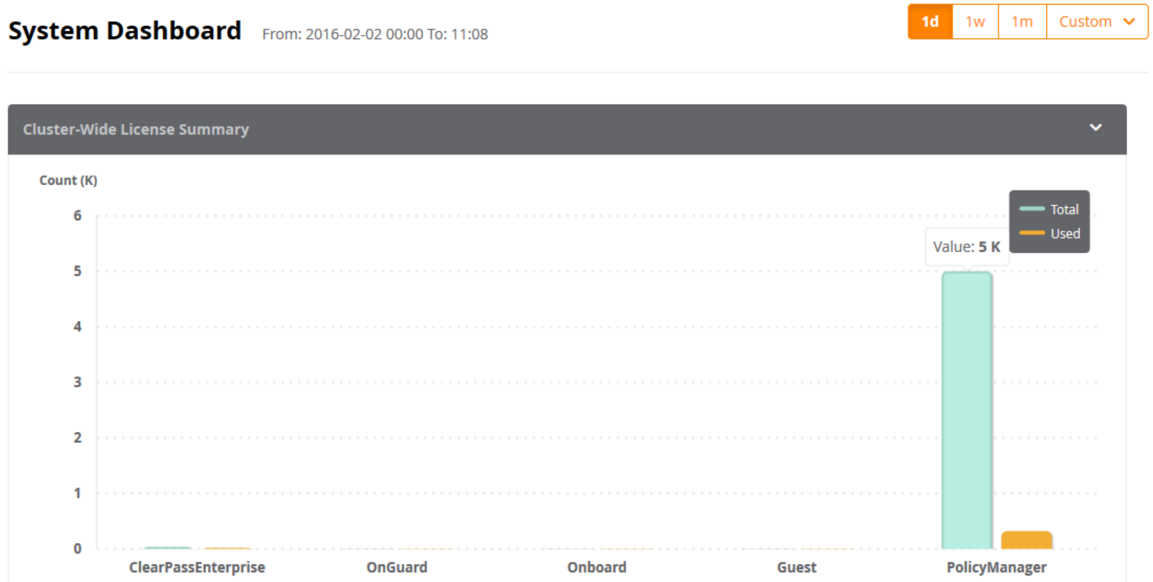
- Health Status
- Unhealthy Devices

For more information about the Posture-related reports, see OnGuard Category Reports on page 748.

System Dashboard

To access the System Dashboard, navigate to **Dashboard** > **System**.

Figure 720: *System Dashboard*



The following widgets are included by default on the **System Dashboard**:

- Cluster-Wide License Summary
- Policy Manager License Usage
- Guest License Usage Trend
- Top 10 Restarted Services

For more information about the System-related reports, see System Category Reports on page 753.

System Monitor Dashboard

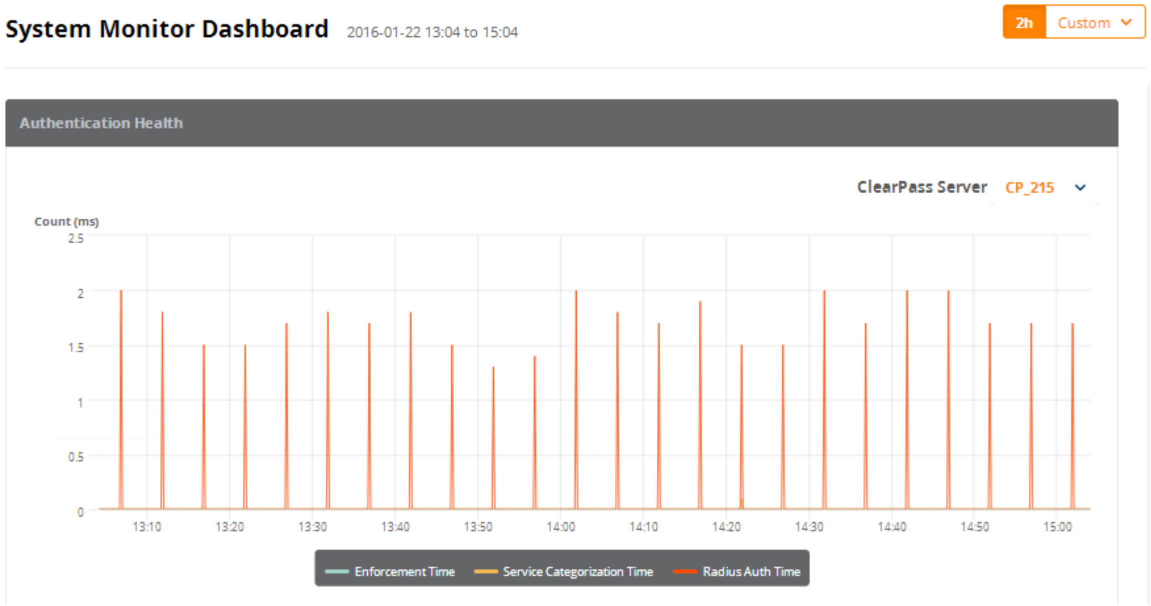
The System Monitor Dashboard widgets focus on health, including Authentication health, processing time, and CPU, memory, and disk usage.

NOTE

You cannot pin System Monitor widgets to the Dashboard.

To access the System Monitor Dashboard, navigate to **Dashboard** > **System Monitor**.

Figure 721: *System Monitor Dashboard*



The following widgets are included by default on the **System Monitor Dashboard**:

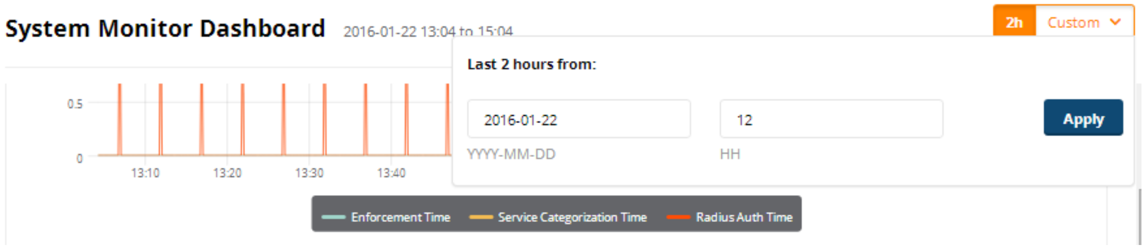
- Authentication Health
- End-to-End Request Processing Time
- Memory Usage
- Swap Memory Usage
- Disk Usage
- CPU Usage
- CPU Load

The **System Monitor** Dashboard differs from the other Dashboard pages in that it can show data for two hours only (**2h**).

To define a custom two-hour time slot:

1. Click the **Custom** drop-down list.

Figure 722: *Specifying the Hour to Start System Monitor Scan*



Last 2 hours from:

2016-01-22
YYYY-MM-DD

12
HH

2. Select the starting date.
3. Click the **HH** field, then use the up- and down-arrows to specify the hour to start the system monitor scan.

   For example, specifying **13** in the **HH** field indicates that the start time for the two-hour period is **1:00 p.m**.
4. Click **Apply**.

Searching the Insight Database

This section provides the following information:

- About Insight Search
- Search Example

About Insight Search

Use the **Insight Search** feature to query the Insight database.

You can search for the following entities:

- Endpoint IP address (Framed-IP-Address)
- Clients by MAC address, hostname, or IP address
- User name
- ClearPass servers by name or IP address
- Network access devices by name or IP address

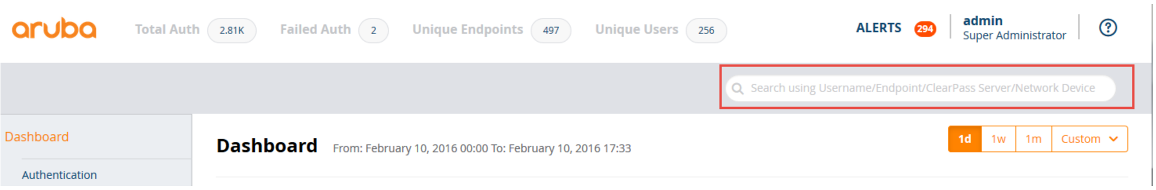
You can add clients and users to the Watchlist from Search results. For details, see Adding or Removing Users from the Watchlist on page 730.

The Insight Search window is always available at the top of every page.

NOTE

Search works on all pages except the Report Configuration and Alert Configuration pages.

Figure 723: *Search Window*



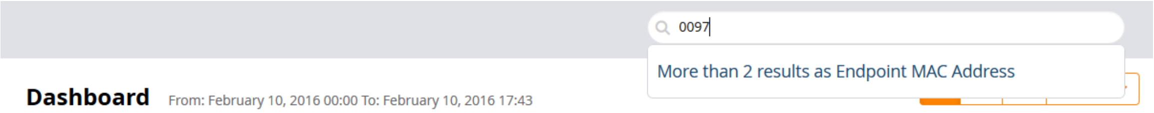
Search Example

Let's take the example of searching for a MAC address:

1. Start entering the MAC address into the Search window.

   As you type in the MAC address in this example, Search discovers that there are two MAC addresses with the same initial characters:

Figure 724: *Search Locating Matching Entities*


0097
More than 2 results as Endpoint MAC Address
Dashboard
From: February 10, 2016 00:00 To: February 10, 2016 17:43

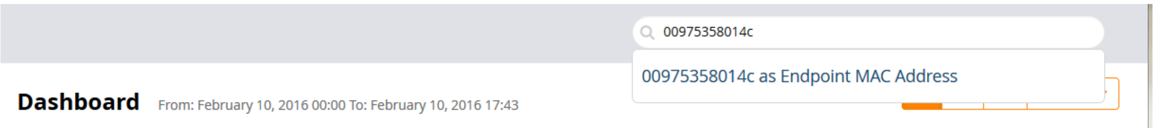
2. To locate the desired MAC address:

   a. Click on the suggestion and see which MAC address you are looking for from the list displayed.

   b. Or refine your search by typing more characters to further specify the search entity.

   In this example, the MAC address is identified as an Endpoint.

Figure 725: *Locating and Identifying the Search Object*



00975358014c

00975358014c as Endpoint MAC Address

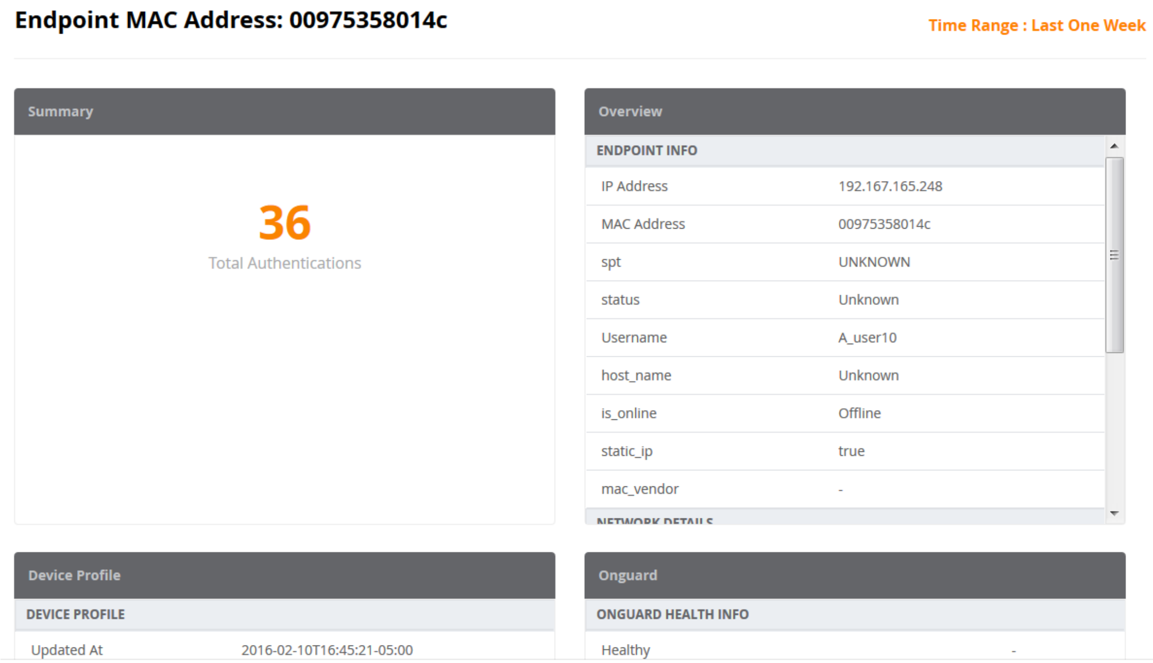
Dashboard From: February 10, 2016 00:00 To: February 10, 2016 17:43

3. Select the search object.

   The Endpoint MAC Address report is automatically displayed (see Figure 726). It includes the following information about the Endpoint:

   - Summary
   - Overview
   - Device Profile
   - OnGuard Health Information
   - Authentication Status Trend

Figure 726: *Report of Search Result*



Endpoint MAC Address: 00975358014c

Time Range : Last One Week

Summary

36

Total Authentications

Overview

ENDPOINT INFO

IP Address	192.167.165.248
MAC Address	00975358014c
spt	UNKNOWN
status	Unknown
Username	A_user10
host_name	Unknown
is_online	Offline
static_ip	true
mac_vendor	-

NETWORK DETAILS

Device Profile

DEVICE PROFILE

Updated At	2016-02-10T16:45:21-05:00

Onguard

ONGUARD HEALTH INFO

Healthy	-

Creating Alerts

This section provides the following information:

- Introduction
- Creating New Alerts
- Modifying the User Watchlist
- Adding or Removing Users from the Watchlist

Introduction

Alerts provide network managers with near-real-time messages on anomalous network activity. Such activity could consist of:

- Irregular authentication activity

- Irregular network device access activity
- Users attempting privileged commands on network devices
- Irregular activity on the ClearPass servers

Reports and alerts include templates for easy configuration. These templates allow you to quickly configure and monitor network activity. In addition to email notifications, you can also send alerts to mobile devices via SMS, providing the capability to receive mission-critical information on the go.

NOTE

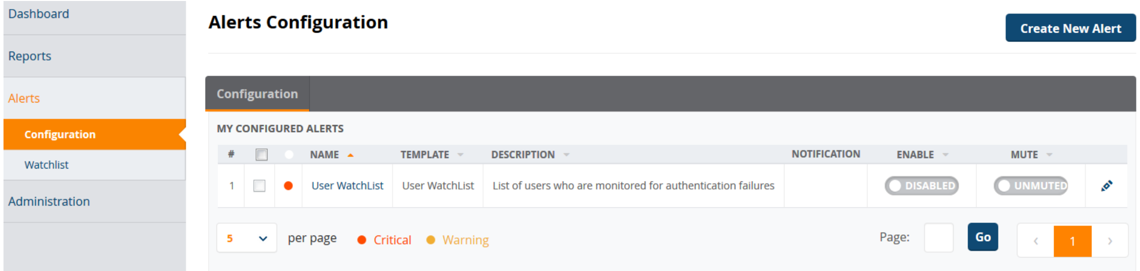
Any Error-level System Event/Event Viewer entries in ClearPass servers are notified with a System Alert Notification.

Creating New Alerts

To create a new alert:

1. Navigate to the **Alerts** page.

Figure 727: *Alerts Configuration Page*



Alerts Configuration

MY CONFIGURED ALERTS

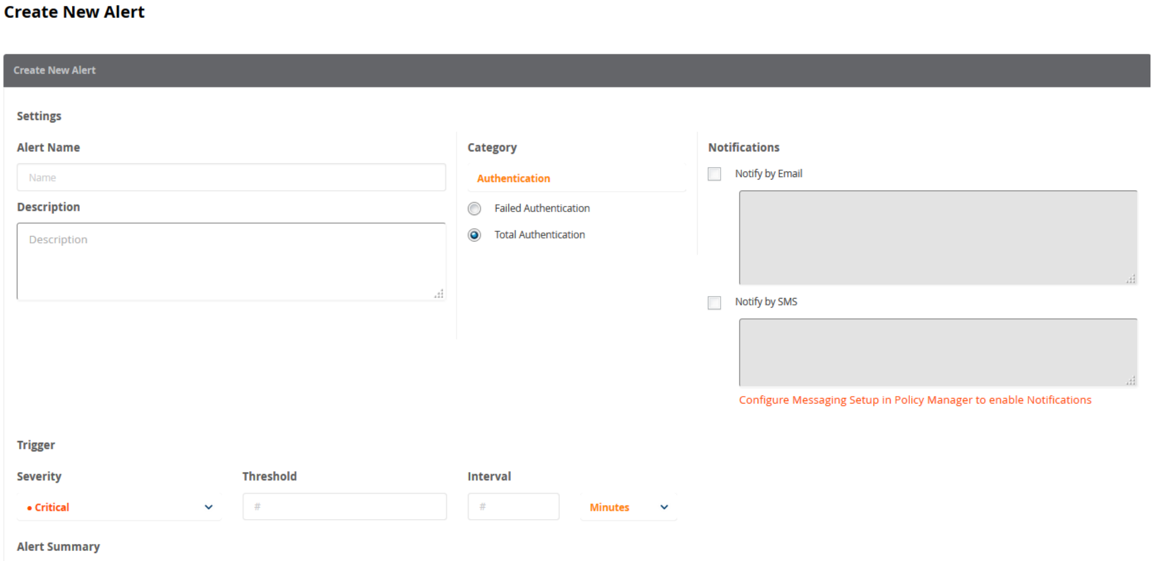
#	☐	●	NAME	TEMPLATE	DESCRIPTION	NOTIFICATION	ENABLE	MUTE	
1	☐	●	User WatchList	User WatchList	List of users who are monitored for authentication failures		DISABLED	UNMUTED	

5 per page ● Critical ● Warning Page: Go ‹ 1 ›

   - **Enable** button: From the switch, you can enable or disable the selected alert.
   - **Mute** button: Allows you to mute alert output while you work to address the alert.

2. Click **Create New Alert**.

Figure 728: *Creating a New Alert*



Create New Alert

Create New Alert

Settings

Alert Name: Name

Description: Description

Category

Authentication

○ Failed Authentication

● Total Authentication

Notifications

☐ Notify by Email

☐ Notify by SMS

Configure Messaging Setup in Policy Manager to enable Notifications

Trigger

Severity	Threshold	Interval	
• Critical	#	#	Minutes

Alert Summary

3. Enter the information for each Alert parameter as described in Table 373.

Table 373: *Create New Alert Parameters*

Alert Field	Action/Description
Alert Name	1. Enter the name of the alert.
Description	2. Optionally, enter a summary description of the alert.
Category	3. Select the alert **Category**, then specify the desired alert type in the selected category: ■ Authentication a. Failed Authentication b. Total Authentication ■ System ■ TACACS a. TACACS Commands b. TACACS Failures
Notifications	4. Specify report notifications. ■ **Notify by Email**. When you select this option, enter the list of email addresses to be notified. The alert notification is sent whenever the trigger threshold is met. **NOTE:** Enabling **Notify by Email** is mandatory. ■ **Notify by SMS**. When you select this option, enter the phone numbers of each recipient. The alert notification is sent whenever the trigger threshold is met. **NOTE:** A warning message appears if you have not configured the SMTP mail server for email notifications. To do so, from the Policy Manager, navigate to **Administration** > **External Servers** > **Messaging Setup**.
Trigger Severity	5. From the **Trigger Severity** drop-down, select one of the following: ■ **Critical** ■ **Warning**
Trigger Threshold	6. Specify **Threshold** and **Interval** values as criteria for determining whether an alert is necessary. For example, if you specify the **threshold** as **25** and the **interval** as **15 minutes**, once the threshold of 25 is met within 15 minutes, an alert is triggered.
Trigger Interval	7. Specify the **Interval**, then select **Minutes** or **Hours**.
Alert Summary	When you have configured the alert settings, the **Alert Summary** displays the settings for your review.
	8. Click **Save**.

Modifying the User Watchlist

A Watchlist is a list of VIPs, executives, and devices known to be problematic that are monitored for authentication failures. ClearPass collects all user authentication status.

When ClearPass finds a user defined in the Watchlist that both fails to authenticate and also matches the Watchlist triggers (severity, threshold, and interval), an alert notification is sent to the notification list via email or to mobile devices via SMS. This allows the authentication failure to be resolved proactively before the problem is reported by the user.

The Watchlist generates an alert only when an unsuccessful authentication for a specific device occurs.

Default Watchlist Trigger Settings

The default Watchlist trigger settings are as follows:

- **Severity** = Critical
- **Threshold** = 1
- **Interval** = 30 seconds

NOTE

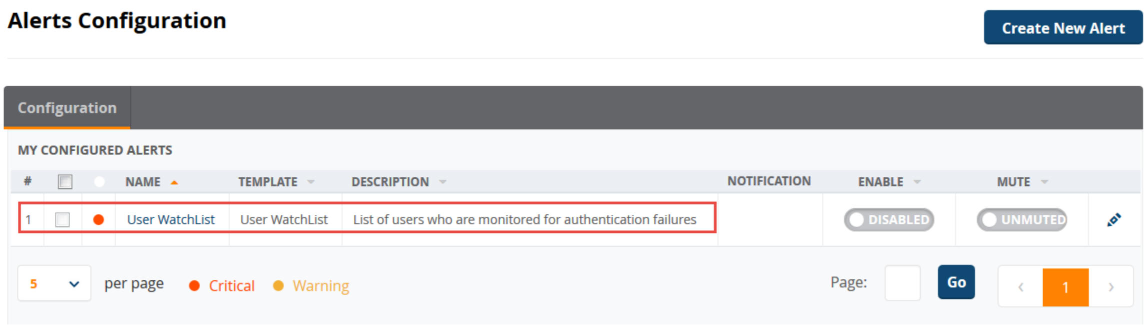
You cannot edit the The Watchlist trigger settings.

To modify the User Watchlist:

1. From the Insight navigation panel, choose **Alerts**, then select **Watchlist**.

   The **User Watchlist** opens (see Figure 729).

Figure 729: *User Watchlist*



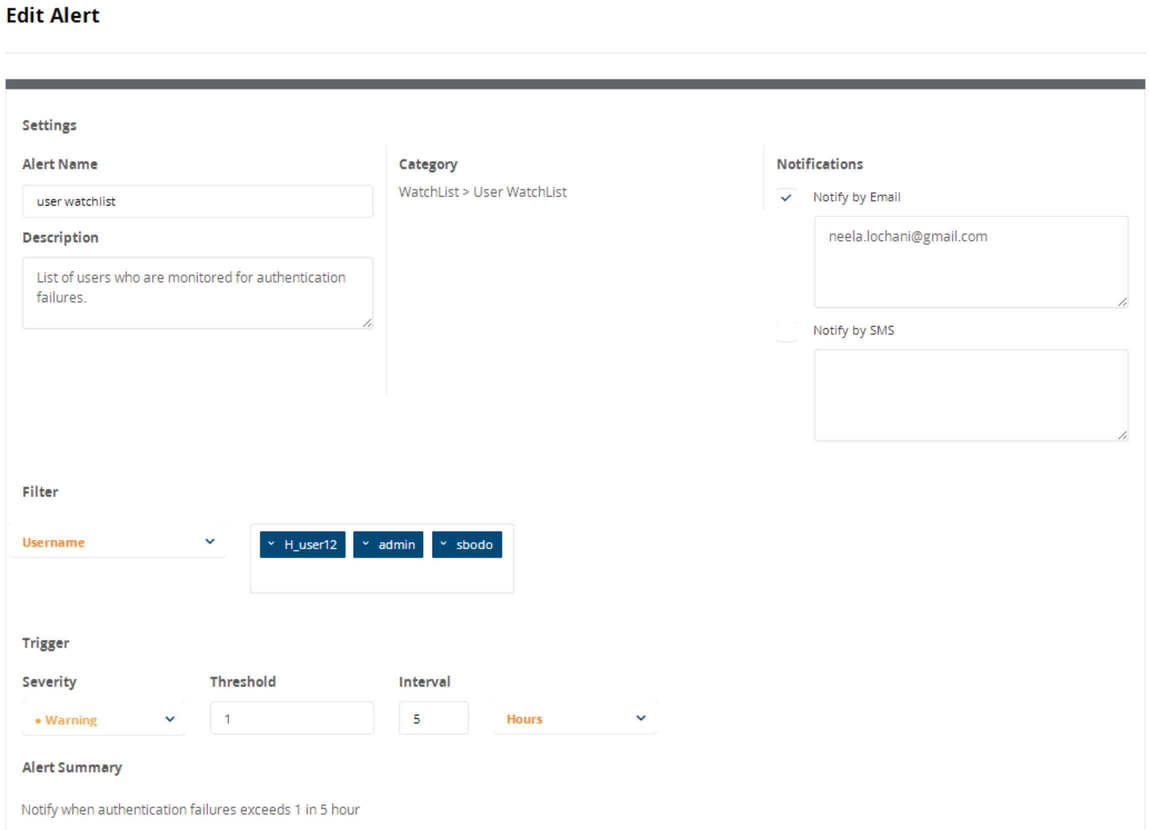
#	□	○	NAME	TEMPLATE	DESCRIPTION	NOTIFICATION	ENABLE	MUTE
1	□	●	User WatchList	User WatchList	List of users who are monitored for authentication failures		DISABLED	UNMUTED

   The users who are currently on the Watchlist are displayed. By default, the User Watchlist includes the **Authentication Trend** report widget.

2. Click **Modify Watchlist**.

   The **Edit Alert** page appears.

Figure 730: *Modifying the User Watchlist*



Edit Alert

Settings

Alert Name: user watchlist

Description: List of users who are monitored for authentication failures.

Category: WatchList > User WatchList

Notifications

☑ Notify by Email: neela.lochani@gmail.com

☐ Notify by SMS

Filter

Username: H_user12, admin, sbodo

Trigger

Severity: Warning

Threshold: 1

Interval: 5 Hours

Alert Summary

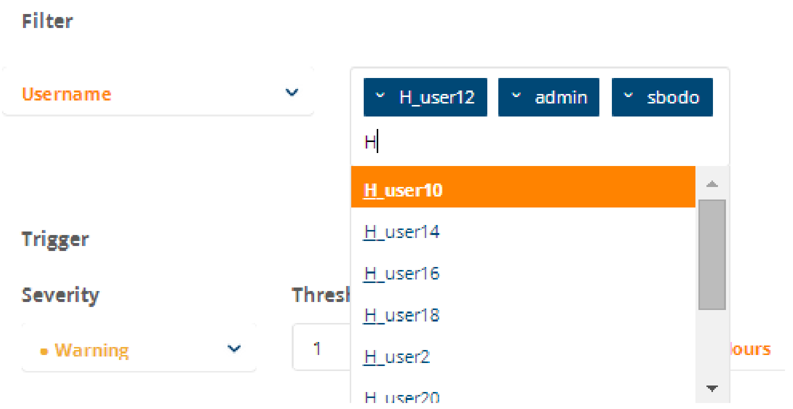
Notify when authentication failures exceeds 1 in 5 hour

3. Enter the desired settings for each **User Watchlist** parameter as described in Table 374.

Table 374: *Modify User Watchlist Parameters*

Alert Field	Action/Description
Alert Name	1. Optionally, you can modify the name of the User Watchlist.
Description	2. Optionally (and recommended), enter a summary description of the User Watchlist.
Category	The **Category** is set to **Alert** > **User Watchlist**. This is not an editable field.
Notifications	3. Specify Watchlist notifications. ■ **Notify by Email**. When you select this option, enter the list of email addresses to be notified. The alert notification is sent whenever the threshold is met. ■ **Notify by SMS**. When you select this option, enter the phone numbers of each recipient. An SMS message is sent with an alert notification whenever threshold is met. **NOTE:** A warning message appears if you have not configured the SMTP mail server for email notifications. To do so, navigate to **Administration** > **External Servers** > **Messaging Setup**.
Filter: Username	The User Watchlist has only one filter: **Username**. 4. From the Username drop-down, select one or more users to add to the Watchlist.

Table 374: *Modify User Watchlist Parameters (Continued)*

Alert Field	Action/Description
	 Filter Username: H_user12, admin, sbodo H H_user10 H_user14 H_user16 H_user18 H_user2 H_user20 Trigger Severity: Warning Threshold: 1 Hours
Alert Summary	When you have configured the Watchlist settings, the **Alert Summary** displays the settings for your review.
Save your changes	5. Click **Save**.

Adding or Removing Users from the Watchlist

You can use the Insight Search function to add users to or remove users from the Watchlist.

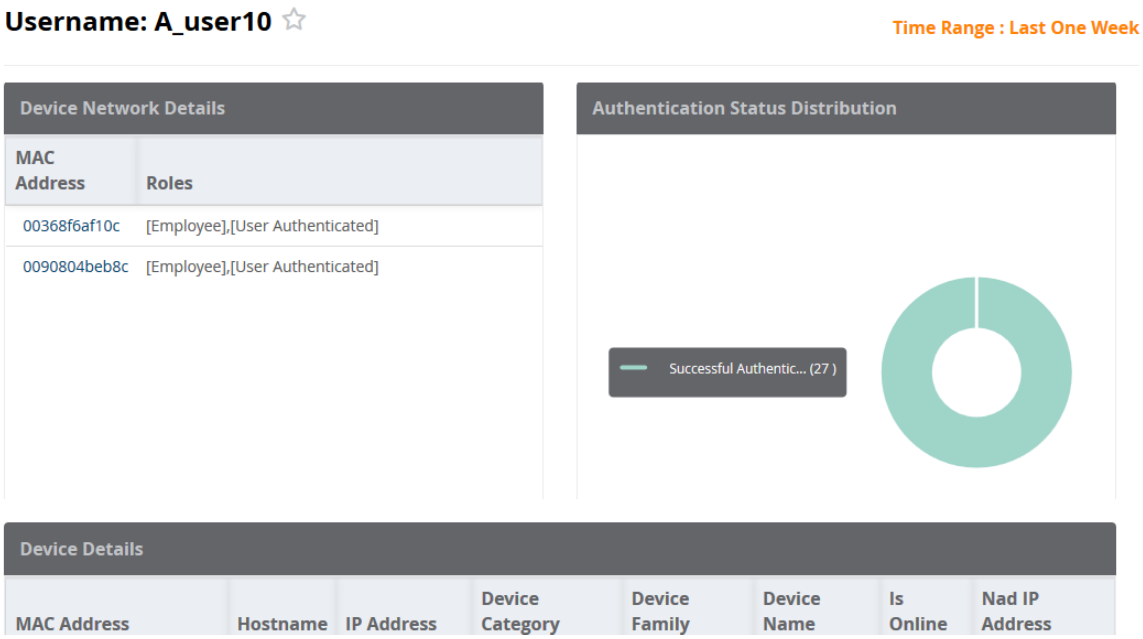
Adding a User to the Watchlist

To add a user to the Watchlist:

1. In the Insight Search window, enter the name of the user.

   The Insight **User Information** page for the selected user is displayed.

Figure 731: *Insight User Information Page*



Username: A_user10 ☆

Time Range : Last One Week

Device Network Details

MAC Address	Roles
00368f6af10c	[Employee],[User Authenticated]
0090804beb8c	[Employee],[User Authenticated]

Authentication Status Distribution

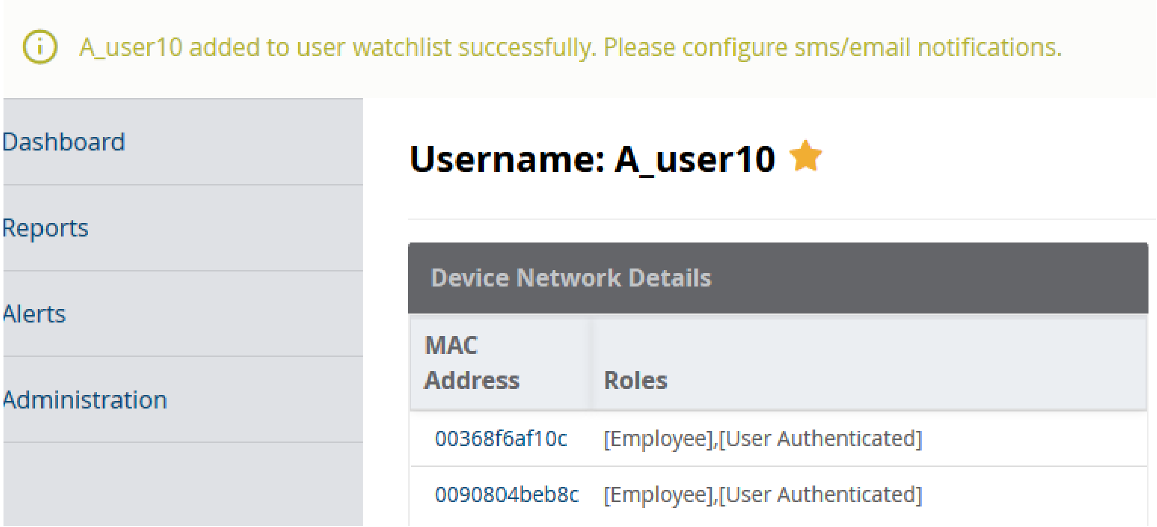
Device Details

MAC Address	Hostname	IP Address	Device Category	Device Family	Device Name	Is Online	Nad IP Address

2. To add a user to the Watchlist, click the star icon next to the username as shown in Figure 731.

The **User Information** page now displays the following information:

Figure 732: *User Successfully Added to Watchlist*



A_user10 added to user watchlist successfully. Please configure sms/email notifications.

Username: A_user10 ★

Device Network Details

MAC Address	Roles
00368f6af10c	[Employee],[User Authenticated]
0090804beb8c	[Employee],[User Authenticated]

The star icon color is now set to orange, indicating the user has been added to the Watchlist.

The following message is displayed:

<User> added to User Watchlist successfully. Please configure SMS and email notifications.

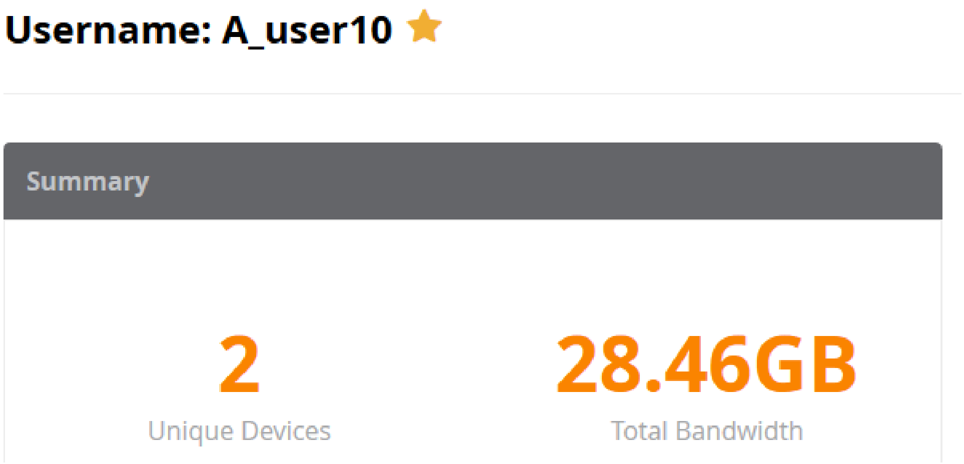
Removing a User from the Watchlist

To remove a user from the Watchlist:

1. In the Insight Search window, enter the name of the user.

   The Insight **User Information** page for the selected user opens.

Figure 733: *Removing a User from the Watchlist*



Username: A_user10 ★

Summary

2. Click the orange star icon next to the username.

   The user is removed from the Watchlist. The star icon is now white. You receive the following message:

   <User> removed from User Watchlist successfully.

Creating Reports

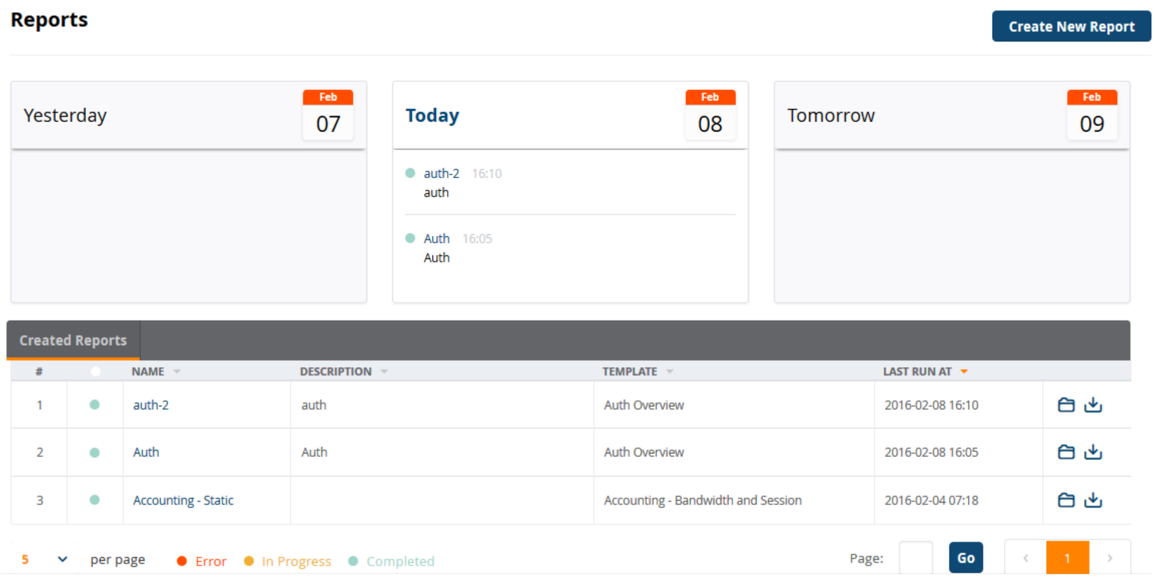
This section provides the following information:

- Overview
- Settings Configuration
- Report Filters Configuration
- Specifying the Logo and Branding
- Report Summary Page
- Configured Reports Page
- Viewing Reports

Overview

The **Reports** page provides a method for creating reports with data filters and customized time ranges up to the previous two months.

Figure 734: *Reports Page*



auth-2 16:10
auth

Auth 16:05
Auth

#		NAME	DESCRIPTION	TEMPLATE	LAST RUN AT	
1	●	auth-2	auth	Auth Overview	2016-02-08 16:10	
2	●	Auth	Auth	Auth Overview	2016-02-08 16:05	
3	●	Accounting - Static		Accounting - Bandwidth and Session	2016-02-04 07:18	

Run Reports Now or on a Specified Schedule

You can set up reports to run immediately or you can schedule a report to run on a daily, weekly, or monthly basis. Although Insight reports show data over the previous two-month period, Insight can retain data for up to two years.

Select Report Filters

Many reports allow you to select filters that include a simple AND condition. For example, you can use filters to create a report that displays data for RADIUS Authentications from the Active Directory AND the Guest User Repository source.

PDF, CSV, and HTML Report Formats Are Available

After a report is configured and run, the report is available for download in PDF and CSV formats. You can also open a report and view it in HTML format.

NOTE

Deleting a configured report deletes both the report configuration and all related report output.

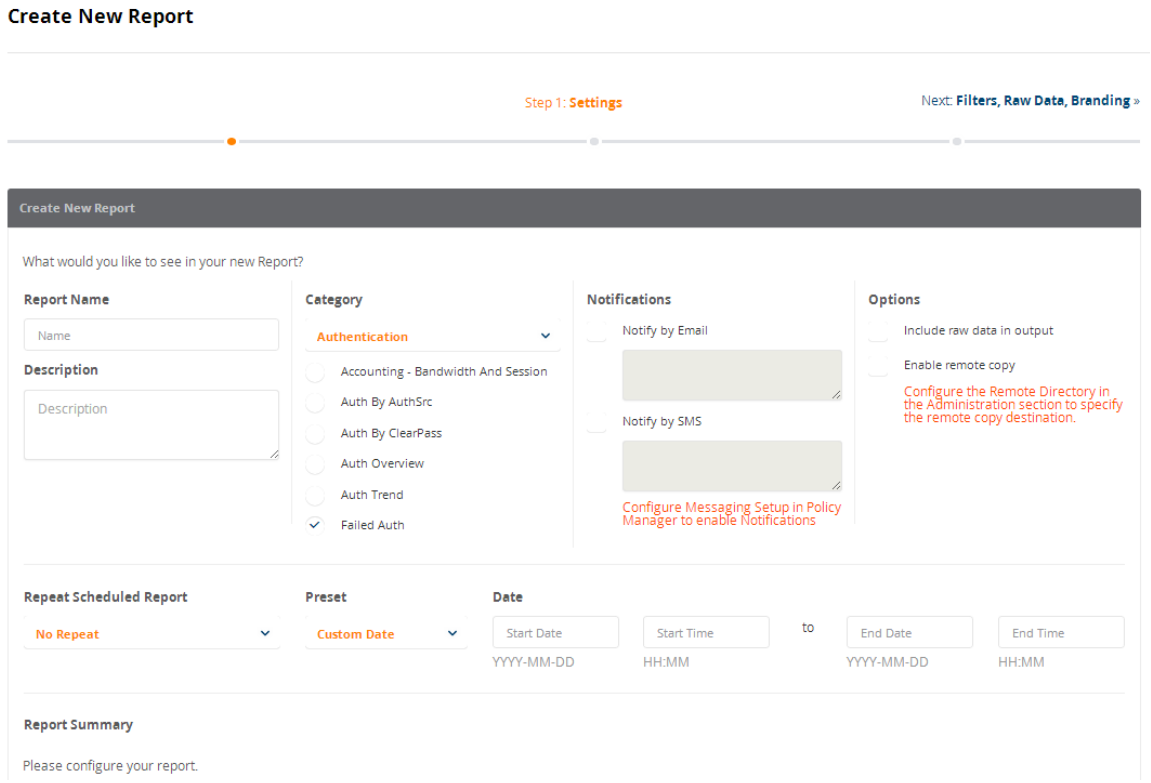
Settings Configuration

To create a new report:

1. From the Insight navigation panel, click **Reports**.
2. Select **Create New Report**.

   The **Settings** page of the **Create New Report Wizard** opens.

Figure 735: *Create New Report Wizard: Settings*



Create New Report

Step 1: **Settings**

Next: **Filters, Raw Data, Branding** »

Create New Report

What would you like to see in your new Report?

Report Name

Name

Description

Description

Category

Authentication

○ Accounting - Bandwidth And Session
○ Auth By AuthSrc
○ Auth By ClearPass
○ Auth Overview
○ Auth Trend
✓ Failed Auth

Notifications

□ Notify by Email

□ Notify by SMS

Configure Messaging Setup in Policy Manager to enable Notifications

Options

□ Include raw data in output

□ Enable remote copy

Configure the Remote Directory in the Administration section to specify the remote copy destination.

Repeat Scheduled Report

No Repeat

Preset

Custom Date

Date

Start Date YYYY-MM-DD Start Time HH:MM to End Date YYYY-MM-DD End Time HH:MM

Report Summary

Please configure your report.

3. Enter the appropriate information as described in Table 375.

Table 375: *Specifying the Report Settings Parameters*

Report Parameter	Action/Description
Report Name	1. Enter the name of the report.
Description	2. Optionally, enter a summary description of the report.
Category	3. Select the report **Category**, then specify the desired report type in the selected category: ▪ Authentication ▪ Endpoint ▪ Guest Authentication ▪ Network ▪ OnGuard

Table 375: *Specifying the Report Settings Parameters (Continued)*

Report Parameter	Action/Description
	■ Onboard ■ RADIUS Authentication ■ System ■ TACACS **NOTE:** For detailed information about what report types are provided for each report category, see Insight Report Categories Reference on page 740.
Notifications	4. Optionally, specify report notifications. ■ **Notify by Email**. When you select this option, enter the list of email addresses to be notified. ■ **Notify by SMS**. When you select this option, enter the phone numbers of each recipient (separated by commas). **NOTE:** A warning message appears if you have not configured the SMTP mail server for email notifications. To do so, from the Policy Manager, navigate to **Administration** > **External Servers** > **Messaging Setup**. For details, see Messaging Setup on page 579.
Options	**NOTE:** Before you can enable one or both of these two options, you must configure the **File Transfer Settings** (including the Remote Directory) in the **Administration** section. For more information, see File Transfer Settings Configuration on page 756. ● **Include raw data in output** A full set of raw data is customizable in the CSV reports only. ● **Enable remote copy** This option lets you copy reports to the location specified in the **Administration** > **Remote Directory** setting.
Repeat Scheduled Report	5. Specify whether you want to generate this report **Daily**, **Weekly**, or **Monthly**. The default is **No Repeat**. ■ To rerun a **No Repeat** report or a static report, edit and save the report. Insight will then automatically run the report. ■ When you create a report with the **No Repeat** option selected, the report runs when you click **Save**. ■ When you create a periodic report (**Daily**, **Weekly**, or **Monthly**), the report is run according to the specified schedule.
Preset Date Range	6. You can choose to specify a **Preset Date Range** for this report: ■ Custom Date When you select **Custom Date**, specify the **Start Date** and **Time** and the **End Date** and **Time**. ■ Today ■ Since Yesterday ■ This Week ■ Within Last Week ■ Within Last 2 Weeks ■ This Month ■ Within Last Month When you select one of these date range options (with the exception of **Custom Date**), Insight automatically populates the **Start Date/Time** and **End Date/Time**

Table 375: *Specifying the Report Settings Parameters (Continued)*

Report Parameter	Action/Description
	settings.
Report Summary	When you have configured the report settings, the **Report Summary** displays them for your review.
	7. Click **Next**.

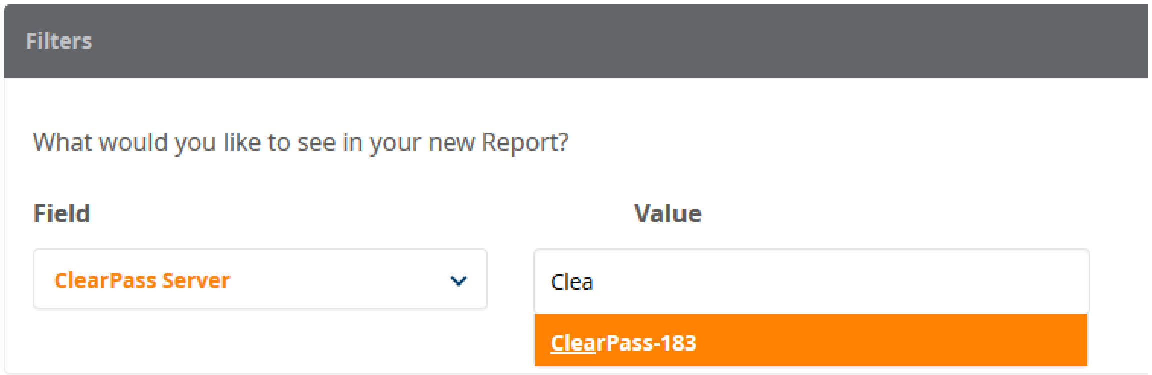
Report Filters Configuration

When you complete the **Settings** page in the **Create New Report** wizard and click **Next**, the page that opens allows you to configure the filters for your report. Each type of report has a specific set of filters available.

Report filters apply the data fetched from the database, then Insight displays the result in the report. The filters that are available depend on the report category you specify.

If you don't apply a filter, Insight includes all the data in the generated report that matches the report category.

Figure 736: *Specifying a Report Filter*



Filters

What would you like to see in your new Report?

Field: ClearPass Server

Value: Clea

ClearPass-183

To specify a report filter:

1. **Field**: From the **Field** drop-down, select the parameter you wish to filter on.
2. **Value**: From the **Value** drop-down, select the appropriate value.

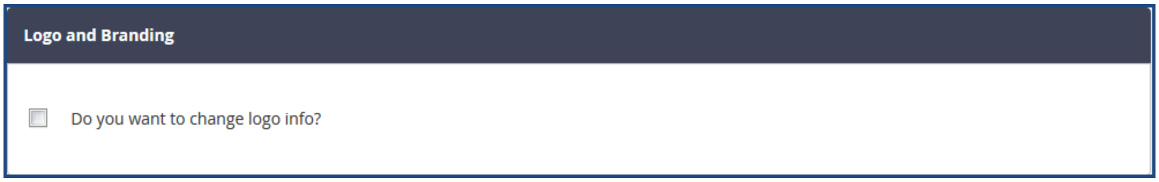
   As you enter characters in the **Value** field, Insight searches for the matching value.

Specifying the Logo and Branding

When you complete the report filters configuration, scroll to the **Logo and Branding** section on the same page.

The initial Logo and Branding screen presents a prompt, asking if you want to change the logo:

Figure 737: *Prompt for Changing the Logo*



Logo and Branding

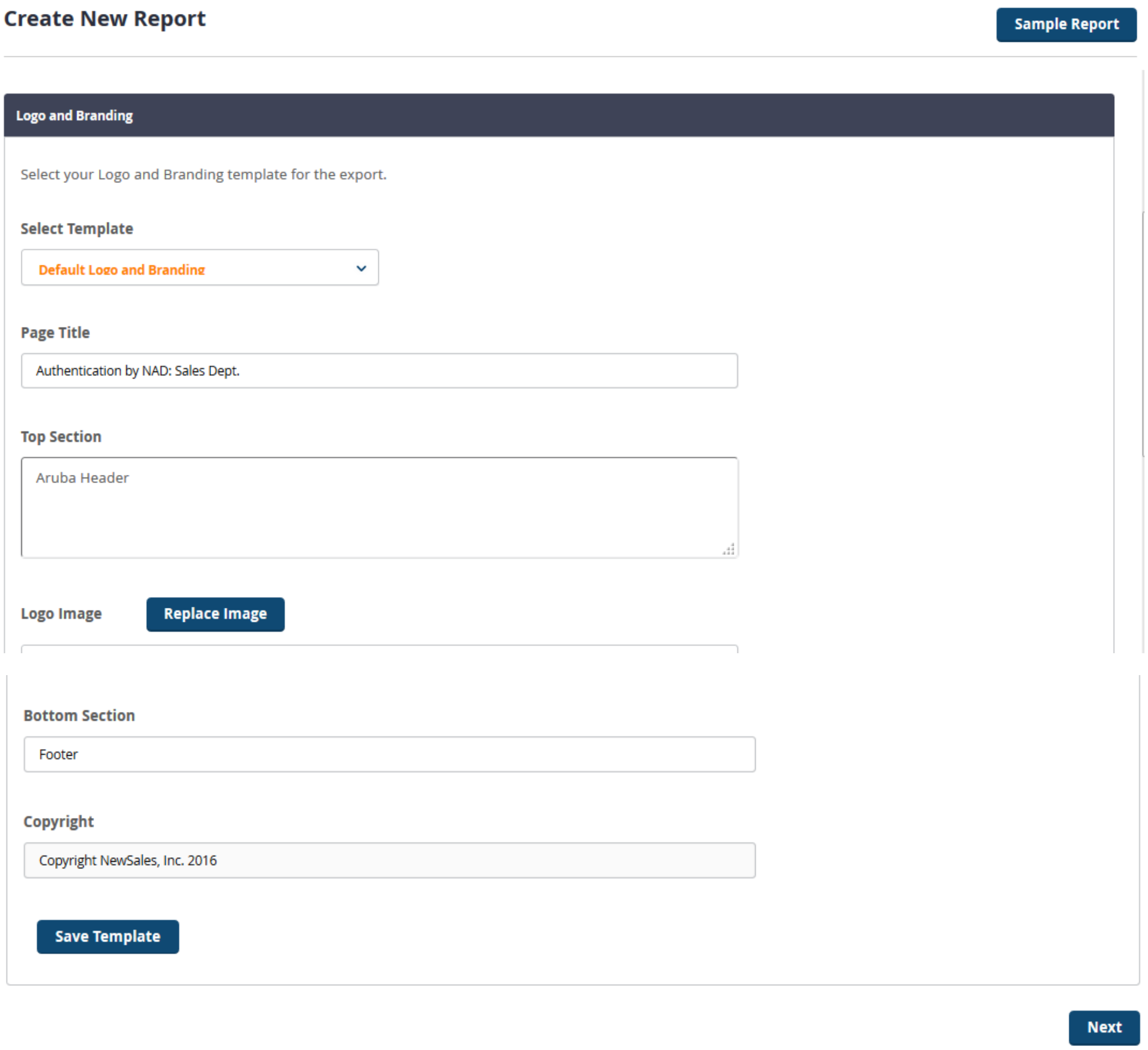
☐ Do you want to change logo info?

1. If you don't wish to change the logo, simply click **Next** to proceed.

2. If you do want to change the logo, click the check box.

   The Logo and Branding configuration section opens:

Figure 738: *Logo and Branding Section*



Create New Report

Logo and Branding

Select your Logo and Branding template for the export.

Select Template: Default Logo and Branding

Page Title: Authentication by NAD: Sales Dept.

Top Section: Aruba Header

Bottom Section: Footer

Copyright: Copyright NewSales, Inc. 2016

To specify the logo and branding information:

1. Enter the information as described in Table 376, then click **Next**.

Table 376: *Specifying Logo and Branding Parameters*

Report Parameter	Action/Description
Select Template	1. From the drop-down, select the logo and branding template.
Page Title	2. Enter the page title.
Top Section	3. Enter the header for the top of the page.
Logo Image	4. To browse to the appropriate logo image, click **Replace Image**.

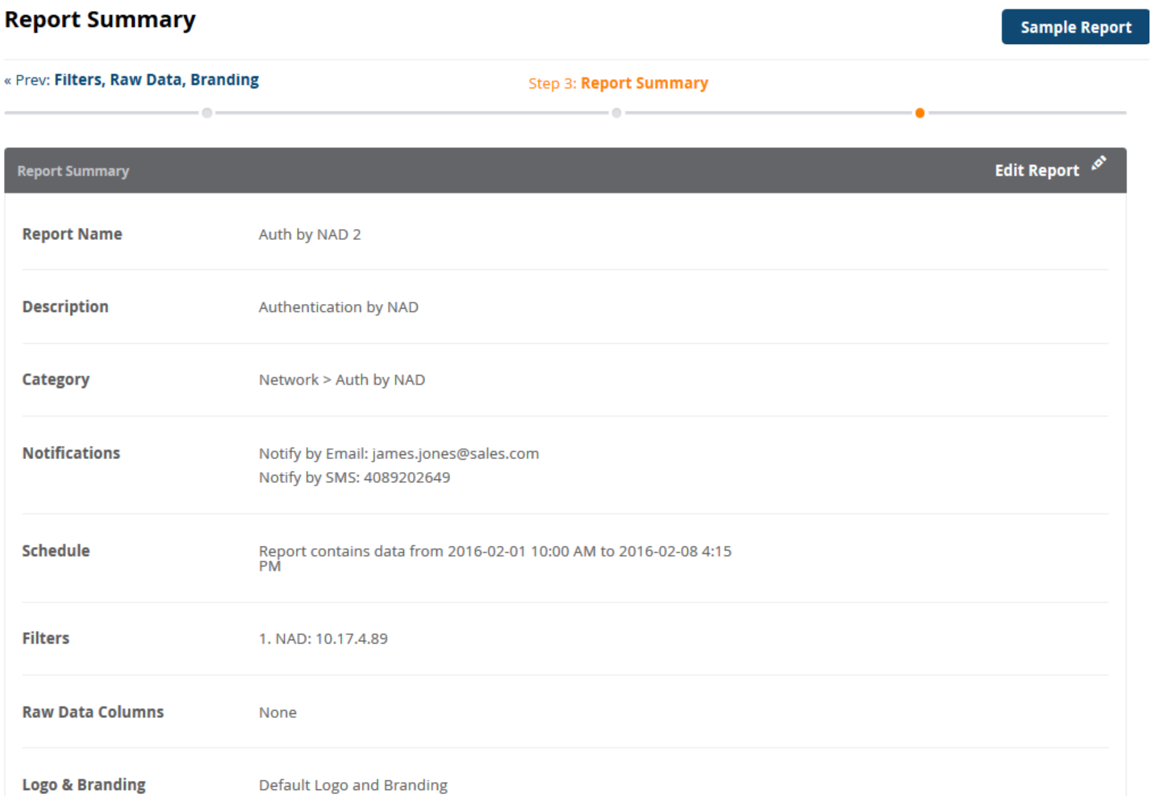
Table 376: *Specifying Logo and Branding Parameters (Continued)*

Report Parameter	Action/Description
Bottom Section	5. Enter the footer text.
Copyright	6. Enter the copyright information. For example, "Copyright 2016 NewSales, Inc."
Save Template	7. To save the new branding and logo settings, click **Save Template**.

Report Summary Page

When you complete the **Logo and Branding** section, the **Report Summary** is displayed.

Figure 739: *Report Summary*



Report Name	Auth by NAD 2
Description	Authentication by NAD
Category	Network > Auth by NAD
Notifications	Notify by Email: james.jones@sales.com Notify by SMS: 4089202649
Schedule	Report contains data from 2016-02-01 10:00 AM to 2016-02-08 4:15 PM
Filters	1. NAD: 10.17.4.89
Raw Data Columns	None
Logo & Branding	Default Logo and Branding

1. Review the Report Summary.
   a. If you wish to change any aspect of the report, click **Edit Report**.

      The **Report Summary** dialog opens. You can edit the current report settings as needed.

   b. Make any necessary changes, then click **Save**.
2. When the report settings are satisfactory, click **Save**.

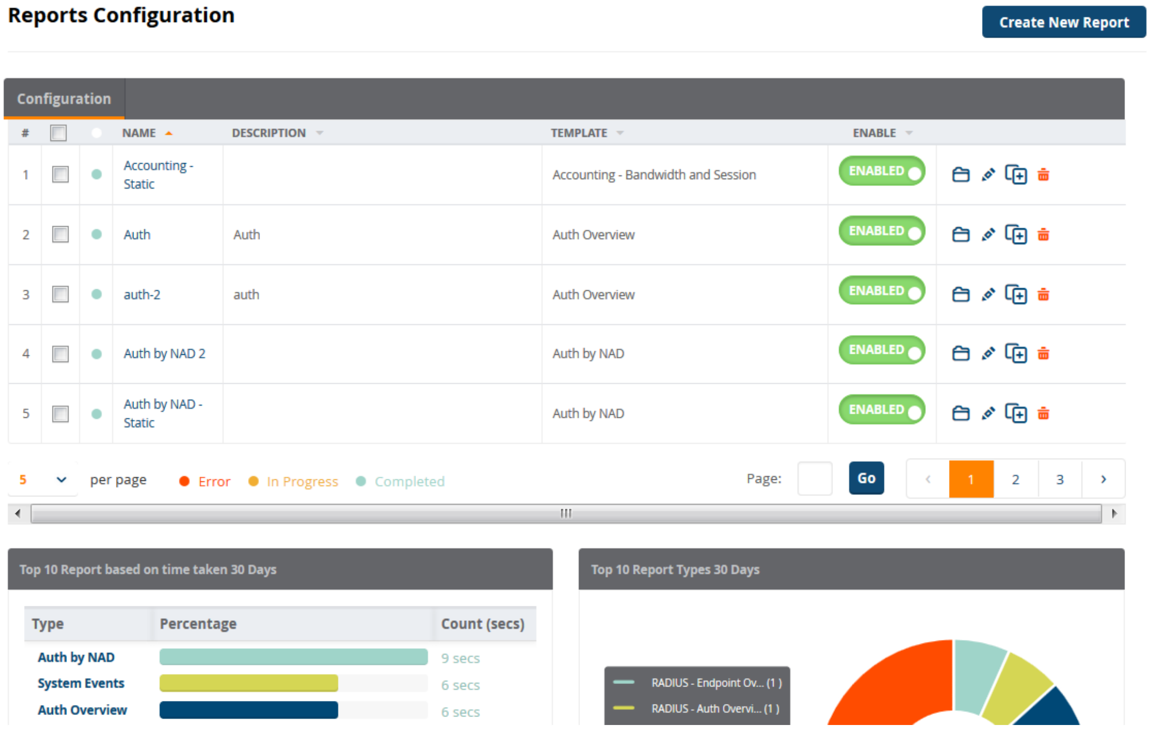
   Insight generates the report. You return to the **Configured Reports** page.

Configured Reports Page

To see the set of configured reports, select **Reports** > **Configuration**.

The **Configured Reports** page opens.

Figure 740: *Configured Reports Page*



Reports Configuration

#	☐		NAME	DESCRIPTION	TEMPLATE	ENABLE	
1	☐	●	Accounting - Static		Accounting - Bandwidth and Session	ENABLED	
2	☐	●	Auth	Auth	Auth Overview	ENABLED	
3	☐	●	auth-2	auth	Auth Overview	ENABLED	
4	☐	●	Auth by NAD 2		Auth by NAD	ENABLED	
5	☐	●	Auth by NAD - Static		Auth by NAD	ENABLED	

5 per page ● Error ● In Progress ● Completed Page: Go ‹ 1 2 3 ›

Top 10 Report based on time taken 30 Days

Type	Percentage	Count (secs)
Auth by NAD		9 secs
System Events		6 secs
Auth Overview		6 secs

Top 10 Report Types 30 Days

The blue dot next to a report name indicates that the report generation is complete.

From this view, you can edit, copy, or delete a configured report.

This page also provides two report widgets:

- **Top 10 Reports Time to Run 30 Days**

  This widget lists the ten reports that took the longest (in seconds) to run over the last 30 days.
- **Top 10 Reports Last 30 Days**

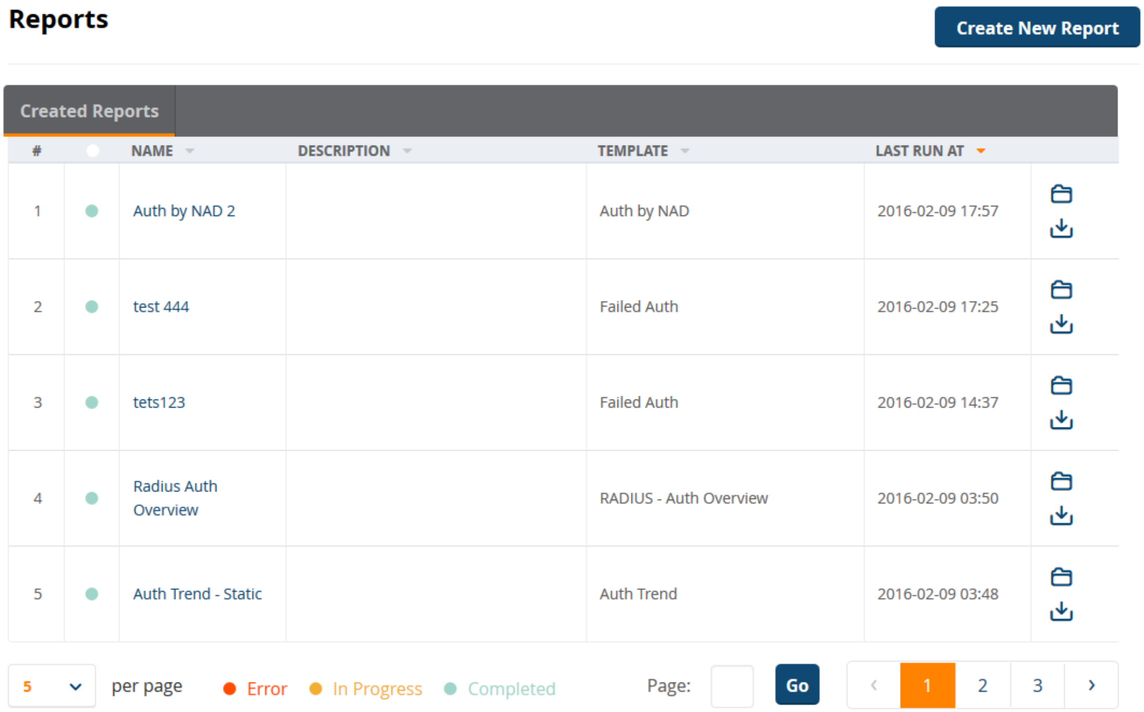
  This widget lists the ten most frequently run reports over the last 30 days.

Viewing Reports

To view a generated report:

1. From the navigation panel, click **Reports**.
2. Scroll to the **Created Reports** section.

Figure 741: *Created Reports*



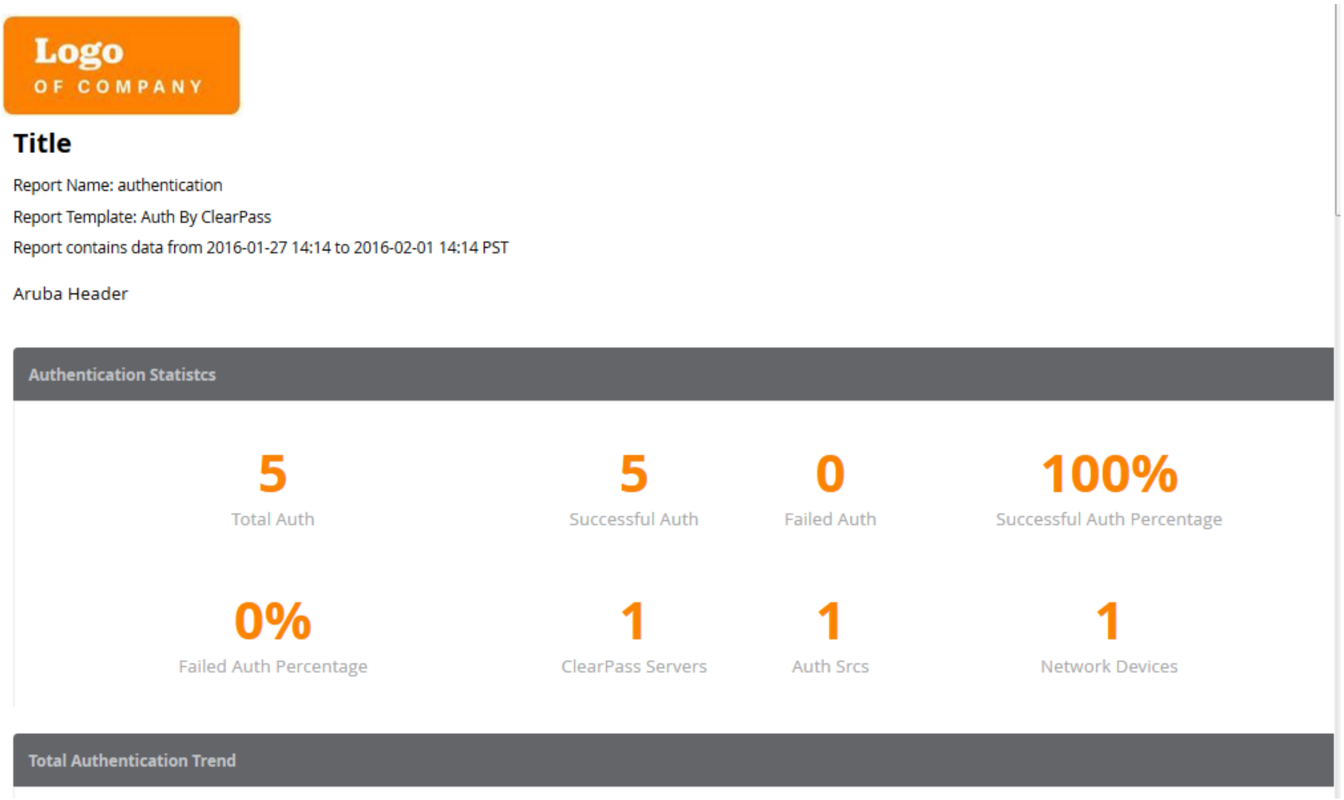
Reports

#	○	NAME	DESCRIPTION	TEMPLATE	LAST RUN AT	
1	●	Auth by NAD 2		Auth by NAD	2016-02-09 17:57	
2	●	test 444		Failed Auth	2016-02-09 17:25	
3	●	tets123		Failed Auth	2016-02-09 14:37	
4	●	Radius Auth Overview		RADIUS - Auth Overview	2016-02-09 03:50	
5	●	Auth Trend - Static		Auth Trend	2016-02-09 03:48	

3. To download the zip file that contains the reports in PDF and CSV formats, click the **Download** icon (as shown in Figure 741).
4. To view the desired report in HTML format (which opens in new tab), click the name of the report.

   The generated report is displayed (see Figure 742).

Figure 742: *Report Displayed in HTML Format*



Title

Report Name: authentication

Report Template: Auth By ClearPass

Report contains data from 2016-01-27 14:14 to 2016-02-01 14:14 PST

Aruba Header

Authentication Statistcs

Total Authentication Trend

Insight Report Categories Reference

This section provides the following information:

- Introduction
- Authentication Category Reports
- Endpoint Category Reports
- Guest Authentication Category Reports
- Network Category Reports
- OnGuard Category Reports
- Onboard Category Report
- RADIUS Authentication Category Reports
- System Category Reports
- TACACS Category Reports

Introduction

This section provides detailed information about each of the report types and their associated widgets available for each Insight Report category. The Insight report templates are organized into categories, where each category has multiple report types that each contain a unique set of report data.

The following sections describe each report category, including the available reports within each category, and the contents of each report.

Authentication Category Reports

The reports available in the Authentication category described in Table 377 provide the list of authentications that occurred during the report duration.

Additional authentication statistics are displayed on the **Authentication Dashboard**. For more information, see Authentication Dashboard on page 718.

Table 377: *Authentication Category Reports*

Report Type	Report Widgets
Accounting—Bandwidth and Session Provides the statistics using the accounting data generated during report duration. This report allows you to filter the report data by: - ClearPass server - Network access device IP address - Device category - Device family - Device name - SSID - Endpoint IP address - User name	This report type includes the following bandwidth and session information: - Bandwidth Statistics: Total Bandwidth, Average Bandwidth, Maximum Bandwidth, Maximum Upstream Bandwidth, Maximum Downstream Bandwidth, Sessions, Maximum Duration, Users, Endpoints - Upstream Bandwidth and Downstream Bandwidth Trend - Total Bandwidth and Average Bandwidth Trend - Average Session Time Trend - Unique Session Trend - Top 10 Device Categories with Most Bandwidth Consumed - Top 10 Device Categories with Most Sessions - Top 10 Device Categories with Most Duration - Top 10 Device Families with Most Bandwidth Consumed - Top 10 Device Families with Most Sessions - Top 10 Device Families with Most Duration - Top 10 Endpoints with Most Bandwidth Consumed - Top 10 Endpoints with Most Sessions - Top 10 Endpoints with Most Duration - Top 20 Users with Most Bandwidth Consumed - Top 10 Users with Most Sessions - Top 10 Users with Most Duration - Domain Summary: Provides an overview of authentications per domain.
Authentication by Authentication Source Provides the statistics for successful and failed authentications per authentication source.	This report type includes the following information: - Authentication Statistics - Total Authentication Trend - Failed Authentication Trend - Authentication Distribution Across Authentication Source - Authentication Distribution Across Authorization Source - Authentication Distribution Across Authentication Source **NOTE:** This report allows you to filter the report data by authentication source.
Authentication by ClearPass Provides the statistics for successful and failed authentications per ClearPass servers in a cluster.	This report type includes the following information: - Authentication Statistics - Total Authentication Trend - Failed Authentication Trend - Authentication Distribution—Error Types - Authentication Distribution Across Service - Top 10 ClearPass with Most Authentications - Top 10 ClearPass with Most Failed Authentications - Top 10 ClearPass with Most MAC Address Authentications - Top 10 ClearPass with Most Users **NOTE:** This report allows you to filter the report data by ClearPass Policy Manager server.

Table 377: *Authentication Category Reports (Continued)*

Report Type	Report Widgets
Authentication Overview Provides statistics in general for the report duration, such as total authentications per day, unique devices authentications trend by day, unique users authentication trend by day, authentication distribution based on authentication status, service, ClearPass server, SSID, VLAN, enforcement profile, authentication source, and top 10 users with most authentications, and so on.	This report type includes the following information: ● Authentication Statistics ● Total Authentication Trend ● Authentication Status Trend ● Unique Devices Authentication Trend ● Unique Users Authentication Trend ● Authentication Distribution Across Auth Status ● Authentication Distribution Across Cluster ● Authentication Distribution Across Service ● Authentication Distribution Across VLAN ● Authentication Distribution Across SSID ● Authentication Distribution Across Enforcement Profiles ● Authentication Distribution Across Role ● Authentication Distribution Across Authentication Source ● Top 10 Users with Most Authentications ● Top 10 MAC Addresses with Most Authentications ● Top 10 Services with Most Authentications ● Top 10 Auth Sources with Most Authentications ● Top 10 ClearPass Roles Assigned ● Top 10 Authorization Sources ● Top 20 NADs with Most Authentications ● Top 10 Enforcement Profiles Users **NOTE:** This report allows you to filter the report data by ClearPass Policy Manager host name, Network Attached Device (NAD) IP address, SSID, and Error Code.
Authentication Trend Provides authentication trend statistics for today and yesterday, today and the same day a week ago, and so on.	This report type includes the following information: ● Authentication Statistics ● Total Authentication Trend ● Authentication Trend for Today and Yesterday ● Authentication Trend for Today and Same Day Week Ago ● Total Authentication for 1 Month (per month) **NOTE:** This report allows you to filter the report data by ClearPass Policy Manager host name, Network Access Device (NAD) IP address, and SSID.
Failed Authentication Provides statistics based on failed authentications.	This report type includes the following information: ● Error Statistics ● Failed Authentication Trend ● Authentication Distribution—Error Types ● Failed Authentication Distribution across Service ● Failed Authentication Distribution across Authentication Source ● Top 10 Errors with Most Failed Authentications ● Top 20 NADs with Most Failed Authentications ● Top 10 ClearPass Servers with Most Failed Authentications ● Top 10 Users with Most Failed Authentications ● Top 10 Endpoints with Most Failed Authentications

Table 377: *Authentication Category Reports (Continued)*

Report Type	Report Widgets
	- Top 10 Services with Most Failed Authentications **NOTE:** This report allows you to filter the report data by ClearPass Policy Manager host name, Network Access Device (NAD) IP address, SSID, and Error Code.

Endpoint Category Reports

The Endpoint category provides information on endpoints discovered during the report duration.

The reports available in the Endpoint category described in Table 378 contain data that can also be found in the Endpoints widgets on the **Endpoints Dashboard**.

For additional information about the Endpoints Dashboard, see Endpoints Dashboard on page 719.

Table 378: *Endpoint Category Reports*

Report Type	Report Widgets
Endpoint Authentication Overview	This report type includes the following information for all endpoint types: - Endpoint Statistics - Endpoints Distribution Across Device Category - Endpoints Distribution Across Device Family - Endpoints Distribution Across Device Name - Top 10 Users with Most Endpoints - Top 10 Device Categories with Most Endpoints - Top 10 Device Names with Most Endpoints - Top 10 Device Families with Most Endpoints **NOTE:** This report also allows you to filter the report data by Network Access Device (NAD) IP address, Device Category, Device Family, Device name, and SSID.
Endpoint Overview	This report type includes the following information for all endpoint types: - Top 10 Reports Time to Run 30 Days - Top 10 Reports Last 30 Days
Guest—Endpoint Overview	This report type includes the following information for endpoints using Guest Authentication: - Endpoint Statistics - Endpoints Distribution Across Device Category - Endpoints Distribution Across Device Family - Endpoints Distribution Across Device Name - Top 10 Users with Most Endpoints - Top 10 Device Categories with Most Endpoints - Top 10 Device Names with Most Endpoints - Top 10 Device Families with Most Endpoints **NOTE:** This report also allows you to filter the report data by Network Access Device (NAD) IP address, Device Category, Device Family, Device name, and SSID.

Table 378: *Endpoint Category Reports (Continued)*

Report Type	Report Widgets
RADIUS—Endpoint Overview	This report type includes the following information for endpoints using RADIUS authentication: - Endpoint Statistics - Endpoints Distribution Across Device Category - Endpoints Distribution Across Device Family - Endpoints Distribution Across Device Name - Top 10 Users with Most Endpoints - Top 10 Device Categories with Most Endpoints - Top 10 Device Names with Most Endpoints - Top 10 Device Families with Most Endpoints **NOTE:** This report also allows you to filter the report data by Network Access Device (NAD) IP address, Device Category, Device Family, Device name, and SSID.

Guest Authentication Category Reports

The reports available in the Guest Authentication category described in Table 379 provide statistics based on Guest authentications from the Guest database. The statistics for authentication trend and usage for guest users are drawn from the accounting data.

Additional authentication statistics are displayed on the **Guest Dashboard**. For additional information about the Guest Dashboard, see Guest Dashboard on page 720.

Table 379: *Guest Authentication Category Reports*

Report Type	Report Widgets
Guest—Authentication by ClearPass	This report type includes the following information guest authentication by ClearPass: - Authentication Statistics - Total Authentication Trend - Failed Authentication Trend - Authentication Distribution—Error Types - Authentication Distribution Across Service - Top 10 ClearPass with Most Authentications - Top 10 ClearPass with Most Failed Authentications - Top 10 ClearPass with Most MAC Authentications - Top 10 ClearPass with Most Guests **NOTE:** This report also allows you to filter the report data by ClearPass Policy Manager host name.
Guest—Authentication Overview	This report type includes the following information for guest authentication: - Authentication Statistics - Total Authentication Trend - Authentication Status Trend - Unique Devices Authentication Trend - Unique Guests Authentication Trend - Authentication Distribution Across Authentication Status - Authentication Distribution Across Cluster - Authentication Distribution Across Service - Authentication Distribution Across VLAN - Authentication Distribution Across SSID - Authentication Distribution Across Enforcement Profiles - Authentication Distribution Across Role - Authentication Distribution Across Authentication Sources - Top 10 Guests with Most Authentications - Top 10 MAC Addresses with Most Authentications - Top 10 IP Addresses with Most Authentications - Top 10 Services with Most Authentications - Top 10 Authentication Sources with Most Authentications - Top 10 ClearPass Roles Assigned - Top 10 Authorization Source - Top 20 NADs with Most Authentications - Top 10 Enforcement Profiles Used **NOTE:** This report also allows you to filter the report data by ClearPass host name and Network Access Device (NAD) IP address.
Guest—Authentication Trend	This report type includes the following information for guest authentication trends: - Authentication Statistics - Total Authentication Trend - Authentication Trend for Yesterday and Today - Authentication Trend for Today and Same Day Week Ago - Total Authentication for 1 Month - Sponsor List

Table 379: *Guest Authentication Category Reports (Continued)*

Report Type	Report Widgets
	NOTE: This report also allows you to filter the report data by ClearPass Policy Manager host name and Network Access Device (NAD) IP address.
Guest—Expired	The Guest—Expired report lets you view information about expired guest accounts. This report type includes the following report widgets: - Guest Expiry Statistics - Guest Expiry List
Guest—Social Login	This report type includes the following information for guest authentication for Social Logins: - Social Authentication Trend - Endpoint Distribution Across Social Providers - Authentication Distribution Across Authentication Source **NOTE:** This report also allows you to filter the report data by ClearPass host name and Network Access Device (NAD) IP address.
Guest Accounting—Bandwidth and Session This report allows you to filter the report data by: - ClearPass server - Network access device IP address - Device category - Device family - Device name - SSID - Endpoint IP address - User name	This report type includes the following bandwidth and session information: - Bandwidth Statistics: Total Bandwidth, Average Bandwidth, Maximum Bandwidth, Maximum Upstream Bandwidth, Maximum Downstream Bandwidth, Sessions, Maximum Duration, Guests, Endpoints - Upstream Bandwidth and Downstream Bandwidth Trend - Total Bandwidth and Average Bandwidth Trend - Average Session Time Trend - Unique Session Trend - Top 10 Device Categories with Most Bandwidth Consumed - Top 10 Device Categories with Most Sessions - Top 10 Device Categories with Most Duration - Top 10 Device Families With Most Bandwidth Consumed - Top 10 Device Families With Most Sessions - Top 10 Device Families With Most Duration - Top 10 Endpoints with Most Bandwidth Consumed - Top 10 Endpoints with Most Sessions - Top 10 Endpoints with Most Duration - Top 20 Guests with Most Bandwidth Consumed - Top 10 Guests with Most Sessions - Top 10 Guests with Most Duration

Network Category Reports

The reports available in the Network category described in Table 380 contain data about network access devices and ives details on authentication trends such as successful and failed authentications on a per-day basis.

Similar information can also be found in the Network widgets on the **Network Dashboard**. For additional information, see Network Dashboard on page 721.

Table 380: *Network Category Reports*

Report Type	Report Widgets
Authentication by NAD	This report type includes the following information for Network Access Devices (NADs) using guest authentication. - Authentication Statistics - Total Authentication Trend - Failed Authentication Trend - Authentication Distribution Across NAD Ports - Top 20 NADs with Most Authentication - Top 10 Services with Most Authentications - Top 20 NADs with Most Failed Authentications - Top 20 NADs with Most MAC Addresses - Top 20 NADs with Most Users **NOTE:** This report also allows you to filter the report data by NAD IP address.
Guest—Authentication by NAD	This report type includes the following information for Network Access Devices (NADs) using guest authentication - Authentication Statistics - Total Authentication Trend - Failed Authentication Trend - Authentication Distribution Across NAD Ports - Top 20 NADs with Most Authentication - Top 10 Services with Most Authentications - Top 20 NADs with Most Failed Authentications - Top 20 NADs with Most MAC Addresses - Top 20 NADs with Most Guests **NOTE:** This report also allows you to filter the report data by NAD IP address.
RADIUS—Auth by NAD	This report type includes the following information for Network Access Devices (NADs) using guest authentication: - Authentication Statistics - Authentication Distribution Across NAD Ports - Top 20 NADs with Most Authentication - Top 10 Services with Most Authentications - Top 20 NADs with Most Failed Authentications - Top 20 NADs with Most MACs - Top 20 NADs with Most Users **NOTE:** This report also allows you to filter the report data by NAD IP address.

OnGuard Category Reports

The reports available in the OnGuard category provide analysis on the devices' posture and health status.

These widgets contain data that can also be found in the Posture widgets on the **Posture Dashboard**. For additional information, see Posture Dashboard on page 721.

Table 381: *OnGuard Category Reports*

Report Type	Report Widgets
Apple Mac Endpoint Posture	This report type includes the following posture information for Apple/Macintosh endpoints: - OnGuard Statistics - OnGuard Device Authentication Trend - OnGuard Device Distribution Across Health Status - Antispyware Product Name - Antspyware Dat File Version - Antispyware Engine Version - OnGuard Device Distribution Across Antispyware Real-Time Protection Status - Antispyware Version - Antivirus Product Name - Antivirus Dat File Version - Antivirus Engine Version - OnGuard Device Distribution Across Antivirus RealTimeProtection Status - Antivirus Version - Disk Encryption Product Name - Disk Encryption Version - Firewall Product Name - OnGuard Device Distribution Across Firewall Status - Firewall Version - OnGuard Device Distribution Across Network Connection Type - OnGuard Device Distribution Across P2P Application Name - OnGuard Device Distribution Across P2P Status - OnGuard Device Distribution Across Patch Agent Name - Missing Patches Count - OnGuard Device Distribution Across Patch Agent Status - OnGuard Device Distribution Across Client Operating System - OnGuard Device Distribution Across Client Running as VM **NOTE:** This report also allows you to filter the report data by System Posture Token (SPT).
Endpoint Posture Overview	This report type includes the following endpoint posture information: - OnGuard Statistics - OnGuard Device Distribution Across Health Status - Unhealthy OnGuard Device Distribution Across Device Family - OnGuard Device Distribution Across Agent Type - OnGuard Device Distribution Across Agent Version - Health Class - Missing Hotfixes **NOTE:** This report also allows you to filter the report data by System Posture Token (SPT).
Linux Endpoint Posture	This report type includes the following posture information for endpoints

Table 381: *OnGuard Category Reports (Continued)*

Report Type	Report Widgets
	using a Linux operating system: - OnGuard Statistics - OnGuard Device Authentication Trend - OnGuard Device Distribution Across Health Status - Antivirus Product Name - Antivirus Dat File Version - Antivirus Engine Version - OnGuard Device Distribution Across Antivirus RealTimeProtection Status - Antivirus Version **NOTE:** This report also allows you to filter the report data by System Posture Token (SPT).
Windows Endpoint Posture	This report type includes the following posture information for endpoints using a Windows operating system: - OnGuard Statistics - OnGuard Device Authentication Trend - OnGuard Device Distribution Across Health Status - Antispyware Product Name - Antspyware Dat File Version - Antispyware Engine Version - OnGuard Device Distribution Across Antispyware Real-Time Protection Status - Antispyware Version - Antivirus Product Name - Antivirus Dat File Version - Antivirus Engine Version - OnGuard Device Distribution Across Antivirus RealTimeProtection Status - Antivirus Version - Disk Encryption Product Name - Disk Encryption Version - Firewall Product Name - OnGuard Device Distribution Across Firewall Status - Firewall Version - OnGuard Device Distribution Across Network Connection Type - OnGuard Device Distribution Across P2P Application Name - OnGuard Device Distribution Across P2P Status - OnGuard Device Distribution Across Patch Agent Name - Missing Patches Count - OnGuard Device Distribution Across Patch Agent Status - OnGuard Device Distribution Across Client Operating System - OnGuard Device Distribution Across Client Running as VM **NOTE:** This report also allows you to filter the report data by System Posture Token (SPT).

Onboard Category Report

The reports available in the Onboard category provides analysis on onboarded devices during the report period, such as the active users and devices count, revoked devices count, onboarded devices distribution based on device type, and Onboard enrollment details.

Table 382: *Onboard Report Content*

Report Type	Report Widgets
Onboard Certificate	This report type includes the following certificate information: ● Onboard statistics for numbers of revoked devices, active devices, and users ● Latest Onboard Device Distribution ● Active Onboard Device Distribution ● Top 10 Users with Most Active Devices
Onboard Enrollment	This report type provides the following information: ● Total Devices Onboarded ● Onboarded Devices Enrollment Trend ● Onboarded Devices ● Unique Users and Their Associated Total Number of Devices ● Unique Onboarded Devices

RADIUS Authentication Category Reports

The reports available in the RADIUS Authentication provide detailed analysis on authentication trends on successful and failed RADIUS authentication.

Additional authentication statistics are displayed on the **Authentication Dashboard**. For additional information, see Authentication Dashboard on page 718.

Table 383: *RADIUS Authentication Category Reports*

Report Type	Report Widgets
RADIUS—Authentication by Authentication Source	This report type includes the following information for RADIUS authentication: ● Authentication statistics for numbers and percentages of authentications successes and failures ● Total Authentication Trend ● Failed Authentication Trend ● Authentication Distribution Across Authentication Source ● Authentication Distribution Across Authorization Source ● Failed Authentication Distribution Across Authentication Source **NOTE:** This report also allows you to filter the report data by ClearPass Policy Manager host name.
RADIUS—Authentication by ClearPass	This report type includes the following information for RADIUS authentication: ● Authentication Statistics, including numbers and percentages of authentications successes and failures ● Total Authentication Trend ● Failed Authentication Trend ● Authentication Distribution Error Types ● Authentication Distribution Across Service ● Top 10 ClearPass with Most Authentications ● Top 10 ClearPass with Most Failed Authentications ● Top 10 ClearPass with Most MAC Addresses ● Top 10 ClearPass with Most Users **NOTE:** This report also allows you to filter the report data by authentication source.
RADIUS—Authentication Overview	This report type includes the following information for RADIUS authentication: ● Authentication statistics, including numbers and percentages of authentications successes and failures, and numbers of users, endpoints, network devices, roles, ClearPass servers and enforcement profiles ● Total Authentication Trend ● Authentication Status Trend ● Unique Devices Authentication Trend ● Unique Users Authentication Trend ● Authentication Distribution Across Auth Status ● Authentication Distribution Across Cluster ● Authentication Distribution Across Service ● Authentication Distribution Across VLAN ● Authentication Distribution Across SSID

Table 383: *RADIUS Authentication Category Reports (Continued)*

Report Type	Report Widgets
	- Authentication Distribution Across Enforcement Profiles - Authentication Distribution Across Role - Authentication Distribution Across Auth Source - Top 10 Users with Most Authentications - Top 10 MACs with Most Authentications - Top 10 Services with Most Authentications - Top 10 ClearPass Roles Assigned - Top 10 Authorization Sources - Top 20 NADs with Most Authentications - Top 10 Enforcement Profiles Used **NOTE:** This report also allows you to filter the report data by ClearPass Policy Manager host name, Network Access Device (NAD) IP address, SSID and authentication service name.
RADIUS—Authentication Trend	This report type includes the following information: - Authentication Statistics, including authentication data for the previous day and week - Total Authentication Trend - Authentication Trend for Today and Yesterday - Authentication Trend for Today and Same Day Week Ago - Total Authentication for 1 Month (per month) **NOTE:** This report also allows you to filter the report data by ClearPass Policy Manager name, Network Access Device (NAD) IP address, and SSID.
RADIUS—Failed Authentication	This report type includes the following information: - Error Statistics - Failed Authentication Trend - Authentication Distribution—Error Types - Failed Authentication Distribution Across Service - Failed Authentication Distribution Across Authentication Sources - Top 10 Errors with Most Failed Authentications - Top 10 ClearPass Servers with Most Failed Authentications - Top 20 NADs with Most Failed Authentications - Top 10 Users with Most Failed Authentications - Top 10 Endpoints with Most Failed Authentications - Top 10 Services with Most Failed Authentications **NOTE:** This report also allows you to filter the report data by ClearPass Policy Manager host name, Network Access Device (NAD) IP, SSID, and Error Code.

System Category Reports

The reports available in the **System** category provide information about system-level events, such as configuration changes performed on the ClearPass server (configuration audit), license usage, and system events.

Additional system statistics are displayed on the **System Dashboard**. For additional information about the System Dashboard, see System Dashboard on page 722.

Table 384: *System Category Reports*

Report Type	Report Widgets
Configuration Audit	This report type includes the following information for each configuration audit record: ● Name of change ● Action (for example, modify, add, or delete) ● Category ● Updated by ● Update timestamp
License Usage	This report type includes the following licensing information: ● License Statistics, including the total licenses and used licenses for Policy Manager, Guest, ClearPass Enterprise, Onboard, and OnGuard ● Endpoints Trend ● Policy Manager License Usage Trend ● Guest License Usage Trend ● Policy Manager License Distribution ● Policy Manager License Usage ● Guest License Usage Distribution Across Cluster ● Onboard License Usage Distribution Across Cluster ● OnGuard License Usage Distribution Across Cluster ● ClearPass Enterprise License Usage Distribution Across Cluster **NOTE:** This report also allows you to filter the report data by ClearPass Policy Manager host name.
System Events	This report type includes the following information for each system event : ● ClearPass host name ● Source of Event ● Event Category ● Event Level ● Timestamp ● Description **NOTE:** This report also allows you to filter the report data by ClearPass Policy Manager host name.

TACACS Category Reports

The reports available in the TACACS category provide TACACS authentication trends such as successful and failed TACACS authentication and command authorizations.

Table 385: *TACACS Reports Content*

Report Type	Report Widgets
TACACS—Authentication	This report type includes the following licensing information - TACACS statistics, including the numbers and percentages of successful and failed authentications, and the numbers of users, ClearPass servers, and network devices. - Total Authentication Trend - Authentication Status Trend - Authentication Trend For Today and Yesterday - Command List - Authentication Distribution Across Authentication Status - Authentication Distribution Across Cluster - Top 10 Errors with Most Failed Authentications - Top 20 NADs with Most Authentication - Top 10 Users with Most Authentications **NOTE:** This report also allows you to filter the report data by ClearPass server and NAD IP address.

Administration Operations

This section provides the following information:

- Overview
- File Transfer Settings Configuration
- Database Settings Configuration

Overview

You can use the **Administration** page to do the following tasks:

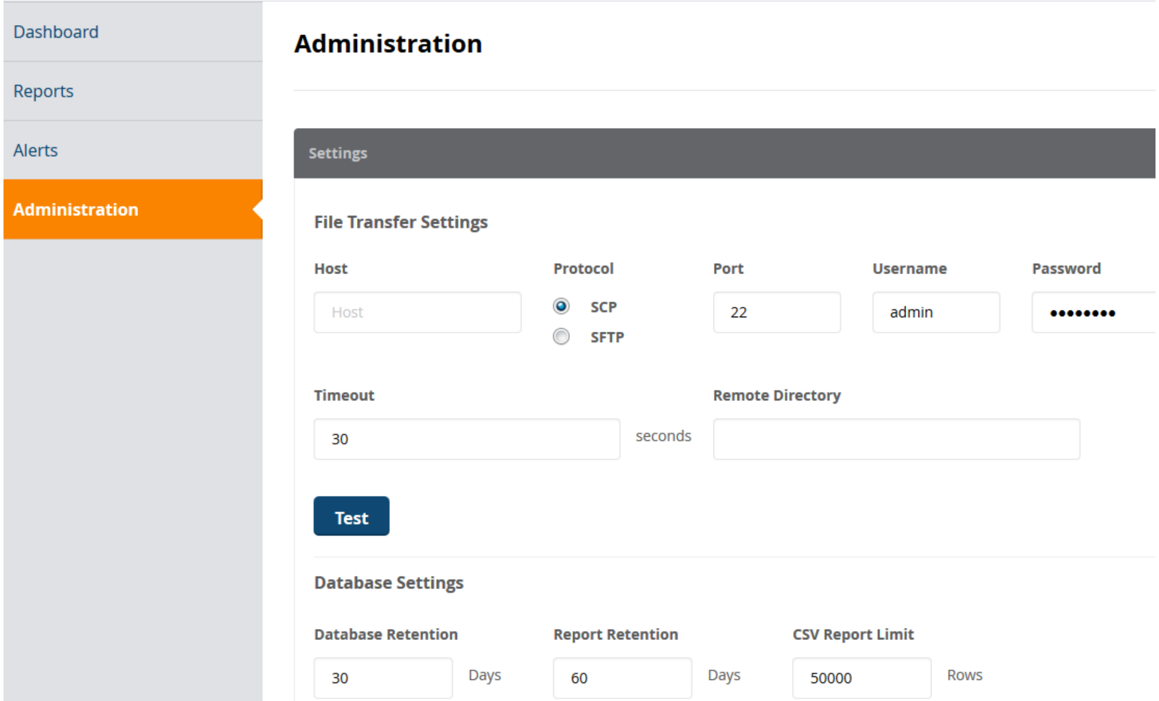
- Specify the number of days to retain information in the database.
- Test the new notification settings to review Insight log files.
- Store reports offline using SCP or SFTP.

To access the **Administration** page:

1. From the Insight navigation pane, click **Administration**.

   The **Administration** page appears.

Figure 743: *Administration Page*



Administration

File Transfer Settings

Host: Host

Protocol: ● SCP ○ SFTP

Port: 22

Username: admin

Password: ••••••••

Timeout: 30 seconds

Remote Directory:

Database Settings

Database Retention: 30 Days

Report Retention: 60 Days

CSV Report Limit: 50000 Rows

Support Information

- Insight database migration is supported.
- Configuration migration is not supported.
- Database retention default: 30 days
- Report retention default: 60 days
- CSV report limit: 50,000 rows

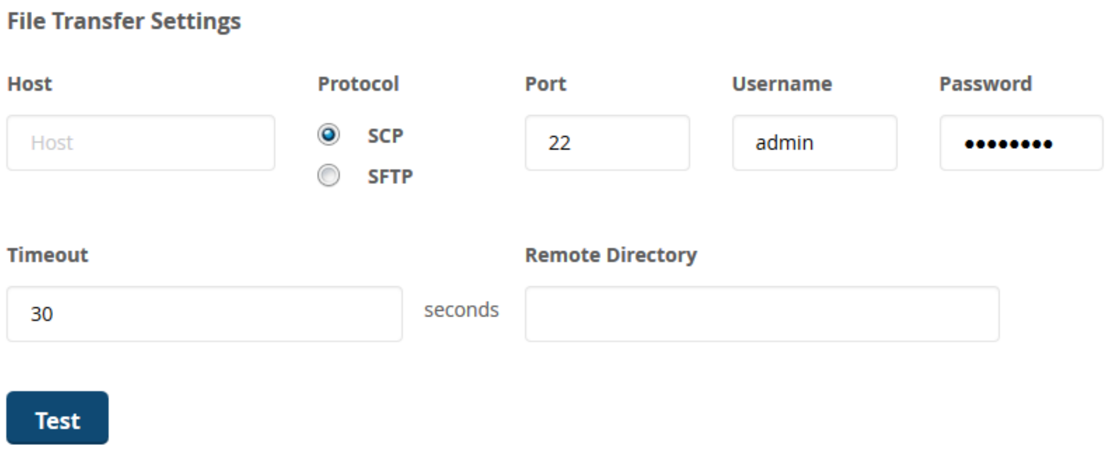
File Transfer Settings Configuration

You can specify the file transfer settings for uploading generated Insight reports to a FileStore.

To configure the File Transfer settings:

1. Navigate to the **Administration** page.

Figure 744: *Specifying the Insight File Transfer Settings*



File Transfer Settings

Host: Host

Protocol: ● SCP ○ SFTP

Port: 22

Username: admin

Password: ••••••••

Timeout: 30 seconds

Remote Directory:

2. In the **File Transfer Settings** section, enter the appropriate values as described in Table 386.
3. When finished, click **Save**.

Table 386: *Insight File Transfer Parameters*

Parameter	Action/Description
Host	1. Specify the IP address of the destination host FTP server.
Protocol	2. Specify the protocol to be used to upload the generated reports to a FileStore. You can select from the following protocols: ■ **SCP** (Session Control Protocol) ■ **SFTP** (SSH File Transfer Protocol)
Port	3. Specify the destination port number. The default destination port is **22**.
Username/Password	4. Enter the username and password of the host FTP server.
Timeout	5. Specify the timeout value in seconds. The default value is **30 seconds**.
Remote Directory	6. Specify the location where the generated reports are to be copied. If the remote directory location is same as default root of FTP, you can leave this field blank. **NOTE:** To copy reports to a remote directory, you must enable the **Reports** > **Create New Report** > **Enable remote copy** option.

Testing File Transfer Configuration

When you have configured the Insight file transfer settings, you can then test to see if file transfer is operational.

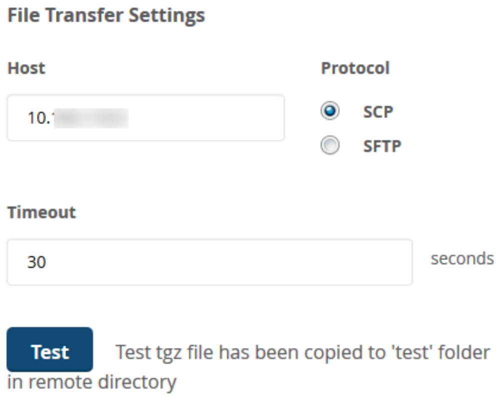
To test the Insight file transfer configuration:

1. Review the File Transfer Settings to ensure they are correct.
2. Click the **Test** button.

   You see the message: *File Transfer Settings testing in progress...*

   Then the following screen appears:

Figure 745: *Successful File Transfer Test*



File Transfer Settings

Host	Protocol	Port	Username	Password
10.[redacted]	● SCP ○ SFTP	22	root	••••••

Timeout: 30 seconds

Remote Directory: /tmp/test

Test

Test tgz file has been copied to 'test' folder in remote directory

You are now ready to commence transferring Insight files to the FTP server as needed.

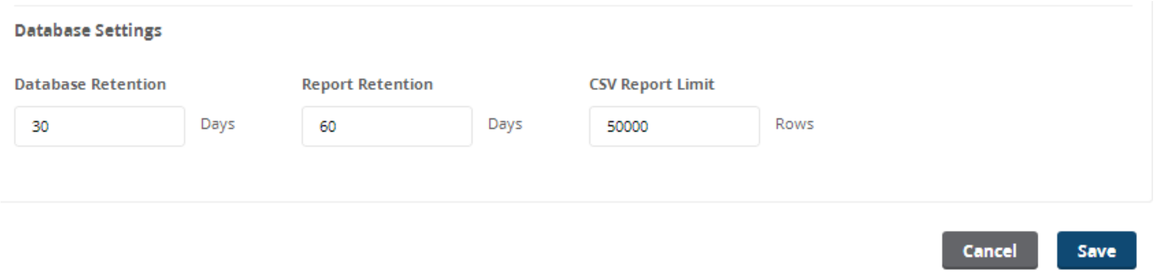
Database Settings Configuration

To configure the Insight database parameters:

1. Navigate to the **Administration** page.

   The **Database Settings** section is at the bottom of the **Administration** page.

Figure 746: *Specifying the Insight Database Settings*



Database Settings

Database Retention: 30 Days

Report Retention: 60 Days

CSV Report Limit: 50000 Rows

2. In the **Database Settings** section, enter the appropriate values as described in Table 387.
3. When finished, click **Save**.

Table 387: *Insight Database Parameters*

Parameter	Action/Description
Database Retention	1. Specify the number of days to retain the database. The supported range is from **1** to **730** days. The default value is **30 days**.
Report Retention	2. Specify the number of days to retain the generated reports. The supported range is from **1** to **365** days. The default value is **60 days**.
CSV Report Limit	3. Specify the number of rows for a CSV report. The supported range is from **1** to **50,000** rows. The default value is **50000** rows.

Managing Insight Admin Privileges

This section provides the following information:

- Overview
- Viewing the Default Insight Admin Privileges
- Defining Custom Insight Admin Privileges
- Insight UI Differences for Read-Only Users

Overview

ClearPass supports multilevel Insight administrators, each with a different level of administrative access to Insight.

ClearPass provides a default Admin Privileges Read-only Administrator. The default sets of admin privileges cannot be modified.

Each of the Insight modules (Dashboard, Reports, Alerts, and Administration) can have three privilege levels or no privileges:

- Read-only
- Read and Write

- Read, Write, and Delete

In the case of a user with no Insight admin privileges, the navigation panel on the left side of the Insight user interface is not visible.

Viewing the Default Insight Admin Privileges

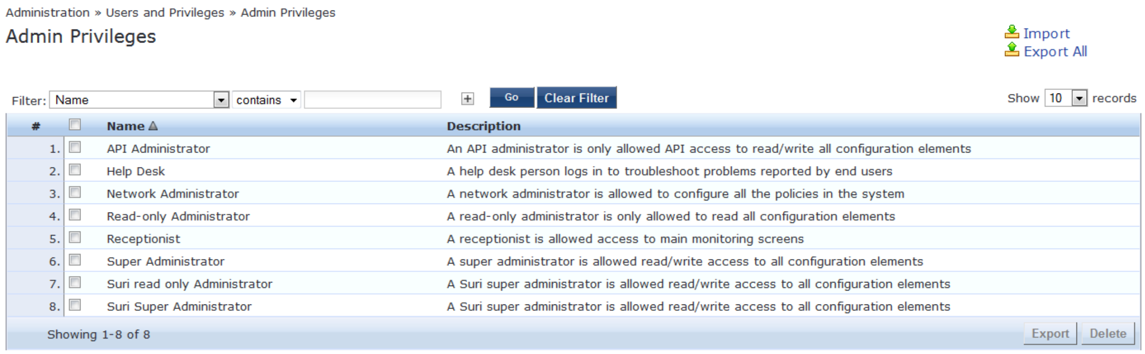
The settings for the default admin privileges cannot be modified.

To view the default Insight admin privileges defined in ClearPass:

1. Navigate to **Administration** > **Users and Privileges** > **Admin Privileges**.

   The **Admin Privileges** page opens.

Figure 747: *Admin Privileges Page*



Administration » Users and Privileges » Admin Privileges

Admin Privileges

#	□	Name ▲	Description
1.	□	API Administrator	An API administrator is only allowed API access to read/write all configuration elements
2.	□	Help Desk	A help desk person logs in to troubleshoot problems reported by end users
3.	□	Network Administrator	A network administrator is allowed to configure all the policies in the system
4.	□	Read-only Administrator	A read-only administrator is only allowed to read all configuration elements
5.	□	Receptionist	A receptionist is allowed access to main monitoring screens
6.	□	Super Administrator	A super administrator is allowed read/write access to all configuration elements
7.	□	Suri read only Administrator	A Suri super administrator is allowed read/write access to all configuration elements
8.	□	Suri Super Administrator	A Suri super administrator is allowed read/write access to all configuration elements

Showing 1-8 of 8

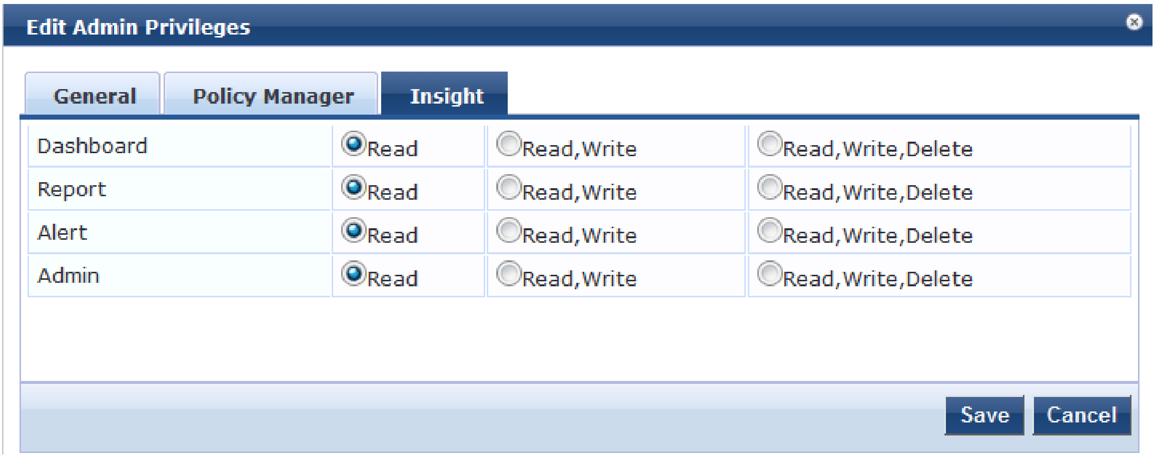
2. To view the Read-only admin privileges for Insight, select **Read-only Administrator**.

   The **Edit Admin Privileges** dialog opens.

3. Select the **Insight** tab.

   The default Insight admin privileges for the Read-only Administrator are displayed.

Figure 748: *Insight Read-Only Administrator Admin Privileges*



Edit Admin Privileges

Dashboard	● Read	○ Read,Write	○ Read,Write,Delete
Report	● Read	○ Read,Write	○ Read,Write,Delete
Alert	● Read	○ Read,Write	○ Read,Write,Delete
Admin	● Read	○ Read,Write	○ Read,Write,Delete

As shown in Figure 748, the default admin privileges for the Insight Read-only Administrator specifies Read-only access to all of the Insight modules—Dashboard, Reports, Alerts, and Administration.

Defining Custom Insight Admin Privileges

As described above, ClearPass provides a default Read-only Administrator. The default sets of admin privileges cannot be modified.

When a different set of admin privileges is needed (for example, if you require different admin privileges for the Report module than the admin privileges defined for the other Insight modules), you must create a new admin privileges administrator.

Insight privileges can be defined from two locations:

- Operator Profiles in ClearPass Guest
- Admin Privileges in ClearPass

To define custom admin privileges for Insight:

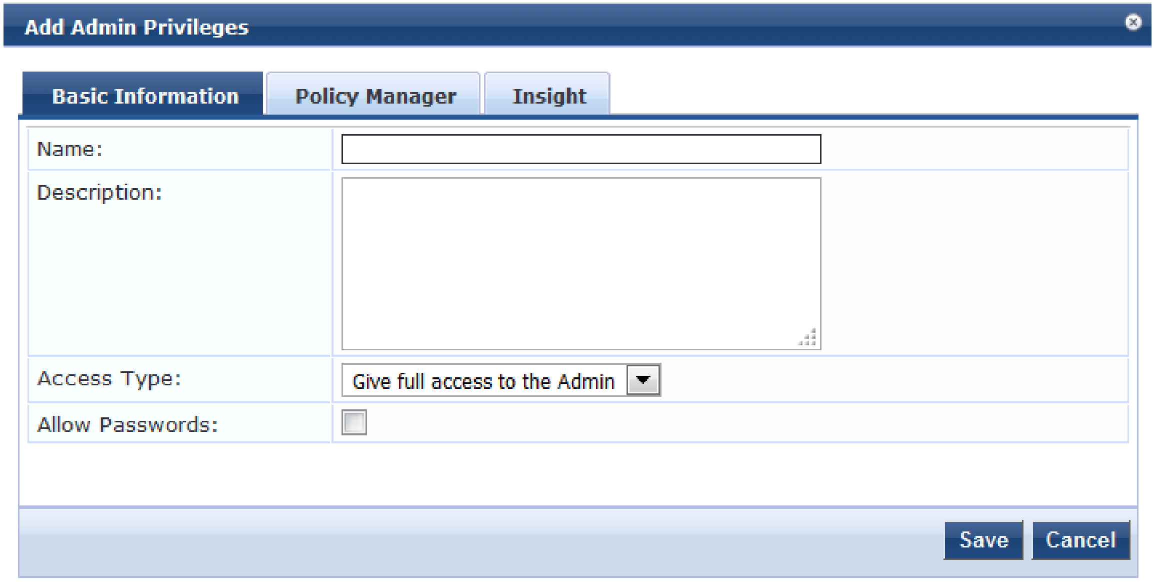
1. Navigate to **Administration** > **Users and Privileges** > **Admin Privileges**.

   The **Admin Privileges** page opens.

2. Click the **Add** link.

   The **Add Admin Privileges** dialog opens.

Figure 749: *Add Admin Privileges Dialog: Basic Information Tab*



Add Admin Privileges

Name:	
Description:	
Access Type:	Give full access to the Admin
Allow Passwords:	□

3. Specify the parameters in the **Basic Information** tab as described in Table 388.

Table 388: *Add Admin Privileges Parameters: Basic Information Tab*

Parameter	Action/Description
Name	1. Enter the name of the Admin Privileges administrator.
Description	2. Provide a description of this new admin privileges administrator.
Access Type	3. Select one of the following Access Types: ▪ Give full access to the Admin ▪ Give UI access to the Admin ▪ Give API access to the Admin
Allow Passwords	4. Select this check box if you want to allow password access.

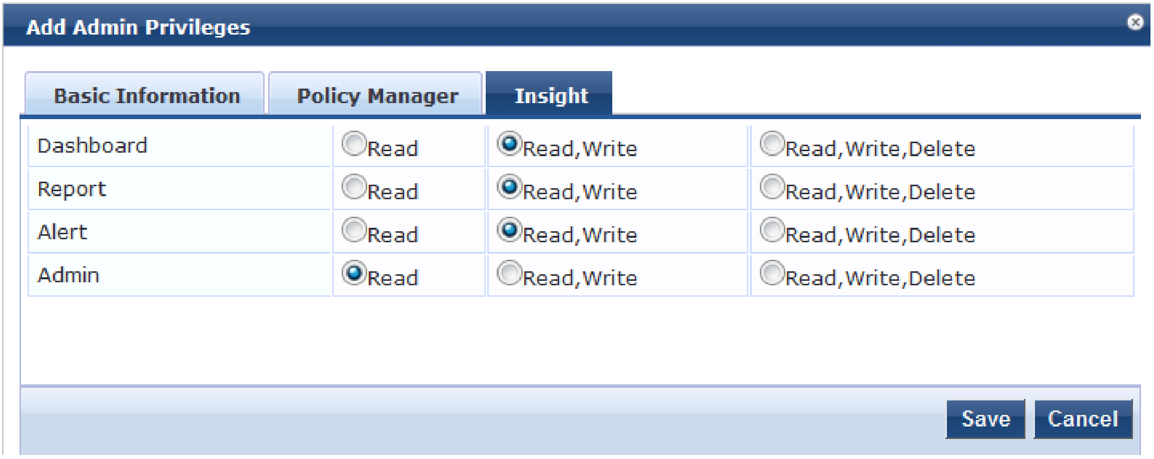
Specifying Insight Admin Privileges

To specify the Insight admin privileges for the new administrator:

1. When you complete the **Basic Information** parameters, select the **Insight** tab.

   The **Add Admin Privileges** > **Insight** dialog opens.

Figure 750: *Add Admin Privileges > Insight Dialog*



Dashboard	○Read	●Read,Write	○Read,Write,Delete
Report	○Read	●Read,Write	○Read,Write,Delete
Alert	○Read	●Read,Write	○Read,Write,Delete
Admin	●Read	○Read,Write	○Read,Write,Delete

You must configure the admin privileges for Policy Manager also, otherwise the changes to the Insight admin privileges cannot be saved.

2. Specify the desired admin privileges for each of the Insight modules, then click **Save**.

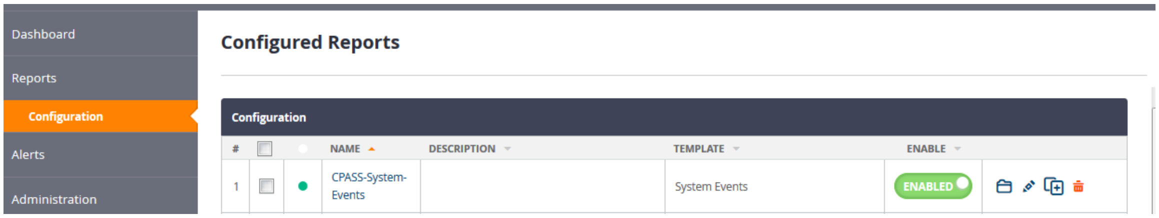
Insight UI Differences for Read-Only Users

When Insight is accessed by a user who has Read-only privileges for all four Insight modules (Dashboard, Reports, Alerts, and Administration), that user is not allowed to create or delete reports.

As shown in Figure 751, when a Read-only administrator logs in to Insight, the **Create New Report** button is not visible.

Likewise, the **Delete** icon on the **Configured Reports** table is not visible for a Read-only administrator.

Figure 751: *Create New Report Button Not Present for Read-Only User*



Configured Reports

Configuration

#	☐		NAME	DESCRIPTION	TEMPLATE	ENABLE	
1	☐	●	CPASS-System-Events		System Events	ENABLED	

Various action buttons, icons, and so on throughout the Insight user interface are shown only to users who are allowed to execute the actions provided by their admin privilege level.

Appendix A
Command Line Interface

Refer to the following sections to perform various tasks using the Command Line Interface (CLI):

- Cluster Commands on page 763
- Configure Commands on page 766
- Miscellaneous Commands on page 778
- Network Commands on page 772
- Service Commands on page 786
- Show Commands on page 788
- SSH Timed Account Lockout
- System Commands on page 797

Cluster Commands

The Policy Manager command line interface includes the following cluster commands:

- cluster drop-subscriber
- cluster list
- cluster make-publisher
- cluster make-subscriber
- cluster reset-database
- cluster set-cluster-passwd
- cluster sync-cluster-passwd

cluster 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
```

Table 389 describes the required and optional parameters for the **drop-subscriber** command:

Table 389: *Drop-Subscriber Command Parameters*

Parameter/Flag	Action/Description
-f	Enter the -f parameter to force ClearPass to drop even the nodes that are down.
-i <*IP Address*>	Specify the Management IP address of the node. If this IP address is not specified and the current node is a Subscriber, Policy Manager drops the current node.
-s	Restricts resetting the database on the dropped node. By default, Policy Manager drops the current node—if it's 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
```

cluster list

Use the **cluster list** command to list all the nodes in the cluster.

Syntax

```
cluster list
```

Example

The following example lists all the nodes in a cluster:

```
[appadmin]# cluster list
```

cluster make-publisher

Use the **cluster make-publisher** command to promote a specific subscriber node to be the publisher node in the same cluster.

When running this command, do not close the shell or interrupt the command execution.

Example

The following example promotes a subscriber node to publisher node status:

```
[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
```

To continue the **make-publisher** operation, enter **y**.

cluster make-subscriber

Run the **cluster make-subscriber** command on a standalone Publisher to make the standalone node a Subscriber node and add it to the cluster.

Syntax

```
cluster make-subscriber -b -i <IP address> [-l]
```

Table 390 describes the required and optional parameters for the **make-subscriber** command:

Table 390: *Cluster Make-Subscriber Command Parameters*

Parameter/Flag	Action/Description
-b	Generates a backup of the publisher before you make it a subscriber in the event the **make-subscriber** process fails and you need to restore the Publisher.
-i <*IP address*>	Specify the Publisher's IP address. This field is mandatory.
-l	Restores the local log database after this operation. This field is optional.

Example

The following example converts the node with IP address 192.xxx.1.1 to a subscriber node:

```
[appadmin]#  cluster make-subscriber –i 192.xxx.1.1 -l
```

cluster reset-database

Use the **reset-database** command to reset the local database and erase its configuration.

WARNING

Running this command erases the Policy Manager configuration and resets the database to its default configuration—all the configured data will be lost.

NOTE

When running this command, do not close the shell or interrupt the command execution.

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
```

To continue the **reset-database** operation, enter **y**.

cluster set-cluster-passwd

Use the **cluster set-cluster-passwd** command to change the cluster password on all nodes in the cluster. You may only issue this command from the publisher node.

NOTE

Setting the cluster password changes the **appadmin** password for all the nodes in the cluster

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

Continue? [y|n]: y

Enter Cluster Passwd: college.162

Re-enter Cluster Passwd: college.162

INFO - Password changed on local (publisher) node
Cluster password changed
```

cluster sync-cluster-passwd

Use the **cluster sync-cluster-passwd** command to synchronize the cluster (**appadmin**) password currently set on the publisher with all the subscriber nodes in the cluster.

> NOTE
>
> Synchronizing the cluster password changes the **appadmin** password for all the nodes in the cluster

Syntax

```
cluster sync-cluster-passwd
```

Example

The following example synchronizes the cluster password:

```
[appadmin]# cluster sync-cluster-passwd
Continue? [y|n]: y

Enter Password: college.205

Re-enter Password: college.205
```

Configure Commands

The Policy Manager command line interface includes the following **configure** commands:

- configure date
- configure dns
- configure fips-mode
- configure hostname
- configure ip
- configure ip6
- configure mtu
- configure timezone

configure date

Use the **configure date** command to set the 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 parameters for the **configure date** command:

Table 391: *Configure Date Command Parameters*

Flag/Parameter	Action/Description
-s <*ntpserver*>	Synchronize time with the specified NTP server name (see *Example 2* below). This field is optional. **NOTE:** You can specify a destination node with an IPv6 address enabled.
-d <*date*>	Specify the date with the syntax: **yyyy-mm-dd**. This field is mandatory.
-t <*time*>	Specify the time with the syntax: **hh:mm:ss**. This field is optional.
-z <*timezone*>	Specify the time zone syntax. To view the list of supported time zone values, enter **show all-timezones**. This field is optional.

Example 1

The following example configures the date, time, and the time zone:

```
[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]# configure date -s pool.ntp.org
```

configure dns

Use the **configure dns** command to configure DNS servers. You must specify a minimum of one DNS server; you can specify a maximum of three DNS servers.

Syntax

```
configure dns <primary> [secondary] [tertiary]
```

Example 1: DNS Server

The following example configures a DNS server:

```
[appadmin]# configure dns 192.168.xx.1
```

Example 2: Primary and Secondary DNS Servers

The following example configures the primary and secondary DNS servers. You can configure IPv6 address as described in this example.

```
[appadmin]# configure dns 192.168.xx.1 2001:4860:4860::8888
```

Example 3: Primary, Secondary, and Tertiary DNS Servers

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
```

configure fips-mode

Use the **configure fips-mode** command to enable or disable **FIPS** (Federal Information Processing Standard) mode.

> WARNING
>
> Running this command erases the ClearPass Policy Manager configuration settings and returns the database to the default configuration. All configured data will be lost. This command also shuts down all running applications and reboots the system.

Syntax

```
configure fips-mode [0|1]
```

The following table describes the parameters for the **configure fips-mode** command:

Table 392: *Configure fips-mode Command Parameters*

Flag/Parameter	Action/Description
0	To disable **FIPS** mode, enter **0**. Read the warning message carefully before enabling or disabling **FIPS** mode.
1	To enable **FIPS** mode, enter **1.**

Example 1

The following example disables **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
```

Clicking **y** in this example disables **FIPS** mode.

configure hostname

Use the **configure hostname** command to configure the hostname.

Syntax

```
configure hostname <hostname>
```

Example

The following example configures a hostname:

```
[appadmin]# configure hostname sun.us.arubanetworks.com
```

configure ip

Use the **configure ip** command to configure the IPv4 address of the management interface or the data interface, netmask, and gateway address.

Syntax

```
[appadmin]# configure ip <mgmt|data> <ipaddress> netmask <netmask address> gateway <gateway
address>
```

The following table describes the parameters used in the **configure ip** command:

Table 393: *Configure IP Command Parameters*

Flag/Parameter	Action/Description
ip <*mgmt*|*data*> <*IP address*>	Specify the network interface type: *management port interface* or *data point interface*. **<ip address>** specifies the IPv4 address of the host.
netmask <*netmask*>	Specify the netmask for the IP address.
gateway <*gateway address*>	Specify the IP address for the network gateway.

Example

The following example configures the IP address for the data interface, the netmask for that address, and the gateway address:

```
[appadmin]# configure ip data 192.168.xx.12 netmask 255.255.255.0 gateway 192.168.xx.1
```

configure ip6

Use the **configure ip6** command to configure the IPv6 address, netmask, and gateway address of the host.

Syntax

```
configure ip6 <mgmt|data> <IPv6 address/PrefixLen> gateway <gateway address>
```

```
configure ip6 <mgmt|data> <IPv6 address> netmask <netmask> gateway <gateway address>
```

The following table describes the parameters used in the `ip6` command:

Table 394: *Configure ip6 Command Parameters*

Flag/Parameter	Action/Description
ip6 <mgmt|data> <ip address>	Specifies the network interface type: management interface or data interface.
netmask <netmask>	Specifies the netmask. 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 interface, netmask, and gateway address:

```
[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
```

configure mtu

Use the **configure mtu** command to set the MTU (Maximum Transmission Unit) for the management and data port interfaces.

Running this command might cause the ClearPass server to lose network connectivity.

Syntax

```
configure mtu <mgmt|data> <mtu-value>
```

The following table describes the **configure mtu** command parameters:

Table 395: *Configure mtu Command Parameters*

Flag/Parameter	Action/Description
mtu <*mgmt|data*>	Specify the network interface types: *management port interface* or *data port interface*.
<*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

Use the **show ip** command to display 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

===========================================
```

configure timezone

Use the **configure timezone** command to interactively configure the time zone.

Syntax

```
configure timezone
```

Example

The following example configures the time zone 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 ClearPass Policy Manager command line interface includes the following **network** commands:

- network ip6
- network ip
- nslookup
- Network Commands on page 772
- network ping6
- network reset
- network traceroute6
- network traceroute

network ip6

Use the **network ip6** command to add, delete, or list custom routes to the data or management interface routing table in IPv6 networks.

Syntax: network ip6 add

```
network ip6 add <mgmt|data> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]> [-g <ViaAddr>]
```

The following table describes the required and optional parameters for the **network ip6** command:

Table 396: *Network IP6 Add Command Parameters*

Flag/Parameter	Description
<mgmt|data>	Specifies the management or the 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. A valid IPv6 address or a netmask or 0/0 values are allowed. This parameter is optional.

Table 396: *Network IP6 Add Command Parameters (Continued)*

Flag/Parameter	Description
`-d <DestAddr>`	Specifies the destination interface IPv6 address or netmask where the network IPv6 rule is specified. A valid IPv6 address or a 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. A valid IPv6 address is allowed. This parameter is optional.

Example: Adding an IPv6 Custom Route

You can use an IPv6 address when adding a custom route.

The following example adds a custom route:

```
[appadmin]# network ip6 add data -s fe82::20c:29ff:fe7e:d3e1/d3e24
```

Syntax: network ip6 del

This command deletes an IPv6 custom route.

```
network ip6 del <-i <id>>
```

Syntax: network ip6 list

This command lists all custom routing rules.

```
network ip6 list
```

Example: Listing All IPv6 Custom Routing Rules

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
===============================================
```

Syntax: network ip6 reset

network ip6 reset

This command resets the routing table to the factory default settings and all custom routes are removed.

network ip

Use the **network ip** command to add, delete, or list custom routes to the data or management interface routing table.

Syntax: network ip add

```
network ip add <mgmt|data|greN|vlanN> [-i <id>] <[-s <SrcAddr>] [-d <DestAddr>]> [-g
<ViaAddr>]
```

The following table describes the required and optional parameters for the **network ip add** command:

Table 397: *Network IP Add Command Parameters*

Flag/Parameter	Description
<mgmt | data| greN |vlanN>	Configures the management interface, data interface, the name of the GRE tunnel, or the VLAN number. - <greN>: N specifies the GRE tunnel number ranging from 1,2,3...N. - <vlanN>: N specifies the VLAN number.
-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 source IP address. 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 destination IP address. This parameter is optional.
-g <ViaAddr>	Specifies the via or gateway IP address through which the network traffic should flow. A valid IP address is allowed. This parameter is optional.

Syntax: network ip del

```
network ip del <-i <id>>
```

The following table describes the parameter for the **network ip del** command:

Table 398: *Network IP Del Command Parameters*

Flag/Parameter	Description
-i <id>	Specifies the ID of the rule to delete.

Syntax: network ip list

```
network ip list
```

This command lists all routing rules.

Example: Adding a Custom Route

The following example adds a custom route:

```
[appadmin]# network ip add data -s 192.168.xx.0/24
```

Example: Listing All Custom Routes

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
===============================================
```

Syntax: network ip reset

```
network ip reset
```

This command resets the routing table to the factory default settings. All custom routes are removed.

nslookup

Use the **network nslookup** command to get the IP address of the host using DNS.

Syntax: network nslookup

```
network nslookup -q <record-type> <host>
```

The following table describes the required and optional parameters for the **nslookup** command:

Table 399: *Network Nslookup Command Parameters*

Flag/Parameter	Description
<record-type>	Specifies the type of DNS record. The record types available are: - A - AAAA - CNAME - PTR - SRV
<host>	Specifies the host or domain name to be queried.

Example: Obtaining Address of Host or Domain

The following examples obtain the IPv4 and IPv6 addresses of the host or domain using DNS:

```
[appadmin]# nslookup sun.us.arubanetworks.com
[appadmin]# network nslookup 2001:4860:4860::8888
```

Example: Querying for SRV Records

The following example queries a host or domain for SRV records:

```
[appadmin]# nslookup -q SRV arubanetworks.com
```

Syntax

Use the **AAAA** flag with the **-q** option to perform network nslookup with IPv6 destinations.

```
nslookup -q  AAAA <IPv6_addr>
```

Example: Nslookup for IPv6 Address

The following example performs network nslookup for the destination with an IPv6 address:

```
[appadmin]# network nslookup 2001::93
Server:    2001::94
Address:   2001::94#53
3.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.2.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
```

network ping6

Use the **network ping6** command to test the reachability of the network host.

Syntax: network ping6

```
network ping6 [-i <SrcIPv6Addr>] [-t] <host>
```

The following table describes the required and optional parameters for the **network ping6** command:

Table 400: *Network Ping6 Command Parameters*

Flag/Parameter	Description
-i <SrcIPv6Addr>	Specifies the originating IPv6 address for the 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 an IPv6 network host to test its reachability:

```
[appadmin]# network ping6 -i fe82::20c:29ff:fe7e:d3e1 -t sun.us.
     arubanetworks

     .com
```

network ping

Use the **network ping** command to test the reachability of the network host.

Syntax: network ping

```
network ping [-i <SrcIpAddr>] [-t] <host>
```

The following table describes the required and optional parameters for the **network ping** command:

Table 401: *Network Ping Command Parameters*

Flag/Parameter	Description
-i <SrcIpAddr>	Specifies the originating IP address for the ping. This field is optional.
-t	Use this parameter to ping indefinitely. This field is optional.
<host>	Specifies the host to be pinged.

Example: Testing Reachability

The following example pings a network host to test the reachability:

```
[appadmin]# network ping –i 192.168.xx.10 –t sun.us.arubanetworks.com
```

network reset

Use the **network reset** command to reset the network data and management ports. You can use this command to reset both IPv4 and IPv6 addresses.

Syntax: network reset

```
network reset <data[v4|v6]/mgmt>
```

The following table describes the required and optional parameters for the **network reset** command:

Table 402: *Network Reset Command Parameters*

Flag/Parameter	Description
data [v4|v6]	Specifies the name of network data port to reset, as well as whether it is an IPv4 or IPv6 address. This parameter is mandatory.
mgmt	Specifies the name of network management port to reset.

Example

The following example resets the IPv6 network data port:

```
[appadmin]# network reset data v6
```

network traceroute6

Use the **network traceroute6** command to print the route taken to reach the IPv6 network host.

Syntax: network traceroute6

```
network traceroute6 <host>
```

The following table describes the required and optional parameters for the **network traceroute6** command:

Table 403: *Network Traceroute6 Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of network host. You can specify the host with an IPv6 address.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]# network traceroute6 sun.us.arubanetworks.com
```

network traceroute

Use the **network traceroute** command to print the route taken to reach the network host.

Syntax: network traceroute

```
network traceroute <host>
```

The following table describes the required parameter for the **network traceroute** command:

Table 404: *Network Traceroute Command Parameters*

Flag/Parameter	Description
<host>	Specifies the name of the network host.

Example

The following example prints the route taken to reach the network host:

```
[appadmin]# network traceroute sun.us.arubanetworks.com
```

Miscellaneous Commands

The Policy Manager command line interface includes the following miscellaneous commands:

- ad auth on page 778
- ad netjoin on page 779
- ad netleave on page 780
- ad passwd-server
- ad testjoin on page 781
- alias on page 781
- backup on page 781
- dump certchain on page 782
- dump logs on page 782
- dump servercert on page 783
- exit on page 783
- help on page 784
- krb auth on page 784
- krb list on page 784
- ldapsearch on page 785
- quit on page 785
- restore on page 785

ad auth

Use the **ad auth** command to authenticate the user against Active Directory.

Syntax

```
ad auth <username> -n <domain NetBIOS name>
```

The following table describes the parameters for the **ad auth** command:

Table 405: *AD Auth Command Parameter*

Flag/Parameter	Description
<username>	Specifies the username of the authenticating user. This is a mandatory parameter.
<domain NetBIOS name>	Specifies the domain name. This field is optional.

Example

The following example authenticates the user against Active Directory:

```
[appadmin]# ad auth jbrown -n cppm.sanfran1
```

ad netjoin

Use the **ad netjoin** command to join the host to the domain.

Syntax

```
ad netjoin <domain-controller.domain-name> [domain NetBIOS name] [domain REALM name]
[ou=<object container>]
```

The following table describes the parameters for the **ad netjoin** command:

Table 406: *AD Netjoin Command Parameters*

Parameter	Action/Description
<domain-controller. domain-name>	Specify the complete Fully Qualified Domain Name (FQDN) of the domain controller, including its hostname. For example, if **atlas.org** is the Domain FQDN and **DC01.atlas.org** is one of its domain controllers, then this argument would be correctly expressed as **DC01.atlas.org** This field is mandatory.
[domain NetBIOS name]	Specify the NetBIOS name of the domain (optional argument). You can specify this argument if the derived NetBIOS name is different from the actual name. This is an optional argument.
[domain REALM name]	You can specify this argument if the derived REALM is different from the actual. This is an optional argument.
[ou=<object container>]	If the computer account must be created in a different OU, this argument specifies the Object Container . For example '`ou=Domain Computer`' OR '`ou=Domain Computer+Linux Hosts`'. Note the usage of the separator '**+**' to specify the OU hierarchy.

Example

The following example joins the host to the domain:

```
[appadmin]# ad netjoin DC01.atlas.org.arubanetworks.com
```

ad netleave

Use the **ad netleave** command to remove the host from the domain.

Syntax

```
ad netleave <domain NetBIOS name> [-f]
```

Table 407: *AD Netleave Command Parameters*

Flag/Parameter	Description
<domain NetBIOS name>	Specifies the host to be joined to the domain. This field is mandatory.
-f	Forces the removal of Active Directory domain membership even if the operation fails.

Example

The following example removes the host from the domain:

```
[appadmin]# ad netleave balsamcollege.edu -f
```

ad passwd-server

Use the **ad passwd-server** command to do the following tasks:

- Set the password servers.
- List the configured password servers.
- Reset the password servers.

Syntax

```
ad passwd-server <server> <list> <reset>
```

Table 408: *AD passwd-server Command Parameters*

Flag/Parameter	Description
set ● -n <domain NetBIOS name> ● -s <Server1> [Server2 Server3 Server4 ...]	Sets the password servers. The **-n** parameter specifies the domain name. The **-s** parameter specifies one or more password server names.
list -n <domain NetBIOS name>	Lists the configured password servers.
reset -n <domain NetBIOS name>	Resets the password servers.

Example

The following example sets the configured password servers:

```
[appadmin]# ad passwd-server set -n balsamcollege.edu -s cppm.campus1
```

ad testjoin

Use the **ad testjoin** command to test if the **ad netjoin** command succeeded. This command also tests whether Policy Manager is a member of the Active Directory domain.

Syntax

```
ad testjoin <domain NetBIOS name>
```

Table 409: *AD Netjoin Command Parameter*

Flag/Parameter	Description
<domain NetBIOS name>	Specifies the host to be joined to the domain. This field is mandatory.

Example

The following example tests if the **ad testjoin** command succeeded:

```
[appadmin]# ad testjoin balsamcollege.edu
```

alias

Use the **alias** command to create or remove aliases.

Syntax

```
alias <name>=<command>
```

The following table describes the parameters for the **alias** command:

Table 410: *Alias Command Parameters*

Flag/Parameter	Description
<name>=<command>	Sets <name> as the alias for <command>.
<name>=	Removes the association.

Example 1

This example set the alias "**sh**" for the **show** command:

```
[appadmin]# alias sh=show
```

Example 2

This example removes the alias "**sh**":

```
[appadmin]# alias sh=
```

backup

Use the **backup** command to create a backup of Policy Manager configuration data. If no arguments are entered, the system automatically generates a filename and backs up the configuration to this file.

Syntax

```
backup [-f <filename>] [-c] [-l] [-r] [-w] [-P]
```

The following table describes the parameters for the **backup** command:

Table 411: *Backup Command Parameters*

Flag/Parameter	Description
[-f <filename>]	Specifies the backup target. If not specified, Policy Manager automatically generates a filename. This field is optional.
-c	Backs up ClearPass Policy Manager configuration data.
-l	Backs up ClearPass Policy Manager session log data.
-r	Backs up Insight data.
-P	Does not backup password fields from the configuration database. This field is optional.
-w	Backs up only the most recent records from the log database (the last one week).

Example

```
[appadmin]# backup -f PolicyManager-data.tar.gz
Continue? [y|Y]:  y
```

dump certchain

Use the **dump certchain** command to remove the certificate chain of any SSL-secured server.

Syntax

```
dump certchain <hostname:port-number>
```

The following table describes the parameter for the **dump certchain** command:

Table 412: *Dump Certchain Command Parameter*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example 1

The following example dumps the certificate chain of an SSL-secured server:

```
[appadmin]# dump certchain ldap.acme.com:636
```

dump logs

Use the **dump logs** command to remove 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 parameters for the **dump logs** command:

Table 413: *Dump Logs Command Parameters*

Flag/Parameter	Description
-f <output-file-name>	Specifies the target for concatenated logs.
-s yyyy-mm-dd	Specifies the start date range. The default value is today's date. This field is optional.
-e yyyy-mm-dd	Specifies the end date range. The default value is today's date. 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 the available log types:

```
[appadmin]# dump logs -h
```

dump servercert

Use the **dump servercert** command to remove the server certificate of an SSL-secured server.

Syntax

```
dump servercert <hostname:port-number>
```

The following table describes the parameter for the **dump servercert** command:

Table 414: *Dump Servercert Command Parameter*

Flag/Parameter	Description
<hostname:port-number>	Specifies the hostname and SSL port number.

Example

The following example removes the server certificate of the specified SSL-secured server:

```
[appadmin]# dump servercert ldap.acme.com:636
```

exit

Use the **exit** command to exit the 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 Active Directory).

Syntax

```
krb auth <user@domain>
```

The following table describes the parameter for the **krb auth** command:

Table 415: *Kerberos Authentication Command Parameter*

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 parameters for the **ldapsearch** command:

Table 416: *LDAP Search Command Parameter*

Flag/Parameter	Description
-B	Finds the bind DN (Distinguished Name) of the LDAP directory.
<user@hostname>	Specifies the username and the full qualified domain name of the host.

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 the 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 1

```
restore user@hostname:/<backup-filename> [-l] [-i] [-b] [-c] [-r] [-n|-N] [-s]
```

Syntax 2

```
restore http://hostname/<backup-filename>[-l] [-i] [-b] [-c] [-e] [-n|-N] [-s]
```

Syntax 3

```
restore <backup-filename>[-l] [-i] [-b] [-c] [-e] [-n|-N] [-s]
```

The following table describes the parameters for the **restore** command:

Table 417: *Restore Command Parameters*

Flag/Parameter	Description
- user@hostname:/<backup-filename> - http://hostname/<backup-filename> - <backup-filename>	Specifies the filepath of the the restore source.
-b	Does not backup the current configuration data before the restore operation starts.
-c	Restores ClearPass Policy Manager configuration data.
-l	If it exists in the backup file, restores the ClearPass Policy Manager log database. This field is optional.
-i	Ignores version mismatch errors and attempts data migration. This field is optional.
-n	Retains local node configuration data, such as certificates, after the restore operation (default).
-N	Does not retain local node configuration data after the restore operation.
-r	Restores Insight data if it exists in the backup.
-s	Restores cluster server/node entries from the backup file. Node entries are in a disabled state upon restore. This field is optional.

Example

The following example restores Policy Manager configuration data from the backup file:

```
[appadmin]# restore user@hostname:/tmp/cppm1-backup.tgz -l -i -c -s
```

Service Commands

The Policy Manager CLI includes the following **service** <*action*> commands:

- service list
- service restart
- service start
- service status
- service stop

service <*action*> <*service-name*>

Use the **service** <*action*> <*service-name*> command to control the specified Policy Manager service.

Syntax

```
service <action> <service-name>
```

Table 418: *Service Action Command Parameters*

Service Parameter	Description
action	1. Choose an action: - *list* - *restart* - *start* - *status* - *stop*
service-name	2. Choose a service: - *cpass-policy-server* - *cpass-tacacs-server* - *cpass-radius-server* - *cpass-admin-server* - *cpass-dbwrite-server* - *cpass-dbcn-server* - *cpass-repl-server* - *cpass-system-auxiliary-server* - *cpass-sysmon-server* - *cpass-domain-server_<NetBIOS_name>* - *airgroup-notify* - *fias_server* - *cpass-ipsec-service* - *cpass-vip-service* - *cpass-async-netd* - *cpass-statsd-server* - *cpass-igssyslog-server* - *cpass-igslogger-server* - *cpass-igslogrepo-server* - *cpass-carbon-server* - *cpass-multi-master-cache-server*

Example

```
[appadmin]# service list all
Policy server  [ cpass-policy-server ]
Admin UI service  [ cpass-admin-server ]
System auxiliary services  [ cpass-system-auxiliary-server ]
Radius server  [ cpass-radius-server ]
Tacacs server  [ cpass-tacacs-server ]
Async DB write service [ cpass-dbwrite-server ]
DB change notification server [ cpass-dbcn-server ]
DB replication service  [ cpass-repl-server ]

System monitor service  [ cpass-sysmon-server ]
Async network services [ cpass-async-netd ]
Multi-master cache [ cpass-multi-master-cache-server ]
Virtual IP service [ cpass-vip-service ]
Stats collection service [ cpass-statsd-server ]
Stats aggregation service [ cpass-carbon-server ]
ClearPass IPsec service [ cpass-ipsec-service ]
AirGroup notification service [ airgroup-notify ]
Micros Fidelio FIAS [ fias_server ]
Ingress logger service [ cpass-igslogger-server ]
Ingress syslog service [ cpass-igssyslog-server ]
```

Show Commands

The Policy Manager command line interface includes the following **show** commands:

- show all-timezones
- show date
- show dns
- show domain
- show fipsmode
- show fipsmode
- show hostname
- show ip
- show license
- show ntp
- show sysinfo
- show timezone
- show version

show all-timezones

Use the **show all-timezones** command to view all available time zones.

Syntax

```
show all-timezones
```

Example

The following displays an example of the **show all-timezones** command output:

```
[appadmin]# show all-timezones
America/Aruba
America/Barbados
America/Belem
America/Belize
[More]
```

show date

Use the **show date** command to view the system date, time, and time zone information.

Syntax

```
show date
```

Example

The following displays an example of the **show date** command output:

```
[appadmin]# show date
Wed Jan 27 14:33:39 UTC 2016
```

show dns

Use the **show dns** command to view DNS (Domain Name System) servers.

Syntax

```
show dns
```

Example

The following example of **show dns** command output displays the DNS servers configured for the current ClearPass server:

```
[appadmin]# show dns
===========================================
DNS Information
-------------------------------------------
Primary   DNS  :   192.xxx.5.3
Secondary DNS  :   <not configured>

Tertiary  DNS  :   <not configured>

===========================================
```

show domain

Use the **show domain** command to view the Active Directory Domain controller information.

NOTE

The **show domain** command is operational only when the current ClearPass server is joined to an Active Directory domain.

Syntax

```
show domain
```

Example

The following displays an example of the **show domain** command output:

```
[appadmin]# show domain

===============================================================

Domain Information

-------------------------------------------------------

Domain Name              : COLLEGE152.COM
Domain NETBIOS Name      : COLLEGE152
Domain Server IP Address : 10.xx.110

Domain Server Name       : balsam.college152.com
Domain Status            : online

-------------------------------------------------------

===============================================================
```

show fipsmode

Use the **show fipsmode** command to find whether **FIPS** (Federal Information Processing Standard) mode is enabled or disabled.

Example

The following example shows that **FIPS** mode is enabled:

```
[appadmin]# show fipsmode
FIPS Mode: Enabled
```

show hostname

Use the **show hostname** command to view the hostname of the current ClearPass server.

Syntax

```
show hostname
```

Example

The following displays an example of the **show hostname** command:

```
[appadmin]# show hostname

cppm.chicago.1
```

show ip

Use the **show ip** command to view the IPv4, IPv6, and DNS information of the host.

Syntax

```
show ip
```

Example

The following example of the **show ip** command 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:29:70:27:40
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.30

Secondary DNS  :   10.1.xx.50

Tertiary  DNS  :   10.1.xx.200

===========================================
```

show license

Use the **show license** command to view the Policy Manager license information.

Syntax

```
show license
```

Example

The following displays an example of the **show license** command output:

```
[appadmin]# show license
-------------------------------------------------------
Application              : PolicyManager
License key              : VKQO-MW62AB-VMVF-B7GNJX-OHUABC-IAAM-RTQUPQ-WODIFNJI-CD7N-I1325A

License key type         : Permanent
License added on         : 2016-01-11 10:16:38

Validity                 : <not applicable>
Issued for               : 5000 users
Customer id              : JCC

Licensed features         : <not applicable>

-------------------------------------------------------
Application              : PolicyManager
License key              : VKQO-MW62AB-VMVF-B7GNJX-OHUABC-IAAM-RTQUPQ-WODIFNJI-CD7N-I1325A
License key type         : Permanent
License added on         : 2016-01-11 10:16:38

Validity                 : <not applicable>
Issued for               : 5000 users
Customer id              : JCC

Licensed features         : <not applicable>

=======================================================
```

show ntp

Use the **show ntp** command to view the IP addresses of the primary and secondary Network Time Protocol (NTP) servers configured for the current ClearPass server.

Syntax

```
show ntp
```

Example

The following displays an example of the **show ntp** command output:

```
[appadmin]# show ntp

=================================================

NTP Server Information

-------------------------------------------

Primary   NTP  :    10.xx.x.1

Secondary NTP  :    <not configured>

===========================================
```

show sysinfo

Use the **show sysinfo** command to view the node uptime, disk utilization, and memory utilization information:

Syntax

```
show sysinfo
```

Example

The following displays an example of the **show sysinfo** command output:

```
[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%)
===========================================
```

show timezone

Use the **show timezone** command to view the current system time zone.

Syntax

```
show timezone
```

Example

The following displays an example of the **show timezone** command output:

```
[appadmin]#  show timezone

Timezone is set to 'Asia/Kolkata'
```

show version

Use the **show version** command to view the Policy Manager software version and the hardware model.

Syntax

```
show version
```

Example

The following displays an example of the **show version** command output:

```
[appadmin]# show version
=======================================
Policy Manager software version : 6.6(4).6649

Policy Manager model number     : ET-5010
=======================================
```

SSH Timed Account Lockout

This section provides the following information:

- Introduction
- SSH Account Lockout Configuration
- SSH Account Lockout Alerts
- SSH Account Lockout Behavior

Introduction

The **SSH Timed Account Lockout** feature provides an administrator with the ability to configure the number of successive unsuccessful authentication attempts for administrators attempting to authenticate remotely.

When the defined number of unsuccessful authentication attempts has occurred, the CLI account is locked and administrators cannot log in to the system via the CLI until one of the following conditions are met:

- Prevent the offending remote administrator from successfully authenticating until an action is taken by a local administrator.
- Prevent the offending remote administrator from successfully authenticating until time period defined by the administrator has elapsed.

Node-Specific

This feature is node-specific. In a cluster with multiple nodes, SSH timed account lockout must be configured on each node in the cluster.

NOTE

The **cluster reset-database** command does not impact this feature.

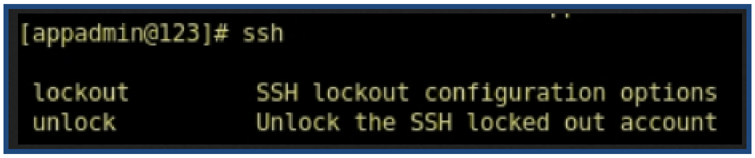
Account Lockout Persistence

- The SSH timed account lockout feature configuration persists across reboots, updates and upgrades.
- The account lock status persists across reboots.

SSH Account Lockout Configuration

The **SSH Timed Lockout** options are exposed as a part of the **ssh** command set.

Figure 752: *SSH Command Set*



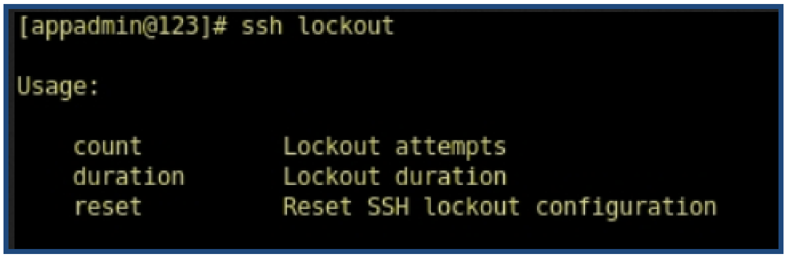
```
[appadmin@123]# ssh

 lockout          SSH lockout configuration options
 unlock           Unlock the SSH locked out account
```

SSH Lockout

The **ssh lockout** command set provides ability to configure SSH lockout configuration options. This command exposes three options :

- count
- duration
- reset

Figure 753: *SSH Lockout Command Set*

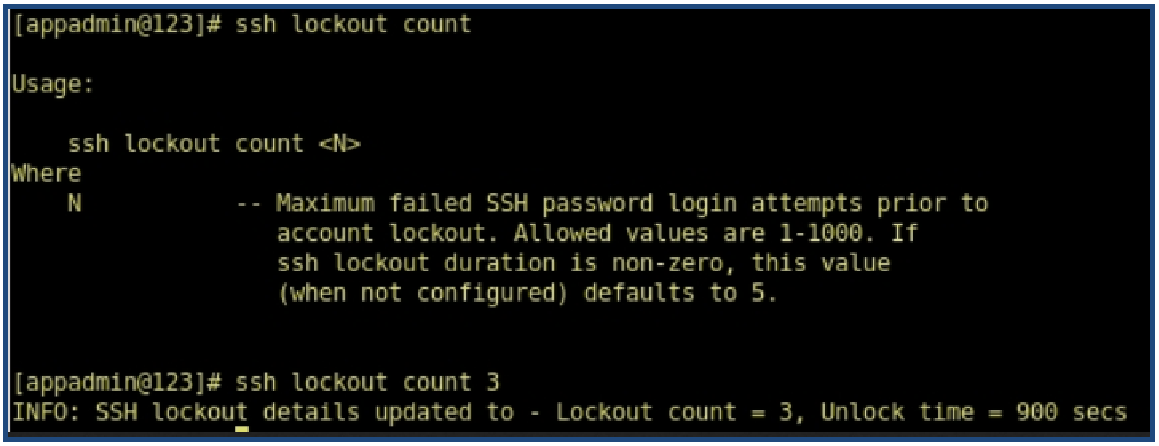


```
[appadmin@123]# ssh lockout

Usage:

    count          Lockout attempts
    duration       Lockout duration
    reset          Reset SSH lockout configuration
```

SSH Lockout Count

Sets the maximum number of failed login attempts before the account is locked out. The default is **5**.

Figure 754: *SSH Lockout Count Command*



```
[appadmin@123]# ssh lockout count

Usage:

    ssh lockout count <N>
Where
    N           -- Maximum failed SSH password login attempts prior to
                   account lockout. Allowed values are 1-1000. If
                   ssh lockout duration is non-zero, this value
                   (when not configured) defaults to 5.


[appadmin@123]# ssh lockout count 3
INFO: SSH lockout details updated to - Lockout count = 3, Unlock time = 900 secs
```

Syntax

```
ssh lockout count <N>
```

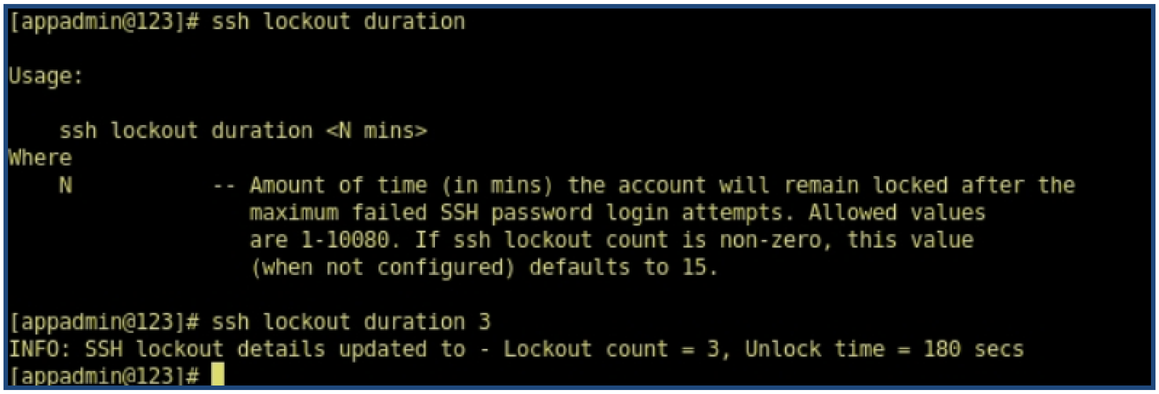
Example

ssh lockout count 3

SSH Lockout Duration

Sets the amount of time in minutes that the account will remain locked after the number of SSH password login attempts exceeds the SSH lockout count.

Figure 755: *SSH Lockout Duration Command*



```
[appadmin@123]# ssh lockout duration

Usage:

    ssh lockout duration <N mins>
Where
    N            -- Amount of time (in mins) the account will remain locked after the
                    maximum failed SSH password login attempts. Allowed values
                    are 1-10080. If ssh lockout count is non-zero, this value
                    (when not configured) defaults to 15.

[appadmin@123]# ssh lockout duration 3
INFO: SSH lockout details updated to - Lockout count = 3, Unlock time = 180 secs
[appadmin@123]#
```

Syntax

```
ssh lockout duration <N minutes>
```

Example

```
ssh lockout duration 3
```

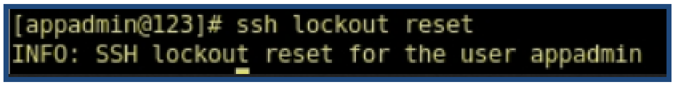
SSH Lockout Reset

Resets the SSH lockout count and duration to factory defaults and disables this feature.

NOTE

The SSH timed account lockout feature is disabled by default.

Figure 756: *SSH Lockout Reset Command*



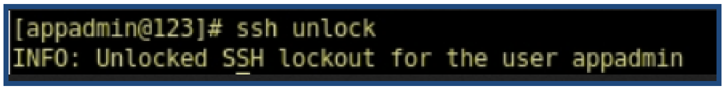
```
[appadmin@123]# ssh lockout reset
INFO: SSH lockout reset for the user appadmin
```

SSH Unlock

Unlocks any SSH locked accounts.

When the account is locked, you can perform this operation by logging into the system via the console or from a host that is enabled for SSH public key authentication with ClearPass.

Figure 757: *SSH Unlock Command*

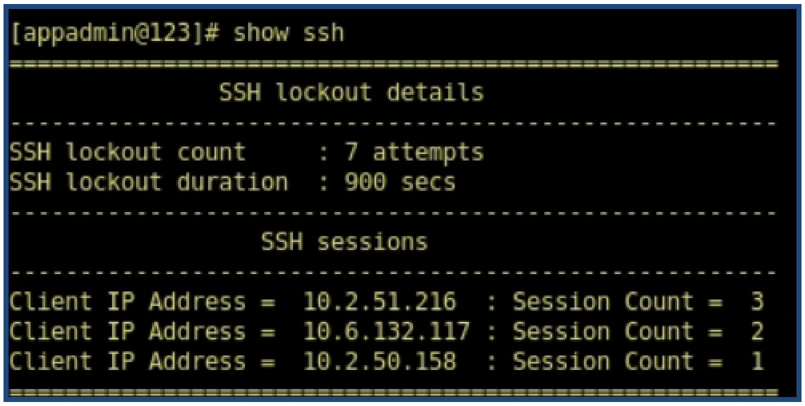


```
[appadmin@123]# ssh unlock
INFO: Unlocked SSH lockout for the user appadmin
```

Show SSH

Shows the SSH lockout configuration settings and the active SSH client sessions.

Figure 758: *Show SSH Command*



```
[appadmin@123]# show ssh
=======================================================
               SSH lockout details
-------------------------------------------------------
SSH lockout count      : 7 attempts
SSH lockout duration   : 900 secs
-------------------------------------------------------
                  SSH sessions
-------------------------------------------------------
Client IP Address =  10.2.51.216  : Session Count =  3
Client IP Address =  10.6.132.117 : Session Count =  2
Client IP Address =  10.2.50.158  : Session Count =  1
=======================================================
```

SSH Account Lockout Alerts

Alerts for SSH lockout events are logged in to the Event Viewer when any of the following conditions are present:

- SSH lockout configurations are performed
- Account is locked
- Account is unlocked
- Failed SSH login attempts

SSH Account Lockout Behavior

The SSH account lockout feature is disabled by default.

1. To enable SSH account lockout:
   - Perform the **ssh lockout count** or **ssh lockout duration** configuration options.
2. To disable the feature, perform **ssh lockout reset**.
3. If the SSH account lockout feature is configured with **failed attempts=3** and **unlock time = 5 minutes:**
   - CLI access via SSH (password-based) authentication is locked on three consecutive failed login attempts.
   - If the failed password attempt continues (even after the account is locked), the unlock time shifts for the next five minutes (as in this example) from the current time from the last failed login attempt.
   - Successful password-based SSH logins are rejected during the lockout period.
   - Console-based logins are allowed during the lockout period.
   - SSH logins via public key methods are allowed during the lockout period.
4. Administrators can use any of the above options to reset the SSH account lockout by issuing the **ssh unlock** command.
5. After the lockout period, successful SSH logins are accepted and the account is unlocked.

System Commands

The Policy Manager command line interface (CLI) includes the following **system** commands:

- system apps-access-reset
- system boot-image
- system cleanup
- system create-api-client
- system gen-recovery-key
- system gen-support-key
- system install-license
- system morph-vm
- system refresh-license
- system reset-server-certificate
- system restart
- system shutdown
- system sso-reset
- system start-rasession
- system status-rasession
- system terminate-rasession
- system update
- system upgrade

system apps-access-reset

Use the **system 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
```

system boot-image

Use the **system boot-image** command 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 **system boot-image** command:

Table 419: *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
```

system cleanup

Use the **system cleanup** command to perform a system cleanup operation that purges the following records:

- System and application log files
- Past authentication records
- Audit records
- Expired guest accounts
- Past auto and manual backups
- Stored reports

Syntax

```
system cleanup <num_days>
```

The following table describes the required parameter for the **system cleanup** command:

Table 420: *System Cleanup Command Parameter*

Flag/Parameter	Description
<num_days>	This is the cleanup interval that specifies the number of days to retain the data. This field is mandatory.

Example

The following example performs a system cleanup operation that retains records for four days:

```
[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
```

system create-api-client

Use the **system create-api-client** command create a new API client.

Syntax

```
system create-api-client <Client_ID> <Client_Secret>
```

Example

The following example creates an API client and specifies the client ID and client secret:

```
system create-api-client Win.139 college52
```

system gen-recovery-key

Use the **system 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='
```

system gen-support-key

Use the **system 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='
```

system install-license

Use the **system 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 parameter for the **system install-license** command:

Table 421: *System Install-License Command Parameter*

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 API11-3117-90982-007
```

system morph-vm

Use the **system morph-vm** command to convert an evaluation virtual machine (VM) to a production virtual machine .

With this command, licenses are still required to be installed after the morph operation is completed.

To convert an evaluation virtual machine to a production virtual machine:

1. Determine the type of the appliance to which you want to morph your evaluation virtual machine .
2. Procure the license for the target virtual appliance.
3. Shut down the virtual machine.
4. Determine the required capacity of an additional hard disk and attach it to the target virtual appliance.
5. Adjust the CPU and Memory settings for the evaluation virtual machine to match the target virtual appliance.
6. Boot the virtual machine.
7. Execute the **system morph-vm** command.

   The configuration data from the evaluation virtual machine will be migrated to the newly-attached disk. The node will reboot as a virtual machine of the selected appliance model.
8. Log in to the user interface and enter the permanent license.

   The evaluation virtual machine is now a production virtual machine .

Syntax

```
system morph-vm <CP-VA-500 | CP-VA-5K | CP-VA-25K>
```

The following table describes the parameters for the **system morph-vm** command:

Table 422: *System Morph-VM Command*

Flag/Parameter	Description
<vm-version>	This is the updated ClearPass version of the virtual appliances. The following 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 to a production CP-25K virtual appliance:

```
[appadmin]# system morph-vm CP-VA-25K
```

system refresh-license

Use the **system 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
```

system reset-server-certificate

Use the **system reset-server-certificate** command to reset the HTTP server certificate or RADIUS server certificate or both.

After executing the command, the Policy Manager services are restarted to reflect the changes.

Syntax

```
System reset-server-certificate
```

Example

The following example resets both HTTP and RADIUS server certificates:

```
[appadmin]# system reset-server-certificate

***************************************************************
*                                                             *
* WARNING: When the command is completed Policy Manager services *
* are restarted to reflect the changes.                       *
*                                                             *
***************************************************************
Continue? [y|n]: y
0: Reset Http and Radius Server Certificates
1: Reset Radius Server Certificate
2: Reset Http Server Certificate
3: Quit
2
Updating the server certificate...
Updation of server certificate complete
```

system restart

Use the **system restart** command to restart the system.

CAUTION

Executing this command shuts down all running applications and reboots the system.

Syntax

```
system restart
```

Example

The following example restarts the system with a confirmation before proceeding:

```
[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
```

system shutdown

Use the **system shutdown** command to shut down the current ClearPass server.

CAUTION

Executing this command shuts down all running applications and powers off the system.

Syntax

```
system shutdown
```

Example

The following example shuts down the system with a confirmation before proceeding:

```
[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
```

system sso-reset

Use the **system sso-reset** command to reset the Single Sign-On (SSO) configuration.

Syntax

```
system sso-reset
```

system start-rasession

Use the **system start-rasession** command to start a Remote Assistance (RA) session.

Syntax

```
system start-rasession [duration_hours | duration_mins | contact_id | cppm_server_ip]
```

The following table describes the parameters for the **system start-rasession** command:

Table 423: *System Start Remote Assistance Session Command Parameters*

Flag/Parameter	Action/Description
duration_hours	1. Specify the session duration in hours. You can specify values from 0 to 12.
duration_mins	2. Specify the session duration in minutes. You can specify values from 0 to 59.
contact_id	3. Enter the username ID part of the Aruba TAC or Engineering contact.
cppm_server_ip	4. Specify the ClearPass Policy Manager server IP address.

system status-rasession

Use the **system status-rasession** command to view the status of a Remote Assistance session.

Syntax

```
system status-rasession <session_id>
```

Example

The following example displays the status of a Remote Assistance session 3001:

```
[appadmin]# system status-rasession 3001
```

system terminate-rasession

Use the **system terminate-rasession** command to terminate a running Remote Assistance session.

Syntax

```
system terminate-rasession <session_id>
```

Example

The following example terminates a running RemoteAssist session 3001:

```
[appadmin]# system terminate-rasession 3001
```

system update

The **system 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 **system update** command:

Table 424: *System Update Command Parameters*

Flag/Parameter	Description
-i user@hostname:/<filename> | http://hostname/<filename>	Installs the specified patch on the system. This field is optional.
-f	Reinstalls 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.

NOTE

This command supports Secure Copy (SCP), HTTPS, HTTP, and local uploads.

Example

The following example of the system update command will reinstall the patch if necessary and list the patches currently installed on the ClearPass server:

```
[appadmin]# system update -f -l
```

system upgrade

The **system upgrade** command upgrades the system. This command provides you with the following system upgrade options:

- From a Linux server
- From a Web server
- Performing an offline upgrade

Syntax

- **Upgrading from a Linux server**

  ```
  system upgrade user@hostname:/<filepath> [-w] [-l] [-L]
  ```

  See Example 1: Upgrading from a Linux Server.

- **Upgrading from a Web server**

  ```
  system upgrade http://hostname/<filepath> [-w] [-l] [-L]
  ```

  See Example 2: Upgrading from a Web Server.

- **Performing an offline upgrade**

  ```
  system upgrade <filepath> [-w] [-l] [-L]
  ```

  See Example 3: Performing an Offline Upgrade.

Table 425: *System Upgrade Command Parameters*

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.

Table 425: *System Upgrade Command Parameters (Continued)*

Flag/Parameter	Description
<filepath>	Enter the filepath using the syntax provided in the two examples below. This field is mandatory.

NOTE

This command supports Secure Copy (SCP), HTTPS, HTTP, and local uploads.

NOTE

If none of these **system upgrade** command options are specified, 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.arubanetworks.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.arubanetworks.com/downloads/PolicyManager-x86-64-upgrade-71.tgz
   ```

Example 3: Performing an Offline Upgrade

To perform an offline upgrade:

1. Log in to the Aruba 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 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 ClearPass Policy Manager.

SNMP Private MIB, SNMP Traps, System Events, Error Codes

This appendix contains the following information:

- ClearPass SNMP Private MIB
- SNMP Trap Details
- Important System Events
- Error Codes

ClearPass SNMP Private MIB

This section contains the following information:

- Introduction
- System MIB Entries
- RADIUS Server MIB Entries
- Policy Server MIB Entries
- Web Authentication Server MIB Entries
- TACACS+ Server MIB Entries
- Network Traffic MIB Entries

Introduction

A MIB (Management Information Base) is a collection of definitions that define the properties of the managed object within the device to be managed. The various pieces of information are accessed by a protocol such as SNMP.

This section describes the MIB objects exposed and traps sent through the ClearPass Policy Manager Private SNMP MIB.

System MIB Entries

Table 426 describes the *CPPMSystemTableEntry* MIB objects.

Table 426: *CPPMSystemTableEntry System MIB Objects*

MIB Object	Description
cppmClusterNodeType	ClearPass cluster node type indicating whether the node is a Publisher or Subscriber
cppmNwDataPortIPAddress	ClearPass server data port IP address
cppmNwDataPortMACAddress	ClearPass server data port MAC address
cppmNwMgmtPortIPAddress	ClearPass server management port IP address

Table 426: *CPPMSystemTableEntry System MIB Objects (Continued)*

MIB Object	Description
cppmNwMgmtPortMACAddress	ClearPass server management port MAC address
cppmSystemDiskSpaceFree	Amount of disk space free (in bytes) in the ClearPass server
cppmSystemDiskSpaceTotal	Total amount of disk space available (in bytes) in the ClearPass server
cppmSystemHostname	ClearPass server host name
cppmSystemMemoryFree	Amount of memory free (in bytes) in the ClearPass server
cppmSystemMemoryTotal	Total amount of memory available (in bytes) in the ClearPass server
cppmSystemModel	Model of the ClearPass server
cppmSystemNumCPUs	Total number of CPUs in the ClearPass server
cppmSystemSerialNumber	Serial number of the ClearPass server
cppmSystemUptime	Amount of time the ClearPass server has been up
cppmSystemVersion	Product version of the ClearPass server

RADIUS Server MIB Entries

RadiusServerTableEntry

Table 427 describes the *RadiusServerTableEntry* objects.

Table 427: *RadiusServerTableEntry Objects*

MIB Object	Description
radAuthRequestTime	Total time taken for an end-to-end RADIUS request
radPolicyEvalTime	Time taken for policy evaluation from the RADIUS server perspective
radServerCounterCounts	Total number of successful RADIUS authentications
radServerCounterFailure	Total number of failed RADIUS authentications
radServerCounterSuccess	Total number of successful RADIUS authentications

RadiusServerAuthTableEntry

RadiusServerAuthTableEntry exposes the following counters that refer to *authSourceName* wherever applicable (see Table 428). Counters and delays reflect details that are logged into Graphite.

Table 428: *RadiusServerAuthEntry MIB MIB Objects*

MIB Object	Description
radAuthCounterCount	Total number of RADIUS authentications
radAuthCounterFailure	Total number of failed RADIUS authentications
radAuthCounterSuccess	Total number of successful RADIUS authentications
radAuthCounterTime	Time taken to perform RADIUS authentications
radAuthSourceName	Name of the RADIUS server authentication source

Policy Server MIB Entries

PolicyServerTableEntry

PolicyServerTableEntry exposes the following MIB objects (see Table 429). Counters and delays reflect details logged into Graphite.

Table 429: *PolicyServerTableEntry Objects*

MIB Object	Description
psAuditPolicyEvalCount	Audit policy evaluation count
psAuditPolicyEvalTime	Audit policy evaluation time
psAuthCounterFailure	Number of failed Policy Server authentications
psAuthCounterSuccess	Number of successful Policy Server authentications
psAuthCounterTotal	Total number of Policy Server authentications
psEnforcementPolicyEvalCount	Enforcement policy evaluation count
psEnforcementPolicyEvalTime	Enforcement policy evaluation time
psPosturePolicyEvalCount	Posture policy evaluation count
psRestrictionPolicyEvalCount	Authorization restriction policy evaluation count
psRolemappingPolicyEvalCount	Role mapping policy evaluation count

Table 429: *PolicyServerTableEntry Objects (Continued)*

MIB Object	Description
psRolemappingPolicyEvalTime	Role mapping policy evaluation time
psPosturePolicyEvalTime	Posture policy evaluation time
psRestrictionPolicyEvalTime	Restriction policy evaluation time
psServicePolicyEvalCount	Service policy evaluation count
psServicePolicyEvalTime	Service policy evaluation time
psSessionlogTime	Policy Server session logging time

PolicyServerProtoTableEntry

PolicyServerProtoTableEntry exposes MIB objects for the counter values for the RADIUS, TACACS, WEBAUTH, and APPLICATION protocols.

Table 430: *PolicyServerProtoTableEntry MIB Objects*

MIB Object	Description
psPolicyEvalTime	Policy evaluation time for the protocol
psProtocolName	Name of the protocol

PolicyServerAutzTableEntry

PolicyServerAutzTableEntry exposes MIB objects for authorization counters (see Table 431).

Table 431: *PolicyServerAutzTableEntry MIB Objects*

MIB Object	Description
psAutzCounterCount	Total number of Policy Server authorizations
psAutzCounterFailure	Number of failed Policy Server authorizations
psAutzCounterSuccess	Number of successful Policy Server authorizations
psAutzCounterTime	Time taken to perform Policy Server authorizations
psAutzAuthSourceName	Name of the Policy Server authorization source

Web Authentication Server MIB Entries

WebAuthProtoTableEntry exposes MIB objects for the WebLogin, AppLogin, SamlIdp, and SamlSp web authentication protocols.

Table 432: *WebAuthProtoTableEntry MIB Objects*

MIB Object	Description
waAuthCounterAuthTime	Time taken for web authentication
waAuthCounterCount	Total number of web authentications
pwaAuthCounterFailure	Number of failed web authentications
waAuthCounterSuccess	Number of successful web authentications
waAuthCounterTime	Total time taken for web login
waPolicyEvalTime	Time taken to perform policy evaluation
waProtocolName	Name of the protocol
pwaServicePolicyEvalTime	Time taken to perform service policy evaluation

TACACS+ Server MIB Entries

TacacsAuthTableEntry

TacacsAuthTableEntry exposes MIB objects for TACACS+ authentication counters.

Table 433: *TacacsAuthTableEntry Objects*

MIB Object	Description
tacAuthCounterAuthTime	Time taken for TACACS+ authentications
tacAuthCounterCount	Total number of TACACS+ server authentications
tacAuthCounterFailure	Number of failed TACACS+ server authentications
tacAuthCounterSuccess	Number of successful TACACS+ server authentications
tacAuthCounterTime	Total time taken for TACACS+ login
tacPolicyEvalTime	Time taken to perform policy evaluation
tacServicePolicyEvalTime	Time taken to perform service policy evaluation

TacacsAutzTableEntry

TacacsAutzTableEntry exposes MIB objects for TACACS+ authorization counters.

Table 434: *TacacsAuthTableEntry Objects*

MIB Object	Description
tacAutzCounterCount	Total number of TACACS+ server authorizations
tacAutzCounterFailure	Number of failed TACACS+ server authorizations
tacAutzCounterSuccess	Number of successful TACACS+ server authorizations
tacAutzCounterTime	Total time taken for TACACS+ authorizations

Network Traffic MIB Entries

NetworkTrafficTableEntry exposes MIB objects for network protocol and applications. These MIB objects cover the following:

- agent_controller (6658)
- db (5432)
- http (80)
- https (443)
- ntp (123)
- radius (1645, 1646, 1812, 1813)
- ssh (22)
- tacacs (49)

Table 435: *TacacsAuthTableEntry Objects*

MIB Object	Description
nwAppPort	Application port
nwAppName	Application name
nwTrafficTotal	Total network traffic in bytes

ClearPass SNMP Traps and OIDs

This section provides the following information:

- Introduction
- ClearPass SNMP Traps

Introduction

This section describes the traps that ClearPass Policy Manager supports as part of the ClearPass SNMP Private MIB.

Table 436 provides the description and OID (Object Identifier) for each ClearPass SNMP trap. OIDs uniquely identify managed objects in a MIB hierarchy.

ClearPass SNMP Traps

Table 436: *SNMP Traps Supported by the SNMP Private MIB*

SNMP Trap	Description and OID
cppmLicenseExpiry	● Indicates that one or more licenses associated with a ClearPass application <*cppmNodeApplicationName*> on the ClearPass server will expire in <*cppmLicenseDaysRemaining*> days. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1001
cppmActivationExpiry	● Indicates that one or more licensing activations associated with the <*cppmNodeApplicationName*> on the ClearPass Server will expire in <*cppmActivationDaysRemaining*> days. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1002
cppmNodeCertExpiry	● Indicates that a server certificate associated with the <*cppmNodeCertApplicationName*> on the ClearPass Server will expire in <*cppmCertDaysRemaining*> days. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1003
cppmLowDiskSpace	● Indicates that the system is running low on disk space as indicated by <*cppmDiskSpaceRemaining*> with the units specified in <*cppmResourceUnit*>. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1004
cppmLowMemory	● Indicates that the system is running low on memory as indicated by <*cppmMemoryRemaining*> with the units specified in <*cppmResourceUnit*>. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1005
cppmClusterNodeAddNotification	● Indicates the addition of a ClearPass node to the cluster. ■ <*cppmClusterServerIp*> indicates the IP address of the node added to the cluster. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1006
cppmClusterNodeDelNotification	● Indicates that a ClearPass node has been deleted from the cluster. ■ <*cppmClusterServerIp*> indicates the IP address of the node removed from the cluster. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1007
cppmClusterNodePromNotification	● Indicates the promotion of a ClearPass node to Publisher status. ■ <*cppmClusterServerIp*> indicates the IP address of the node promoted to Publisher. ● **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1008
cppmClusterNodeDbldNotification	● Indicates that a ClearPass node in the cluster has been disabled. ■ <*cppmClusterServerIp*> indicates the IP address of the disabled node.

Table 436: *SNMP Traps Supported by the SNMP Private MIB (Continued)*

SNMP Trap	Description and OID
	- **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1009
cppmClusterNodeNSyncNotification	- Indicates the ClearPass node in the cluster that is in the out-of-sync state. ■ <*cppmClusterServerIp*> indicates the IP address of the out-of-sync node. ■ <*cppmClusterOutOfSyncMinutes*> indicates the number of minutes that the node has been out-of-sync. - **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1010
cppmClusterPwdChangedNotification	- Indicates that the cluster password has been changed. - **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1011
cppmConfigReset	- Indicates that the ClearPass node's configuration has been reset. - **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1012
cppmConfigRestore	- Indicates that the ClearPass node's configuration has been restored. - **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1013
cppmUpdateNotification	- Indicates that the CPPM node's installation has been updated. - **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1014
cppmUpgradeNotification	- Indicates that the CPPM node's installation has been upgraded. - **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1015
cppmClusterLicenseUsage	- Indicates the ClearPass cluster license utilization details. ■ <*clearpassServerApplicationName*> indicates the name of the application. ■ <*clearpassClusterLicenseTotalCount*> indicates the application's total cluster-wide license count. ■ <*clearpassClusterLicenseUsageCount*> indicates the count of the application's used cluster-wide licenses. - **OID:** .1.3.6.1.4.1.14823.1.6.1.1.200.1016

SNMP Trap Details

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 815
- ClearPass Processes Stop and Start Events on page 815
- Network Interface up and Down Events on page 815

- Disk Utilization Threshold Exceed Events on page 816
- CPU Load Average Exceed Events for 1, 5, and 15 Minute Thresholds on page 824
- SNMP Daemon Traps on page 815
- Process Status Traps on page 816
- Network Interface Status Traps on page 815
- Disk Space Threshold Traps on page 816
- CPU Load Average Traps on page 824

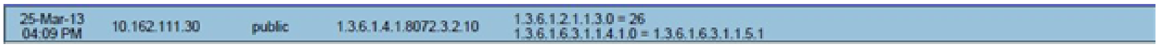
SNMP Daemon Traps

This section contains OIDs for various trap events that are sent from ClearPass Policy Manager.

.1.3.6.1.6.3.1.1.5.1 ==> Coldstart trap indicating the reinitialization of the **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 the **netsnmp** daemon and its configuration file is not altered.

Figure 759: *SNMP daemon traps example*



25-Mar-13 04:09 PM	10.162.111.30	public	1.3.6.1.4.1.8072.3.2.10	1.3.6.1.2.1.1.3.0 = 26 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1

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

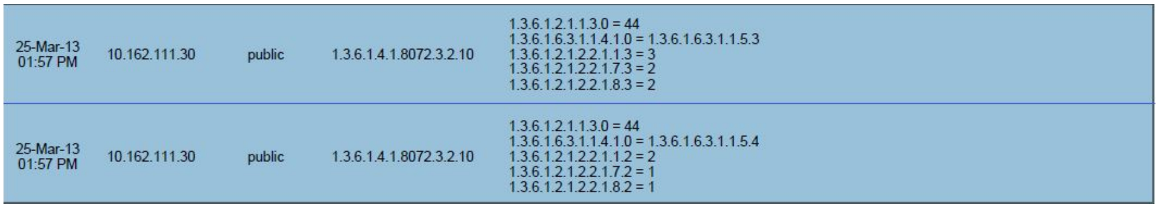
Network Interface Status Traps

.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 760: *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

ClearPass Processes Stop and Start Events

OIDs:

.1.3.6.1.4.1.2021.8.1.2.X ==> Process Name

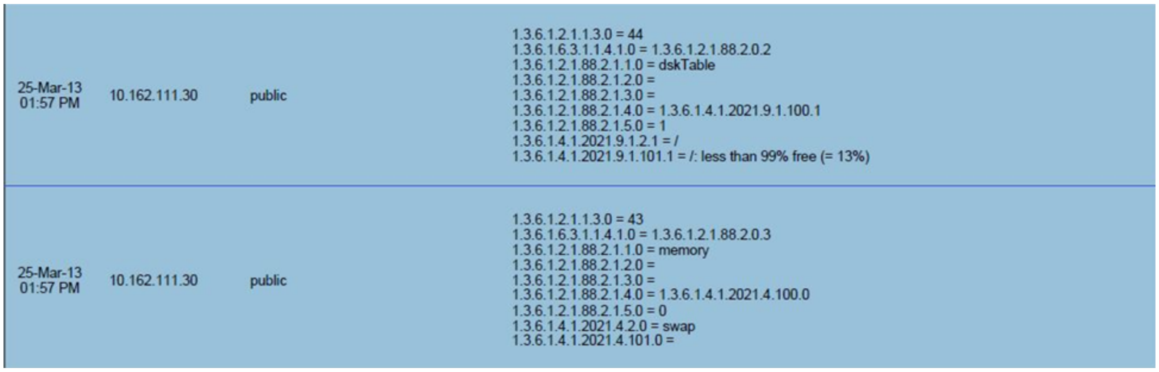
.1.3.6.1.4.1.2021.2.1.101.X ==> Process Status Message

Disk 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 761: *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 =

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

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.

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

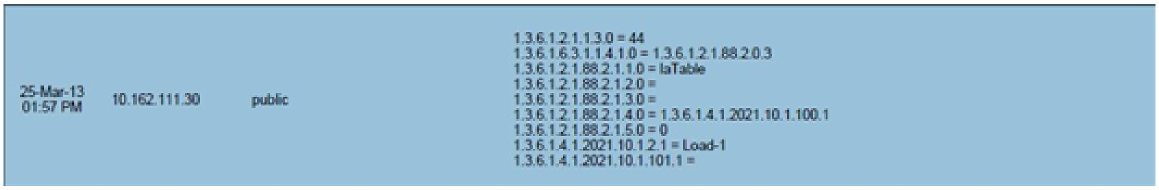
CPU Load Average Traps

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 762: *CPU load-1 average example*

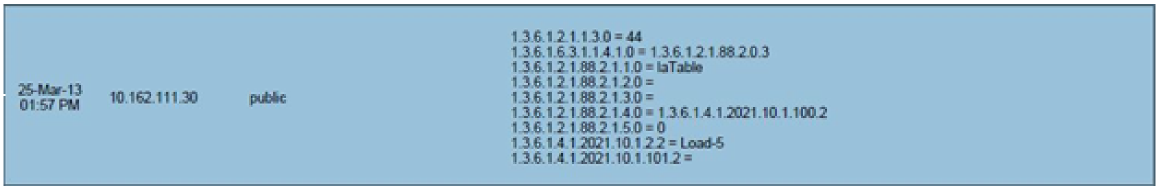


```
                                                  1.3.6.1.2.1.1.3.0 = 44
                                                  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3
                                                  1.3.6.1.2.1.88.2.1.1.0 = laTable
25-Mar-13                                         1.3.6.1.2.1.88.2.1.2.0 =
01:57 PM   10.162.111.30   public                 1.3.6.1.2.1.88.2.1.3.0 =
                                                  1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.1
                                                  1.3.6.1.2.1.88.2.1.5.0 = 0
                                                  1.3.6.1.4.1.2021.10.1.2.1 = Load-1
                                                  1.3.6.1.4.1.2021.10.1.101.1 =
```

.1.3.6.1.4.1.2021.10.1.100.2 ==> Error flag on the CPU load-5 average. Value of 1 indicates the load-5 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.2 ==> Name of CPU load-5 average

Figure 763: *CPU load-5 average example*

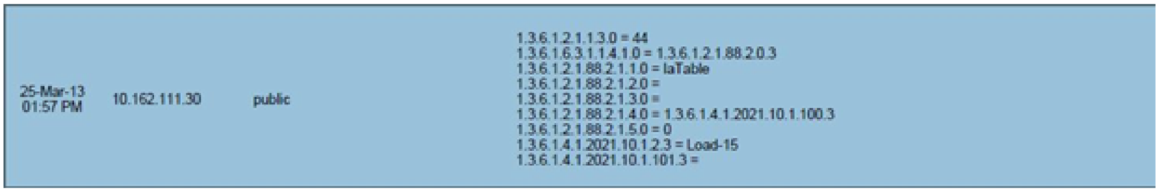


```
                                                  1.3.6.1.2.1.1.3.0 = 44
                                                  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3
                                                  1.3.6.1.2.1.88.2.1.1.0 = laTable
25-Mar-13                                         1.3.6.1.2.1.88.2.1.2.0 =
01:57 PM   10.162.111.30   public                 1.3.6.1.2.1.88.2.1.3.0 =
                                                  1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.2
                                                  1.3.6.1.2.1.88.2.1.5.0 = 0
                                                  1.3.6.1.4.1.2021.10.1.2.2 = Load-5
                                                  1.3.6.1.4.1.2021.10.1.101.2 =
```

.1.3.6.1.4.1.2021.10.1.100.3 ==> Error flag on the CPU load-15 average. Value of 1 indicates the load-15 has crossed its threshold and 0 indicates otherwise.

.1.3.6.1.4.1.2021.10.1.2.3 ==> Name of CPU load-15 average.

Figure 764: *CPU load-15 average example*



```
                                                  1.3.6.1.2.1.1.3.0 = 44
                                                  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.88.2.0.3
                                                  1.3.6.1.2.1.88.2.1.1.0 = laTable
25-Mar-13                                         1.3.6.1.2.1.88.2.1.2.0 =
01:57 PM   10.162.111.30   public                 1.3.6.1.2.1.88.2.1.3.0 =
                                                  1.3.6.1.2.1.88.2.1.4.0 = 1.3.6.1.4.1.2021.10.1.100.3
                                                  1.3.6.1.2.1.88.2.1.5.0 = 0
                                                  1.3.6.1.4.1.2021.10.1.2.3 = Load-15
                                                  1.3.6.1.4.1.2021.10.1.101.3 =
```

Important System Events

This section provides the following information:

- Admin User Interface Events
- Admin Server Events
- Async Service Events
- ClearPass/Domain Controller Events
- ClearPass System Configuration Events
- ClearPass Update Events
- Cluster Events
- Command Line Events
- Database Replication Services Events
- Licensing Events
- Policy Server Events
- RADIUS/TACACS+ Server Events
- Service Names
- SNMP Events
- Support Shell Events
- System Auxiliary Service Events
- System Monitor 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 angle brackets (for example, <*content*>) are variable, and are substituted by ClearPass as applicable (such as an IP address).

For the list of available service names, refer to Service Names on page 828.

Admin User Interface 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"

"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= 2016-07-13 17:00:01, System time 5 mins back = 2016-06-20 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"

Database 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”

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

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:customersupport”

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

Error Codes

Table 437 describes the ClearPass Policy Manager error codes:

Table 437: *ClearPass Policy Manager 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 Authentication Source	Authentication failure
204	Failed to classify request to service	Authentication failure
205	Authentication Source not configured for service	Authentication failure
206	Access denied by policy	Authentication failure
207	Failed to get client MAC Address in order to perform Web authentication	Authentication failure
208	No response from home server	Authentication failure
209	No password in request	Authentication failure
210	Unknown CA in client certificate	Authentication failure
211	Client certificate not valid	Authentication failure
212	Client certificate has expired	Authentication failure
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

Table 437: *ClearPass Policy Manager Error Codes (Continued)*

Code	Description	Type
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
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

Table 437: *ClearPass Policy Manager Error Codes (Continued)*

Code	Description	Type
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	Phase 2 PAC failure	RADIUS Protocol
9004	Client rejected after PAC provisioning	RADIUS Protocol
9005	Client does not support posture request	RADIUS Protocol
9006	Received error TLV from client	RADIUS Protocol
9007	Received failure TLV from client	RADIUS Protocol
9008	Phase 2 PAC not found	RADIUS Protocol
9009	Unknown Phase 2 PAC	RADIUS Protocol
9010	Invalid Phase 2 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

Table 437: *ClearPass Policy Manager Error Codes (Continued)*

Code	Description	Type
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

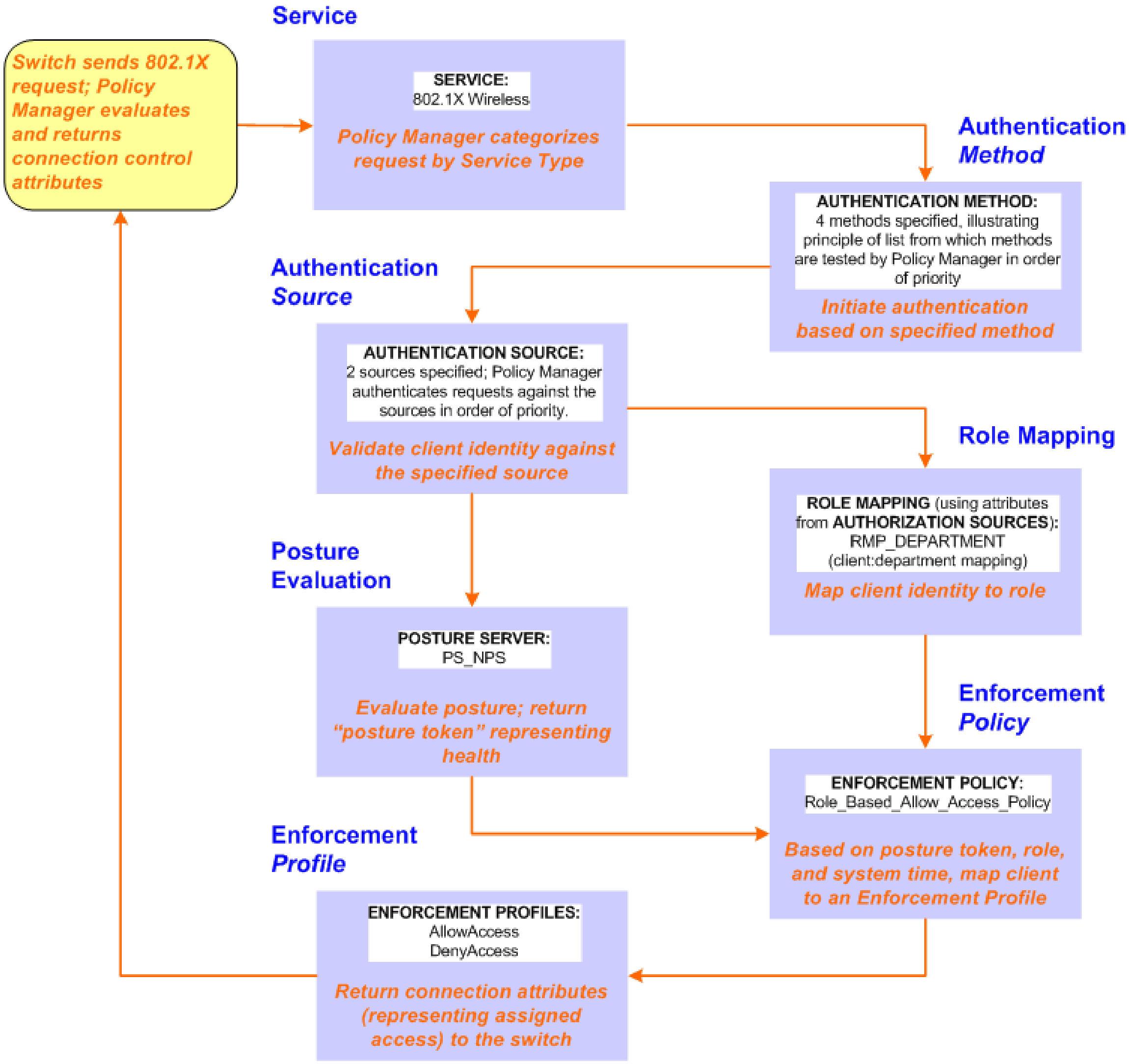
This appendix contains several specific ClearPass Policy Manager use cases. Each one explains what it is typically used for, and then describes how to configure Policy Manager for that use case.

- 802.1X Wireless Use Case on page 835
- Web Based Authentication Use Case on page 841
- MAC Authentication Use Case on page 848
- TACACS+ Use Case on page 851
- Single Port Use Case on page 853

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 765: *Flow of Control, Basic 802.1X Configuration Use Case*


Service
Switch sends 802.1X request; Policy Manager evaluates and returns connection control attributes
SERVICE: 802.1X Wireless
Policy Manager categorizes request by Service Type
Authentication Method
AUTHENTICATION METHOD: 4 methods specified, illustrating principle of list from which methods are tested by Policy Manager in order of priority
Initiate authentication based on specified method
Authentication Source
AUTHENTICATION SOURCE: 2 sources specified; Policy Manager authenticates requests against the sources in order of priority.
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (using attributes from AUTHORIZATION SOURCES): RMP_DEPARTMENT (client:department mapping)
Map client identity to role
Posture Evaluation
POSTURE SERVER: PS_NPS
Evaluate posture; return "posture token" representing health
Enforcement Policy
ENFORCEMENT POLICY: Role_Based_Allow_Access_Policy
Based on posture token, role, and system time, map client to an Enforcement Profile
Enforcement Profile
ENFORCEMENT PROFILES: AllowAccess DenyAccess
Return connection attributes (representing assigned access) to the switch

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

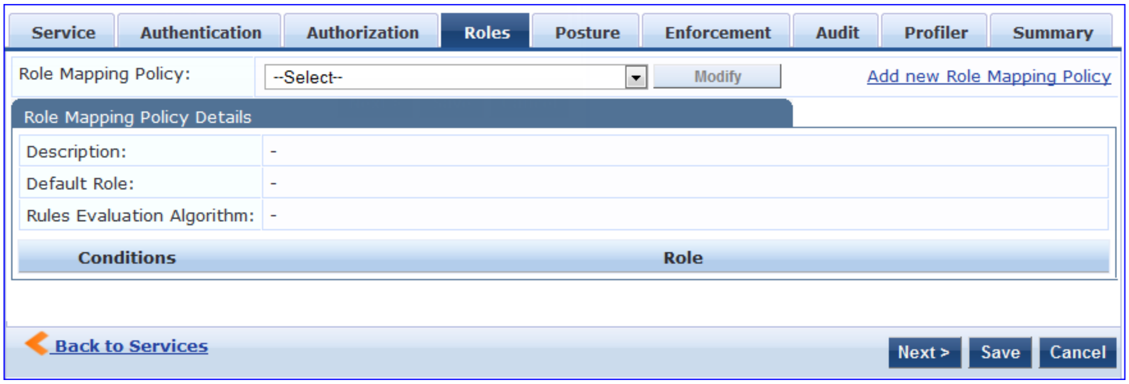
1. Navigate to **Configuration > Services.**
2. Click the ➕ Add icon to add a service. The **Configuration > Services > Add** window opens.
3. If it is not already selected, click the **Service** tab and define basic service information.
   a. Enter a name for the service in the **Name** field.
   b. 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 766: *Role Mapping Navigation and Settings*



Role Mapping Policy: --Select--

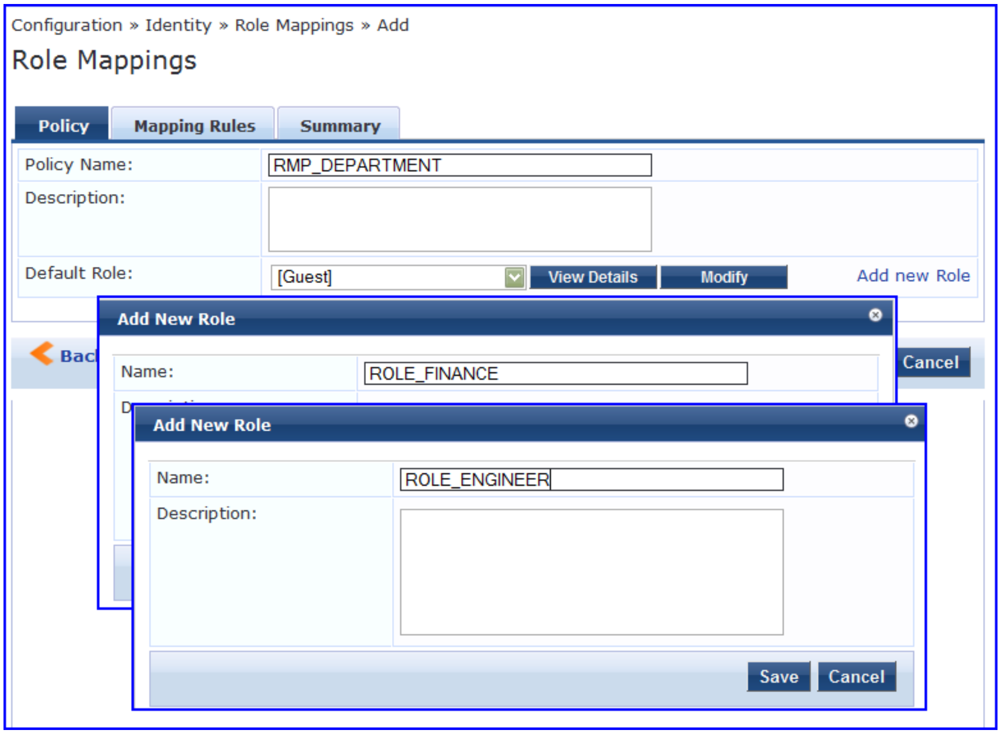
Description: -

Default Role: -

Rules Evaluation Algorithm: -

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 767: *Policy Tab*



Policy Name: RMP_DEPARTMENT

Description:

Default Role: [Guest]

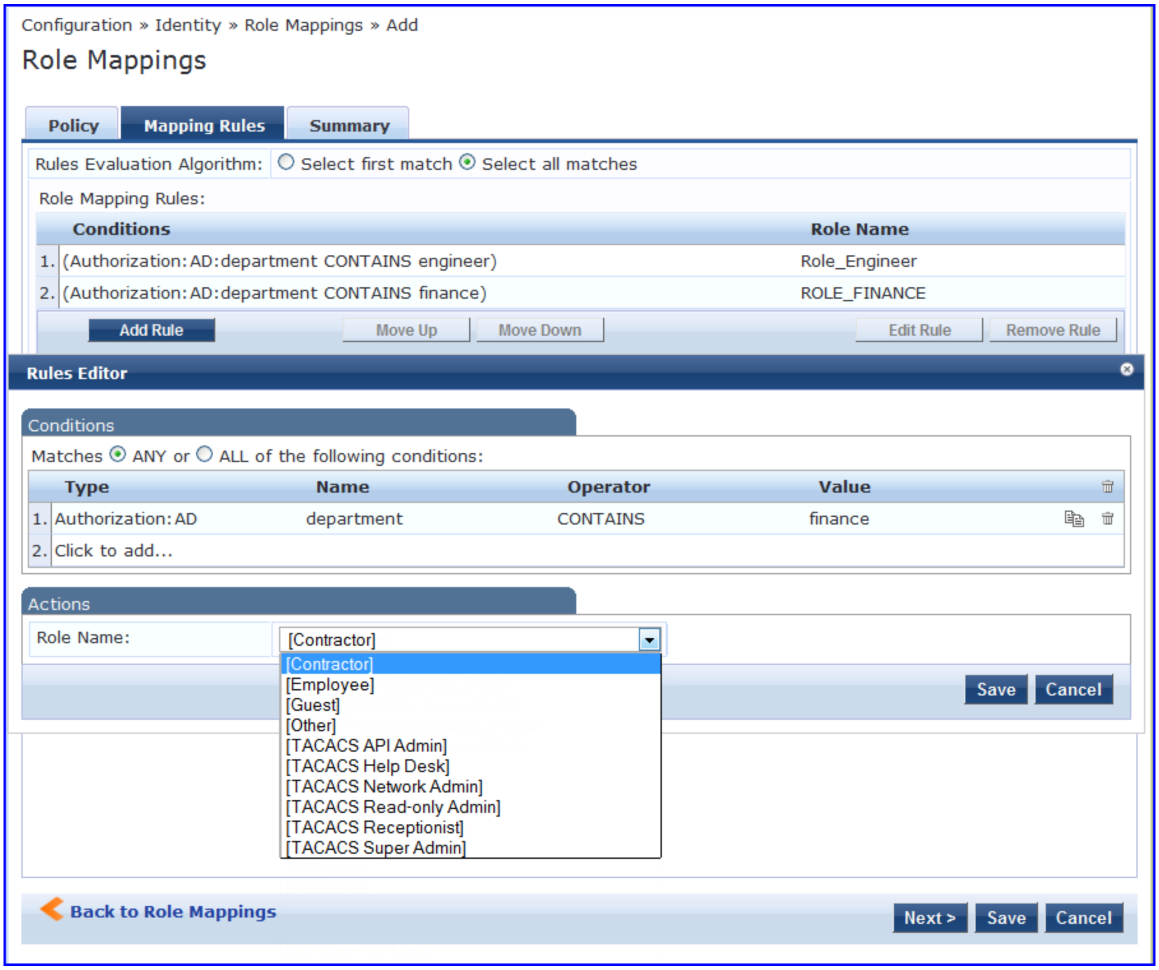
Name: ROLE_FINANCE

Name: ROLE_ENGINEER

Description:

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 768: *Mapping Rules Tab*



Rules Evaluation Algorithm: ○ Select first match ● Select all matches

Role Mapping Rules:

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

Matches ● ANY or ○ ALL of the following conditions:

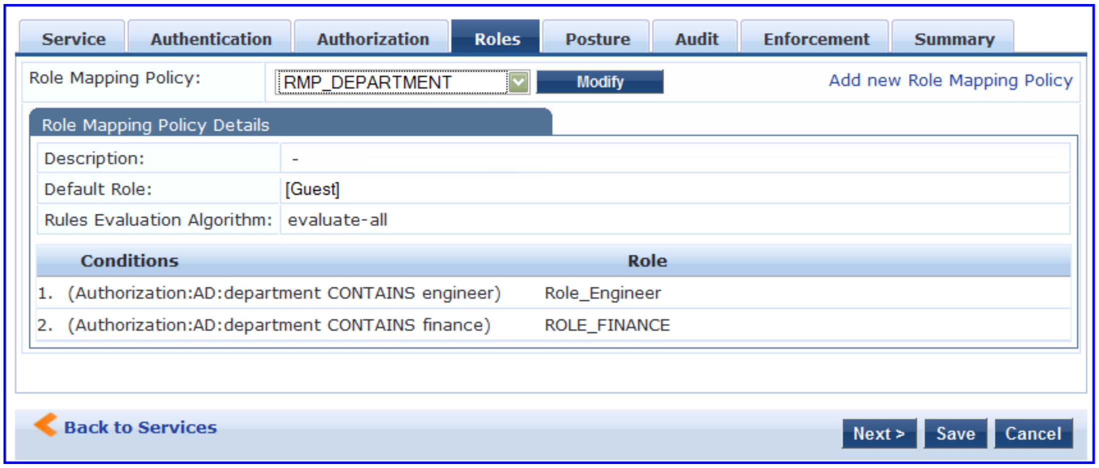
	Type	Name	Operator	Value
1.	Authorization:AD	department	CONTAINS	finance
2.	Click to add...			

Role Name: [Contractor]

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

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 769: *Roles Tab*



Role Mapping Policy: RMP_DEPARTMENT

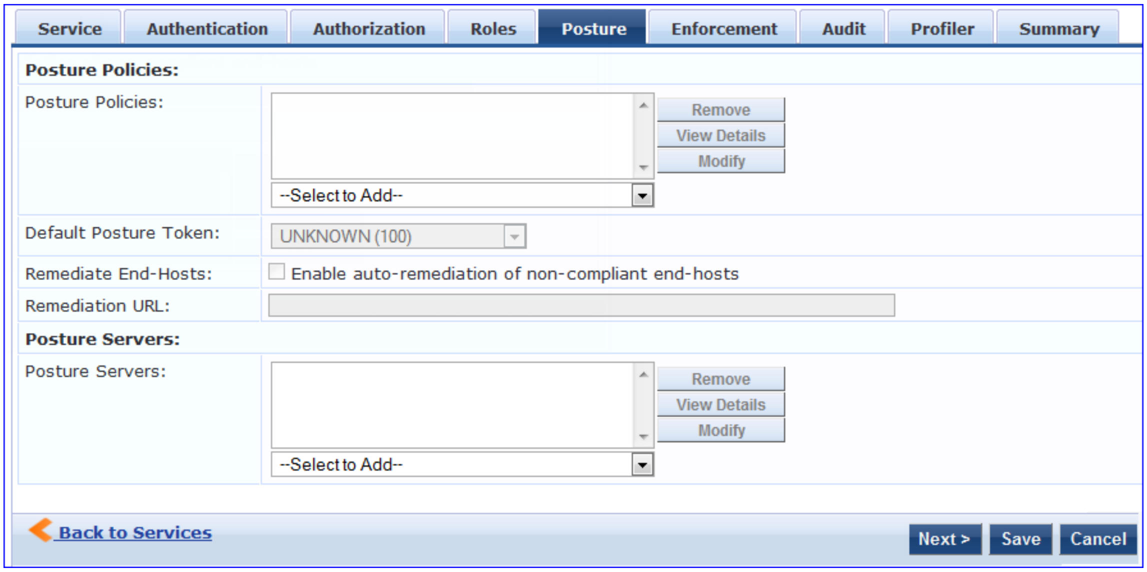
Description:	-
Default Role:	[Guest]
Rules Evaluation Algorithm:	evaluate-all

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

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 770: *Posture Tab*



Posture Policies:

Posture Policies: --Select to Add--

Default Posture Token: UNKNOWN (100)

Remediate End-Hosts: □ Enable auto-remediation of non-compliant end-hosts

Remediation URL:

Posture Servers:

Posture Servers: --Select to Add--

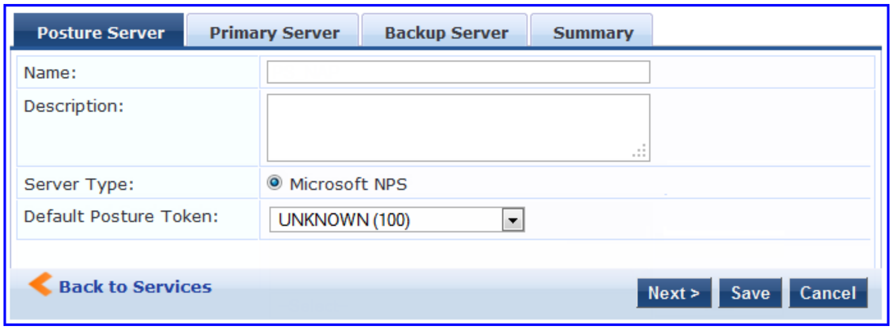
12. Click **Add new Posture Server** to add a new posture server.

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 771: *Posture Server Tab*



Name:

Description:

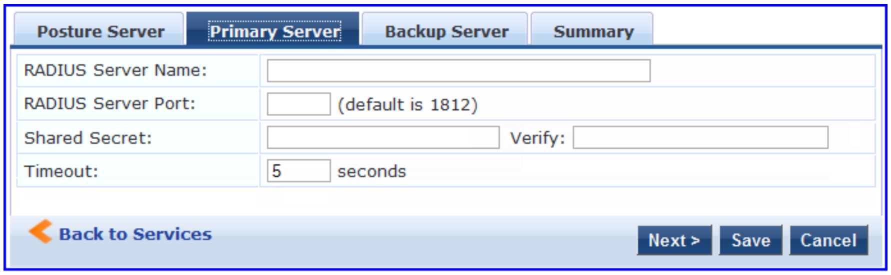
Server Type: ● Microsoft NPS

Default Posture Token: UNKNOWN (100)

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:

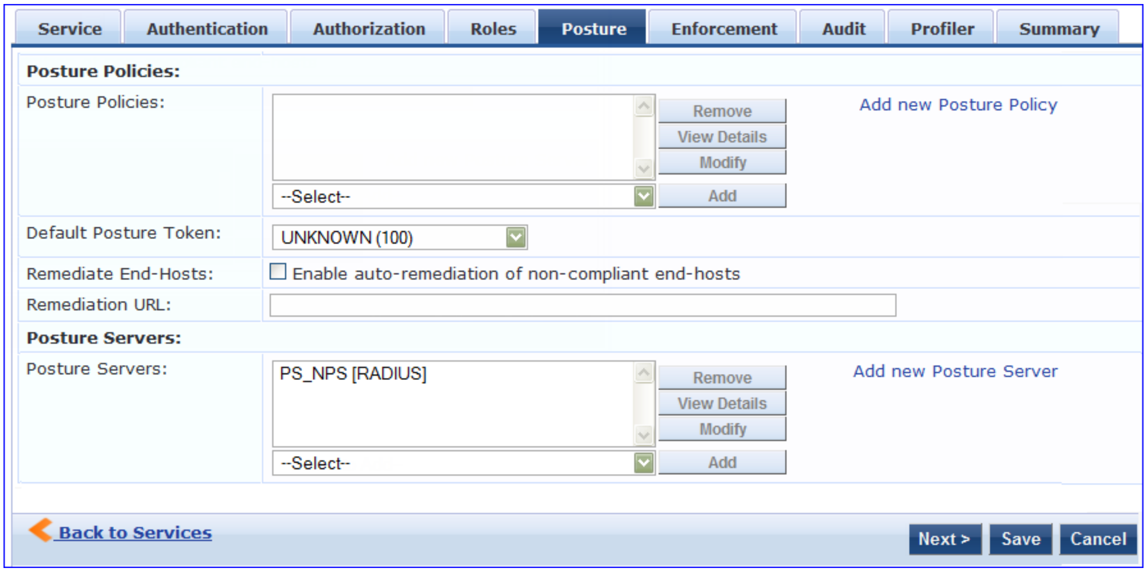
Figure 772: *Primary Server Tab*



RADIUS Server Name:	
RADIUS Server Port:	(default is 1812)
Shared Secret:	Verify:
Timeout:	5 seconds

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 773: *Posture Tab*



Posture Policies:

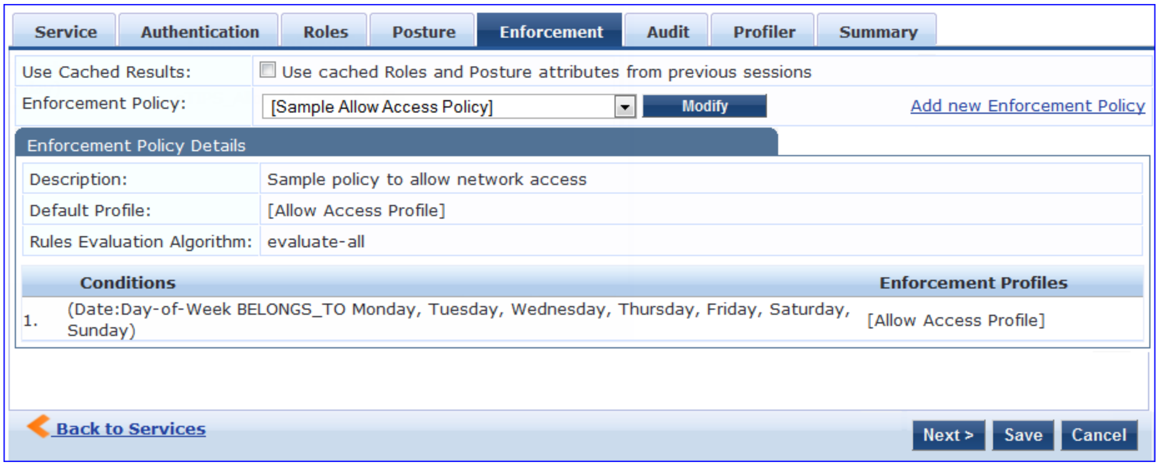
Posture Policies:	--Select--
Default Posture Token:	UNKNOWN (100)
Remediate End-Hosts:	□ Enable auto-remediation of non-compliant end-hosts
Remediation URL:	

Posture Servers:

Posture Servers:	PS_NPS [RADIUS] --Select--

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 438: *Enforcement Policy Navigation and Settings*



Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	[Sample Allow Access Policy]

Enforcement Policy Details

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

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

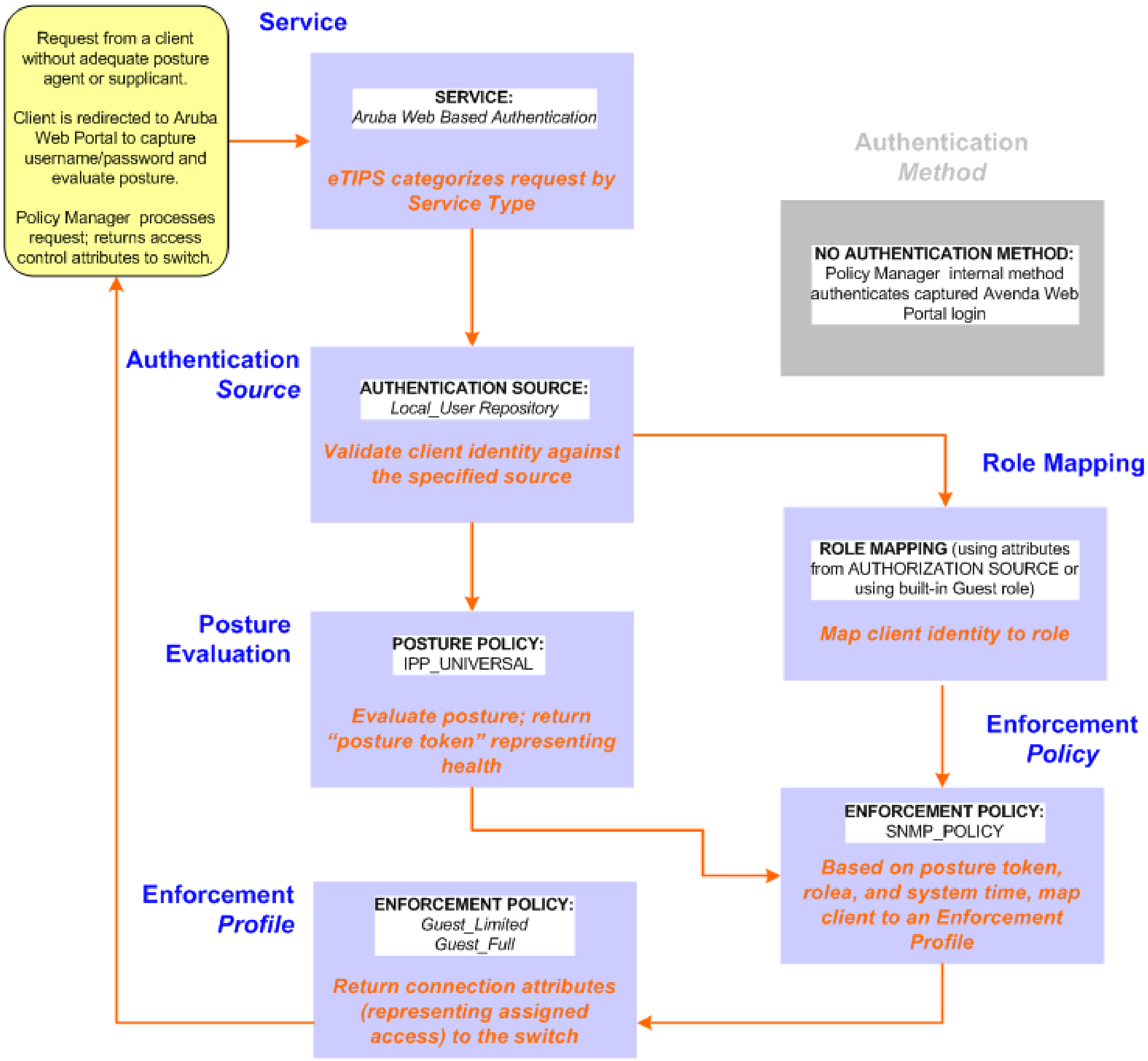
20. From the **Enforcement** tab, select the **Enforcement Policy.** For instructions about how to build an enforcement policy, refer to Configuring Enforcement Policies on page 355.

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 774: *Flow-of-Control of Web-Based Authentication for Guests*



Request from a client without adequate posture agent or supplicant.
Client is redirected to Aruba Web Portal to capture username/password and evaluate posture.
Policy Manager processes request; returns access control attributes to switch.
Service
SERVICE:
Aruba Web Based Authentication
eTIPS categorizes request by Service Type
Authentication Method
NO AUTHENTICATION METHOD:
Policy Manager internal method authenticates captured Avenda Web Portal login
Authentication Source
AUTHENTICATION SOURCE:
Local_User Repository
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (using attributes from AUTHORIZATION SOURCE or using built-in Guest role)
Map client identity to role
Posture Evaluation
POSTURE POLICY:
IPP_UNIVERSAL
Evaluate posture; return "posture token" representing health
Enforcement Policy
ENFORCEMENT POLICY:
SNMP_POLICY
Based on posture token, rolea, and system time, map client to an Enforcement Profile
Enforcement Profile
ENFORCEMENT POLICY:
Guest_Limited
Guest_Full
Return connection attributes (representing assigned access) to the switch

Configuring a Service

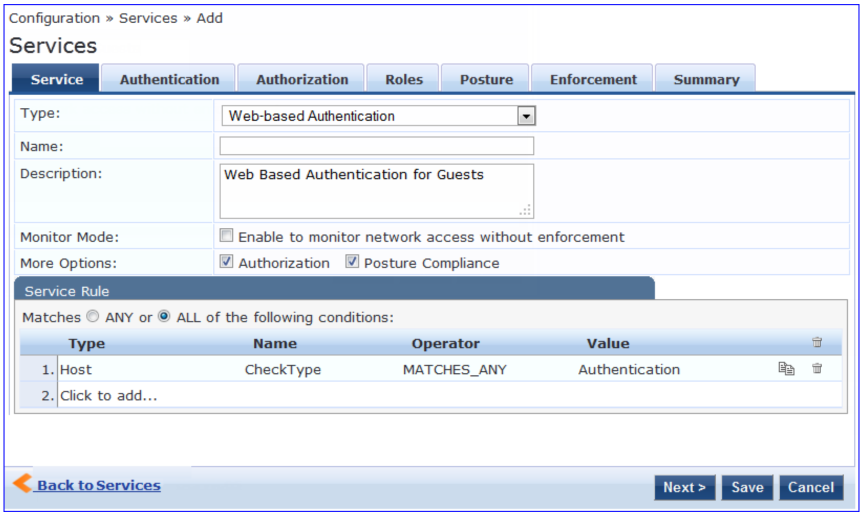
Perform the following steps to configure Policy Manager for WebAuth-based Guest access.

1. Prepare the switch to pre-process WebAuth requests for the Policy Manager *Aruba WebAuth* service.

   Refer to your Network Access Device documentation to configure the switch such that it redirects HTTP requests to the *Aruba Guest Portal*, which captures username and password and optionally launches an agent that returns posture data.

2. Create a WebAuth-based Service.

Table 439: *Service Navigation and Settings*

Navigation	Settings
Create a new Service: - **Services** > - **Add Service** >	 Configuration » Services Services Add Import Export All
Name the Service and select a pre-configured Service Type: - **Service** (tab) > - **Type** (selector): Aruba Web-Based Authentication > - **Name/Description** (freeform) > - Upon completion, click **Next**.	 Configuration » Services » Add Services Service | Authentication | Authorization | Roles | Posture | Enforcement | Summary Type: Web-based Authentication Name: Description: Web Based Authentication for Guests Monitor Mode: □ Enable to monitor network access without enforcement More Options: ☑ Authorization ☑ Posture Compliance Service Rule Matches ○ ANY or ● ALL of the following conditions: Type | Name | Operator | Value 1. Host | CheckType | MATCHES_ANY | Authentication 2. Click to add... Back to Services Next > | Save | Cancel

3. Set up the Authentication.
   a. Method: The Policy Manager WebAuth service authenticates WebAuth clients internally.
   b. Source: Administrators typically configure Guest Users in the local Policy Manager database.
4. Configure a Posture Policy.

NOTE

For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options. This use case demonstrates the Posture Policy.

As of the current version, Policy Manager ships with five pre-configured posture plugins that evaluate the health of the client and return a corresponding posture token.

To add the internal posture policy *IPP_UNIVERSAL_XP*, which (as you will configure it in this Use Case, checks any Windows® XP clients to verify the most current Service Pack).

Table 440: *Local Policy Manager Database Navigation and Settings*

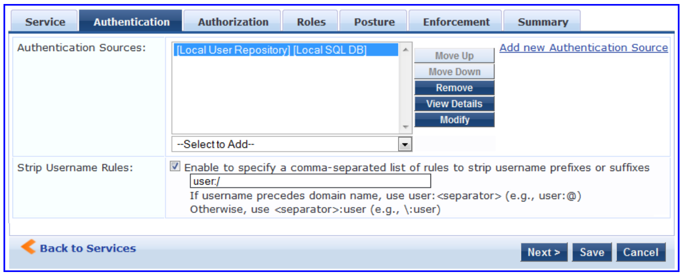
Navigation	Settings
Select the local Policy Manager database: - **Authentication** (tab) > - **Sources** (**Select** drop-down list): **[Local User Repository]** > - **Add** > - **Strip Username Rules** (check box) > - Enter an example of preceding or following separators (if any), with the phrase "user" representing the username to be returned. For authentication, Policy Manager strips the specified separators and any paths or domains beyond them. - Upon completion, click **Next** (until you reach Enforcement Policy).	 Service Authentication Authorization Roles Posture Enforcement Summary Move Up Move Down Remove View Details Modify Add new Authentication Source Back to Services Next > Save Cancel Authentication Sources: [Local User Repository] [Local SQL DB] --Select to Add-- Strip Username Rules: ☑ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes user:/ If username precedes domain name, use user:<separator> (e.g., user:@) Otherwise, use <separator>:user (e.g., \:user)

Table 441: *Posture Policy Navigation and Settings*

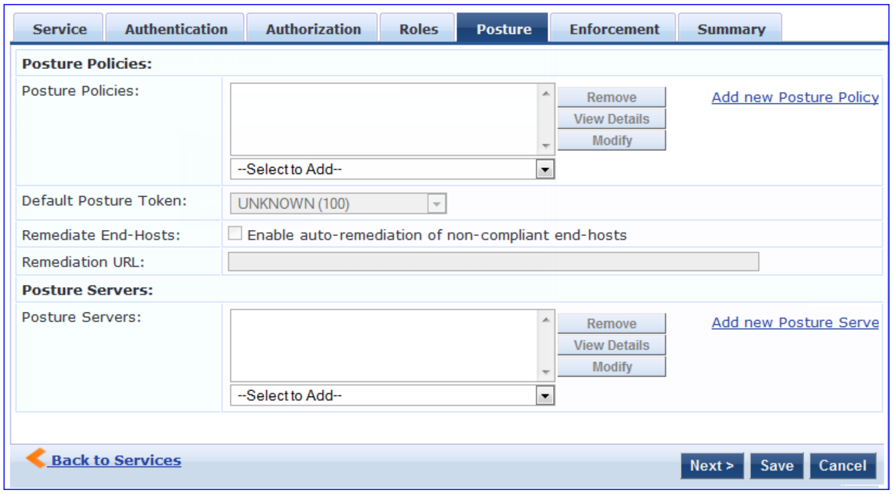
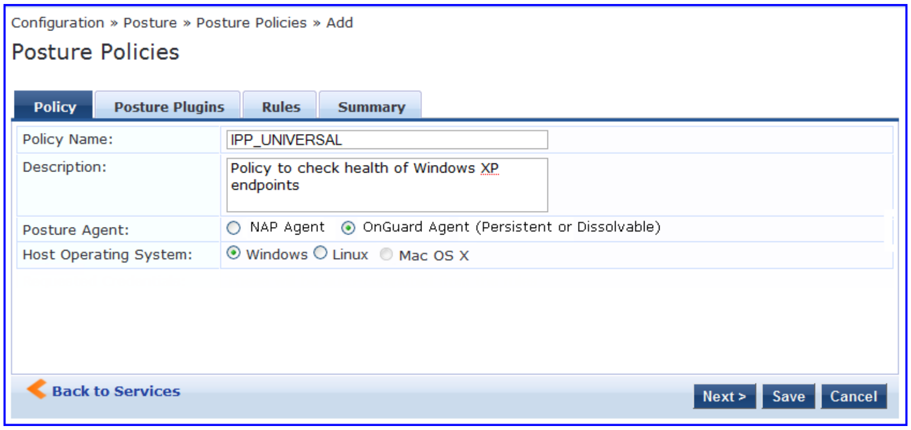
Navigation	Setting
Create a Posture Policy: - **Posture** (tab) > - Enable **Validation Check** (check box) > - **Add new Internal Policy** (link) >	 Service Authentication Authorization Roles Posture Enforcement Summary Remove View Details Modify Add new Posture Policy Add new Posture Serve Back to Services Next > Save Cancel **Posture Policies:** Posture Policies: --Select to Add-- Default Posture Token: UNKNOWN (100) Remediate End-Hosts: ☐ Enable auto-remediation of non-compliant end-hosts Remediation URL: **Posture Servers:** Posture Servers: --Select to Add--
Name the Posture Policy and specify a general class of operating system: - **Policy** (tab) > - **Policy Name** (freeform): *IPP_ UNIVERSAL* > - **Host Operating System** (radio buttons): **Windows** > - When finished working in the **Policy** tab, click **Next** to open the Posture Plugins tab	 Configuration » Posture » Posture Policies » Add Policy Posture Plugins Rules Summary Back to Services Next > Save Cancel Posture Policies Policy Name: IPP_UNIVERSAL Description: Policy to check health of Windows XP endpoints Posture Agent: ○ NAP Agent ● OnGuard Agent (Persistent or Dissolvable) Host Operating System: ● Windows ○ Linux ○ Mac OS X

Table 441: *Posture Policy Navigation and Settings (Continued)*

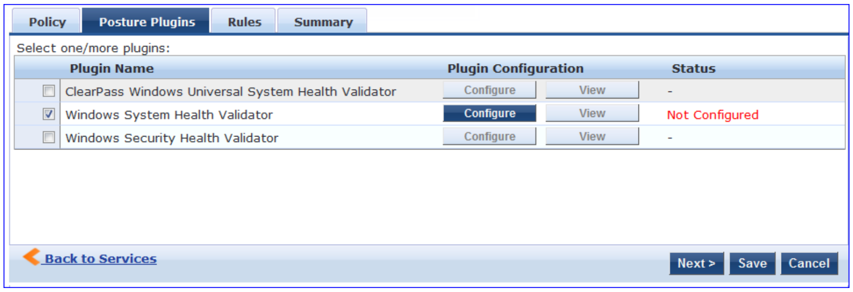
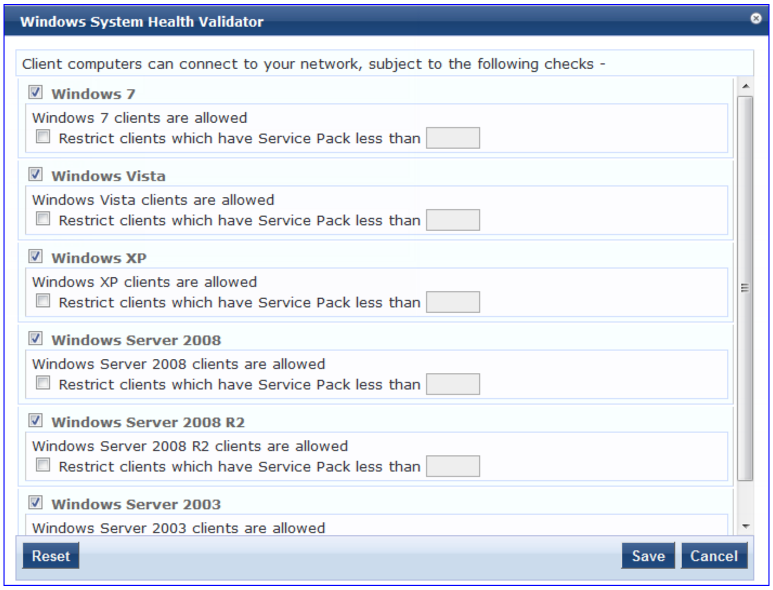
Navigation	Setting
Select a Validator: - **Posture Plugins** (tab) > - Enable **Windows Health System Validator** > - **Configure** (button) >	 Policy Posture Plugins Rules Summary Back to Services Next > Save Cancel Select one/more plugins: Plugin Name | Plugin Configuration | Status ☐ ClearPass Windows Universal System Health Validator | Configure | View | - ☑ Windows System Health Validator | Configure | View | Not Configured ☐ Windows Security Health Validator | Configure | View | -
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) >	 **Windows System Health Validator** Client computers can connect to your network, subject to the following checks - ☑ **Windows 7** Windows 7 clients are allowed ☐ Restrict clients which have Service Pack less than ☑ **Windows Vista** Windows Vista clients are allowed ☐ Restrict clients which have Service Pack less than ☑ **Windows XP** Windows XP clients are allowed ☐ Restrict clients which have Service Pack less than ☑ **Windows Server 2008** Windows Server 2008 clients are allowed ☐ Restrict clients which have Service Pack less than ☑ **Windows Server 2008 R2** Windows Server 2008 R2 clients are allowed ☐ Restrict clients which have Service Pack less than ☑ **Windows Server 2003** Windows Server 2003 clients are allowed

Table 441: *Posture Policy Navigation and Settings (Continued)*

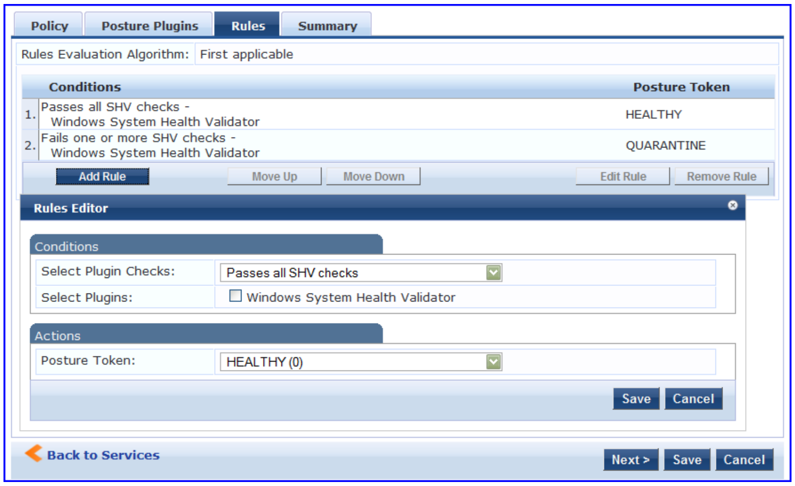
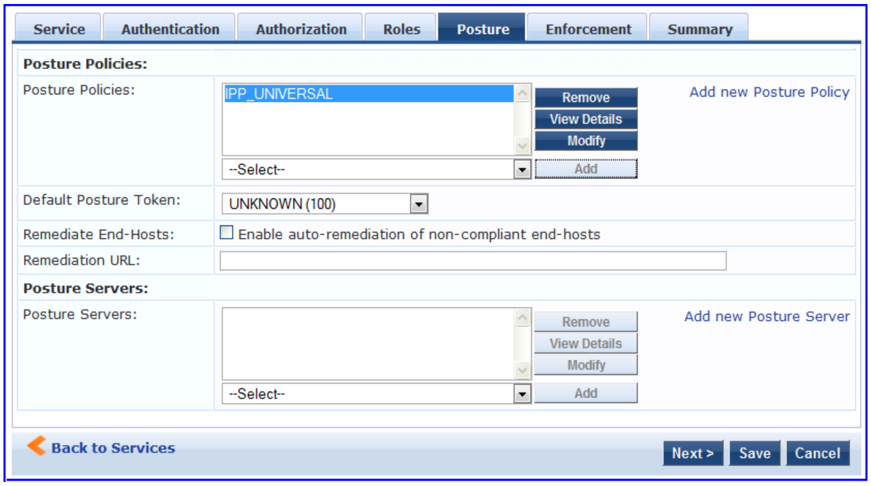
Navigation	Setting
- When finished working in the **Posture Plugin** tab click **Next** to move to the Rules tab)	
Set rules to correlate validation results with posture tokens: - **Rules** (tab) > - **Add Rule** (button opens popup) > - **Rules Editor** (popup) > - **Conditions/ Actions:** match Conditions (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.	 Policy | Posture Plugins | Rules | Summary Rules Evaluation Algorithm: First applicable Conditions | Posture Token 1. Passes all SHV checks - Windows System Health Validator | HEALTHY 2. Fails one or more SHV checks - Windows System Health Validator | QUARANTINE Add Rule | Move Up | Move Down | Edit Rule | Remove Rule Rules Editor Conditions Select Plugin Checks: Passes all SHV checks Select Plugins: □ Windows System Health Validator Actions Posture Token: HEALTHY (0) Save | Cancel Back to Services | Next > | Save | Cancel

Table 441: *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	 Service | Authentication | Authorization | Roles | Posture | Enforcement | Summary **Posture Policies:** Posture Policies: IPP_UNIVERSAL — Remove, View Details, Modify — --Select-- Add — Add new Posture Policy Default Posture Token: UNKNOWN (100) Remediate End-Hosts: ☐ Enable auto-remediation of non-compliant end-hosts Remediation URL: **Posture Servers:** Posture Servers: Remove, View Details, Modify — --Select-- Add — Add new Posture Server Back to Services — Next > Save Cancel

The following fields deserve special mention:

- **Default Posture Token.** Value of the posture token to use if health status is not available.
- **Remediate End-Hosts.** When a client does not pass posture evaluation, redirect to the indicated server for remediation.
- **Remediation URL.** URL of remediation server.

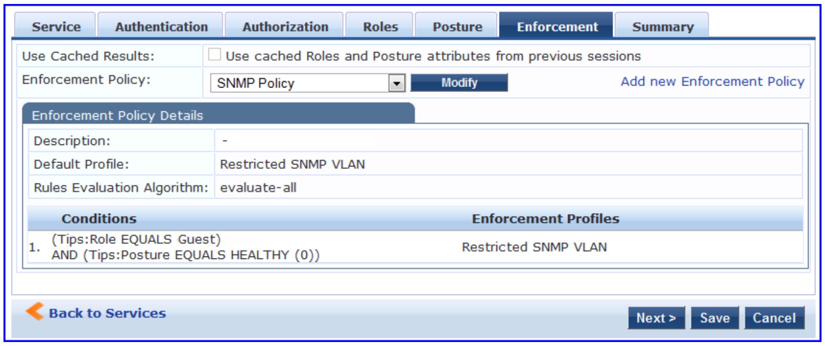
5. Create an Enforcement Policy.

   Because this Use Case assumes the *Guest* role, and the *Aruba Web Portal* agent has returned a posture token, it does not require configuration of Role Mapping or Posture Evaluation.

NOTE

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 442: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Add a new Enforcement Policy: ● **Enforcement** (tab) > ● Enforcement Policy (selector): **SNMP_POLICY** ● Upon completion, click **Save**.	 Service | Authentication | Authorization | Roles | Posture | Enforcement | Summary Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions Enforcement Policy: SNMP Policy — Modify — Add new Enforcement Policy Enforcement Policy Details Description: - Default Profile: Restricted SNMP VLAN Rules Evaluation Algorithm: evaluate-all Conditions | Enforcement Profiles 1. (Tips:Role EQUALS Guest) AND (Tips:Posture EQUALS HEALTHY (0)) | Restricted SNMP VLAN Back to Services — Next > Save Cancel

6. Save the Service.

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

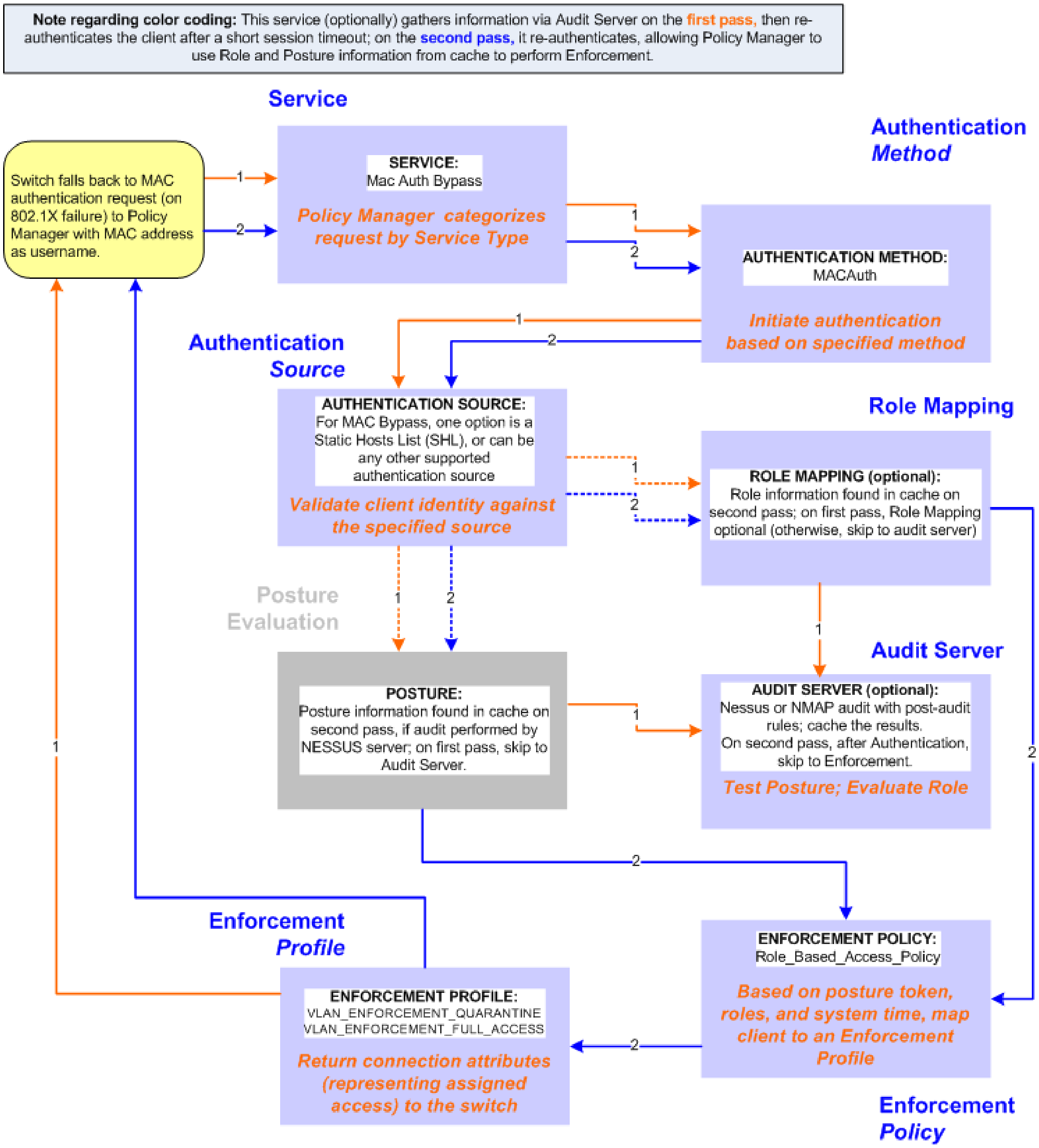
MAC Authentication Use Case

This service supports *Network Devices,* such as printers or hand-helds.

In this service, an audit is initiated on receiving the first MAC Authentication request. A subsequent MAC Authentication request (triggered after the audit, or triggered after a short session timeout) uses the cached results from the audit to determine the posture and role(s) for the device.

The following diagram illustrates the overall flow of control for this Policy Manager service.

Figure 775: *Flow-of-Control of MAC Authentication for Network Devices*



Note regarding color coding: This service (optionally) gathers information via Audit Server on the **first pass**, then re-authenticates the client after a short session timeout; on the **second pass**, it re-authenticates, allowing Policy Manager to use Role and Posture information from cache to perform Enforcement.

Service
Switch falls back to MAC authentication request (on 802.1X failure) to Policy Manager with MAC address as username.
SERVICE:
Mac Auth Bypass
Policy Manager categorizes request by Service Type
Authentication Method
AUTHENTICATION METHOD:
MACAuth
Initiate authentication based on specified method
Authentication Source
AUTHENTICATION SOURCE:
For MAC Bypass, one option is a Static Hosts List (SHL), or can be any other supported authentication source
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (optional):
Role information found in cache on second pass; on first pass, Role Mapping optional (otherwise, skip to audit server)
Posture Evaluation
POSTURE:
Posture information found in cache on second pass, if audit performed by NESSUS server; on first pass, skip to Audit Server.
Audit Server
AUDIT SERVER (optional):
Nessus or NMAP audit with post-audit rules; cache the results.
On second pass, after Authentication, skip to Enforcement.
Test Posture; Evaluate Role
Enforcement Profile
ENFORCEMENT PROFILE:
VLAN_ENFORCEMENT_QUARANTINE
VLAN_ENFORCEMENT_FULL_ACCESS
Return connection attributes (representing assigned access) to the switch
ENFORCEMENT POLICY:
Role_Based_Access_Policy
Based on posture token, roles, and system time, map client to an Enforcement Profile
Enforcement Policy
1
2

Configuring the Service

To configure ClearPass for MAC-based network device access:

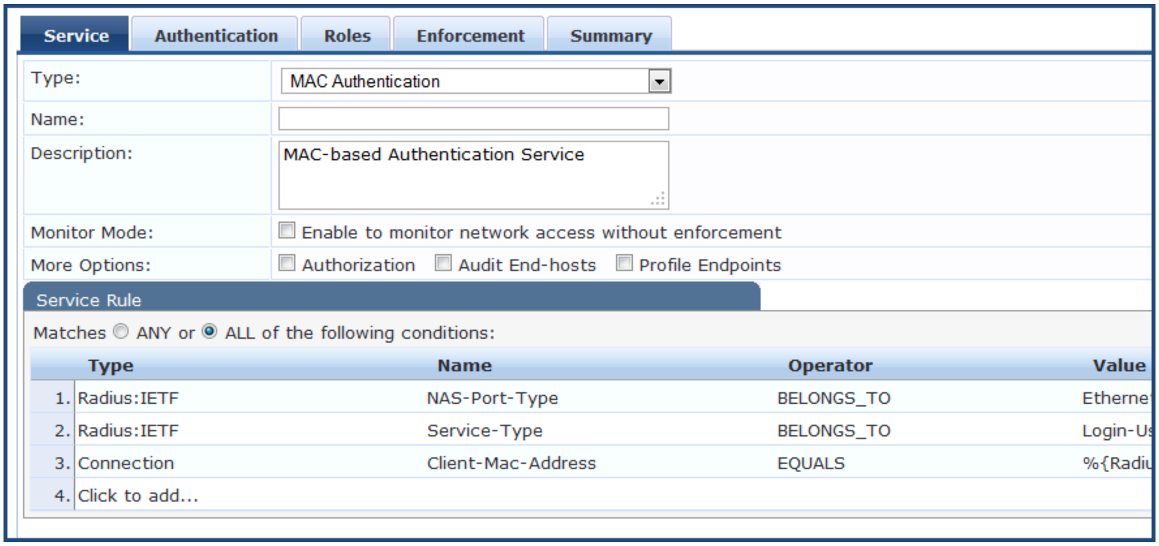
1. First create a MAC Authentication Service by navigating to **Configuration** > **Services**.

   The **Services** page opens.

2. Click the **Add** link.

   The **Add Services** dialog opens.

Figure 776: *MAC Authentication Service Configuration Dialog*



Service | Authentication | Roles | Enforcement | Summary

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

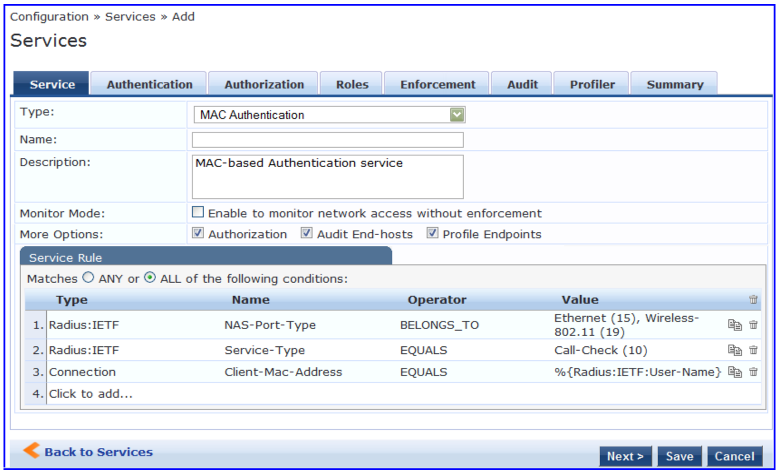
Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

3.

Table 443: *MAC Authentication Service Navigation and Settings*

Navigation	Settings
Create a new Service: - **Services** > - **Add Service** (link) >	 Configuration » Services Services Add Import Export All
Name the Service and select a pre-configured Service Type: - **Service** (tab) > - **Type** (selector): **MAC Authentication** > - **Name/Description** (freeform) > - Upon completion, click **Next** to configure Authentication	

Configuration » Services » Add

Services

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

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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

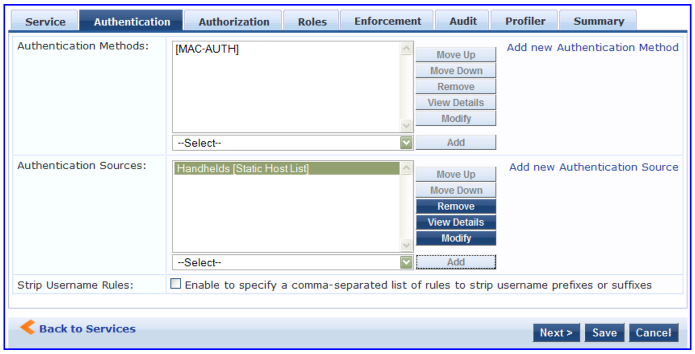
	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	EQUALS	Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Click to add...			

4. 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**).

   For more information on static host list, see Managing Static Host Lists on page 252. You can also select any other supported type of authentication source.

Table 444: *Authentication Method Navigation and Settings*

Navigation	Settings
Select an Authentication Method and two authentication sources—one of type **Static Host List** and the other of type **Generic LDAP** server (that you have already configured in Policy Manager): • **Authentication** (tab) > • **Methods** (This method is automatically selected for this type of service): **[MAC AUTH]** > • **Add** > • **Sources** (**Select** drop-down list): **Handhelds [Static Host List]** and Policy Manager Clients White List [Generic LDAP] > • **Add** > • Upon completion, **Next** (to Audit)	 Service Authentication Authorization Roles Enforcement Audit Profiler Summary Authentication Methods: [MAC-AUTH] Move Up Move Down Remove View Details Modify --Select-- Add Add new Authentication Method Authentication Sources: Handhelds [Static Host List] Move Up Move Down Remove View Details Modify --Select-- Add Add new Authentication Source Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes Back to Services Next > Save Cancel

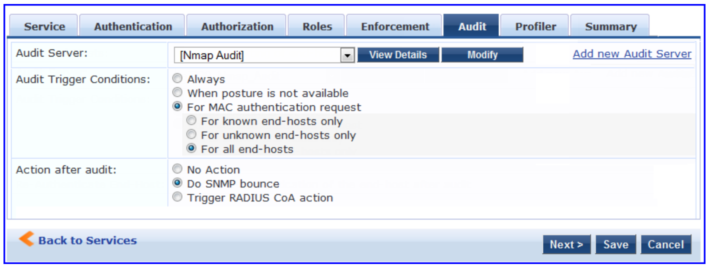
5. Configure an Audit Server.

   This step is optional if no Role Mapping Policy is provided, or if you want to establish health or roles using an audit. For more information, see Configuring Audit Servers on page 338.

   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.

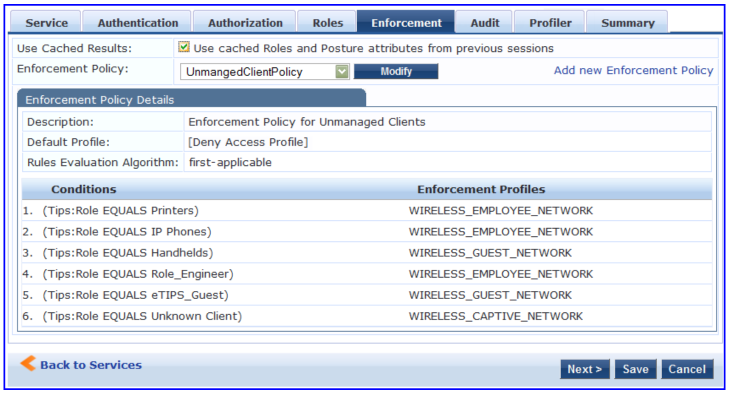
Table 445: *Audit Server Navigation and Settings*

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**	 Service Authentication Authorization Roles Enforcement Audit Profiler Summary Audit Server: [Nmap Audit] View Details Modify Add new Audit Server Audit Trigger Conditions: ○ Always ○ When posture is not available ● For MAC authentication request ○ For known end-hosts only ○ For unknown end-hosts only ● For all end-hosts Action after audit: ○ No Action ● Do SNMP bounce ○ Trigger RADIUS CoA action Back to Services Next > Save Cancel

Upon completion of the audit, Policy Manager caches Role (Nmap and Nessus) and Posture (Nessus), then resets the connection (or the switch reauthenticates after a short session timeout), triggering a new request, which follows the same path until it reaches Role Mapping/Posture/Audit; this appends cached information for this client to the request for passing to Enforcement.

6. Select the Enforcement Policy *Sample_Allow_Access_Policy*:

Table 446: *Enforcement Policy Navigation and Settings*

Navigation	Setting
Select the Enforcement Policy: ● **Enforcement** (tab) > ● **Use Cached Results** (check box): Select **Use cached Roles and Posture attributes from previous sessions** > ● **Enforcement Policy** (selector): UnmanagedClientPolicy ● When you are finished with your work in this tab, click **Save**.	

Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: UnmangedClientPolicy

Description:	Enforcement Policy for Unmanaged Clients
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role EQUALS Printers)	WIRELESS_EMPLOYEE_NETWORK
2. (Tips:Role EQUALS IP Phones)	WIRELESS_EMPLOYEE_NETWORK
3. (Tips:Role EQUALS Handhelds)	WIRELESS_GUEST_NETWORK
4. (Tips:Role EQUALS Role_Engineer)	WIRELESS_EMPLOYEE_NETWORK
5. (Tips:Role EQUALS eTIPS_Guest)	WIRELESS_GUEST_NETWORK
6. (Tips:Role EQUALS Unknown Client)	WIRELESS_CAPTIVE_NETWORK

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).

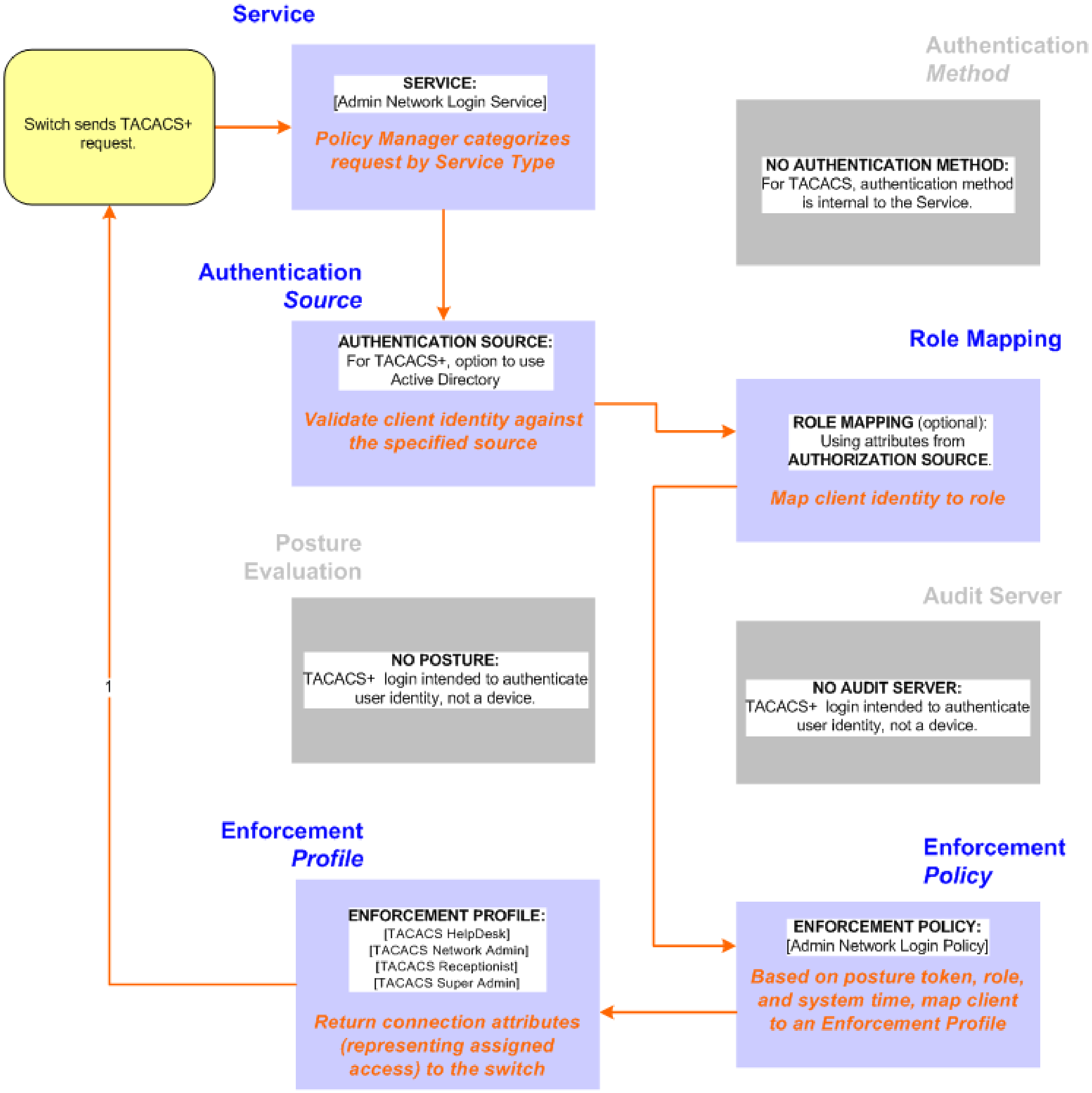
7. Click **Save**.

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 777: *Administrator connections to Network Access Devices via TACACS+*


Service
Switch sends TACACS+ request.
SERVICE: [Admin Network Login Service]
Policy Manager categorizes request by Service Type
Authentication Method
NO AUTHENTICATION METHOD: For TACACS, authentication method is internal to the Service.
Authentication Source
AUTHENTICATION SOURCE: For TACACS+, option to use Active Directory
Validate client identity against the specified source
Role Mapping
ROLE MAPPING (optional): Using attributes from AUTHORIZATION SOURCE.
Map client identity to role
Posture Evaluation
NO POSTURE: TACACS+ login intended to authenticate user identity, not a device.
Audit Server
NO AUDIT SERVER: TACACS+ login intended to authenticate user identity, not a device.
1
Enforcement Profile
ENFORCEMENT PROFILE: [TACACS HelpDesk] [TACACS Network Admin] [TACACS Receptionist] [TACACS Super Admin]
Return connection attributes (representing assigned access) to the switch
Enforcement Policy
ENFORCEMENT POLICY: [Admin Network Login Policy]
Based on posture token, role, and system time, map client to an Enforcement Profile

Configuring the Service

Perform the following steps to configure Policy Manager for TACACS+-based access:

1. 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)**.

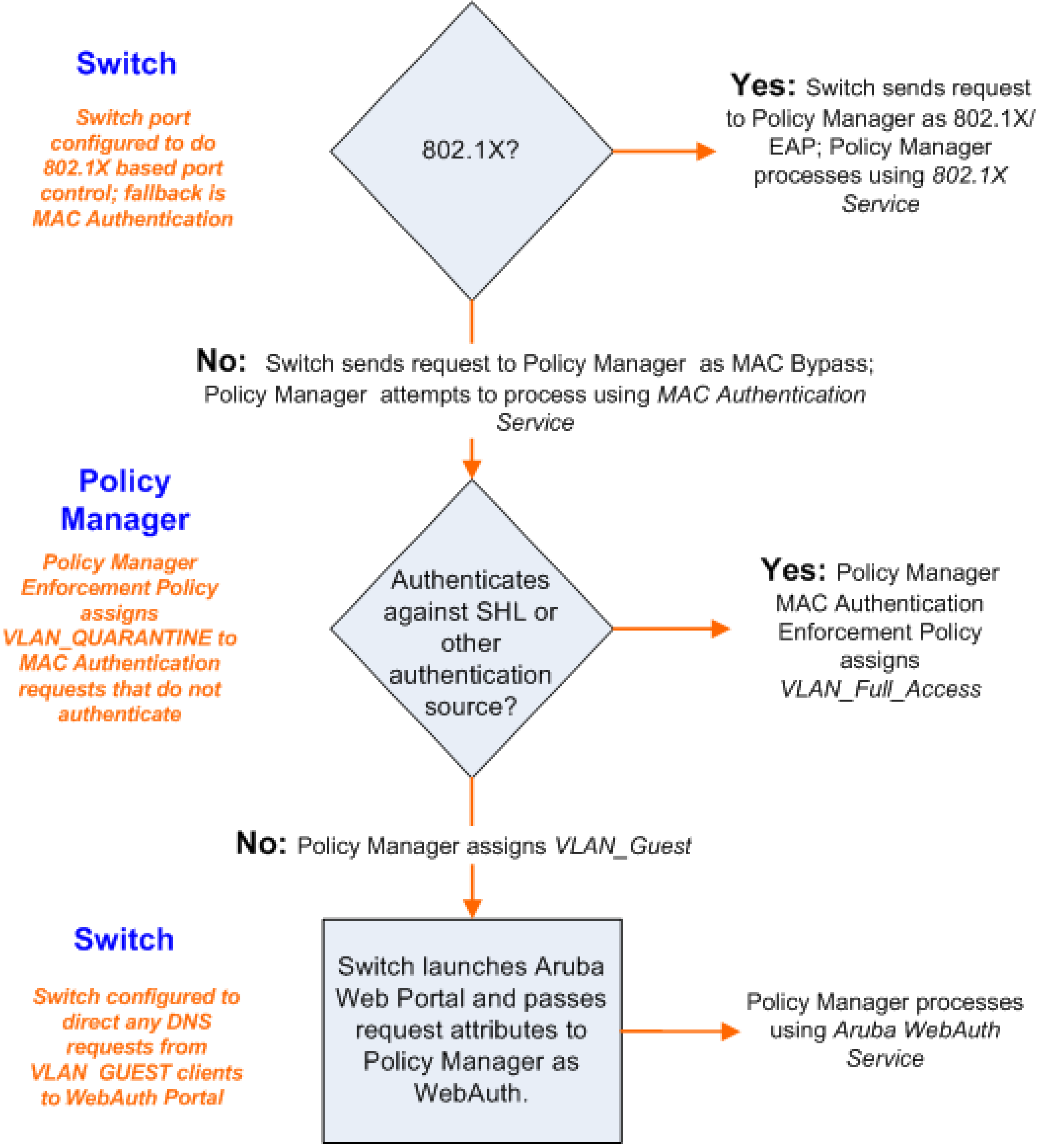
6. Click **Save.** The Service now appears at the bottom of the **Services** list.

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 778: *Flow of the Multiple Protocol Per Port Case*



Switch
Switch port configured to do 802.1X based port control; fallback is MAC Authentication
802.1X?
Yes: Switch sends request to Policy Manager as 802.1X/ EAP; Policy Manager processes using 802.1X Service
No: Switch sends request to Policy Manager as MAC Bypass; Policy Manager attempts to process using MAC Authentication Service
Policy Manager
Policy Manager Enforcement Policy assigns VLAN_QUARANTINE to MAC Authentication requests that do not authenticate
Authenticates against SHL or other authentication source?
Yes: Policy Manager MAC Authentication Enforcement Policy assigns VLAN_Full_Access
No: Policy Manager assigns VLAN_Guest
Switch
Switch configured to direct any DNS requests from VLAN GUEST clients to WebAuth Portal
Switch launches Aruba Web Portal and passes request attributes to Policy Manager as WebAuth.
Policy Manager processes using Aruba WebAuth Service

Appendix D
OnGuard Dissolvable Agent

This appendix includes the following information:

- Introduction
- Native Agents Only Mode
- Native Agents with Java Fallback Mode
- Configuring Web Agent Flow - Java Only Mode
- Native Dissolvable Agent Supported Operating Systems and Browsers
- OnGuard Dissolvable Agent Supported Browsers and Java Versions

Introduction

ClearPass OnGuard controls compromised devices by detecting and blocking access to unsecure or unhealthy devices. The client is denied access to network resources across wired, wireless, and remote networks when it is determined as unsecure, which is accomplished by running an extensive posture assessment.

The OnGuard Agent is supported by Windows, Linux, and Mac OS X devices.

You can configure the OnGuard Dissolvable Agent flow in different modes to perform health scans on endpoints. This section provides information on the end-to-end flow and how to configure OnGuard Dissolvable Agent in the following modes:

- **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 OnGuard Dissolvable Agent Supported Browsers and Java Versions on page 869.

Native Agents Only Mode

The 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 447: *Supported Operating Systems and Browsers*

OS	Browsers
Windows	● Internet Explorer ● FireFox ● Google Chrome
Mac OS X	● Safari ● FireFox ● Google Chrome
Linux	● FireFox

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** page for Windows (.exe) and Mac OS X (.DMG).

Navigate to: **Administration** > **Agents and Software Updates** > **OnGuard Settings**.

Configuring Workflow in Native Agents Only Mode

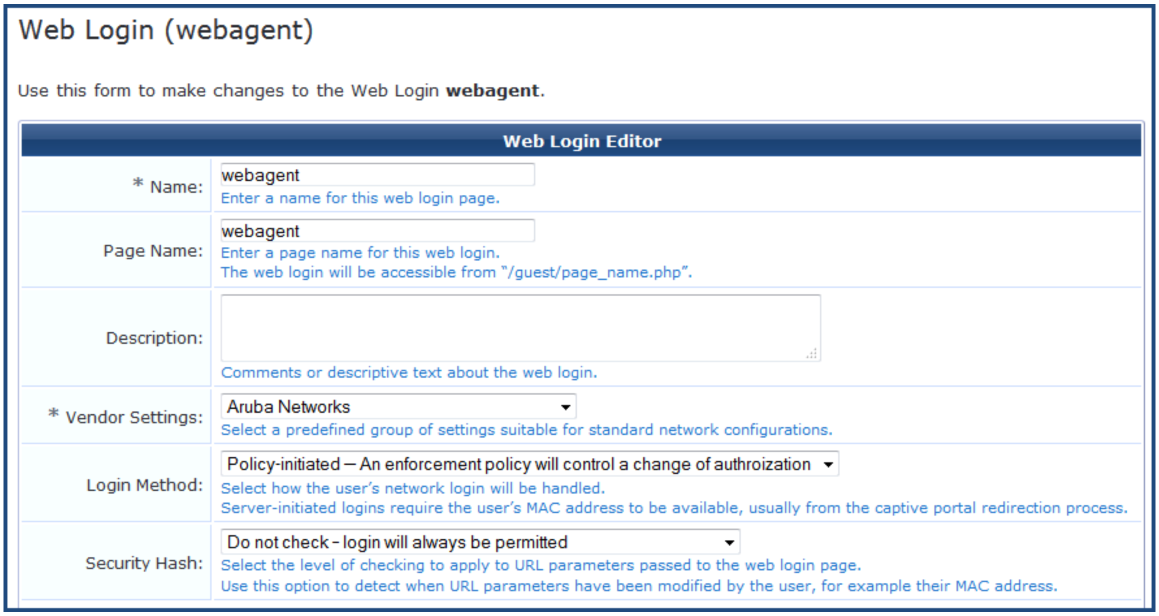
In ClearPass Guest, the web login page is enhanced to avoid an additional web authentication service and simplifies the configuration on dissolvable agent flow with the policy-initiated login method.

To configure the OnGuard Dissolvable Agent in Native agents only mode:

1. In the **Login Method** field, select the **Policy-initiated - An enforcement policy will control a change of authorization** option .

   The following figure displays the policy-initiated login method in the **Web Login Editor** page:

Figure 779: *Policy-Initiated Log-in Method*



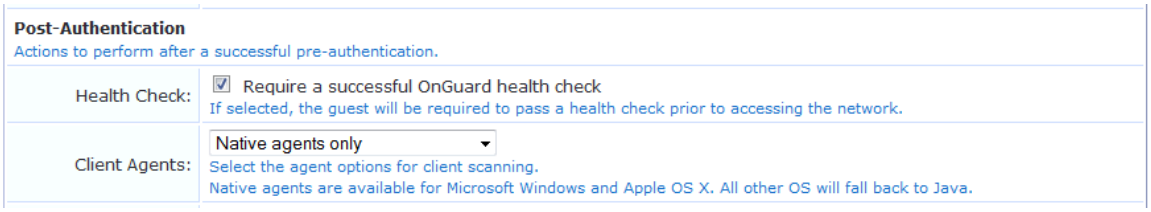
Web Login (webagent)

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 only** mode in the **Client Agents** field:

Figure 780: *Native Agents Only Mode*



Post-Authentication
Actions to perform after a successful pre-authentication.

Health Check:	☑ Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Client Agents:	Native agents only ▾ Select the agent options for client scanning. Native agents are available for Microsoft Windows and Apple OS X. All other OS will fall back to Java.

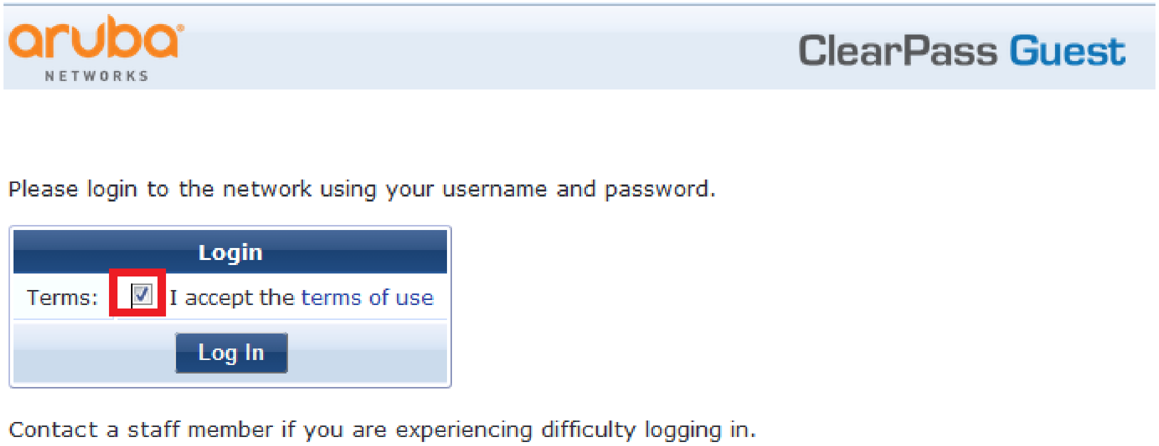
End-to-End Flow in Native Agents Only Mode

The following steps describe the end-to-end flow of the OnGuard Dissolvable Agent running on Native agents only mode:

1. You are redirected to the ClearPass Guest Portal where you can download the native agent installer.
2. After accepting the terms and conditions for collecting end point posture assessment scan checks and performing remediation actions, run the Native Agent Installer.

   The following figure shows an example of the Native Dissolvable Agent **Login** page:

Figure 781: *Native Dissolvable Agent - Login Page*



ClearPass Guest

Please login to the network using your username and password.

Login

Terms: ☑ I accept the terms of use

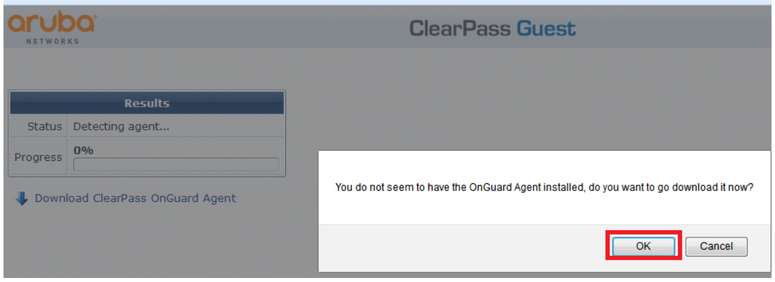
Log In

Contact a staff member if you are experiencing difficulty logging in.

> The **Terms** specified in the **Login** page are optional. You can configure this optionally by selecting the **Require a Terms and Conditions confirmation** check box in the **Terms** field in the ClearPass Guest Login Form.

3. The figure similar to the following OnGuard Agent download prompt appears when you log in for the first time to the Native Dissolvable Agent:

Figure 782: *Native Dissolvable Agent Installer Prompt*



ClearPass Guest

Results

Status	Detecting agent...
Progress	0%

Download ClearPass OnGuard Agent

You do not seem to have the OnGuard Agent installed, do you want to go download it now?

OK Cancel

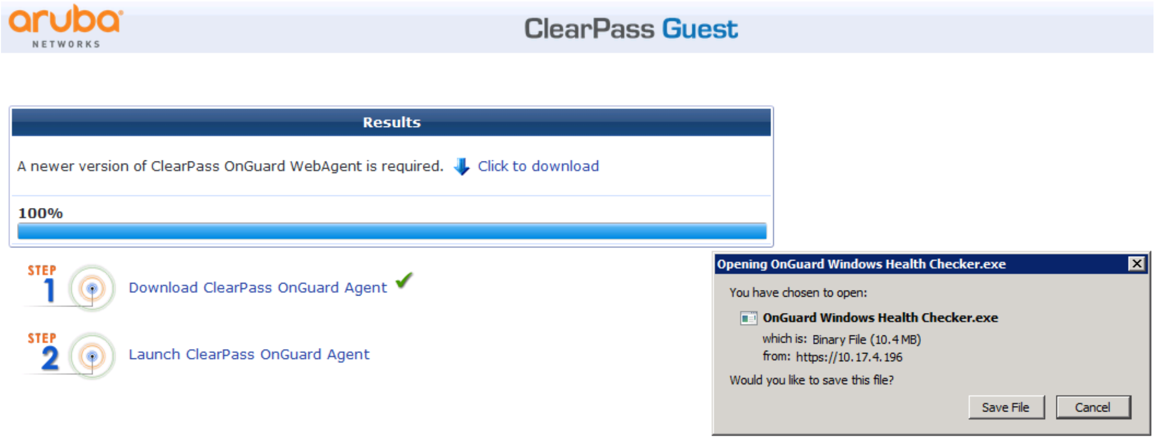
NOTE

The download options are available only when you log in for the first time. Alternatively, you can download the OnGuard agent by clicking the **Download ClearPass OnGuard Agent** link.

4. To download the OnGuard Agent, click **OK**.

   The figure shows an example of the **OnGuard Windows Health Checker** binary download window:

Figure 783: *Native Dissolvable Agent Binary Downloader*


aruba NETWORKS
ClearPass Guest
Results
STEP 1
Download ClearPass OnGuard Agent ✓
STEP 2
Launch ClearPass OnGuard Agent
Save File
Cancel

A newer version of ClearPass OnGuard WebAgent is required. Click to download

100%

Opening OnGuard Windows Health Checker.exe

You have chosen to open:

OnGuard Windows Health Checker.exe

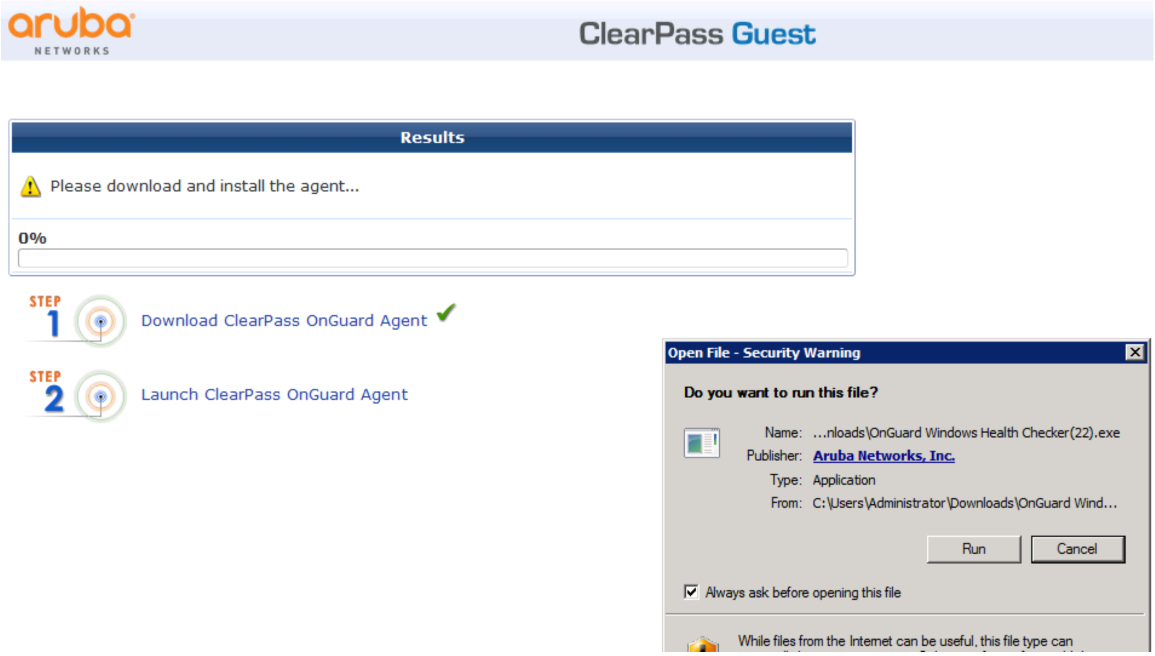
which is: Binary File (10.4 MB)

from: https://10.17.4.196

Would you like to save this file?

5. To download the OnGuard agent, click **Save File**.
6. To install the OnGuard agent, click **Run**.

Figure 784: *Native Dissolvable Agent Installation*


aruba NETWORKS
ClearPass Guest
Results
STEP 1
Download ClearPass OnGuard Agent ✓
STEP 2
Launch ClearPass OnGuard Agent
Run
Cancel

Please download and install the agent...

0%

Open File - Security Warning

Do you want to run this file?

Name: ...nloads\OnGuard Windows Health Checker(22).exe

Publisher: Aruba Networks, Inc.

Type: Application

From: C:\Users\Administrator\Downloads\OnGuard Wind...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can

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.

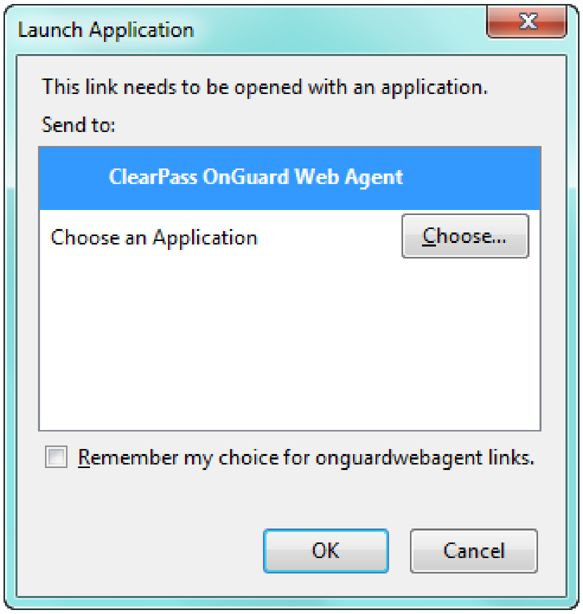
NOTE

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.

7. From the **Launch Application** page, select the **ClearPass OnGuard Web Agent** application.
8. To register and perform auto-launch of native OnGuard agent on successive log-ins, select **Remember my choice for onguardwebagent links**, then click **OK**.

Figure 785: *Native Dissolvable Agent Application Launcher*



Launch Application

This link needs to be opened with an application.

Send to:

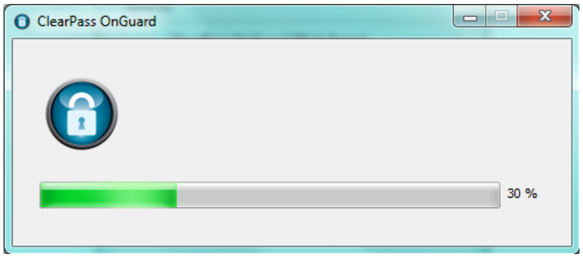
ClearPass OnGuard Web Agent

Choose an Application

□ Remember my choice for onguardwebagent links.

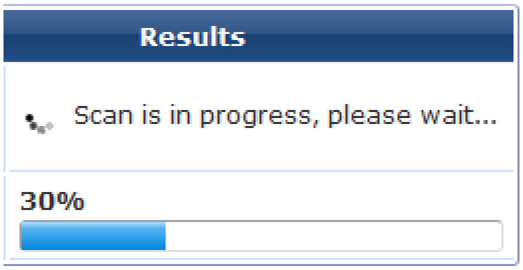
9. The following progress screen appears and shows the progress:

Figure 786: *Native Dissolvable Agent Installation Progress*



10. After the successful installation, the health check scanning is initiated. The following figure shows an example of the progress indicator:

Figure 787: *Health Check Progress*



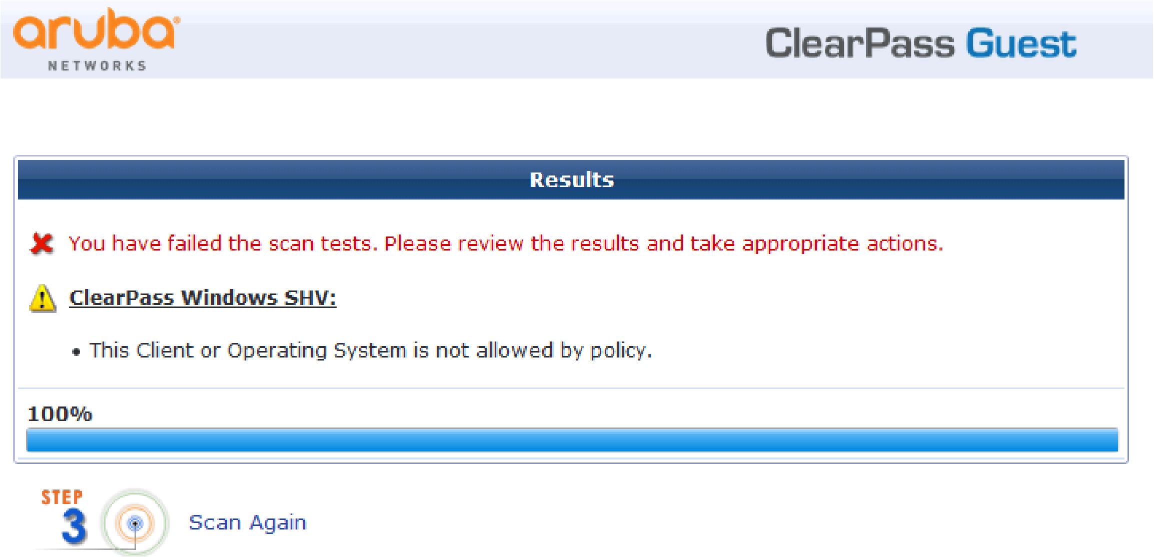
Results

Scan is in progress, please wait...

30%

11. 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 788: *Health Check Results*



ClearPass Guest

Results

✖ You have failed the scan tests. Please review the results and take appropriate actions.

⚠ ClearPass Windows SHV:

- This Client or Operating System is not allowed by policy.

100%

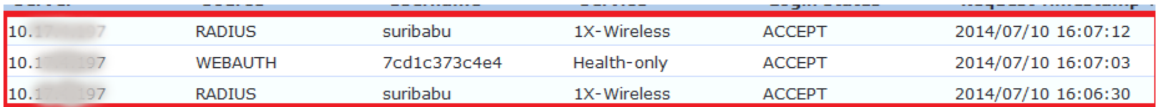
12. Take the appropriate actions to fix the issues listed in remediation and agent enforcement messages, then click **Scan Again**.

    Repeat this step until the client becomes healthy. Once the client is healthy, you can access the destination URL.

13. 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 789: *Access Tracker Page*



10.[redacted]7	RADIUS	suribabu	1X-Wireless	ACCEPT	2014/07/10 16:07:12
10.1[redacted]197	WEBAUTH	7cd1c373c4e4	Health-only	ACCEPT	2014/07/10 16:07:03
10.1[redacted]97	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 the **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

This section provides the following information:

- Configuring Native Agents with Java Fallback Mode

- End-to-End Flow in 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 work flow. The posture assessment is performed based on your selection.

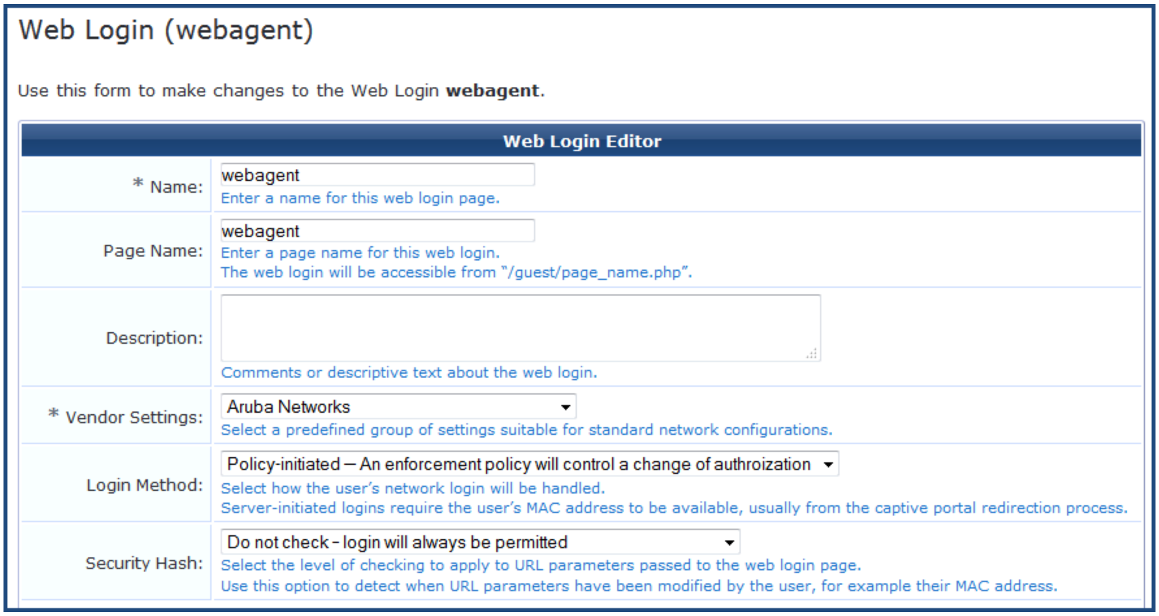
Configuring Native Agents with Java Fallback Mode

To configure the OnGuard Dissolvable Agent in **Native agents with Java fallback** mode:

1. From the drop-down list in the **Login Method** field, select the **Policy-initiated - An enforcement policy will control a change of authorization** option.

   The following figure shows an example configuration of the Policy-initiated **Login** method:

Figure 790: *Policy-Initiated Log-in Method*



Web Login (webagent)

Use this form to make changes to the Web Login **webagent**.

Web Login Editor

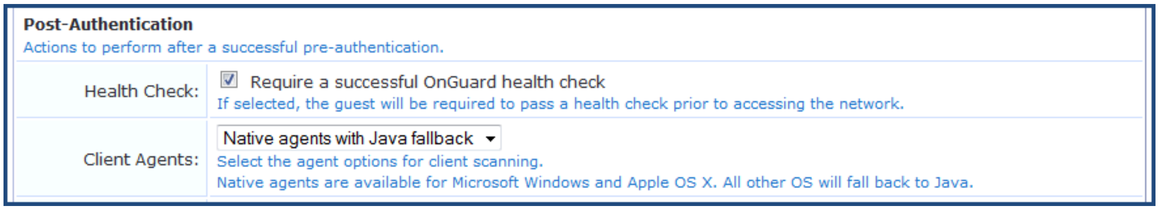
* Name:	webagent Enter a name for this web login page.
Page Name:	webagent Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	Comments or descriptive text about the web login.
* Vendor Settings:	Aruba Networks Select a predefined group of 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. In the **Health Check** field, select the **Require a successful OnGuard health check** option.

   If you select this field, the guest needs to pass a health check before accessing the network.

3. In the **Client Agents** field, select the **Native agents with Java fallback** mode:

Figure 791: *Native Agents with Java Fallback Mode*



Post-Authentication
Actions to perform after a successful pre-authentication.

Health Check:	☑ Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Client Agents:	Native agents with Java fallback Select the agent options for client scanning. Native agents are available for Microsoft Windows and Apple OS X. All other OS will fall back to Java.

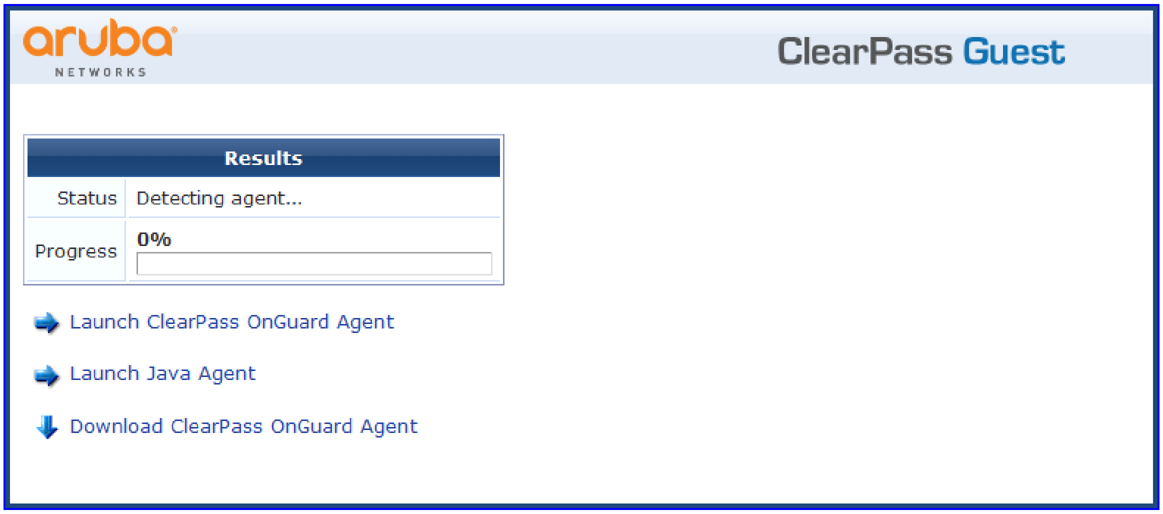
End-to-End Flow in Native Agents with Java Fallback Mode

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 792: *Native Dissolvable Agents with Java Fallback*



aruba NETWORKS
ClearPass Guest

Results	
Status	Detecting agent...
Progress	0%

Launch ClearPass OnGuard Agent
Launch Java Agent
Download ClearPass OnGuard Agent

Configuring Web Agent Flow - Java Only Mode

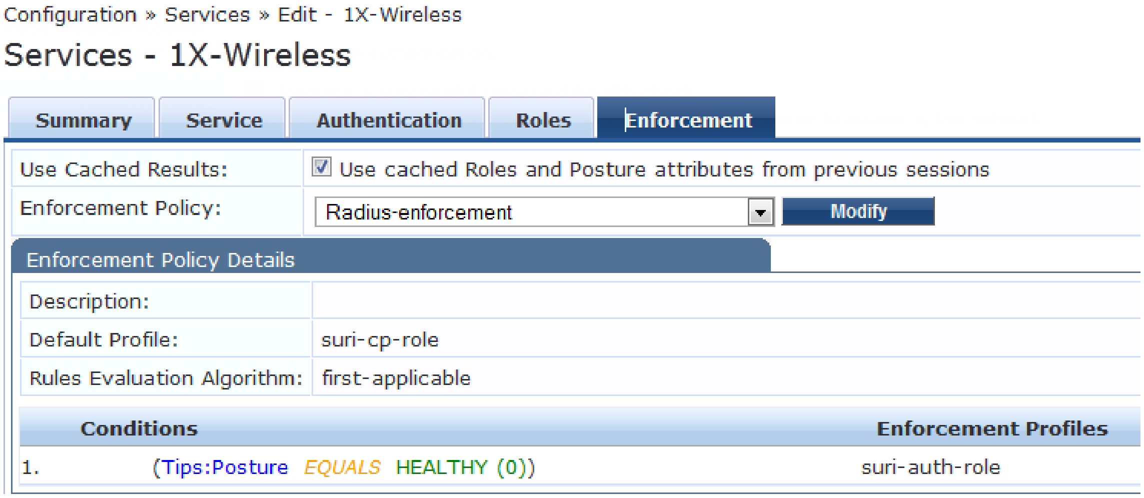
You can configure a new web agent flow in two different locations (ClearPass Policy Manager and ClearPass Guest) to perform health scan on endpoints.

Configuring Web Agent Flow in ClearPass Policy Manager

Use the following steps to configure a new web agent flow in 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 793: *Web Agent Flow - 802.1X Service*



Use Cached Results: ☑ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Radius-enforcement

Enforcement Policy Details

Description:

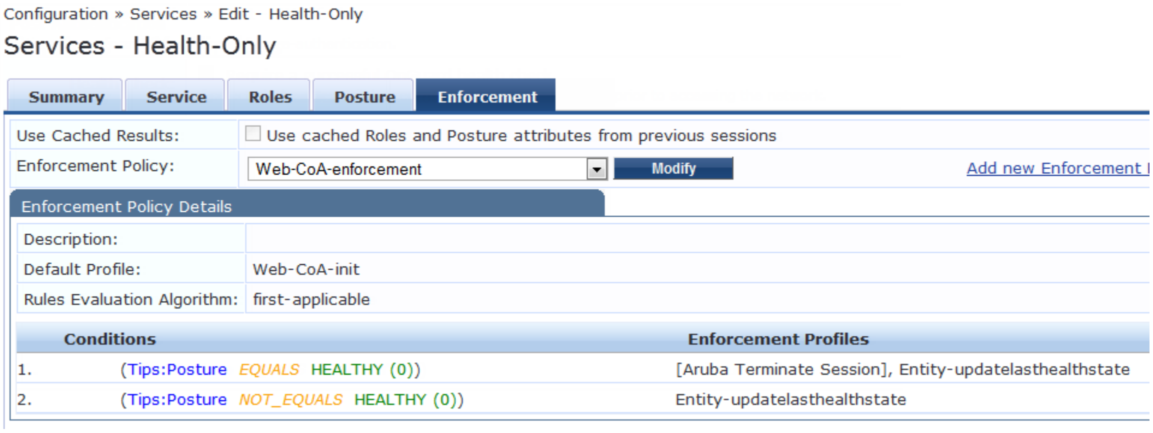
Default Profile: suri-cp-role

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Posture *EQUALS* HEALTHY (0))	suri-auth-role

2. Create a service named **Web-based Health Check Only** on the ClearPass Policy Manager server. The following figure shows an example of the **Web Agent Flow - Health Only** page:

Figure 794: *Web Agent Flow - Health Only*



Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Web-CoA-enforcement

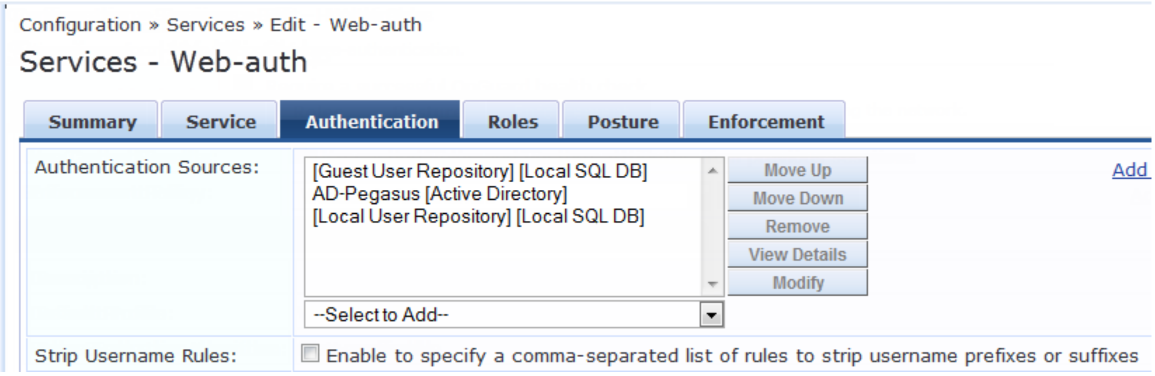
Enforcement Policy Details

Description:	
Default Profile:	Web-CoA-init
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Posture *EQUALS* HEALTHY (0))	[Aruba Terminate Session], Entity-updatelasthealthstate
2.	(Tips:Posture *NOT_EQUALS* HEALTHY (0))	Entity-updatelasthealthstate

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 795: *Web Agent Flow - Services Web Auth*



Authentication Sources:

[Guest User Repository] [Local SQL DB]
AD-Pegasus [Active Directory]
[Local User Repository] [Local SQL DB]

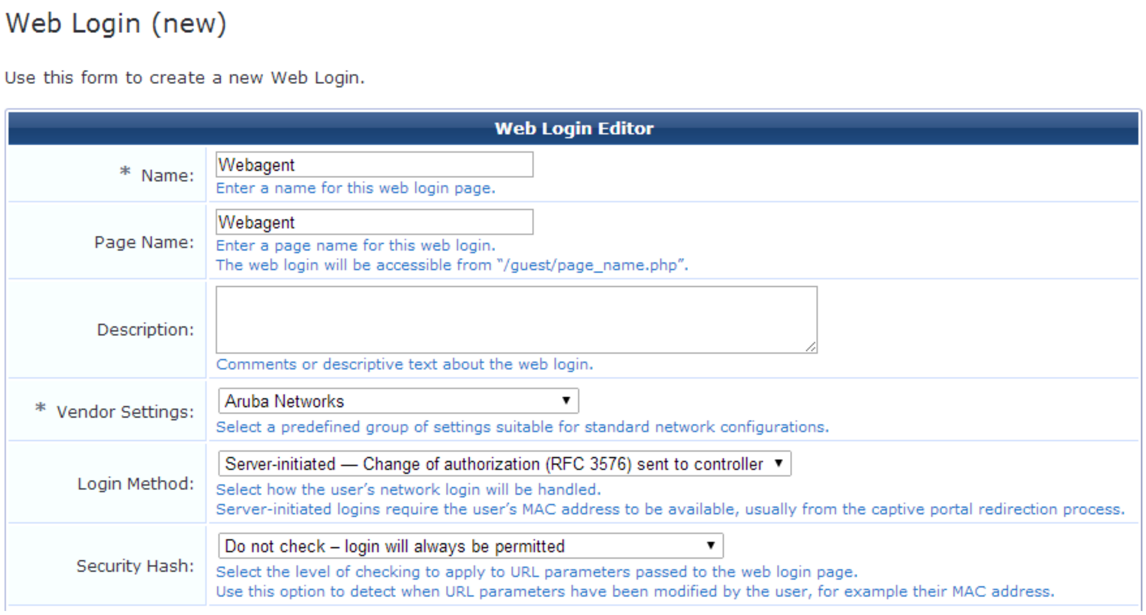
Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

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 796: *Web Login Editor*



Web Login (new)

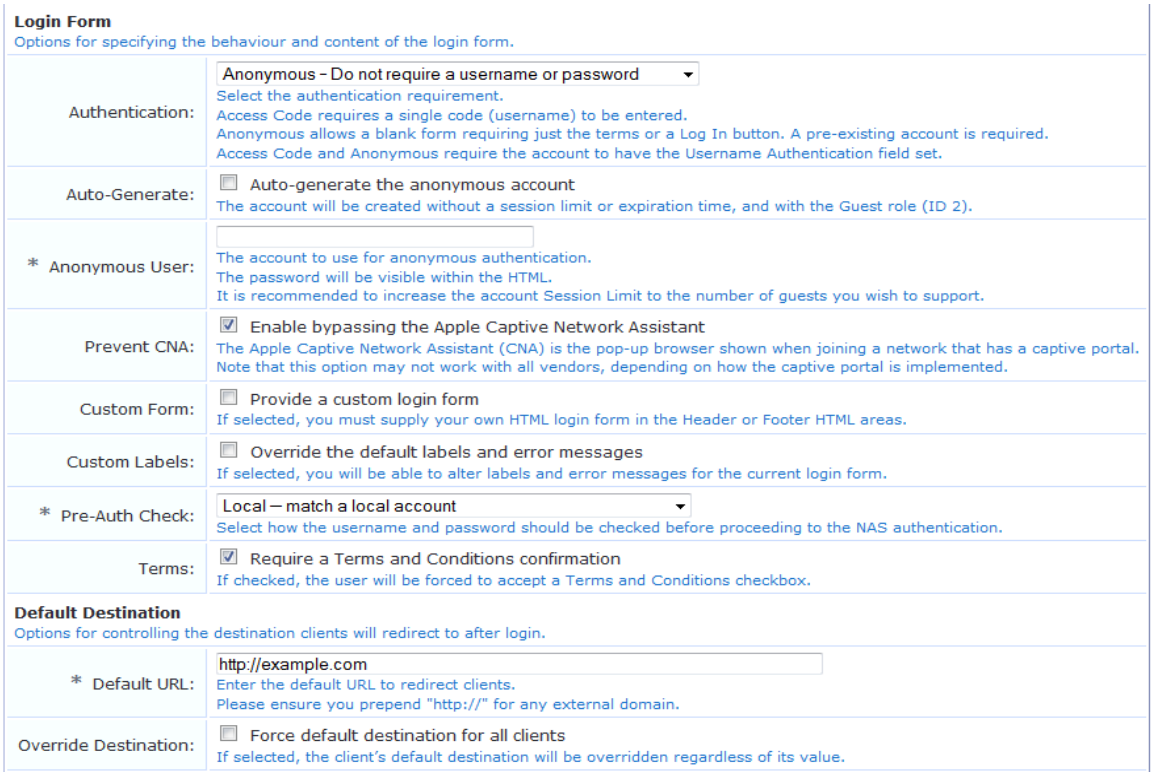
Use this form to create a new Web Login.

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:	Server-initiated — Change of authorization (RFC 3576) sent to controller ▼ 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 **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 797: *Web Login - Login Form*



Login Form
Options for specifying the behaviour and content of the login form.

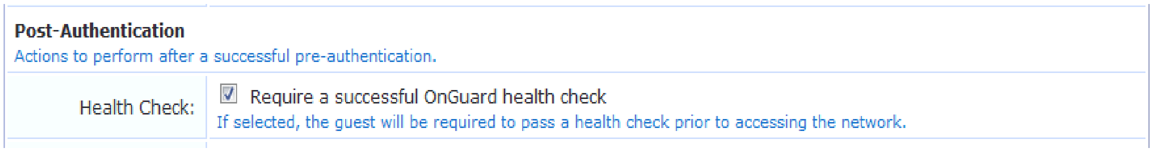
Authentication:	Anonymous - Do not require a username or password ▼ Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Access Code and Anonymous require the account to have the Username Authentication field set.
Auto-Generate:	□ Auto-generate the anonymous account The account will be created without a session limit or expiration time, and with the Guest role (ID 2).
* Anonymous User:	The account to use for anonymous authentication. The password will be visible within the HTML. It is recommended to increase the account Session Limit to the number of guests you wish to support.
Prevent CNA:	☑ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	□ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	□ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	Local — match a local account ▼ Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☑ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

Default Destination
Options for controlling the destination clients will redirect to after login.

* Default URL:	http://example.com Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	□ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

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:

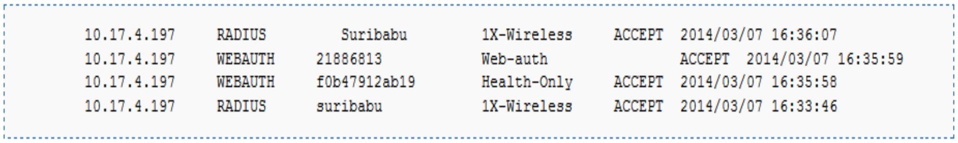
Figure 798: *Web Login - Post-Authentication*



Post-Authentication
Actions to perform after a successful pre-authentication.

Health Check: ☑ Require a successful OnGuard health check
If selected, the guest will be required to pass a health check prior to accessing the network.

The following figure shows an example of the final web agent flow:



```
10.17.4.197    RADIUS      Suribabu       1X-Wireless    ACCEPT  2014/03/07 16:36:07
10.17.4.197    WEBAUTH     21886813       Web-auth               ACCEPT  2014/03/07 16:35:59
10.17.4.197    WEBAUTH     f0b47912ab19   Health-Only    ACCEPT  2014/03/07 16:35:58
10.17.4.197    RADIUS      suribabu       1X-Wireless    ACCEPT  2014/03/07 16:33:46
```

For more information, refer to ClearPass Guest Online Help.

Native Dissolvable Agent Supported Operating Systems and Browsers

This section provides information on the supported operating systems and 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 448: *Native Dissolvable Agent Supported Browsers and Java Versions*

Operating System	Browser	Test Results	Known Issues	Tested Versions
Windows Operating System Support				
Windows 10 64-bit	Chrome	Passed		ClearPass Policy Manager6.6.0.79875 , Chrome 48.X
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		ClearPass Policy Manager 6.6.0.79875 , IE-11.X
Windows 10 32-bit	Chrome	Passed	Health data collection does not work in a 64-bit JRE/ browser	ClearPass Policy Manager6.6.0.79875 , Chrome 48.X
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explore	Passed		ClearPass Policy Manager 6.6.0.79875 , IE-8.X
Windows 8.1 64-bit	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875 , Chrome 49.X

Table 448: *Native Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		ClearPass Policy Manager 6.6.0.79875 , IE-11.x
Windows 7 64-bit	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	Passed	None	ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	Passed	None	ClearPass Policy Manager 6.6.0.79875, IE-11.x
Windows 8 64-bit	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875 , Chrome 48.X
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		ClearPass Policy Manager 6.6.0.79875 , IE-10.X
Windows 8 32-bit	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875 , Chrome 48.X
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875 , Firefox 44.X
	Internet Explorer	Passed		ClearPass Policy Manager 6.6.0.79875 , IE-10.X
Windows 2008 64-bit	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome 41.X
	Firefox	Passed	None	ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE 8.X 32-bit	Passed		ClearPass Policy Manager 6.6.0.79875 , IE-8.x
Windows XP SP3	Chrome	Not supported	None	ClearPass Policy Manager6.6.0.79875, Chrome 34.X
	Firefox	Not supported	None	ClearPass Policy Manager6.6.0.79875, Firefox 30.X
	IE 8.X 32-bit	Not supported		ClearPass Policy Manager 6.6.0.79875, IE-8.x

Table 448: *Native Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
Windows 2003 32-bit	Chrome	Not supported		ClearPass Policy Manager 6.6.0.79875, Chrome 35.X
	Firefox	Not supported		ClearPass Policy Manager 6.6.0.79875, Firefox 30.X
	IE	Not supported		ClearPass Policy Manager 6.6.0.79875, IE-8.x
Windows Vista	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	Passed	None	ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE 7.X 32-bit	Passed	None	ClearPass Policy Manager 6.6.0.79875, IE-7.X
Mac OS X Support				
Mac OS X 10.11	Safari 9.x	Passed		ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox 44.x	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome 48.x	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome-48.x
Mac OS X 10.10	Safari 9.x	Passed		ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox 44.x	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome 48.x	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome-48.x
Mac OS X 10.9	Safari	Passed		ClearPass Policy Manager 6.6.0.79875, Safari 7
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44
	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome-48.
Mac OS X 10.8	Safari	Passed		ClearPass Policy Manager6.6.0.79875, Safari-6.x

Table 448: *Native Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Test Results	Known Issues	Tested Versions
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox-43.x
	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome-47.x
Mac OS X 10.7.5	Safari	Passed		ClearPass Policy Manager6.6.0.79875, Safari-6.x
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox-44.x
	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome-48.x
Mac OS X 10.11	Safari	Passed		ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	Passed		ClearPass Policy Manager 6.6.0.79875, Chrome-48.X
Unbuntu Operating System Support				
Ubuntu 12.04 32-bit LTS	Firefox	Passed		ClearPass Policy Manager6.6.0.79875, Firefox-38.x
	Chrome	No support		ClearPass Policy Manager 6.6.0.79875, Chrome 39.X
Ubuntu 12.04 64-bit LTS	Firefox	Passed	None	ClearPass Policy Manager 6.6.0.79875, Firefox-34.x
	Chrome	No support		ClearPass Policy Manager 6.6.0.79875, Chrome 39.X
Ubuntu 14.04 32-bit LTS	Firefox	Passed	None	ClearPass Policy Manager 6.6.0.79875, Firefox-38.x
	Chromium	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome 39.X
Ubuntu 14.04 64-bit LTS	Firefox	Passed	None	ClearPass Policy Manager 6.6.0.79875, Firefox-44.X
	Chromium	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome 39.X1 and Chromium 39.X

For more information on known issues, refer to the *ClearPass Policy Manager 6.6 Release Notes*.

OnGuard Dissolvable Agent Supported Browsers and Java Versions

This section provides information on supported browsers and Java versions for the OnGuard Dissolvable Agent. The versions given in the following table are tested and are up-to-date at the time of this release:

Table 449: *OnGuard Dissolvable Agent Supported Browsers and Java Versions*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 10 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	ClearPass Policy Manager 6.6.0.79875, Chrome 41.X
	Firefox 44.x	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Internet Explorer 11.x	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, IE-11.x
Windows 10 32-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	ClearPass Policy Manager 6.6.0.79875, Chrome 414
	Firefox 44.x	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Internet Explorer 11.x	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, IE11.x
Windows 7 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		ClearPass Policy Manager6.6.0.79875, IE-11.X

Table 449: *OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 7 32-bit	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome 44.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, IE-11.X
Windows 8 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE 32-bit	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, IE-10.X
Windows 8 32-bit	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, IE-10.X
Windows 8.1 64-bit	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome 44.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 40.X
	IE	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, IE-11.X

Table 449: *OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
Windows 8.1 32-bit	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.80940, Chrome 49.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.80940, Firefox 45.X
	IE	8u73	Passed		ClearPass Policy Manager 6.6.0.80940, IE-11.x
Windows 2008 64-bit	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	ClearPass Policy Manager 6.6.0.79875, Chrome 41.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		ClearPass Policy Manager6.6.0.79875, IE-7.x
Windows Vista	Chrome	8u73	Failed	Health data collection does not work in a 64-bit JRE/ browser	ClearPass Policy Manager 6.6.0.79875, Chrome 48.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	IE	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, IE-9.X
Windows 2003 32-bit	Chrome	8u73	Not supported		ClearPass Policy Manager 6.6.0.79875, Chrome 35.X
	Firefox	8u73	Not supported		ClearPass Policy Manager 6.6.0.79875, Firefox 30.X
	IE	8u73	Not supported		ClearPass Policy Manager 6.6.0.79875, IE

Table 449: *OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
					8.X
Windows XP 32-bit	Chrome	8u73	Not supported		ClearPass Policy Manager 6.6.0.79875, Chrome 35.X
	Firefox	8u73	Not supported		ClearPass Policy Manager 6.6.0.79875, Firefox 30.X
	IE	8u73	Not supported		ClearPass Policy Manager 6.6.0.79875, IE-8.x
Mac 10.11	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Mac 10.10	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	ClearPass Policy Manager 6.6.0.79875, Safari 9.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Mac 10.9.5	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	ClearPass Policy Manager 6.6.0.79875, Safari 7.X

Table 449: *OnGuard Dissolvable Agent Supported Browsers and Java Versions (Continued)*

Operating System	Browser	Java Version	Test Results	Known Issues	Tested Versions
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Mac 10.8	Safari	8u73	Passed	Java plug-in must be enabled to "Run in Unsafe Mode"	ClearPass Policy Manager6.6.0.79875, Safari 6.X
	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
	Chrome	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Chrome-44.x
Unbuntu	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
Fedora	Firefox	8u73	Failed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
CentOS	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.79875, Firefox 44.X
RedHat	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.7987, Firefox 44.X
Suse	Firefox	8u73	Passed		ClearPass Policy Manager 6.6.0.7987, Firefox 44.X

For more information on Known Issues, refer to *ClearPass Policy Manager 6.6 Release Notes*.

Appendix E
Rules Editing and Namespaces

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 875
- Variables on page 885
- Operators on page 886

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 876
- Audit Namespaces on page 877

- Authentication Namespaces on page 877
- Authorization Namespaces on page 879
- Certificate Namespaces on page 880
- Connection Namespaces on page 881
- Date Namespaces on page 882
- Device Namespaces on page 882
- Endpoint Namespaces on page 883
- Guest User Namespaces on page 883
- Host Namespaces on page 883
- Local User Namespaces on page 883
- Posture Namespaces on page 884
- RADIUS Namespaces on page 884
- TACACS Namespaces on page 885
- Tips Namespaces on page 885

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 450: *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 451: *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 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 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 Configuring Authentication Methods on page 165).
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 451: *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 Configuring Authentication Sources on page 190 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 Configuring Authentication Sources on page 190).

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 452: *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 452: *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 453: *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 453: *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.

NOTE

These attributes can be used only if you have pre-populated the values for these attributes when a network device is configured.

Endpoint Namespaces

Use these attributes to look for attributes of authenticating endpoints, which are present in the Policy Manager endpoints list. The Endpoint namespace has the following attributes:

- Disabled By
- Disabled Reason
- Enabled By
- Enabled Reason
- Info URL

Guest User Namespaces

The GuestUser namespace has the attributes associated with the guest user (resident in the Policy Manager guest user database) who authenticated in this session. This namespace is only applicable if a guest user is authenticated. The GuestUser namespace has six pre-defined attributes:

- Company-Name
- Designation
- Email
- Location
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the guest user.

NOTE

These attributes can be used only if you have pre-populated the values for these attributes when a guest user is configured in Policy Manager.

Host Namespaces

The Host namespace has the following predefined attributes:

- Name*
- OSType*
- FQDN*
- UserAgent**
- CheckType**
- UniqueID
- AgentType*
- InstalledSHAs*

* Only populated when request is originated by a Microsoft NAP-compatible agent.

** Only present if Policy Manager acts as a Web authentication portal.

Local User Namespaces

The LocalUser namespace has the attributes associated with the local user (resident in the Policy Manager local user database) who authenticated in this session. This namespace is only applicable if a local user is authenticated.

The LocalUser namespace has four pre-defined attributes:

- Designation

- Email
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the local user.

NOTE

These attributes can be used only if you have pre-populated the values for these attributes when a local user is configured in Policy Manager.

Posture Namespaces

The dictionaries in the posture namespace are pre-packaged with the product. The administration interface provides a way to add dictionaries into the system (see Posture Dictionary.) 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 664 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 (Terminal Access Controller Access-Control System) 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 run-time rule evaluation.

The following built-in variables are supported in Policy Manager:

Table 454: *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 Configuring Authentication Sources on page 190.
%{RADIUS:IETF:MAC-Address-Colon}	MAC address of client in aa:bb:cc:dd:ee:ff format
%{RADIUS:IETF:MAC-Address-Hyphen}	MAC address of client in aa-bb-cc-dd-ee-ff format
%{RADIUS:IETF:MAC-Address-Dot}	MAC address of client in aabb.ccdd.eeff format
%{RADIUS:IETF:MAC-Address-NoDelim}	MAC address of client in aabbccddeeff format

NOTE

You can also use any other dictionary-based attributes (or namespace attributes) as variables in role mapping rules, enforcement rules, enforcement profiles, and LDAP or SQL filters. For example, you can use %{RADIUS:IETF:Calling-Station-ID}or %{RADIUS:Airespace:Airespace-Wlan-Id} in rules or filters.

Operators

The rules editing interface in Policy Manager supports a rich set of operators.

The type of operators presented are based on the data type of the attribute for which the operator is being used. Where the data type of the attribute is not known, the attribute is treated as a string type.

The following table lists the operators presented for common attribute data types:

Table 455: *Attribute Operators*

Attribute Type	Operators
String	• BELONGS_TO • NOT_BELONGS_TO • BEGINS_WITH • NOT_BEGINS_WITH • CONTAINS • NOT_CONTAINS • ENDS_WITH • NOT_ENDS_WITH • EQUALS • NOT_EQUALS • EQUALS_IGNORE_CASE • NOT_EQUALS_IGNORE_CASE • EXISTS • NOT_EXISTS • MATCHES_REGEX • NOT_MATCHES_REGEX
Integer	• BELONGS_TO • NOT_BELONGS_TO • EQUALS • NOT_EQUALS • EXISTS • NOT_EXISTS • GREATER_THAN • GREATER_THAN_OR_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS
Time or Date	• EQUALS • NOT_EQUALS • GREATER_THAN • GREATER_THAN_OR_EQUALS • LESS_THAN • LESS_THAN_OR_EQUALS • IN_RANGE

Table 455: *Attribute Operators (Continued)*

Attribute Type	Operators
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 456: *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`

Operator	Description
	`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`
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

Operator	Description
	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*`