Copyright Information

© Copyright 2018 Hewlett Packard Enterprise Development LP.
All rights reserved. Specifications in this manual are subject to change without notice.
Originated in the USA. All other trademarks are the property of their respective owners.

Open Source Code

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.
# Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Change Description</th>
<th>Revision Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 01</td>
<td>Initial ClearPass 6.7.0 release</td>
<td>--</td>
</tr>
<tr>
<td>Revision 02</td>
<td>Includes documentation for 6.7.1 features.</td>
<td>February 5, 2018</td>
</tr>
<tr>
<td>Revision 03</td>
<td>Includes documentation for 6.7.2 features</td>
<td>March 21, 2018</td>
</tr>
<tr>
<td>Revision 04</td>
<td>Includes documentation for 6.7.3 features</td>
<td>April 25, 2018</td>
</tr>
<tr>
<td>Revision 05</td>
<td>Includes documentation for 6.7.4 features</td>
<td>June 8, 2018</td>
</tr>
<tr>
<td>Revision 06</td>
<td>Includes documentation for 6.7.5 features</td>
<td>July 18, 2018</td>
</tr>
<tr>
<td>Revision 07</td>
<td>Includes documentation for 6.7.6 features</td>
<td>September 14, 2018</td>
</tr>
<tr>
<td>Copyright Information</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>About ClearPass Policy Manager</strong></td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Initial Login and Activation of the ClearPass Platform License</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Using the Policy Manager Dashboard</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Accessing Configuration Information</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Importing and Exporting Information</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Viewing the List of Services</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Configuring Services Using Service Templates &amp; Wizards</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Configuring Other Policy Manager Services</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>Modifying and Managing Services</td>
<td>96</td>
<td></td>
</tr>
<tr>
<td><strong>Live Monitoring</strong></td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Live Monitoring: Access Tracker</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Live Monitoring: Accounting</td>
<td>115</td>
<td></td>
</tr>
<tr>
<td>Live Monitoring: OnGuard Activity</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>Live Monitoring: Analysis and Trending</td>
<td>134</td>
<td></td>
</tr>
<tr>
<td>Live Monitoring: System Monitor</td>
<td>135</td>
<td></td>
</tr>
<tr>
<td>Monitoring Endpoint Profiler and Network Scan</td>
<td>139</td>
<td></td>
</tr>
<tr>
<td>Monitoring Discovered Devices</td>
<td>142</td>
<td></td>
</tr>
<tr>
<td>Audit Viewer</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>Event Viewer</td>
<td>148</td>
<td></td>
</tr>
<tr>
<td>Data Filters</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>Restoring Blacklisted Users to the Network</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication Methods and Sources</strong></td>
<td>158</td>
<td></td>
</tr>
<tr>
<td>Supported Authentication Methods</td>
<td>158</td>
<td></td>
</tr>
</tbody>
</table>
Default Authentication Sources ................................................................. 158
Adding and Modifying Authentication Methods ............................................. 161
Adding and Configuring Authentication Sources ............................................. 184
Modifying Authentication Methods or Sources for an Existing Service .......... 218

Configuring Identity Settings ........................................................................... 220
Configuring Single Sign-On ........................................................................... 220
Managing Local Users ................................................................................. 222
Adding and Modifying Endpoints ................................................................... 229
Managing Static Host Lists ............................................................................ 239
Configuring a Role and Role-Mapping Policy ................................................. 243
Identity Roles Architecture and Workflow ...................................................... 244

Posture Policies and Audit Servers ................................................................. 250
Posture Architecture and Flow ....................................................................... 250
Creating a New Posture Policy ....................................................................... 252
Configuring Posture Policy Agents and Hosts ............................................... 253
Configuring Posture Policy Plug-ins .............................................................. 257
Configuring Posture Policy Rules .................................................................. 335
Configuring Posture for Services ................................................................... 336
Configuring Audit Servers ............................................................................ 338

Configuring Enforcement Profiles and Policies .............................................. 354
Configuring Enforcement Profiles ............................................................... 354
Configuring Enforcement Policies .............................................................. 409
Configuring Deep-Nested Active Directory Queries ...................................... 413
Adding and Modifying Network Devices ....................................................... 418
Adding and Modifying Device Groups .......................................................... 428
Adding and Modifying Proxy Targets ............................................................ 431
Configuring the Ingress Event Source ............................................................ 432

Network Scan and Profile Settings ................................................................. 434
Configuring SNMP, SSH, and WMI Credentials ................................................................. 434
Scheduling Network Scans and Subnet Scans ................................................................. 440

**Configuring Policy Simulation** ........................................................................ 448

Active Directory Authentication Simulation ........................................................... 448
Application Authentication Simulation ................................................................. 450
Audit Simulation ........................................................................................................ 451
Chained Simulation .................................................................................................... 453
Enforcement Policy Simulation ................................................................................ 455
RADIUS Authentication Simulation ......................................................................... 458
Role Mapping Simulation .......................................................................................... 463
Service Categorization Simulation .......................................................................... 466

**ClearPass Profiler** .......................................................................................... 470

ClearPass Device Profiler Overview ......................................................................... 470
About the Device Profile ............................................................................................. 474
Endpoint Information Collectors .............................................................................. 474

**Administration** ............................................................................................... 480

ClearPass Portal .......................................................................................................... 481
Managing Admin Users ............................................................................................ 482
Managing Admin Privileges ...................................................................................... 487
Server Manager .......................................................................................................... 496
Server Configuration Operations ............................................................................. 496
Configuring the ClearPass Policy Manager Server ............................................... 496
ClearPass Cluster Configuration Options .................................................................. 543
Managing Policy Manager Zones ............................................................................ 560
Log Configuration ...................................................................................................... 572
Downloading Local Shared Folders .......................................................................... 576
License Management .................................................................................................. 576
External Servers .......................................................................................................... 588
SNMP Trap Receivers ................................................................. 589
Syslog Targets ........................................................................... 594
Syslog Export Filters ................................................................. 595
Messaging Setup ......................................................................... 607
Endpoint Context Servers ............................................................. 609
Configuring Endpoint Context Server Actions ............................... 617
Adding Vendor-Specific Endpoint Context Servers ......................... 624
File Backup Servers ..................................................................... 684
Certificate Store ........................................................................... 686
Service Certificates ...................................................................... 698
Associating a RADIUS Service Certificate with a Service ................. 703
Certificate Trust List ..................................................................... 705
Certificate Revocation Lists .......................................................... 707
Using ClearPass Dictionaries ......................................................... 710
RADIUS Dictionary ...................................................................... 710
RADIUS CoA Templates ................................................................. 712
TACACS+ Services Dictionary ....................................................... 714
Device Fingerprints Dictionary ....................................................... 715
Dictionary Attributes ................................................................. 719
Applications Dictionaries .............................................................. 722
Configuring Endpoint Context Server Actions ............................... 723
Enabling Ingress Event Dictionaries ............................................. 731
OnGuard Settings and Agent Library Updates ................................ 732
Onguard Agent Installers ............................................................... 744
OnGuard Global Agent Settings .................................................... 746
Creating OnGuard Custom Web Pages ......................................... 750
Software Updates ......................................................................... 756
Support Services ........................................................................... 761
Administration Operations ................................................................. 863
Managing Insight Admin Privileges ...................................................... 866

Command Line Interface ........................................................................ 872
Cluster Commands ................................................................................. 872
Configure Commands ............................................................................... 875
Network Commands ................................................................................ 881
Miscellaneous Commands ....................................................................... 887
Service Commands .................................................................................. 896
Show Commands ....................................................................................... 898
SSH Timed Account Lockout ................................................................. 903
System Commands .................................................................................... 907

SNMP, System Events & Error Codes ..................................................... 918
ClearPass SNMP Private MIB ................................................................. 918
ClearPass SNMP Traps and OIDs ........................................................... 923
SNMP Trap Details .................................................................................. 927
Important System Events ........................................................................ 930
Error Codes ............................................................................................... 935

Use Cases ................................................................................................. 938
802.1X Wireless Use Case ....................................................................... 938
Web Based Authentication Use Case ....................................................... 944
MAC Authentication Use Case ............................................................... 950
TACACS+ Use Case ................................................................................ 954
Single Port Use Case ............................................................................... 956

Rules Editing and Namespaces ............................................................... 958
Namespaces ............................................................................................. 958
Variables ................................................................................................ 968
Operators ................................................................................................ 969
Applications Dictionaries ......................................................................... 973
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.

ClearPass Access Management System Overview
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.

About Policies, Profiles, and Services
In ClearPass Policy Manager, a policy provides the rules that tells ClearPass when to execute profiles. Profiles are actions that are taken by ClearPass; for example assigning a certain role to a user or enabling command authorization for different types of users on a switch. The actions specified in a policy are the profiles to be activated when specific conditions or rules are met.

Then a policy is associated with a service—a service ties all the elements together: authentication sources, authorization sources, role-mapping, and enforcement policies.

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.
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, macOS, iOS, Android, ChromeOS, and Ubuntu devices via a built-in enrollment workflow. 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.

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.
For a list of common configuration tasks and pointers to information about how to perform each task, refer to Accessing Configuration Information.

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.

Key Features

ClearPass’s key features are as follows:

- 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
- Role-based network access enforcement for multivendor Wi-Fi, wired, and VPN networks
- Virtual and hardware appliances that can be deployed in a cluster to increase scalability and redundancy.
- Support for popular virtualizations platforms such as VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, and Amazon AWS (EC2).
- Intuitive policy configuration templates and visibility troubleshooting tools.
- Supports multiple authentication/authorization sources—AD, LDAP, and SQL dB.
- Self-service device onboarding with built-in certificate authority (CA)
- Guest access with extensive customization, branding and sponsor-based approvals.
- Supports NAC and EMM/MDM integration for mobile device assessments.
- Comprehensive integration with the Aruba 360 Security Exchange Program.
- SAML 2.0 Identity Provider allowing seamless single sign-on (SSO) to cloud or on-premise applications
- SAML 2.0 Service Provider allowing seamless and secure access to ClearPass components using federated/unified identity
- Advanced reporting and granular alerts.
- Active and passive device fingerprinting
- 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
- Social and Cloud Identity Network and Cloud Application SSO via OAuth2 OAuth 2.0
- Facebook, Twitter, LinkedIn, Azure Active Directory and Office 365 Office365, Google G Suite Google Apps, and so on
- Device and User certificate enrollment via Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) and REST API-based workflows
- Advanced reporting of all user authentications and failures
- Enterprise Reporting, Monitoring, and Alerting
- 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

**System Specifications and Requirements**

**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)
- EAP-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
- OAuth 2.0
- Microsoft Network Access Protection (NAP) and Network Access Control (NAC)
- Active Directory machine authentication
- Online Certificate Status Protocol (OCSP)
- SNMP generic MIB, SNMP private MIB
- Common Event Format (CEF), Log Event Extended Format (LEEF)
- Simple Certificate Enrollment Protocol (SCEP)
- Enrollment over Secure Transport (EST)

**Supported Identity Stores**
- Microsoft Active Directory
- Kerberos
- Any LDAP-compliant directory
- Microsoft SQL, PostgreSQL, MariaDB, and Oracle 11g ODBC-compliant SQL server
- Built-in SQL store
- Built-in static-hosts list
- Token servers
- Built-in SQL store, static hosts list
- Microsoft Azure Active Directory (via SAML and OAuth 2.0)
- Google G Suite (via SAML and OAuth 2.0)
- Any SAML 2.0-compliant identity provider

**Supported Browsers**
The supported browsers for ClearPass are:
- Mozilla Firefox on Windows 7, Windows 8.x, Windows 10, and macOS
- Google Chrome for macOS and Windows
- Apple Safari 9.x and later on macOS
- Mobile Safari 5.x on iOS
- Microsoft Edge on Windows 10
Microsoft Internet Explorer 10 and later on Windows 7 and Windows 8.x. When accessing ClearPass Insight with Internet Explorer (IE), IE 11 or above is required.

Special Characters Supported in Passwords

The special characters that are supported in passwords for all ClearPass modules (Policy Manager, ClearPass Guest, ClearPass Onboard, ClearPass OnGuard and ClearPass Insight) are described in the following table:

<table>
<thead>
<tr>
<th>Special Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Plus sign</td>
</tr>
<tr>
<td>,</td>
<td>Comma</td>
</tr>
<tr>
<td>-</td>
<td>Hyphen</td>
</tr>
<tr>
<td>.</td>
<td>Period</td>
</tr>
<tr>
<td>;</td>
<td>Semicolon</td>
</tr>
<tr>
<td>=</td>
<td>Equal sign</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
</tr>
<tr>
<td>_</td>
<td>Underscore</td>
</tr>
</tbody>
</table>

Initial Login and Activation of the ClearPass Platform License

This section contains the following information:

- Specifying the ClearPass Platform License Key Upon Initial Login
- Logging in to the ClearPass Server
- Customizing the Landing Page Layout
- ClearPass Menu

Specifying the ClearPass Platform License Key Upon Initial Login

Upon initial login to a Policy Manager 6.7.x server and later, you are prompted to enter the ClearPass Platform License Key. The Policy Manager licenses on each cluster node are converted to ClearPass Platform Licenses. The ClearPass Platform License provides a platform activation code that is installed on all the nodes in a ClearPass cluster.

The ClearPass Platform License is the base-level license. Each ClearPass server has one ClearPass Platform License for the physical hardware. Virtual devices have a ClearPass Platform License as well on a per-expected device level.

For details about managing ClearPass licenses, see License Management.

You cannot have more than one ClearPass Platform license installed on a ClearPass node.
To specify the ClearPass Platform License Key upon initial login:

1. Navigate to the ClearPass Policy Manager Publisher node:
   
   `https://x.x.x.x/tips/`

   where `x.x.x.x` is the IP address of the management interface defined for the server.

2. Log in to the ClearPass 6.7.x or later server. The ClearPass Policy Manager End-User Software License Agreement dialog appears.

   The **Select Application** field is preset to **ClearPass Platform**.

**Figure 2  Entering the ClearPass Platform License Key**

![Image of the ClearPass Policy Manager Publisher node](image)

3. Enter the **ClearPass Platform License Key**.

4. Click the check box for **I agree to the above terms and conditions**. The **Add License** button is now enabled.

5. Click **Add License**. The **Admin Login** screen appears with a message indicating that you have 90 days to activate the product and a link to activate the product.

**Figure 3  Activating the ClearPass Node**

![Image of the Admin Login screen](image)

6. To activate the ClearPass Platform License on this appliance, click the **Activate Now** link. The **Activate License** dialog opens:
7. If the ClearPass server is connected to the Internet, click the **Activate Now** button. The message, "*Product has been successfully activated*" appears, and the **Admin Login** dialog is displayed.

**Figure 5 Activation Successful: Admin Login Available**

---

**Logging in to the ClearPass Server**

The password you use upon initial login depends on the following scenarios:

- If you installed a ClearPass version before 6.7, set the cluster password. If a system is upgraded from ClearPass 6.x.x to 6.7, **eTIPS123** is the default password.
- If your ClearPass installation is a fresh 6.7 installation, **eTIPS123** is not supported as the default password. You must enter the password that was set up during the installation process.
- If a ClearPass 6.7 OVF (Open Virtualization Format Virtual Machine) is deployed, you are prompted for the default password (**eTIPS123**) to initiate bootstrapping. After assigning all network parameters, hostname, etc. to the ClearPass server, you are prompted for a new password during the bootstrapping process.

1. Log in to the ClearPass server with the following credentials:
   - **Username**: admin
   - **Password**: Enter the ClearPass cluster password.

2. Click **Log In**. The **ClearPass Policy Manager Landing Page** opens.
Customizing the Landing Page Layout

To customize the Landing Page layout to display the information you most want to see (refer to Using the Policy Manager Dashboard), drag and drop from the list of the Widget elements on Dashboard to one of the available Dashboard slots in the right pane.

ClearPass Menu

The ClearPass Menu is available on the upper-right corner of every page in the ClearPass user interface.

Figure 6  ClearPass Policy Manager Landing Page

Figure 7  ClearPass Menu
From the ClearPass Menu, you can:

- Navigate to any of the ClearPass modules: **Guest**, **Insight**, **Policy Manager**, and **Onboard**.
- Bring up online Help for the current page of the ClearPass user interface.
- Access the Contact Support information.
- Log out

**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, and viewing the Access Tracker.

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**

<table>
<thead>
<tr>
<th>Widget Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts</td>
<td>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.</td>
</tr>
<tr>
<td>All Requests</td>
<td>To view the graph that displays all requests (such as RADIUS, TACACS+, and WebAuth requests) processed by Policy Manager over the past week, drag and drop the All Requests widget. Clicking on each bar in the graph drills down to the Access Tracker page and shows the requests for the selected day.</td>
</tr>
<tr>
<td>Applications</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication Status</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Cluster Status | 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.  
  - **Last Replication**: Date of the last replication. |
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **Status:** Indicates the status of the cluster node. | 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 |
| ![]() | To view the device family of a particular device category, drag and drop the **Device Category** widget to the Dashboard, then select the device category from the drop down menu. For example, selecting **Computer** would show that the device family is **Windows**. |
| ![]() | 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. |
| ![]() | 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. |
| ![]() | 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.  
- **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. |
<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Latest Authentications</strong>&lt;br&gt;Latest Authentications</td>
<td>To view the table with the latest authentications, drag and drop the <strong>Latest Authentications</strong> widget to the Dashboard. Clicking on a row in the table drills down to the <strong>Access Tracker</strong> page that shows requests sorted by timestamp with the latest request displayed on the top.</td>
</tr>
</tbody>
</table>
| **License Usage**<br>License Usage | To view the table that displays the **Available Count** and **Used Count** of the application licenses installed on the current ClearPass server, drag and drop the **License Usage** widget to the Dashboard.  
- From the **Select Application** drop-down, select the Application License of interest. |
| **MDM Discovery Summary**<br>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 depend 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**<br>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** widget to the Dashboard. |
| **Quick Links**<br>Shortcuts to different configuration interfaces | 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**  
- **ClearPass Insight**  
- **ClearPass Extensions** |
| **Request Processing Time**<br>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. |
| **Service Categorization**<br>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. |
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.

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.

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**
- **Service Templates & Wizards**
- **Services**
- **Authentication and Authorization**
- **Identity**
- **Posture**
- **Enforcement**
- **Network**
- **Policy Simulation**
- **Profile and Network Scan**
- **Accessing Configuration Information**
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 opens (see Figure 8):

**Figure 8  ClearPass Policy Manager Configuration Menu**

![Configuration Menu](image)

Service Templates & Wizards

The ClearPass Policy Manager Service Templates & Wizards page provides the ability to create templates for services that will allow you to define baseline policies and require specific data when you create services.

For more information, see Configuring Services Using Service Templates & Wizards.

Services

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

- Services Flow and Creation Methods on page 1
- Modifying and Managing Services
- Using Templates to Create ClearPass Services
- Configuring Other Policy Manager Services

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 Modifying Authentication Methods on page 161
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 220
- Managing Local Users on page 222
- Adding and Modifying Endpoints on page 229
- Managing Static Host Lists
- Adding and Modifying Roles
- Adding and Modifying Role-Mapping Policies

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
- Creating a New Posture Policy
- 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 sections:
- Configuring Enforcement Profiles
- Configuring Enforcement Policies

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
- Adding and Modifying Device Groups
- Adding and Modifying Proxy Targets
- Configuring the Ingress Event Source

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.
Profile and Network Scan

The Profile and Network Scan page provides options to configure the following elements:

- Subnet scans: See Scheduling Network Scans and Subnet Scans.
- Network scans: See Scheduling Network Scans and Subnet Scans.
- SNMP Configuration: See SNMP Credentials Configuration.
- SSH Configuration: See SSH Credentials Configuration.
- 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 information into or export information from a ClearPass server is available from every top-level page in the ClearPass Policy Manager user interface. The Add, Import, and Export All options are displayed in the top-right corner of the configuration and administration pages:

![Add Import Export All]

Importing Information Into ClearPass

ClearPassPolicy Manager allows 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.

To import information into the current ClearPass server:

1. Click the Import link. The Import from file dialog opens.

   ![Figure 9 Import From File Dialog]

2. Click Browse.
3. Browse to the file you want to import.
   - Be sure to select an XML file that is in the correct format.

about the format and contents of XML files.

4. **Enter secret for the file (if any):** If you entered a secret key to encrypt the exported file, enter the same secret key to import the device back into this ClearPass server.

5. Click Import.

**Exporting Information From ClearPass**

ClearPassPolicy Manager allows you to export configuration and administration-related information from the current ClearPass server to an XML file. You can set this file to be password protected (see Table 1 for details).

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

To export information from the current ClearPass server:

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

   **Figure 10 Export to File Dialog**

   ![Export to File Dialog](image)

2. Specify the export parameters based on Table 1.
   
   Specify the **Export to file** parameters as described in Table 1:

   **Table 1: Export to File Dialog Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>To export the file with password protection, choose Yes.</td>
</tr>
<tr>
<td>Secret Key/ Verify Secret</td>
<td>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 Enter the secret key. Then reenter the secret key.</td>
</tr>
</tbody>
</table>

3. Click Export.
   
   An export dialog named for the selected ClearPass function opens:
4. Specify to open the zip file or save the XML file to your system.
5. Click OK to proceed.

**Export Considerations**

The XML file generated from an export operation has a specific layout that is unique for each function in the ClearPass user interface. If you import an XML file with an incorrect layout (usually because it's from the wrong function), it will be rejected. Aruba recommends that you note the message displayed when the XML operation is incorrect and what the issue is—typically either because it's from the wrong export file or because it was modified incorrectly before being imported.
This chapter describes the following topics:

- Viewing the List of Services
- Configuring Services Using Service Templates & Wizards
- Configuring Other Policy Manager Services
- Modifying and Managing Services

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

### 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. To view the list of services on the current ClearPass server, navigate to Configuration > Services to display the Services page:

**Figure 12  Services Page**

![Services Page](image)

Services included in square brackets "[]" indicate default services.

To view a service's details, select the service of interest. As shown in **Figure 13**, the Edit Services page opens to the Summary page, which provides the detailed information about the selected service's configuration.
For information about additional common service tasks, see also "Modifying and Managing Services."

**Configuring Services Using Service Templates & Wizards**

ClearPass Policy Manager Service templates provide a way to step through the service-creation process for the most common use cases, allowing you to easily create services and configure their specific components, such as role-mapping policies, enforcement policies, and associated network devices. Other service types can be configured manually, or using the service wizards.

**Using Templates to Create ClearPass Services**

You can use templates to create services for common use cases by defining baseline policies and required data:

1. Navigate to the Configuration > Service Templates & Wizards page. The Service Templates & Wizards page opens.
2. Select the desired service template. The configuration dialog for the selected service template opens, as shown in the following example:

**Figure 15  Auto Sign-On Service Template**

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.
List of Provided Service Templates

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
- Aruba Auto Sign-On Service Template
- Aruba VPN Access with Posture Checks Service Template
- Certificate/Two-Factor Authentication for ClearPass Application Login Service Template
- ClearPass Admin Access Service Template
- ClearPass Admin SSO Login (SAML SP Service) Service Template
- Cloud Identity/Social Media Authentication Service Template
- ClearPass Identity Provider (SAML IdP Service) Service Template
- Device MAC Authentication Service Template
- Eduroam Service Template
- Encrypted Wireless Access via 802.1X Public PEAP Method Service Template
- Guest Access Service Template
- Guest Access Web Login Service Template
- Guest Authentication with MAC Caching Service Template
- OAuth2 API User Access Service Template
- Onboard Service Template

Using Wizards to Create ClearPass Services

Although Policy Manager includes templates to define services for the most common use cases, you can manually configure services for any of the other supported service types using service Wizards, or by manually creating your services on the Configuration > Services > Add page.

For more information on wizards and the procedures to manually define these other service types, see Configuring Other Policy Manager Services.

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

ClearPass Policy Manager includes the following 802.1X service templates. All three of these 802.1X service templates are configured using identical parameters.

- 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).

Adding a Service to an 802.1X Template

To access the 802.1X Wired and Wireless service templates:

1. Navigate to Configuration > Service Templates & Wizards.
2. From the **Service Templates & Wizards** page, select the desired **802.1X Wired** or **Wireless** service template. The desired **802.1X Wired** or **Wireless** service template page opens to the **General** tab.

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

3. Specify a unique **Name Prefix** (applies only to the selected template) in the **General** tab.

4. Update the required fields in the **Authentication** and **Enforcement Details** sections.

5. Click **Add Service**. An entry for the new set of configuration is created under the **Services, Roles, Role Mapping, Enforcement Policies** and **Profiles** menus.

---

**NOTE**

Not all the Policy Manager service templates include the same sections as the 802.1X 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.

6. 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>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Select Prefix</strong></td>
<td>Select a prefix from the existing list of prefixes. This populates the preconfigured information in the <strong>Authentication</strong> and <strong>Enforcement Details</strong> sections. The <strong>Name Prefix</strong> field is not editable.</td>
</tr>
<tr>
<td><strong>Name Prefix</strong></td>
<td>Enter a prefix that is appended to services using this template. Use this to identify the services that use this template.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Select Authentication Source</strong></td>
<td>Select any available authentication source from the drop-down list. When you select an existing authentication source, the &quot;Create an Active Directory Authentication Source&quot; section is removed. The information required for the <strong>Authentication</strong> and <strong>Enforcement Details</strong> tabs is automatically populated.</td>
</tr>
<tr>
<td><strong>Create an Active Directory Authentication Source</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Active Directory Name</strong></td>
<td>To create a new Active Directory authentication source, enter the name of the Active Directory. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter a description that helps you to identify the characteristics of this template.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP port where the server is listening for a connection. This field is mandatory.</td>
</tr>
<tr>
<td>Identity</td>
<td>Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password. This field is mandatory.</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Enter the server Active Directory domain name. This field is mandatory.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the Distinguished Name (DN) of the node in your directory tree from which to start searching for records. This field is mandatory.</td>
</tr>
</tbody>
</table>

**Enforcement Details**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>The attributes defined in the Authentication Source are listed here. Configure an optional enforcement policy based on the following attributes:</th>
</tr>
</thead>
</table>
|                | Account Expires  
|                | Department  
|                | Email  
|                | Name  
|                | Phone  
|                | UserDN  
|                | Company  
|                | member of  

For example, you can configure an enforcement policy for a contractor specifying that "If Name equals <contractor_name>, then assign the [Contractor] Role."

<table>
<thead>
<tr>
<th>Attribute Value</th>
<th>Enter the active directory attribute value for the selected name in the Attribute Name field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Enter the standard RADIUS-IETF VLAN ID.</td>
</tr>
</tbody>
</table>

| Default VLAN/Role | You can specify a default VLAN or role for instances in which the VLAN or role is not specified.                                           |

**Wired Network Settings**

<table>
<thead>
<tr>
<th>Select Switch</th>
<th>Select any switch from the drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>When you select a switch from the drop-down list, ClearPass automatically populates the name of the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>When you select a switch from the drop-down list, ClearPass automatically populates the IP address of the device.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>When you select a switch from the drop-down list, ClearPass automatically populates the manufacturer of the wired controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>When you select a switch from the drop-down list, ClearPass automatically populates the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>When you select a switch from the drop-down list, ClearPass automatically populates enables RADIUS-initiated Change of Authorization (CoA) on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port 3799 when RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.</td>
</tr>
</tbody>
</table>

**Wireless Network Settings**

- **Wireless Controller Name** Enter the name of the wireless controller.
- **Controller IP Address** Enter the IP address of the wireless controller.
- **Vendor Name** Select the manufacturer of the wireless controller.
- **RADIUS Shared Secret** Enter the shared secret that is configured on the controller and 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.

**Posture Settings**

- **Enable Posture Checks** Select the check box to perform health checks post-authentication. This enables the Host Operating System and Quarantine Message fields.
- **Host Operating System** Select the operating system: Windows, Linux, or macOS.
- **Quarantine Message** 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.

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 were not created using the service template.

**Aruba Auto Sign-On Service Template**

The Aruba 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.

To access the Auto Sign-On Service service template:

1. Navigate to Configuration > Service Templates & Wizards.
2. From the **Service Templates & Wizards** page, select **Aruba Auto Sign-On Service**. The **Service Templates - Auto Sign-On Service** page opens to the **General** tab.

**Figure 17 Auto Sign-On Service Template**

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

**Table 1: Aruba Auto Sign-On Service Template Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use this service template.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Select Authentication Source</td>
<td>Select an authentication source from the list. The information provided in the <strong>Authentication, Enforcement Details</strong>, and <strong>SP details</strong> tabs are auto-populated.</td>
</tr>
<tr>
<td>Active Directory Name</td>
<td>Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that helps you to identify the characteristics of this template. This field is mandatory.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP port where the server is listening for a connection. This value defaults to <strong>389</strong>. This field is mandatory.</td>
</tr>
<tr>
<td>Identity</td>
<td>Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password. This field is mandatory.</td>
</tr>
<tr>
<td>NETBios</td>
<td>Enter the server Active Directory domain name. This field is mandatory.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the Base DN of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Enforcement Details</strong></td>
<td></td>
</tr>
<tr>
<td>Create new Enforcement Policy</td>
<td>Configure an optional enforcement policy based on the following attributes:</td>
</tr>
<tr>
<td></td>
<td>• Department</td>
</tr>
<tr>
<td></td>
<td>• Email</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>UserDN</td>
<td></td>
</tr>
<tr>
<td>company</td>
<td></td>
</tr>
<tr>
<td>memberOf</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
</tbody>
</table>

**SP Details**

<table>
<thead>
<tr>
<th>SP URL</th>
<th>Enter the Service Provider (SP) URL.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Enter attribute names and assign values to those names. These name/value pairs are included in SAML responses.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td></td>
</tr>
</tbody>
</table>

**Aruba VPN Access with Posture Checks Service Template**

The **Aruba VPN Access with Posture Checks** service template authenticates Aruba VPN clients connecting remotely to corporate networks. Differentiated access is based on the result of posture checks.

This template does the following:

- 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).

To access the **Aruba VPN Access with Posture Checks** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select Aruba VPN Access with Posture Checks. The **Service Templates - Aruba VPN Access with Posture Checks** page opens to the **General** tab.
**Figure 18  Aruba VPN Access with Posture Checks Service Template**

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

**Table 1: Aruba VPN Access with Posture Checks Service Template Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>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.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Select Authentication Source</td>
<td>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.</td>
</tr>
<tr>
<td>Active Directory Name</td>
<td>Enter the Active Directory name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that helps you to identify the characteristics of this template.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the host name or the IP address of the Active Directory server.</td>
</tr>
<tr>
<td>Identity</td>
<td>Enter the Distinguished Name (DN) of the administrator account.</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Enter the server Active Directory domain name.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the Distinguished Name (DN) of the node in your directory tree from which to start searching for records.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP port where the server is listening for a connection.</td>
</tr>
<tr>
<td><strong>Aruba Wireless Controller for VPN Access</strong></td>
<td></td>
</tr>
<tr>
<td>Select Wireless Controller</td>
<td>Select a wireless controller from the drop-down list.</td>
</tr>
<tr>
<td>Wireless controller name</td>
<td>Enter the name given to the wireless controller.</td>
</tr>
</tbody>
</table>
## Parameter Action/Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller IP Address</td>
<td>Enter the wireless controller’s IP address.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Select the manufacturer of the wireless controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select this option to enable RADIUS initiated CoA on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port <strong>3799</strong> if RADIUS CoA is enabled. <strong>NOTE:</strong> Change this value only if you defined a custom port on the network device.</td>
</tr>
</tbody>
</table>

### Aruba User Roles for different access privileges - Create a new Enforcement Policy

<table>
<thead>
<tr>
<th>Role</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Role (before posture checks)</td>
<td>Enter the initial role of the client before posture checks are performed.</td>
</tr>
<tr>
<td>Quarantined Role (failed posture checks)</td>
<td>Enter the role of clients that fail posture checks.</td>
</tr>
<tr>
<td>Healthy Role (passed posture checks)</td>
<td>Enter the role of the client after a posture check is passed and deemed healthy.</td>
</tr>
</tbody>
</table>

## 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.

### Adding a Service to the Template

To access the **Certificate/Two-Factor Authentication Service** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select **Certificate/Two-Factor Authentication Service**. The **Service Templates - Certificate/Two-Factor Authentication Service** page opens to the **General** tab.

**Figure 19** Certificate/Two-Factor Authentication Service Template
Specify the **Certificate/Two-Factor Authentication for ClearPass Application Login** service template parameters as described in the following table:

### Table 1: ClearPass Certificate/Two-Factor Authentication Service Template Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>1. Select a prefix from the existing list of prefixes. This field populates the pre-configured information in the <strong>Authentication, SP details,</strong> and <strong>Enforcement Details</strong> sections. The Name Prefix field is not editable.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>2. Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Service Rule</strong></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>3. Select the application for which SAML-based Single Sign-On (SSO) should be enabled from the following options: <strong>Policy Manager, Guest, Insight,</strong> and <strong>Onboard.</strong></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Select Authentication Source</td>
<td>4. Select an authentication source from the list. The information provided in the <strong>Authentication, Enforcement Details,</strong> and <strong>SP details</strong> tabs are auto-populated.</td>
</tr>
<tr>
<td>Active Directory Name</td>
<td>5. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>6. Enter a description that helps you to identify the characteristics of this template. This field is mandatory.</td>
</tr>
<tr>
<td>Server</td>
<td>7. Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>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.</td>
</tr>
<tr>
<td>Identity</td>
<td>9. Enter the DN of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>10. Enter the account password. This field is mandatory.</td>
</tr>
<tr>
<td>NETBIOS</td>
<td>11. Enter the server Active Directory domain name. This field is mandatory.</td>
</tr>
<tr>
<td>Base DN</td>
<td>12. Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td><strong>IdP Details</strong></td>
<td></td>
</tr>
<tr>
<td>Page Name</td>
<td>13. Select the <strong>Web Login</strong> pages from the drop-down list. For more information, see the next section, <strong>Creating a New Web Login Page.</strong></td>
</tr>
<tr>
<td><strong>Enforcement Details</strong></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Certificate Attribute - Super Admin Condition</td>
<td>14. Select the certificate attribute from the drop-down list. 15. Enter the value in the <strong>Super Admin Condition</strong> field that matches the <strong>Certificate Attribute</strong> value to provide the super administrator access.</td>
</tr>
<tr>
<td>Certificate Attribute - Read Only Admin Condition</td>
<td>16. Select the certificate attribute from the drop-down list. 17. Enter the value in the <strong>Read Only Admin Condition</strong> field that matches the <strong>Certificate Attribute</strong> value to provide the Read-Only administrator access.</td>
</tr>
<tr>
<td>Certificate Attribute - Help Desk Admin Condition</td>
<td>18. Select the certificate attribute from the drop-down list. 19. Enter the value in the <strong>Help Desk Admin Condition</strong> field that matches the <strong>Certificate Attribute</strong> value to provide the help desk administrator access.</td>
</tr>
</tbody>
</table>

**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.

To access the **ClearPass Admin Access** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select **ClearPass Admin Access**. The **Service Templates - ClearPass Admin Access** page opens to the **General** tab.

**Figure 20  ClearPass Admin Access Service Template**
Specify the **ClearPass Admin Access** service template parameters as described in the following table:

**Table 1: ClearPass Admin Access Service Template Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>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.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Authentication: Create an Active Directory Authentication Source</strong></td>
<td></td>
</tr>
<tr>
<td>Select Authentication Source</td>
<td>Select an authentication source from the list. The information updated in the Authentication and Role Mapping tabs are auto-populated.</td>
</tr>
<tr>
<td>Active Directory Name</td>
<td>Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that helps to identify the characteristics of this template. This field is mandatory.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP port where the server is listening for a connection. This field is mandatory.</td>
</tr>
<tr>
<td>Identity</td>
<td>Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password. This field is mandatory.</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Enter the server Active Directory domain name. This field is mandatory.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the DN of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Role Mapping</strong></td>
<td></td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Select the Active Directory attribute.</td>
</tr>
<tr>
<td>Super Admin Condition</td>
<td>Defines the various privilege levels.</td>
</tr>
<tr>
<td>Read Only Admin Condition</td>
<td></td>
</tr>
<tr>
<td>Help Desk Condition</td>
<td></td>
</tr>
</tbody>
</table>

**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.

To access the **ClearPass Admin SSO Login** service template:
1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select **ClearPass Admin SSO Login**.
The **Service Templates - ClearPass Admin SSO Login** page opens to the **General** tab.

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>Select a prefix from the existing list of prefixes. This populates the preconfigured information in the <strong>Service Rule</strong> tab. The <strong>Name Prefix</strong> field is not editable.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Service Rule</strong></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Select the application that single-sign-on-authenticated administrative users can access.</td>
</tr>
</tbody>
</table>

**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.

To access the **ClearPass Identity Provider (SAML IdP Service)** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select **ClearPass Identity Provider (SAML IdP Service)**. The **Service Templates - ClearPass Identity Provider (SAML IdP Service)** page opens to the **General** tab.

**Figure 22  ClearPass Identity Provider (SAML IdP Service)**
Specify the ClearPass Identity Provider (SAML IdP Service) service template parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>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.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Select Authentication Source</td>
<td>Select an authentication source from the list, the information updated in the Authentication and SP Details tabs are auto-populated.</td>
</tr>
<tr>
<td>Active Directory Name</td>
<td>Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that helps you to identify the characteristics of this template. This field is mandatory.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the hostname or the IP address of the Active Directory server. This field is mandatory.</td>
</tr>
<tr>
<td>Identity</td>
<td>Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Enter the Active Directory server domain name. This field is mandatory.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the Distinguished Name (DN) of the administrator account. This field is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the account password. This field is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP port where the server is listening for a connection. This field is mandatory.</td>
</tr>
<tr>
<td><strong>SP Details</strong></td>
<td></td>
</tr>
<tr>
<td>SP URL</td>
<td>Enter the Service Provider (SP) URL.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Enter the name of the attributes and assign values to those names. These name/value pairs are included in SAML responses.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td></td>
</tr>
</tbody>
</table>

**Cloud Identity/Social Media Authentication Service Template**

You can use this service template to authenticate guest users who log in to the network via captive portal with their social media accounts. Guests must reauthenticate after their session ends. You can limit the network access for guest devices that do not have a user directly associated with them for a specific duration in days or by a bandwidth limit.

To access the Cloud Identity/Social Media Authentication service template:

1. Navigate to Configuration > Service Templates & Wizards.
2. From the Service Templates & Wizards page, select Cloud Identity/Social Media Authentication.
The **Service Templates - Cloud Identity/Social Media Authentication** page opens to the **General** tab.

**Figure 23  Cloud Identity/Social Media Authentication Service Template**

3. Specify the parameters in the **Service Templates - Cloud Identity/Social Media Authentication** service template as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use this service templates.</td>
</tr>
<tr>
<td><strong>Wireless Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Select Wireless Controller</td>
<td>From the drop-down, select the IP address of the wireless controller.</td>
</tr>
<tr>
<td>Wireless Controller Name</td>
<td>When you select the Wireless Controller, ClearPass automatically populates this field.</td>
</tr>
<tr>
<td>Controller IP Address</td>
<td>When you select the Wireless Controller, ClearPass automatically populates this field.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>When you select the Wireless Controller, ClearPass automatically populates this field.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>When you select the Wireless Controller, ClearPass automatically populates the shared secret that is configured on the controller and in Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>When you select the wireless controller, ClearPass automatically enables RADIUS-initiated CoA (Change of Authorization) on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port 3799 when RADIUS CoA is enabled.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Change this value only if you defined a custom port on the network device.</td>
<td></td>
</tr>
<tr>
<td><strong>Guest Access Restrictions</strong></td>
<td></td>
</tr>
<tr>
<td>Social Login Provider</td>
<td>Select the social media network provider(s): Google, Facebook, LinkedIn, and Twitter.</td>
</tr>
<tr>
<td>Days allowed for access</td>
<td>Deselect the days of the week that the guest users are not allowed network access.  By default, all seven days of the week are enabled for guest access.</td>
</tr>
<tr>
<td>Maximum bandwidth allowed per user</td>
<td>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).</td>
</tr>
</tbody>
</table>
4. Click **Add Service**.
   You return to the Service page where the new service created by the service template has been added and enabled. A message like the following is also displayed:
   - *Added 6 Enforcement Profile(s)*
   - *Added 1 Enforcement Policies*
   - *Added 1 service(s)*

**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.

To access the **Device MAC Authentication** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select **Device MAC Authentication**.
   The **Service Templates - Device MAC Authentication** page opens to the **General** tab.

**Figure 24 Device MAC Authentication Service Template**

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

**Table 1: Device MAC Authentication Template Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>Select a prefix from the existing list of prefixes. This populates the preconfigured information in the <strong>Authentication</strong> and <strong>SP Details</strong> sections. The <strong>Name Prefix</strong> field is not editable.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Select Device</td>
<td>Select a preconfigured device from the drop-down list. To create a new device, leave this field blank and enter the remaining fields.</td>
</tr>
<tr>
<td>Device Name</td>
<td>The name of the device is populated automatically based on the device selected from the <strong>Select Device</strong> field. If you create a new device, enter the name of the device.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device is populated automatically based on the device selected from the <strong>Select Device</strong> field. If you create a new device, enter the name of the device.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>The name of the manufacturer of the device is populated automatically based on the device selected from the <strong>Select Device</strong> field. If you create a new device, enter the name of the manufacturer of the device.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and in Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select to enable RADIUS initiated Change of Authorization (CoA) on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port <strong>3799</strong> if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.</td>
</tr>
</tbody>
</table>

**Device Access Restrictions**

<table>
<thead>
<tr>
<th>Days allowed for access</th>
<th>Select the days on which network access is allowed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum bandwidth allowed per device</td>
<td>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 <strong>0</strong> (zero), the default, means no limit is set.</td>
</tr>
</tbody>
</table>

**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 a local campus or other campuses that are part of the eduroam federation.

To access the **Eduroam** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select Eduroam.
   
   The **Service Templates - Eduroam** page opens to the **General** tab.
**Figure 25** *Eduroam Service Template*

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

<table>
<thead>
<tr>
<th>Table 1: <em>Eduroam Service Template Parameters</em></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td>Select Prefix</td>
</tr>
<tr>
<td>Name Prefix</td>
</tr>
<tr>
<td><strong>Service Rule</strong></td>
</tr>
<tr>
<td>Enter domain details</td>
</tr>
<tr>
<td>Select Vendor</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td>Select Active Directory</td>
</tr>
<tr>
<td>Active Directory Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>Identity</td>
</tr>
<tr>
<td>NetBIOS</td>
</tr>
<tr>
<td>Base DN</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Port</td>
</tr>
</tbody>
</table>

**Wireless Network Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select wireless controller</td>
<td>Select a wireless controller from the drop-down list.</td>
</tr>
<tr>
<td>Wireless controller name</td>
<td>Enter the name given to the wireless controller.</td>
</tr>
<tr>
<td>Controller IP Address</td>
<td>Enter the IP address of the wireless controller.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Select the manufacturer of the wireless controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select to enable RADIUS initiated CoA on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.</td>
</tr>
</tbody>
</table>

**Federation Level RADIUS Server (FLR)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Enter the host name of the federation RADIUS server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the federation RADIUS server.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Select the manufacturer of the wireless controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select to enable RADIUS initiated CoA on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port 3799 if RADIUS CoA is enabled. Change this value only if you defined a custom port on the network device.</td>
</tr>
<tr>
<td>RADIUS Authentication Port</td>
<td>Enter the port number for the RADIUS Authentication Port.</td>
</tr>
<tr>
<td>RADIUS Accounting Port</td>
<td>Enter the port number for the RADIUS Accounting Port.</td>
</tr>
</tbody>
</table>

**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. It configures an **EAP PEAP Public** type authentication method and creates an enforcement policy for network access.

To access the **Encrypted Wireless Access via 802.1X Public PEAP Method** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select **Encrypted Wireless Access via 802.1X Public PEAP Method**.

The **Service Templates - Encrypted Wireless Access via 802.1X Public PEAP Method** page opens to the **General** tab.
Specify the parameters used in the **Encrypted Wireless Access via 802.1X Public PEAP method** service template as described in the following table:

**Table 1: Encrypted Wireless Access via 802.1X Public PEAP Method Service Template Parameters**

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

**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.
To access the **Guest Access** service template:

1. Navigate to **Configuration > Service Templates & Wizards**.
2. From the **Service Templates & Wizards** page, select **Guest Access**. The **Service Templates - Guest Access** page opens to the **General** tab.

**Figure 27 Guest Access Service Template**

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

**Table 1: Guest Access Service Template Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>Select any one prefix from the existing list of prefixes. This populates the pre-configured information in the <strong>Wireless Network Settings</strong> and <strong>Guest Access Restrictions</strong> sections. The <strong>Name Prefix</strong> field is not editable.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Wireless Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Wireless SSID for Guest access</td>
<td>Enter the SSID value here.</td>
</tr>
<tr>
<td>Select wireless controller</td>
<td>Select the wireless controller from the drop-down list if you already configured.</td>
</tr>
<tr>
<td>Wireless controller name</td>
<td>Enter the name of the wireless controller.</td>
</tr>
<tr>
<td>Controller IP Address</td>
<td>Enter the wireless controller’s IP address.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Select the manufacturer of the wireless controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select to enable RADIUS initiated CoA on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port <strong>3799</strong> if RADIUS CoA is enabled. <strong>NOTE:</strong> Change this value only if you defined a custom port on the network device.</td>
</tr>
<tr>
<td>Posture Settings</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Posture Checks</td>
<td>Select the check box to perform health checks post authentication. This enables the Host Operating System and Quarantine Message fields.</td>
</tr>
<tr>
<td>Host Operating System</td>
<td>Select the operating system: Windows, Linux, or macOS.</td>
</tr>
<tr>
<td>Quarantine Message</td>
<td>Specify the quarantine message that will appear on the client.</td>
</tr>
<tr>
<td>Initial Role/VLAN</td>
<td>Enter the initial role of the client before posture checks are performed.</td>
</tr>
<tr>
<td>Quarantine Role/VLAN</td>
<td>Enter the role of clients that fail posture checks.</td>
</tr>
</tbody>
</table>

### Guest Access Restrictions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days allowed for access</td>
<td>Select the days of the week that guest users are allowed network access.</td>
</tr>
<tr>
<td>Maximum bandwidth allowed per user</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Guest Access Web Login Service Template**

This service performs an authentication check for guests logging in using the Guest Portal. To use this service:

1. First create a Guest Web Login page that sets the Pre-Auth Check option to AppAuth - Check using Aruba Application Authentication (for details, see Authentication in Guest Web Login Using OnGuard Native Dissolvable Agent).
3. Select Guest Access - Web Login. The Guest Access Web Login service template opens:

![](image.png)

**Figure 28 Guest Access-Web Login Service Template**

4. Specify the Guest Access - Web Login service template parameters as described in the following table:
Table 1: Guest Web Login Service Template Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>From the drop-down, select Guest Web Login. This prefix is appended to services</td>
</tr>
<tr>
<td></td>
<td>that use this template.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>The prefix you selected is automatically populated into this field.</td>
</tr>
<tr>
<td><strong>Service Rule</strong></td>
<td></td>
</tr>
<tr>
<td>Page name</td>
<td>From the Page name drop-down, select the name of the appropriate Guest Web Login</td>
</tr>
<tr>
<td></td>
<td>page.</td>
</tr>
<tr>
<td>Add New Guest Web Login page</td>
<td>To launch a new Web session to add a new Guest Web Login page, click this link.</td>
</tr>
<tr>
<td><strong>Guest Access Restrictions</strong></td>
<td></td>
</tr>
<tr>
<td>Enable days allowed for guest access</td>
<td>Select the days of the week that guest users are allowed network access.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> All seven days of the week are enabled by default.</td>
</tr>
</tbody>
</table>

5. Click **Add Service**.

**Guest Authentication with MAC Caching Service Template**

This template is designed for authenticating guest accounts based on the cached MAC addresses used during authentication. Users first log in via the Captive Portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the Captive Portal.

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. Network access can be restricted based on day of the week, bandwidth limit, or number of unique devices used by the user. The cache lifetime of the MAC address can vary according to the user’s role (Guest, Employee, or Contractor) and after that the user will have to reauthenticate via the Captive Portal. Optionally, posture checks can be enabled to validate the client device for antivirus or firewall status. These results will determine the enforcement for the device.

To configure the **Guest Authentication with MAC Caching** service template:

1. Navigate to the **Configuration > Service Templates & Wizards** page. The Service Templates & Wizards page opens.
2. Scroll down to and select the **Guest Authentication with MAC Caching** service template:
3. Specify the **Guest Authentication with MAC Caching** service template parameters as described in the following table:

### Table 1: Guest Authentication with MAC Caching Service Template Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>Select a prefix from the existing list of prefixes. This populates the preconfigured information in the Wireless Network Settings, MAC Caching Settings, and Access restrictions tabs. The Name Prefix field is not editable.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Wireless Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Wireless SSID</td>
<td>Enter the SSID name of your network.</td>
</tr>
<tr>
<td>Select Wireless Controller</td>
<td>Select the wireless controller from the drop-down list if you already configured the controller for ClearPass.</td>
</tr>
<tr>
<td>Wireless Controller Name</td>
<td>Enter the name of the wireless controller.</td>
</tr>
<tr>
<td>Controller IP Address</td>
<td>Enter the wireless controller’s IP address.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Select the manufacturer of the wireless controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and in Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select this check box to enable RADIUS initiated CoA (Change of Authorization) on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port <strong>3799</strong> if RADIUS CoA is enabled. <strong>NOTE:</strong> Change this value only if you defined a custom port on the network device.</td>
</tr>
<tr>
<td><strong>MAC Caching Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 **Enable Posture Checks** 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 macOS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Quarantine Message                | Specify the quarantine message that will appear on the client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Initial Role/VLAN                 | Enter the initial role of the client before posture checks are performed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Quarantine Role/VLAN              | Enter the role of clients that fail posture checks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Access Restrictions               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 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.  
  **NOTE:** At least one of **Employee**, **Guest**, or **Contractor Access** must be specified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Captive Portal Access             | Used for unauthenticated users and after the MAC caching has expired.  
  - If you selected **Aruba Role Enforcement** as the **Enforcement Type**, enter the **Aruba Role Name**.  
  - If you selected **VLAN Enforcement** as the **Enforcement Type**, enter the **VLAN ID**.  
  - If you selected **Filter ID-Based Enforcement** as the **Enforcement Type**, enter the **Filter ID**.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
### Parameter | Action/Description
--- | ---
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**
- If you selected Aruba Role Enforcement as the Enforcement Type, enter the Aruba Role Name.
- If you selected VLAN Enforcement as the Enforcement Type, enter the VLAN ID.
- If you selected Filter ID-Based Enforcement as the Enforcement Type, enter the Filter ID.

**Guest Access**
- If you selected Aruba Role Enforcement as the Enforcement Type, enter the Aruba Role Name.
- If you selected VLAN Enforcement as the Enforcement Type, enter the VLAN ID.
- If you selected Filter ID-Based Enforcement as the Enforcement Type, enter the Filter ID.

**Contractor Access**
- If you selected Aruba Role Enforcement as the Enforcement Type, enter the Aruba Role Name.
- If you selected VLAN Enforcement as the Enforcement Type, enter the VLAN ID.
- If you selected Filter ID-Based Enforcement as the Enforcement Type, enter the Filter ID.

---

## 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.

To access the Guest Social Media Authentication service template:

1. Navigate to Configuration > Service Templates & Wizards.
2. From the Service Templates & Wizards page, select Guest Social Media Authentication. The Service Templates - Guest Social Media Authentication page opens to the General tab.
**Figure 30  Guest Social Media Authentication Service Template**

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

**Table 1: Guest Social Media Service Template Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>Select a prefix from the existing list of prefixes.</td>
</tr>
<tr>
<td></td>
<td>This populates the preconfigured information in the Wireless Network Settings,</td>
</tr>
<tr>
<td></td>
<td>MAC Caching Settings, and Guest Access restrictions tabs. The Name Prefix</td>
</tr>
<tr>
<td></td>
<td>field is not editable.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template.</td>
</tr>
<tr>
<td></td>
<td>Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Wireless Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Wireless Controller Name</td>
<td>Enter the name of the wireless controller.</td>
</tr>
<tr>
<td>Controller IP Address</td>
<td>Enter the wireless controller's IP address.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Select the manufacturer of the wireless controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and inside</td>
</tr>
<tr>
<td></td>
<td>Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select to enable RADIUS initiated CoA (Change of Authorization) on the</td>
</tr>
<tr>
<td></td>
<td>network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port <strong>3799</strong> if RADIUS CoA is enabled.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Change this value only if you defined a custom port on the network</td>
</tr>
<tr>
<td></td>
<td>device.</td>
</tr>
<tr>
<td><strong>Guest Access Restrictions</strong></td>
<td></td>
</tr>
<tr>
<td>Social Login Provider</td>
<td>Select the social media network options: Google, Facebook, LinkedIn, and</td>
</tr>
<tr>
<td></td>
<td>Twitter.</td>
</tr>
<tr>
<td>Days allowed for access</td>
<td>Select the days of the week that the guest users are allowed network access.</td>
</tr>
<tr>
<td></td>
<td>By default, all seven days of the week are enabled.</td>
</tr>
<tr>
<td>Maximum bandwidth allowed</td>
<td>Specify the maximum amount of data in Megabytes a user is allowed per day.</td>
</tr>
<tr>
<td>per user</td>
<td>A value of 0 (zero) means no limit is set (the default).</td>
</tr>
</tbody>
</table>
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.

To access the OAuth2 API User Access service template:
1. Navigate to Configuration > Service Templates & Wizards.

Figure 31 OAuth2 API User Access Service Template

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that is appended to services using this template. You can use this prefix to identify the services that use templates.</td>
</tr>
</tbody>
</table>

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.

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

To access the Onboard service template:
1. Navigate to Configuration > Service Templates & Wizards.
2. From the Service Templates & Wizards page, select Onboard. The Service Templates - Onboard page opens to the General tab.
Figure 32  Onboard Pre-Authorization Service Template

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

**Table 1: Onboard Authorization Service Template Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Select Prefix</td>
<td>Select a prefix from the existing list of prefixes or enter the name of a new prefix. This populates the preconfigured information in the <strong>Wireless Network Settings</strong>, <strong>Device Access Restrictions</strong>, and <strong>Provisioning Wireless Network Settings</strong> sections. The <strong>Name Prefix</strong> field is not editable.</td>
</tr>
<tr>
<td>Name Prefix</td>
<td>Enter a prefix that you want to append to services using this template. Use this to identify services that use templates.</td>
</tr>
<tr>
<td><strong>Wireless Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Wireless Controller Name</td>
<td>Enter the name of the wireless controller.</td>
</tr>
<tr>
<td>Controller IP Address</td>
<td>Enter the wireless controller’s IP address.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Select the manufacturer of the wireless controller.</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the shared secret that is configured on the controller and inside Policy Manager to send and receive RADIUS requests.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select to enable RADIUS initiated CoA (Change of Authorization) on the network device.</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>Specifies the default port <strong>3799</strong> if RADIUS CoA is enabled. <strong>NOTE:</strong> Change this value only if you defined a custom port on the network device.</td>
</tr>
<tr>
<td><strong>Device Access Restrictions</strong></td>
<td></td>
</tr>
<tr>
<td>Days allowed for access</td>
<td>Select the days of the week that guest users are allowed network access.</td>
</tr>
<tr>
<td><strong>Provisioning Wireless Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Wireless SSID for Onboard Provisioning</td>
<td>Enter the SSID of your network.</td>
</tr>
<tr>
<td>Add New Onboard Network Settings</td>
<td>Click the <strong>Add New Onboard Network Settings</strong> link to launch the Web UI to modify the Onboard network settings.</td>
</tr>
</tbody>
</table>
Configuring Other Policy Manager Services

Although Policy Manager provides service templates for the most common use cases, you can manually configure services for all of the other supported service types. These Policy Manager services can be defined using the service wizards by selecting the full Wizard link on the Configuration > Service Templates & Wizards page, or by navigating to Configuration > Services and clicking the Add option.

For a list of services that can be defined using templates, see Configuring Service Templates

Click any of the links below for details on defining that service type:

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

Aruba 802.1X Wireless Service

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

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.

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.

To create a RADIUS Enforcement (Generic) service:

1. Navigate to Configuration > Services, then click the Add link. The Add Services dialog opens.
2. From the **Type** drop-down, select **802.1X Wireless**. The **802.1X Wireless** service configuration dialog opens:

**Figure 33  Aruba 802.1X Wireless Service > Service Dialog**

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

**Table 1: Add Aruba 802.1X Wireless Service > Service Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select a service from the drop-down list that defines what type of service can be</td>
</tr>
<tr>
<td></td>
<td>configured.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td><strong>Monitor Mode</strong></td>
<td>Select this check box to monitor network access activity without enforcement.</td>
</tr>
<tr>
<td><strong>More Options</strong></td>
<td>Check these boxes to access the additional configuration tabs:</td>
</tr>
<tr>
<td></td>
<td>- Authorization: See <a href="#">Authorization Configuration on page 62</a></td>
</tr>
<tr>
<td></td>
<td>- Posture Compliance: See <a href="#">Posture Configuration</a></td>
</tr>
<tr>
<td></td>
<td>- Audit End-hosts: See <a href="#">Audit Configuration on page 66</a></td>
</tr>
<tr>
<td></td>
<td>- Profile Endpoints: See <a href="#">Profile Endpoints Configuration on page 67</a></td>
</tr>
<tr>
<td></td>
<td>- Accounting Proxy: See <a href="#">Accounting Proxy Configuration on page 68</a></td>
</tr>
<tr>
<td><strong>Service Rule</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Matches</strong></td>
<td>Select the match condition for this service:</td>
</tr>
<tr>
<td></td>
<td>- Matches ANY</td>
</tr>
<tr>
<td></td>
<td>- Matches ALL of the following conditions</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select <strong>Click to add</strong> to select the service rule type.</td>
</tr>
</tbody>
</table>
**Parameter** | **Action/Description**
--- | ---
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.
Value | Enter the value or select the value from the drop-down list. The value list depends on the **Type** and **Operator** selected.

4. Click a service rule to modify its options.

**Authentication Configuration**

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

**Figure 34 Add Aruba 802.1X Wireless Service > Authentication Dialog**

1. Specify the **Authentication** tab parameters as described in the following table:
Table 2: Add Aruba 802.1X Wireless Service > Authentication Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Authentication Methods   | Select authentication methods using the **Select to Add** field. The authentication methods available 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 Modifying Authentication Methods on page 161  
  - Adding and Configuring Authentication Sources on page 184.                                                                                                                                                                                                                                                         |
| 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:  
  - AD_avenda313 [Active Directory]  
  - Admin User Repository  
  - Blacklist User Repository  
  - Endpoints Repository  
  - Guest Device Repository  
  - Guest User Repository  
  - http_3702  
  - HTTP_Auth_Source  
  - 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 username (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.                                                                                                                                                                                                 |
| Service Certificate      | Select the Service Certificate.                                                                                                                                                                                                                                                                                                                      |

**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 35** *Add Aruba 802.1X Wireless Service > Authorization Dialog*

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Source</td>
<td>Displays the authorization sources from which role mapping attributes are fetched for each authentication source.</td>
</tr>
<tr>
<td>Attributes Fetched From</td>
<td>Displays the source of attributes.</td>
</tr>
</tbody>
</table>
| 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* |
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 36  Add Aruba 802.1X Wireless Service > Roles Dialog**

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

**Table 3: Add Aruba 802.1X Wireless Service > Roles Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Mapping Policy</td>
<td>Select a role mapping policy from the drop-down list. Policy Manager ships a number of preconfigured roles. <strong>NOTE:</strong> A service can be configured without a role-mapping policy, but only one role-mapping policy can be configured for each service.</td>
</tr>
<tr>
<td>Role Mapping Policy Details</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information about the selected role-mapping policy.</td>
</tr>
<tr>
<td>Default Role</td>
<td>Specify the role to which Policy Manager defaults when the role-mapping policy does not produce a match.</td>
</tr>
<tr>
<td>Rules Evaluation Algorithm</td>
<td>Shows the first matched rule.</td>
</tr>
</tbody>
</table>

For information on configuring role-mapping policies, see [Configuring a Role and Role-Mapping Policy on page 243](#).

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

**NOTE**

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 37  Add Aruba 802.1X Wireless Service > Posture Dialog

2. Specify the Wireless Service Posture parameters as described in Table 4:

Table 4: Add Aruba 802.1X Wireless Service > Posture Parameters

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

For more information on configuring posture policies, see Configuring Posture Policy Agents and Hosts on page 253.

**Enforcement Configuration**

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

Figure 38  Aruba 802.1X Wireless Service > Enforcement Dialog

1. Specify the Enforcement parameters as described in the following table:
Table 5: *Aruba 802.1X Wireless Service > Enforcement Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Cached Results</td>
<td>Select this check box to use cached roles and posture attributes from previous sessions.</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td>Select the preconfigured enforcement policy from the drop-down list. This is mandatory. If you do not have any preconfigured enforcement policies, click <em>Add New Enforcement Policy</em> to create a new enforcement policy.</td>
</tr>
</tbody>
</table>

**Enforcement Policy Details**

<table>
<thead>
<tr>
<th>Description</th>
<th>Displays additional information about the selected enforcement policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Profile</td>
<td>Displays a default profile applied by ClearPass Policy Manager.</td>
</tr>
<tr>
<td>Rules Evaluation Algorithm</td>
<td>Shows the first matched rule.</td>
</tr>
</tbody>
</table>

For related information, see [Configuring Enforcement Policies](#).

**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 39 Add Aruba 8021X Wireless Service > Audit Dialog**

2. Specify the Audit End-Hosts parameters as described in the following table:
**Table 6: Add Aruba 802.1X Wireless Service > Audit End-Hosts Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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 40 Add Aruba 802.1X Wireless Service > Profile Endpoints Dialog**
1. Specify the **Profile Endpoints** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Classification</td>
<td>Select one or more endpoint classification items from the drop-down list.</td>
</tr>
</tbody>
</table>
| 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:

![Add Accounting Proxy Dialog](image)

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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 |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Select the name of the RADIUS attribute from the drop-down list.</td>
</tr>
<tr>
<td>Value</td>
<td>Select the value from the Value drop-down list. The values displayed here depend on the RADIUS attribute Type selected.</td>
</tr>
</tbody>
</table>

**Summary Information**

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

**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 59.

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

**Figure 42  Add 802.1X Wired Service Dialog**

**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 69.

The following figure displays the 802.1X Wired—Identity Only Service dialog:
Figure 43 802.1X Wired—Identity Only 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

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.

To create a Cisco Web Authentication Proxy service:

1. Navigate to Configuration > Services, then select the Add link. The Add Services page opens.
2. From the Type drop down, select Cisco Web Authentication Proxy. The Cisco Web Authentication Proxy service configuration dialog opens:
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](#).

### 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**

![MAC Authentication Service Configuration Dialog](image)

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 59](#).

**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**

![RADIUS Authorization Service Configuration Dialog](image)

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 73](#) for more information.
RADIUS Enforcement (Generic) Service

Configure the RADIUS Enforcement (Generic) service for any kind of RADIUS request. 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). For related information, see Configuring Enforcement Policies.

Service Configuration

To create a RADIUS Enforcement (Generic) service:

1. Navigate to Configuration > Services, then click the Add link. The Add Services dialog opens.
2. From the Type drop-down, select RADIUS Enforcement (Generic). The RADIUS Enforcement (Generic) service configuration dialog opens:

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

3. Specify the Service tab parameters as described in the following table.

   **Table 1: Aruba RADIUS Enforcement (Generic) Service > Service Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select a service from the drop-down list that defines what type of service can be configured.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Select this check box to monitor network access activity without enforcement.</td>
</tr>
<tr>
<td>More Options</td>
<td>Check these boxes to access the additional configuration tabs:</td>
</tr>
<tr>
<td></td>
<td>■ Authorization</td>
</tr>
<tr>
<td></td>
<td>■ Posture Compliance</td>
</tr>
<tr>
<td></td>
<td>■ Audit End-hosts</td>
</tr>
<tr>
<td></td>
<td>■ Profile Endpoints</td>
</tr>
<tr>
<td></td>
<td>■ Accounting Proxy</td>
</tr>
</tbody>
</table>
### Table 2: Aruba RADIUS Enforcement (Generic) Service > Service Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select a service from the drop-down list that defines what type of service can be configured.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Select this check box to monitor network access activity without enforcement.</td>
</tr>
<tr>
<td>More Options</td>
<td>Check these boxes to access the additional configuration tabs: Authorization, Posture Compliance, Audit End-hosts, Profile Endpoints, Accounting Proxy</td>
</tr>
</tbody>
</table>

### Service Rule

<table>
<thead>
<tr>
<th>Matches</th>
<th>Select the match condition for this service: Matches ANY, Matches ALL of the following conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>Click to add</strong> to select the service rule type.</td>
</tr>
<tr>
<td>Name</td>
<td>Select the name of the service rule from the drop-down list.</td>
</tr>
<tr>
<td>Operator</td>
<td>Select an appropriate operator from the list of operators for the data type of the attribute.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter the value or select the value from the drop-down list. The value list depends on the <strong>Type</strong> and <strong>Operator</strong> selected.</td>
</tr>
</tbody>
</table>
4. Click **Next**.

**Authentication Configuration**

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

**Figure 49 Add Aruba RADIUS Enforcement (Generic) Service > Authentication Dialog**
### Table 3: Add Aruba RADIUS Enforcement (Generic) Service > Authentication Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| **Authentication Methods** | Select authentication methods using the Select to Add field. The authentication methods available 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 order of authentication is significant, when a client tries to perform an 802.1X authentication. Policy Manager proposes the first authentication method configured. However, the client can accept the authentication method proposed by Policy Manager and continue authentication or send a Negative-Acknowledgment (NAK) and propose a different authentication method. If the newly proposed authentication method is also configured, then the authentication proceeds, otherwise authentication fails.  
If most of the clients in the network use a specific authentication method, that authentication method should be configured first in the list. This would reduce the number of RADIUS packets exchanged.  
For more information, see the following:  
- Adding and Modifying Authentication Methods on page 161  
- Adding and Configuring Authentication Sources on page 184.  

| 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:  
- AD_avenda313 [Active Directory]  
- Admin User Repository  
- Blacklist User Repository  
- Endpoints Repository  
- Guest Device Repository  
- Guest User Repository  
- http_3702  
- HTTP_Auth_Source  
- 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.  

<table>
<thead>
<tr>
<th>Strip Username Rules</th>
<th>Select the check box to preprocess the username (to remove prefixes and suffixes) before authenticating and authorizing against the authentication source.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Certificate</td>
<td>Select the Service Certificate. Once you select the Service Certificate, click the View Certificate Details link to view information about the certificate.</td>
</tr>
</tbody>
</table>
Use the **Roles** tab to associate a role-mapping policy with this service.

The following figure displays the **Aruba RADIUS Enforcement (Generic)** > **Roles** dialog:

**Figure 50** Add Aruba RADIUS Enforcement (Generic) Service > Roles Dialog

![Roles tab in Aruba RADIUS Enforcement (Generic) configuration]

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

**Table 4: Add Aruba 802.1X Wireless Service > Roles Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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.  
For information on configuring role-mapping policies, see [Configuring a Role and Role-Mapping Policy on page 243](#). |
| 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.                                                                                                                  |

2. Click **Next**.

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

**Figure 51  Aruba RADIUS Enforcement (Generic) Service > Enforcement Dialog**

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

   **Table 5: Aruba RADIUS Enforcement (Generic) > Enforcement Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Cached Results</td>
<td>Select this check box to use cached roles and posture attributes from previous</td>
</tr>
<tr>
<td></td>
<td>sessions.</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td>Select the preconfigured enforcement policy from the drop-down list. This is</td>
</tr>
<tr>
<td></td>
<td>mandatory. If you do not have any preconfigured enforcement policies, click Add</td>
</tr>
<tr>
<td></td>
<td>New Enforcement Policy to create a new enforcement policy.</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Displays additional information about the selected enforcement policy.</td>
</tr>
<tr>
<td>Default Profile</td>
<td>Displays a default profile applied by ClearPassPolicy Manager.</td>
</tr>
<tr>
<td>Rules Evaluation Algorithm</td>
<td>Shows the first matched rule.</td>
</tr>
</tbody>
</table>

2. Click **Save**. You return to the **Services** page. The following message is displayed: *Service "RADIUS Enforcement service" has been added.*

**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.

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 52 RADIUS Proxy Service Configuration Dialog**

For configuration details, see RADIUS Enforcement (Generic) Service on page 73.

**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 to these or other generic applications for authenticating and authorizing the users. The following figure displays the Aruba Application Authentication service configuration dialog:

**Figure 53 Aruba Application Authentication Configuration Dialog**

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.

**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 to these or other generic applications for
authorizing the users. The following figure displays the **Aruba Application Authorization** service configuration dialog:

**Figure 54  Aruba Application Authorization Configuration Dialog**

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 59](#).

**ClearPass OnConnect Enforcement Service**

This section provides the following information:

- **Configuring the Service**
- **Configure 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**
- **System Page**

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.

**Configuring the 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 55).
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.

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

Figure 56  Selecting the ClearPass OnConnect Enforcement Policy

---

**Figure 55  Specifying ClearPass OnConnect Enforcement**

![Configuration > Services > Add](image)

---
3. From the **Enforcement Policy** drop-down list, select the appropriate OnConnect Enforcement policy. If you have not configured an OnConnect-type Enforcement policy, click **Add New Enforcement Policy** to create a new enforcement policy to associate with this OnConnect service.

4. Specify the values for the remaining parameters as described in **Table 1**, then click **Save**.

**Table 1: Service Enforcement Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Cached Results</td>
<td>Select this check box to use cached roles and posture attributes from previous sessions.</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td>From the drop-down list, select the preconfigured enforcement policy. This is a mandatory step.</td>
</tr>
</tbody>
</table>

**Enforcement Policy Details**

<table>
<thead>
<tr>
<th>Description</th>
<th>Displays additional information about the selected enforcement policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Profile</td>
<td>Displays a default profile applied by .</td>
</tr>
<tr>
<td>Rules Evaluation Algorithm</td>
<td>Shows first matched rule and return the role or select all matched rules and return a set of roles.</td>
</tr>
</tbody>
</table>

**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 57**).

**Figure 57 Specifying Event-Based Enforcement**

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

**Figure 58 Selecting the Ingress Events Enforcement Policy**

3. From the **Enforcement Policy** drop-down list, select the appropriate Event Enforcement policy.
4. If you have not configured Event-type Enforcement policies, click **Add New Enforcement Policy** to create a new enforcement policy.
5. Specify the values for the remaining parameters as described in **Table 1**, then click **Save**.

<table>
<thead>
<tr>
<th><strong>Table 1: Service Enforcement Page Parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Use Cached Results</td>
</tr>
<tr>
<td>Enforcement Policy</td>
</tr>
<tr>
<td>Enforcement Policy Details</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Default Profile</td>
</tr>
<tr>
<td>Rules Evaluation Algorithm</td>
</tr>
</tbody>
</table>

**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, you can specify service-level authorization sources from the Authorization tab. You can associate a role-mapping policy with this service via 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.

Configuring a TACACS+ Enforcement Service

To create a TACACS+ Enforcement service:
1. Navigate to Configuration > Services, then select the Add link. The Add Services page opens.
2. From the Type drop down, select TACACS+ Enforcement. The TACACS+ Enforcement service configuration dialog opens:

   ![Figure 59 Adding a New TACACS+ Enforcement Service](image)

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>From the drop-down list, select TACACS+ Enforcement.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>The Monitor Mode option is disabled for an enforcement policy.</td>
</tr>
<tr>
<td>More Options</td>
<td>The Authorization tab is not enabled by default. To bring up the Authorization configuration tab, check the Authorization check box.</td>
</tr>
</tbody>
</table>

Service Rule
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| **Type**  | Select one of the following service rule types:  
  - Authentication  
  - Connection  
  - Date  
  - Device  
  - Host  
  - Endpoint |
| **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. |

**Configuring a TACACS+ Multi-Factor Authentication Service**

ClearPass provides a way to differentiate between a TACACS+ login authentication and a TACACS+ enable authentication.

To do so, in Service and Policy rule configuration, you can use the **Authentication** type  
**TacacsAuthenService** parameter. This parameter accepts three values: None, Login, or Enable.

Note that an Enforcement policy can also use the **Authentication: TacacsAuthenService** attribute in the **Rules Editor > Conditions** section of the policy configuration.

**Creating a TACACS+ Multi-Factor Authentication Service**

To apply the **TacacsAuthenService** parameter in a TACACS+ Enforcement service:

1. Navigate to **Configuration > Services**, then select the **Add** link.

   The **TACACS+ Enforcement** service configuration dialog opens:

   **Figure 60**  Configuring a TACACS+ Multi-Factor Authentication Service

2. Specify the **TACACS+ Enforcement Service** parameters as described in the following table:
### Table 2: TACACS+ Enforcement > Service Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>From the drop-down list, select TACACS+ Enforcement.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>The Monitor Mode option is disabled for an enforcement policy.</td>
</tr>
<tr>
<td>More Options</td>
<td>The Authorization tab is not enabled by default. To bring up the Authorization configuration tab, check the Authorization check box.</td>
</tr>
</tbody>
</table>

### Service Rule

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Click to add, then select the Authentication type.</td>
</tr>
<tr>
<td>Name</td>
<td>Select TacacsAuthenService.</td>
</tr>
<tr>
<td>Operator</td>
<td>Select EQUALS.</td>
</tr>
<tr>
<td>Value</td>
<td>Select one of the following values:</td>
</tr>
<tr>
<td></td>
<td>- AUTHEN_SVC_NONE: Choose this option when the user does not require authentication.</td>
</tr>
<tr>
<td></td>
<td>- AUTHEN_SVC_LOGIN: Choose this option when the user is authenticating in Login mode.</td>
</tr>
<tr>
<td></td>
<td>- AUTHEN_SVC_ENABLE: Choose this option when the user is authenticating in Privileged mode.</td>
</tr>
</tbody>
</table>

### 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 1 for details):

- Linux
- macOS
- 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 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 1.

**Configuring a Web-Based Authentication Service**

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:

   ![Web-Based Authentication Service Configuration Dialog](image)

   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**.
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 > Web-Based Authentication 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 1: Service Rule > Web-Based Authentication Host Attributes**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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 Settings and Agent Library Updates](#)). 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. |
| **Installed SHAs** | Specifies the SHAs installed on the client. |
| **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 |
<p>| <strong>OSName</strong> | 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 |</p>
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSNameVersion</td>
<td>Provides the Windows OS name and the build version. This attribute can be used to create different Posture policies for different Windows 10 versions such as <strong>2015 LTSB</strong> or <strong>2016 LTSB</strong>.</td>
</tr>
</tbody>
</table>
| OSType                 | Specifies the Operating System type. The supported values are:  
  - Linux  
  - macOS  
  - Windows XP  
  - Windows 7  
  - Windows 8  
  - Windows 10  
  - Windows Server 2003  
  - Windows Server 2003 R2  
  - Windows Server 2008  
  - Windows Server 2008 R2  |
| SDKType                | Specifies the SDK type. For example, you can specify that the SDK type equals **V4**. For related information, see [Upgrading From OnGuard Plugin Version 1.0 to 2.0](#).                                            |
| SDKVersion             | Specifies the SDK version.                                                                                                                                                                                  |
| 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.                                                        |
| UserAgent              | The value of this attribute contains both **Agent Type** and **Agent Version**. For example, OnGuard 6.6.5.89660.                                                                                          |

Table 2: *Service Rule > Web-Based Authentication Host Attributes*

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Host             | 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 Settings and Agent Library Updates](#)).  
  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.                                    |
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td><strong>Health</strong>: OnGuard Agent is performing health checks; that is, the request contains Posture information.</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong></td>
</tr>
<tr>
<td>FQDN</td>
<td>Indicates the Fully Qualified Domain Name of the client.</td>
</tr>
<tr>
<td>HealthCheckLevel</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>System</strong>: The user is <em>not</em> logged in when health checks are being run.</td>
</tr>
<tr>
<td></td>
<td><strong>User</strong>: The user is logged in when health checks are being run.</td>
</tr>
<tr>
<td>Installed SHAs</td>
<td>Specifies the SHAs installed on the client.</td>
</tr>
<tr>
<td>InterfaceType</td>
<td>Specifies the type of <strong>Network Interface</strong>. This attribute can be used to define different services based on Network Interface type. The supported values are:</td>
</tr>
<tr>
<td></td>
<td><strong>Wired</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Wireless</strong></td>
</tr>
<tr>
<td></td>
<td><strong>VPN</strong></td>
</tr>
<tr>
<td>Name</td>
<td>This is the host name of the client (without the domain name).</td>
</tr>
<tr>
<td>OSArch</td>
<td>Specifies whether the client is running a 32-bit or 64-bit OS. The supported values are:</td>
</tr>
<tr>
<td></td>
<td><strong>i386</strong>: 32-bit OS</td>
</tr>
<tr>
<td></td>
<td><strong>x86_64</strong>: 64-bit OS</td>
</tr>
<tr>
<td>OSName</td>
<td>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</td>
</tr>
<tr>
<td>OSNameVersion</td>
<td>Provides the Windows OS name and the build version. This attribute can be used to create different Posture policies for different Windows 10 versions such as <strong>2015 LTSB</strong> or <strong>2016 LTSB</strong>.</td>
</tr>
<tr>
<td>OSTYPE</td>
<td>Specifies the Operating System type. The supported values are:</td>
</tr>
<tr>
<td></td>
<td><strong>Linux</strong></td>
</tr>
<tr>
<td></td>
<td><strong>macOS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows XP</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows 7</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows 8</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows 10</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows Server 2003</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows Server 2003 R2</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows Server 2008</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Windows Server 2008 R2</strong></td>
</tr>
<tr>
<td>SDKType</td>
<td>Specifies the SDK type. For example, you can specify that the SDK type equals <strong>V4</strong>. For related information, see <a href="#">Upgrading From OnGuard Plugin Version 1.0 to 2.0</a>.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SDKVersion</td>
<td>Specifies the SDK version.</td>
</tr>
</tbody>
</table>
| 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. |
| 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 86](#).

**Creating the Service**

To create a **Web-based Health Check Only** service:

1. Navigate to Configuration > Services, then select the Add link. The **Web-Based Health Check Only** service configuration dialog opens:

   ![Figure 63](#)  

   **Figure 63  Web-Based Health Check Only Service Configuration Dialog**

2. Specify the **Service** tab parameters as described in the following table:
Table 1: Add Web-based Health Check Only Service > Service Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>From the drop-down list, select <strong>Web-based Health Check Only</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Select the check box to monitor network access activity without enforcement.</td>
</tr>
<tr>
<td>More Options</td>
<td>Check these boxes to access the additional configuration tabs:</td>
</tr>
<tr>
<td></td>
<td>- Authorization</td>
</tr>
<tr>
<td></td>
<td>- Posture Compliance</td>
</tr>
</tbody>
</table>

Service Rule

| Type            | Select one of the following service rule types:                                                                                                         |
|                 | - Authentication                                                                                                                                     |
|                 | - Connection                                                                                                                                        |
|                 | - Date                                                                                                                                             |
|                 | - Device                                                                                                                                           |
|                 | - Host                                                                                                                                               |
|                 | - Endpoint                                                                                                                                           |

| 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 Rule > Web-Based Authentication Host Attributes

The following table describes the list of other attributes that can be used to create host services based on the client's information.
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentType</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- OnGuardAgent: OnGuard Agent</td>
</tr>
<tr>
<td></td>
<td>- OnGuardAgentService: OnGuard Agent running as a service</td>
</tr>
<tr>
<td></td>
<td>- NativeWebAgent: Native Dissolvable Agent</td>
</tr>
<tr>
<td></td>
<td>- JavaWebAgent: Java Dissolvable Agent</td>
</tr>
<tr>
<td>Agent Version</td>
<td>OnGuard Agent version. This attribute can be used to create a service based on the OnGuard Agent version.</td>
</tr>
<tr>
<td>CheckType</td>
<td>Specifies the type of check OnGuard Agent is performing based on the Mode setting in the OnGuard Settings page (for details, see OnGuard Settings and Agent Library Updates).</td>
</tr>
<tr>
<td></td>
<td>For Authenticate with health checks, the value of this attribute is Authentication, Health. The supported values are:</td>
</tr>
<tr>
<td></td>
<td>- Authentication: OnGuard Agent is performing authentication; that is, the request contains credentials.</td>
</tr>
<tr>
<td></td>
<td>- Health: OnGuard Agent is performing health checks; that is, the request contains Posture information.</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td>FQDN</td>
<td>Indicates the Fully Qualified Domain Name of the client.</td>
</tr>
<tr>
<td>HealthCheckLevel</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This attribute can be used to see the health check level when OnGuard Agent is running as Service or BothServiceAndUser.</td>
</tr>
<tr>
<td></td>
<td>- System: The user is not logged in when health checks are being run.</td>
</tr>
<tr>
<td></td>
<td>- User: The user is logged in when health checks are being run.</td>
</tr>
<tr>
<td>Installed SHAs</td>
<td>Specifies the SHAs installed on the client.</td>
</tr>
<tr>
<td>InterfaceType</td>
<td>Specifies the type of Network Interface. This attribute can be used to define different services based on Network Interface type. The supported values are:</td>
</tr>
<tr>
<td></td>
<td>- Wired</td>
</tr>
<tr>
<td></td>
<td>- Wireless</td>
</tr>
<tr>
<td></td>
<td>- VPN</td>
</tr>
<tr>
<td>Name</td>
<td>This is the host name of the client (without the domain name).</td>
</tr>
<tr>
<td>OSArch</td>
<td>Specifies whether the client is running a 32-bit or 64-bit OS. The supported values are:</td>
</tr>
<tr>
<td></td>
<td>- i386: 32-bit OS</td>
</tr>
<tr>
<td></td>
<td>- x86_64: 64-bit OS</td>
</tr>
<tr>
<td>OSName</td>
<td>Indicates the full Operating System name. This attribute can be used to create services for a specific OS.</td>
</tr>
<tr>
<td></td>
<td>For example, you can use this attribute to differentiate between Windows 8 and Windows 8.1</td>
</tr>
<tr>
<td>OSNameVersion</td>
<td>Provides the Windows OS name and the build version. This attribute can be used to create different Posture policies for different Windows 10 versions such as 2015 LTSB or 2016 LTSB.</td>
</tr>
<tr>
<td>OSType</td>
<td>Specifies the Operating System type. The supported values are:</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|                | - Linux  
|                | - macOS  
|                | - Windows XP  
|                | - Windows 7  
|                | - Windows 8  
|                | - Windows 10  
|                | - Windows Server 2003  
|                | - Windows Server 2003 R2  
|                | - Windows Server 2008  
|                | - Windows Server 2008 R2  |

**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 86. The following figure displays the Web-based Open Network service page configuration dialog:
Modifying and Managing Services

Following the procedures described in this section to modify and manage your services.

Modifying an Existing Service

You can use service types as configured, or you can edit their settings. To modify an existing service:

1. Navigate to the Configuration > Services page.
2. Select the service you wish to modify. The Services > [service_name] dialog opens.
3. Edit the service parameters, then click Save to save your settings. For complete information on the settings supported by each service type, see Configuring Services Using Service Templates & Wizards and Configuring Other Policy Manager Services.

Creating a Service by Copying an Existing Service

You can perform a service-copy operation only on a Publisher node. To create a service template by making a copying an existing service:

1. From the Services page, select the check box by a service.
2. Click Copy. You receive the following message: Service Copy_of_<service_name> has been added.

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. You receive the prompt: Are you sure you want to delete this service?
3. To cancel the delete operation, click No. To delete the selected service, click Yes.
Restarting ClearPass Services

The Audit Viewer (Monitoring > Audit Viewer) tracks NTP configuration changes.

To restart ClearPass services:
1. Navigate to Administration > Server Manager > Server Configuration.
2. Select the ClearPass Publisher node.
3. From the Server Configuration page, select the Services Control tab.
4. From the Action column, click Start for each service that needs to be restarted. Once the service is restarted, the Start button is changed to Stop.

Figure 65  Restarting Stopped Services

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 associated with the 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 opens.

Figure 66  Services Page Reorder Button
2. Click the Reorder button (located on the lower-right portion of the page). The Reorder Services page opens.

3. Click the service you want to move to another position in the order (see Figure 67). In this example, we will move Guest Operator Logins at the 5th position to the 2nd position.

**Figure 67  Selecting the Service to Be Reordered**

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

**Figure 68  Selecting the Destination Order Position**

5. Click the selected destination position (see Figure 69). The service is now moved to its new position in the services order.

**Figure 69  Service Moved to New Order Position**

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.
Live Monitoring

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

- Live Monitoring: Access Tracker on page 100
- Live Monitoring: Accounting on page 115
- Live Monitoring: Analysis and Trending on page 134
- Live Monitoring: OnGuard Activity
- Live Monitoring: System Monitor on page 135

Additional Monitoring Functions

The following additional monitoring features are provided:

- Audit Viewer on page 145
- Event Viewer on page 148
- Data Filters on page 151
- Restoring Blacklisted Users to the Network on page 155

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

Figure 70  Access Tracker Page

You can adjust and resize the column widths for the columns on the Access Tracker page. Use your mouse to grab the column separator to the left of the column title, then move the column left or right to change the column width.
Table 1 describes the information provided on the Access Tracker page:

### Table 1: Access Tracker Page Columns

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Displays the IP address of the current ClearPass server.</td>
</tr>
<tr>
<td>Source</td>
<td>Displays the authentication source for the session. For example, TACACS or web authentication (WEBAUTH).</td>
</tr>
<tr>
<td>Username</td>
<td>Displays the username or MAC address of the host.</td>
</tr>
<tr>
<td>Service</td>
<td>Displays the name of the service.</td>
</tr>
<tr>
<td>Login Status</td>
<td>Displays the status of the request, such as Accept, Reject, or Timeout.</td>
</tr>
<tr>
<td>Request Timestamp</td>
<td>Displays the date and time when the status was last updated.</td>
</tr>
</tbody>
</table>

### 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.

   ![Edit Access Tracker Page](image)

   **Figure 71**  Edit Access Tracker Page

2. Modify the Edit Access Tracker page parameters as described in the following table, then click Save:
### Table 1: Edit Access Tracker Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server/Domain</td>
<td>From the drop-down, select the server or domain on the <strong>Access Tracker</strong> page. To display transactions from all nodes in the Policy Manager cluster, select the default option.</td>
</tr>
<tr>
<td>Select Filter</td>
<td>Select a filter category to filter the displayed data. For a description of available filters, see <a href="#">Data Filters on page 151</a>.</td>
</tr>
<tr>
<td>Modify Filter</td>
<td>To modify the current data filter, click the <img src="#" alt="icon" />. For more information, see <a href="#">Data Filters on page 151</a>.</td>
</tr>
<tr>
<td>Add Filter</td>
<td>To add a data filter, click the <img src="#" alt="Add" /> icon. For more information, see <a href="#">Data Filters on page 151</a>.</td>
</tr>
<tr>
<td>Select Date Range</td>
<td>To select the start of the range of dates for which the <strong>Access Tracker</strong> table displays data, click the <strong>Last</strong> drop-down list. Available options are one to six days, or one week.</td>
</tr>
<tr>
<td>Select Date</td>
<td>To select a date, click the <img src="#" alt="Date" /> icon.</td>
</tr>
<tr>
<td>Show Latest</td>
<td>To set the date in the <strong>before</strong> field to the current date, click <strong>Show Latest</strong>.</td>
</tr>
<tr>
<td>Select Columns</td>
<td>This section displays the following two fields:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Available Columns</strong>: Displays the data column available to be displayed in an <strong>Access Tracker</strong> table.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Selected Columns</strong>: 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 <strong>Selected Columns</strong> field, then click the <strong>Up</strong> or <strong>Down</strong> buttons.</td>
</tr>
</tbody>
</table>

### Viewing Access Tracker Session Details

The following section describes session details for RADIUS, WebAuth and TACACS+ sessions.

#### View RADIUS Session Information

To view details about a selected RADIUS session, navigate to the **Monitoring > Live Monitoring > Access Tracker** page.
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.

**Change Status Button**

When you click the Change Status button, the Request Details > Access Control Capabilities dialog opens:

**Figure 73  Access Control Capabilities**

Specify the access control capabilities as described in the following table.
Table 1: Access Control Capabilities

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Access Control Type</td>
<td>Select one of the following Access Control Types to view or change any of the supported access control types.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Agent</strong>: This control is available for a session where the endpoint has the OnGuard Agent installed. The following actions are allowed:</td>
</tr>
<tr>
<td></td>
<td>• Bouncing</td>
</tr>
<tr>
<td></td>
<td>• Sending Messages</td>
</tr>
<tr>
<td></td>
<td>• Tagging the status of the endpoint as <strong>Disabled</strong> or <strong>Known</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>SNMP</strong>: This control is available for any session for which Policy Manager has the switch and port-level information associated with the MAC address of the endpoint. Policy Manager uses SNMP to bounce the switch port with which the endpoint is associated. For this type of control, SNMP read and write community strings must be configured for the network device. You must configure Policy Manager as an SNMP trap receiver to receive link up and link down traps. For more information, see <a href="#">SNMP Trap Receivers</a>.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>RADIUS CoA</strong>: This control is available for any session where access was previously controlled by a RADIUS transaction. The network device must be RADIUS CoA-capable and RADIUS CoA-enabled when you configure the network device in Policy Manager (see <a href="#">Adding a Network Device</a>). The actions available depend on the type of device. The <strong>Disconnect</strong> or <strong>Terminate Section</strong> action is supported by all devices. Some devices support setting a session timeout, changing the VLAN for the session, and applying an ACL.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Server Action</strong>: This control is available by default for any session. Select the server action from the <strong>Server Action</strong> drop-down list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS CoA Type</td>
<td>Select one of the following RADIUS CoA (Change of Authorization) types:</td>
</tr>
<tr>
<td></td>
<td>■ Cisco - Terminate Session</td>
</tr>
<tr>
<td></td>
<td>■ Cisco - Disable Host-Port</td>
</tr>
<tr>
<td></td>
<td>■ Cisco - BounceHost-Port</td>
</tr>
<tr>
<td></td>
<td>■ Cisco - Reauthenticate-Session</td>
</tr>
<tr>
<td></td>
<td>■ CPATS CoA Enforcement Profile</td>
</tr>
</tbody>
</table>

**RADIUS > Summary Tab**
The **Summary** page shows the high-level information for the transaction.

**Figure 74  Access Tracker > RADIUS Request Details > Summary Page**

---

**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:

- RADIUS Request
- Computed Attributes
- Endpoint Attributes

All of these attributes can be used in role-mapping rules. To view the **Input** tab, select a RADIUS session in the **Access Tracker** page, then select the **Input** tab.
**Figure 75** Access Tracker > RADIUS Request Details > Input Page

**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 76** Access Tracker > RADIUS Request Details > Output Page

---

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 77  Access Tracker > RADIUS Request Details > Accounting Tab**

---

**View WebAuth Session Information**

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 78**  Access Tracker > WebAuth Request Details > Summary Page

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.
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:
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, navigate to the Monitoring > Live Monitoring > Access Tracker page, then click a TACACS+ session in the Access Tracker table.

**Figure 81  Access Tracker Page with TACACS+ Session**

TACACS+ > Summary Tab
The Session Details for the selected TACACS+ transaction opens to the Summary page.
Table 2 describes the parameters in the TACACS+ Session Details Summary page.

### Table 2: TACACS Session Details > Summary Page Parameters

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

### TACACS+ > Request Tab
The TACACS+ Request page provides the essential information regarding the TACACS+ authentication request.

**Figure 83** Access Tracker > TACACS Session Details > Request Page

Table 3 describes the parameters in the TACACS+ Session Details Request page.

**Table 3: TACACS Session Details > Request Page Parameters**

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

![TACACS+ Session Details](image)

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Action/Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Indicates the name of the ClearPass service through which the user is authenticated.</td>
</tr>
<tr>
<td>Authentication Source</td>
<td>Specifies the authentication source used by the client. For more information, see <a href="#">Adding and Configuring Authentication Sources</a>.</td>
</tr>
<tr>
<td>Role</td>
<td>Indicates the Policy Manager role assigned to the client. For more information, see <a href="#">Adding and Modifying Roles</a>.</td>
</tr>
<tr>
<td>Profiles</td>
<td>Indicates the Enforcement Profile configured for this service. For more information, see <a href="#">Configuring Enforcement Profiles</a>.</td>
</tr>
</tbody>
</table>

**Table 4: TACACS Session Details > Policies Used Page Parameters**

**TACACS+ > Alerts Tab**

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

**Figure 85 Access Tracker > TACACS+ Session Details > Alerts Page**

![TACACS+ Session Details](image)
Table 5: TACACS Session Details > AlertsPage Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Request Messages</td>
<td></td>
</tr>
<tr>
<td>Error Category</td>
<td>Indicates the error category.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Displays the error code.</td>
</tr>
<tr>
<td>Alerts for This Request</td>
<td></td>
</tr>
<tr>
<td>Alert source</td>
<td>Indicates the source for this alert; in this case, the TACACS+ server.</td>
</tr>
<tr>
<td>Alert message</td>
<td>Displays the alert message.</td>
</tr>
</tbody>
</table>

Network Details

The Network Details section of the Access Request > Request Details > Accounting page includes a list of the IPv6 addresses from the Framed-IPv6-Address vendor-specific attributes.

Figure 86 Accounting > Network Details Section

Framed IPv6 Data Available Via Export

Framed-IPv6-Address information is also available when you click Export from the Access Tracker Request Details page. The Dashboard_Details.zip file contains the Dashboard_Details.txt file. In the the Network Details section of the Dashboard_Details.txt file, entries for Framed IPv6 Address are provided:
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 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. To bring up the Accounting page, navigate to Monitoring > Live Monitoring > Accounting.
The following table describes the Accounting parameters:

**Table 1: Accounting Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Specifies the IP address of the host name.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the protocol used.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the user name.</td>
</tr>
<tr>
<td>Access Device</td>
<td>Displays the IP address of the device.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Displays the date and time.</td>
</tr>
</tbody>
</table>

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 117 and TACACS+ Accounting Record Details > Auth Sessions Tab on page 124.

**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.
3. Specify the **Edit Accounting Page** parameters as described in **Table 2**:

**Table 2: Edit Accounting Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server/ Domain</td>
<td>Select the ClearPass server for the dashboard data to be displayed.</td>
</tr>
<tr>
<td>Select Filter</td>
<td>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</td>
</tr>
<tr>
<td>Modify</td>
<td>To modify a data filter, click the Modify Data Filter icon (as shown in Figure 89).</td>
</tr>
<tr>
<td>Add</td>
<td>To create a new data filter, click the Add icon.</td>
</tr>
<tr>
<td>Select Date Range</td>
<td>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.</td>
</tr>
<tr>
<td>Show Latest</td>
<td>To view the latest information, set the date to Today.</td>
</tr>
</tbody>
</table>
| 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 such as the framed IPv6 addresses for the RADIUS protocol. The following figure displays the RADIUS Accounting Record Details > Summary page:
The following table describes the configuration parameters on the RADIUS Accounting Record Details > Summary page:

**Table 1: RADIUS Accounting Record Details Summary Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Specifies the Policy Manager session identifier. You can correlate this record with a record in Access Tracker.</td>
</tr>
<tr>
<td>Account Session ID</td>
<td>Specifies a unique ID for this accounting record.</td>
</tr>
<tr>
<td>Start Timestamp</td>
<td>Shows the start time and end time of the session.</td>
</tr>
<tr>
<td>End Timestamp</td>
<td>Shows the current connection status of the session.</td>
</tr>
<tr>
<td>Status</td>
<td>Usersname associated with this record.</td>
</tr>
<tr>
<td>Termination Cause</td>
<td>Specifies the reason for termination of this session.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Shows the value of the standard RADIUS attribute service type.</td>
</tr>
<tr>
<td>NAS IP Address</td>
<td>Shows the IP address of the network device.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NAS Port Type</td>
<td>Shows the access methods. For example, Ethernet, or 802.11 Wireless.</td>
</tr>
<tr>
<td>Calling Station ID</td>
<td>Specifies the MAC address of the client that is supported by Policy Manager. &lt;br&gt;Note: Policy Manager supports Calling Station ID MAC addresses in the following formats: &lt;br&gt;• aa:bb:cc:dd:ee:ff &lt;br&gt;• aa-bb-cc-dd-ee-ff &lt;br&gt;• aaaa-bbbb-cccc &lt;br&gt;• aabbccddeeff &lt;br&gt;• aaaa-bbbb-cccc</td>
</tr>
<tr>
<td>Called Station ID</td>
<td>Shows the MAC address of the network device.</td>
</tr>
<tr>
<td>Framed IP Address</td>
<td>Shows the IP address of the client (if available).</td>
</tr>
<tr>
<td>Framed IPv6 Address</td>
<td>Displays a list of the IPv6 addresses from the Framed-IPv6-Address vendor-specific attributes.</td>
</tr>
<tr>
<td>Account Auth</td>
<td>Specifies the type of authentication; for example, RADIUS authentication.</td>
</tr>
</tbody>
</table>

**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 Accounting Record Details > Auth Sessions page:

**Figure 91  RADIUS Accounting Record Details > Auth Sessions Page**
The following table describes the **RADIUS Accounting Record Details > Auth Sessions** parameters:

### Table 1: RADIUS Accounting Record Details Auth Sessions Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Authentication Sessions</td>
<td>Specifies the total number of authentications (always 1) and authorizations in this session.</td>
</tr>
</tbody>
</table>

#### Authentication Sessions Details

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Displays the Policy Manager session ID.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of authentication: Initial authentication or reauthentication.</td>
</tr>
<tr>
<td>Time Stamp</td>
<td>Specifies the time when the event occurred.</td>
</tr>
</tbody>
</table>

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

**Table 1: RADIUS Accounting Record Details > Utilization Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Time</td>
<td>Displays the duration of the session that was active.</td>
</tr>
<tr>
<td>Account Delay Time</td>
<td>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).</td>
</tr>
<tr>
<td>Account Input Octets</td>
<td>Specifies the quantity of octets sent to and received from the device port during the session.</td>
</tr>
<tr>
<td>Account Output Octets</td>
<td></td>
</tr>
<tr>
<td>Account Input Packets</td>
<td>Specifies the packets sent and received from the device port during the session.</td>
</tr>
<tr>
<td>Account Output Packets</td>
<td></td>
</tr>
</tbody>
</table>

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

**Table 1: RADIUS Accounting Record > Details Page Summary**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Packet Details</td>
<td>Shows the details of RADIUS attributes sent and received from the network device during an initial authentication and subsequent reauthentications. Each section in the <strong>Details</strong> page corresponds to a session in Policy Manager.</td>
</tr>
</tbody>
</table>
**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 94  TACACS+ Accounting Record Details > Request Page**

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

**Table 1: TACACS+ Accounting Record Request Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Specifies the <strong>Session ID</strong>, which is a unique ID associated with a request.</td>
</tr>
<tr>
<td>User Session ID</td>
<td>Specifies a session ID that correlates authentication, authorization, and accounting records.</td>
</tr>
<tr>
<td>Start and End Timestamp</td>
<td>Shows the start and end times of the session.</td>
</tr>
<tr>
<td>Username</td>
<td>Shows the username associated with this record.</td>
</tr>
<tr>
<td>Client IP</td>
<td>Shows the IP address and tty (text terminal) of the device interface.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>Shows the IP address from which the Administrator is logged in.</td>
</tr>
<tr>
<td>Flags</td>
<td>Shows the identifier corresponding to starting, stopping, or updating the accounting record.</td>
</tr>
<tr>
<td>Privilege Level</td>
<td>Specifies the privilege level of the Administrator. The range is from 1 (lowest) to 15 (highest).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Identifies the authentication method used for network access.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Identifies the authentication type used for network access.</td>
</tr>
<tr>
<td>Authentication Service</td>
<td>Identifies the authentication service used for network access.</td>
</tr>
</tbody>
</table>

**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 95  TACACS+ Accounting Record Details > Auth Sessions Page**

   ![Figure 95 TACACS+ Accounting Record Details > Auth Sessions Page](image)

The following table summarizes the information available on the **TACACS+ Accounting Record Details > Auth Sessions** page:
### Table 1: TACACS+ Accounting Record Details > Authentication Sessions Page Parameters

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

### 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:

![TACACS+ Accounting Record Details > Details Page](image)

The following table summarizes the configuration parameters provided on the TACACS+ Accounting Record > Details tab:
Table 1: TACACS+ Accounting Record > Details Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Packet Details</td>
<td>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.</td>
</tr>
</tbody>
</table>

Live Monitoring: OnGuard Activity

This section provides the following information:

- **About OnGuard Activity**
- **Viewing Authentication Records**
- **Broadcasting Notifications to OnGuard Agents**
- **Sending a Message to Selected Endpoints**
- **Bouncing a Client Using SNMP**
- **Bouncing an Agent Not Using SNMP**

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, restart a session, and 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 97  OnGuard Activity Page**

   The following table describes the action buttons on the **OnGuard Activity** page:
### Table 1: OnGuard Activity Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Message</td>
<td>Click <strong>Send Message</strong> to send a message to the selected endpoints. For details, see <a href="#">Sending a Message to Selected Endpoints</a>.</td>
</tr>
<tr>
<td>Send Notification</td>
<td>Click <strong>Send Notification</strong> to apply the <em>Bounce or Restart Session</em> notification options to one or more endpoints that you selected in the OnGuard Activity list. For details, see <a href="#">Broadcasting Notifications to OnGuard Agents</a>.</td>
</tr>
</tbody>
</table>

### Viewing Authentication Records

From the **OnGuard Activity** page, you can view the authentication records for the online devices that are listed. To view the authentication records for a device that is online, click the **View** button on the pertinent row. The **Endpoint Authentication Details** page opens.

**Figure 98**  *Viewing an Endpoint’s Authentication Records*

### Broadcasting Notifications to OnGuard Agents

This option allows administrators to send bounce or restart notifications to every connected OnGuard Agent. A custom message can be included with the notifications.

To send bounce or restart notifications to selected OnGuard Agents:

2. Select the endpoint(s) to which you want to broadcast notifications. In order for a message or notification to be sent, the endpoint status must be Online (green check icon).

3. Click the **Broadcast Notification** link. The **Broadcast Notification to Agents** dialog opens.

![Broadcast Notification to Agents](image)

4. Specify the **Broadcast Notification to Agents** parameters as described in the following table:
Table 1: Send Notification to Agents Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Message (Optional)</td>
<td>Enter the text of the message you want to send to the selected OnGuard Agents.</td>
</tr>
<tr>
<td>Web link for more details (optional)</td>
<td>Optionally, enter a URL to be included with the message specified for Display Message.</td>
</tr>
<tr>
<td>Action</td>
<td>Select one of the following actions:</td>
</tr>
<tr>
<td>Bounce</td>
<td>Select this option to have the OnGuard Agent bounce the network interface.</td>
</tr>
<tr>
<td>Restart Session</td>
<td>Select this option to have the OnGuard Agent restart the session in order to perform authentication and health checks.</td>
</tr>
<tr>
<td>Endpoint Status</td>
<td>When you select Bounce, you must specify one of the following options:</td>
</tr>
<tr>
<td>No change in status</td>
<td>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.</td>
</tr>
<tr>
<td>Allow network access</td>
<td>Allow network access by white-listing this endpoint. Clicking Allow network access sets the status of the endpoint as Known.</td>
</tr>
<tr>
<td>Block network access</td>
<td>Block network access by blacklisting this endpoint. Clicking Block network access sets the status of the endpoint to Disabled.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>You must configure Enforcement Policy Rules to allow access to the endpoints with the status Known.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>You must configure Enforcement Policy Rules to allow access to the endpoints with the status Disabled.</td>
</tr>
</tbody>
</table>

5. Click Send Notification. The notification, along with the specified Endpoint Status, is sent to the selected endpoints.

Sending a Message to Selected Endpoints
To send a message to selected endpoints:

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 101 Sending a Message to OnGuard Agents
4. Specify the *Send Notification to Agents* parameters as described in the following table:

**Table 1: Send Notification to Agents Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Message</td>
<td>Enter the text of the message you want to send to the selected OnGuard Agents.</td>
</tr>
<tr>
<td>Web link for more details (optional)</td>
<td>Optionally, enter a URL to be included with the text specified for <em>Display Message</em>.</td>
</tr>
</tbody>
</table>

5. Click **Send**. The message is sent to the selected devices.

**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](#).
  - For details about configuring SNMP settings, see [SNMP Read Settings Parameters on page 420](#) and [SNMP Write Settings Parameters](#).
- SNMP traps (link up and/or MAC notification) must be enabled on the switch port (see [ClearPass SNMP Traps and OIDs](#) and [SNMP Trap Details](#)).
- 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](#).
  - For information about configuring the IP helper address, see [DHCP Collector](#).

**Bouncing a Client**

To bounce a client using SNMP:

1. Navigate to **Monitoring > Live Monitoring > OnGuard Activity**. The **OnGuard Activity** page opens.
2. Click the **Bounce Client (using SNMP)** link. The **Bounce Client (using SNMP)** dialog opens.

**Figure 103  Bouncing a Client Using SNMP**

3. Enter the client IP address or MAC address of the client to be bounced, then click **Go**. The rest of the fields in the **Bounce Client (Using SNMP)** dialog are automatically populated (**Host MAC**, **Host IP**, etc.) and the **Send Notification** button is enabled.

4. Click **Go**, then click **Send Notification**. The OnGuard Agent bounces the network interface of the specified client device.

**Bouncing an Agent Not Using SNMP**

This section describes how to initiate a bounce on an endpoint’s managed interface.

---

**Note**

Endpoint bounce works only 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
To bounce an agent:

2. Click a device listed on the OnGuard Activity page. The Agent and Endpoint Details page opens.

Figure 104 Agent and Endpoint Details

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host MAC</td>
<td>Displays the MAC address of the user.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional description of the endpoint.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the endpoint.</td>
</tr>
<tr>
<td>Added by</td>
<td>Displays the server name.</td>
</tr>
<tr>
<td>MAC Vendor</td>
<td>Vendor name and OS of the endpoint device.</td>
</tr>
<tr>
<td><strong>OnGuard Details</strong></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Displays the MAC address of the host.</td>
</tr>
<tr>
<td>Host IP</td>
<td>Displays the IP address of the host.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the status of the agent as either Online or Offline.</td>
</tr>
<tr>
<td>Agent Type</td>
<td>Specifies the agent as an OnGuard agent.</td>
</tr>
<tr>
<td>Host OS</td>
<td>Displays the operating system that runs on the endpoint.</td>
</tr>
<tr>
<td>Registered Policy Manager Server</td>
<td>Displays the name and IP address of the Policy Manager server.</td>
</tr>
<tr>
<td>Registered at</td>
<td>Displays the date and time at which the Policy Manager installation was registered.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Unregistered at</td>
<td>Displays the date and time at which the Policy Manager installation was last unregistered.</td>
</tr>
<tr>
<td>Last Seen Health Status</td>
<td>Displays the health status of the endpoint. For example, QUARANTINED or HEALTHY.</td>
</tr>
<tr>
<td>Unhealthy Health Classes</td>
<td>Displays the health classes that are unhealthy.</td>
</tr>
</tbody>
</table>

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

**Figure 105  Sending Notification to OnGuard Agents**

The following table describes the configuration parameters on the **Send Notification to Agents** dialog:

**Table 2: Send Notification to Agents Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Message (Optional)</td>
<td>An optional message to display on the endpoint using the OnGuard interface.</td>
</tr>
<tr>
<td>Web link for more details (Optional)</td>
<td>An optional clickable URL that is displayed along with the Display Message.</td>
</tr>
<tr>
<td>Action</td>
<td>Select one of the following actions:</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Bounce" />: Select this option to have the OnGuard Agent bounce the network interface.</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Restart Session" />: Select this option to have the OnGuard Agent restart the session in order to perform authentication and health checks.</td>
</tr>
<tr>
<td>Endpoint Status</td>
<td>When you select <strong>Bounce</strong>, you must specify one of the following options:</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="No change in status" />: No change is made to the status of the endpoint. The existing status of <strong>Known</strong>, <strong>Unknown</strong>, or <strong>Disabled</strong> continues to be applied. Access control is granted or denied based on the existing status of an endpoint.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Allow network access:</strong></td>
<td>Allow network access by white-listing this endpoint. Clicking Allow network access sets the status of the endpoint to Known. <strong>NOTE:</strong> You must configure Enforcement Policy Rules to allow access to the endpoints with the status Known. For details, see Configuring Enforcement Policies.</td>
</tr>
<tr>
<td><strong>Block network access:</strong></td>
<td>Block network access by blacklisting this endpoint. Clicking Block network access sets the status of the endpoint to Disabled. <strong>NOTE:</strong> You must configure Enforcement Policy Rules to allow access to the endpoints with the status Disabled.</td>
</tr>
</tbody>
</table>

4. To proceed, click **Send Notification**. The notification is sent to the selected device.

**Posture Info**

The Agent and Endpoint Details page includes the Posture Info tab. This page provides posture information for the selected device in the following categories:

- Posture Request
- Posture Response
- Posture Evaluation Results
- Application Response

**Figure 106  Agent and Endpoint Details > Posture Information**

**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) 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 107 Analysis and Trending**

Use the following components in the user interface to customize and filter the Analysis and Trending page:

<table>
<thead>
<tr>
<th>Component</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server</td>
<td>Select a ClearPass node from the cluster.</td>
</tr>
<tr>
<td>Update Now!</td>
<td>Click to update the display with the latest available data.</td>
</tr>
<tr>
<td>Customize This!</td>
<td>Click to customize the display by adding filters. You can add a maximum of four filters.</td>
</tr>
<tr>
<td>Toggle Chart Type</td>
<td>Click to toggle the chart display between line and bar type.</td>
</tr>
<tr>
<td>Add New Data Filter</td>
<td>Click to add a data filter in the global filter list. For more information on adding filters, refer to Data Filters on page 151.</td>
</tr>
</tbody>
</table>

**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.
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:
2. From the Select Server drop-down, select the desired ClearPass server.

Figure 108  System Monitor Page

Table 1: System Monitor Page Report Widgets

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

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, navigate to Monitoring > Live Monitoring > System Monitor > Process Monitor.

**Figure 109  System Monitoring: Process Monitor Page**

Click the Select Process drop down list and select a process To view CPU Usage and Main Memory usage for the selected process or service.

**System Monitor Process List**

The following processes can be monitored on the Monitoring > Live Monitoring > System Monitor page:

- 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
Network Monitor Page

The Network Monitor page displays information about the selected network traffic type. To view network activity, navigate to Monitoring > Live Monitoring > System Monitor > Network tab, click the Select menu, and select the desired traffic type.

Figure 110 Network Monitor Page

Network Monitor Traffic List

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 on several key ClearPass components.

To access the ClearPass Monitor page:

2. Click the Select drop-down.
ClearPass Component List
You can view statistics for the following ClearPass components on this page.

- 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

Monitoring Endpoint Profiler and Network Scan
This section provides the following information:

- Monitoring Endpoint Profiler
- Monitoring Network Scans and Subnet Scans
- Monitoring Discovered Devices

Monitoring Endpoint Profiler

Viewing Discovered Endpoints
To view the discovered endpoints that are connected to the network:

1. Navigate to Monitoring > Profile and Network Scan > Network Scan. The Network Scan page opens.
2. Click Endpoint Profiler. The Endpoint Profiler page opens.
3. Specify the Device Category, Device Family, and Device Name settings that you wish to view. The list of endpoints that are presented is based on the Device Category, Device Family, and Device Name items that you select.

4. To see graphs that show information about distribution and update frequency for devices and computers, click Change View.

**Viewing Details About a Specific Endpoint**

To view details about a specific endpoint:

1. Click a device in the device table at the bottom of the page. The View Endpoint page opens:

   **Figure 113** Endpoint Profiler Details

   2. To return to the Endpoint Profiler page, select the Cancel button.
Monitoring Network Scans and Subnet Scans

This section provides the following information:

- Viewing Network Scan and Subnet Scan Status
- Updating the Data on Network Scans and Subnet Scans

**Viewing Network Scan and Subnet Scan Status**

After you have scheduled and run network scans and subnet scans, you can view the status of all scans run by the current ClearPass server.

ClearPass retains the scan status information for the last ten network scans and subnet scans that were run.

To view network scan and subnet scan status:

1. Navigate to Monitoring > Profile and Network Scan > Network Scan. The Monitoring > Network Scan page opens.

**Figure 114  Viewing Network and Subnet Scan Status**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Devices Discovered</td>
<td>This section provides the total number of devices and endpoints discovered so far. This does not display the devices discovered by the selected network or subnet scan.</td>
</tr>
<tr>
<td>Filter</td>
<td>You can filter for the following:</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
</tr>
<tr>
<td></td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td>Seed Device/IP Subnet(s)</td>
</tr>
<tr>
<td></td>
<td>Start Time</td>
</tr>
<tr>
<td></td>
<td>End Time</td>
</tr>
<tr>
<td></td>
<td>Endpoints</td>
</tr>
<tr>
<td></td>
<td>Devices</td>
</tr>
<tr>
<td></td>
<td>Status</td>
</tr>
</tbody>
</table>

**Updating the Data on Network Scans and Subnet Scans**

When Auto-Refresh is enabled (it is enabled by default), ClearPass fetches fresh data every few seconds to ensure that the network scan and subnet scan status is always current. 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 so frequently in that case.

To enable or disable Auto Refresh:
1. Navigate to Monitoring > Profile and Network Scan > Network Scan. When Auto-Refresh is enabled, the button in front of the Auto Refresh link is green.

**Figure 115  Network Scan> Auto Refresh**

2. To disable Auto-Refresh, click the green button, which then turns red to indicate that the Auto Refresh is disabled.

**Figure 116  Auto Refresh Disabled**

3. To reenable Auto Refresh, click the red button in front of the Auto Refresh link. The button turns green and Auto Refresh is now reenabled.

### Monitoring Discovered Devices

This section provides the following information:

- Importing Network Devices
- Viewing Details on a Discovered Device

To access the Discovered Devices page:

**Importing Network Devices**

The devices that you import are added to the set of network devices known to ClearPass.

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 117).
   
   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 118**  *Importing a Network Device*

3. Enter the appropriate information in the **Network Device Details** dialog as described in Table 1.
Table 1: Specifying Network Device Details for Importing Devices

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Shared Secret</td>
<td>If using RADIUS, enter the RADIUS Shared Secret for the selected discovered device.</td>
</tr>
<tr>
<td>TACACS+ Shared Secret</td>
<td>If using TACACS+, enter the TACACS+ Shared Secret for the selected discovered device.</td>
</tr>
<tr>
<td>Override Vendor</td>
<td>Optionally, to override the discovered vendor type, select this check box.</td>
</tr>
<tr>
<td>Vendor</td>
<td>This field is displayed when you select Override Vendor. From the Vendor drop-down, select the name of the vendor type to override the discovered vendor type.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>Select this check box to enable RADIUS CoA (Change of Authorization).</td>
</tr>
<tr>
<td>RADIUS CoA Port</td>
<td>The default RADIUS CoA port is 3799. To change the RADIUS CoA port number, enter the new port number.</td>
</tr>
</tbody>
</table>

4. Click Import.
   The selected network device has been added to ClearPass. To see the network device listed, navigate to Configuration > Network > Devices.

Figure 119 Network Device Added to ClearPass

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 > Profile and Network Scan > Discovered Devices.
   The Discovered Devices page opens.
2. Click the name of the device of interest.
   The Network Device Details page opens.
3. When finished, click **Close**.

**Audit Viewer**

This section provides the following information:

- **Introduction**
- **Add Events**
- **Modify Events**
- **Remove Events**

**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, navigate to **Monitoring > Audit Viewer**.
To display detailed information about the selected event, click any row in the audit viewer. The Audit Row Details page opens (see Figure 122). 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 to display the Audit Row Details page.

Figure 122  Audit Row Details for Add Event
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 123** shows the Audit Row Details page for a Modify Event.

**Figure 123  Audit Row Details for Modify Event**

When you view a modify event, the Audit Row Details window contains the following three tabs:

**Table 1: Audit Row Details > Modify Event Page**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old Data</td>
<td>Displays a summary of details about the original data values.</td>
</tr>
<tr>
<td></td>
<td>■ The Profile section shows a summary of the profile values.</td>
</tr>
<tr>
<td></td>
<td>■ The Attributes section shows data about the original attributes and values.</td>
</tr>
<tr>
<td>New Data</td>
<td>Displays a summary of details about the new data values.</td>
</tr>
<tr>
<td></td>
<td>■ The Profile section shows a summary of the profile values.</td>
</tr>
<tr>
<td></td>
<td>■ The Attributes section shows data about the original attributes and values.</td>
</tr>
<tr>
<td>Inline Difference</td>
<td>Displays information about what changed. The information is color-coded to</td>
</tr>
<tr>
<td></td>
<td>indicate the following types of changes:</td>
</tr>
<tr>
<td></td>
<td>■ Modified</td>
</tr>
<tr>
<td></td>
<td>■ Added</td>
</tr>
<tr>
<td></td>
<td>■ Deleted</td>
</tr>
<tr>
<td></td>
<td>■ Moved up</td>
</tr>
<tr>
<td></td>
<td>■ Moved down</td>
</tr>
</tbody>
</table>
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](#)
- [Unsupported Admin Access Attempts Logged to 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.
- Export and import operations for all modules are captured in the Event Viewer. Any configuration items that can be imported or exported, such as services, enforcement profiles, endpoints, devices, and so on are logged.

**Unsupported Admin Access Attempts Logged to the Event Viewer**
If an attempt is made to access the ClearPassPolicy 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](#)).

If an attempt is made to access ClearPassPolicy 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 [Enabling Ingress Events Processing](#)).

To access the Event Viewer:

1. Navigate to **Monitoring > Event Viewer**. The **Event Viewer** page opens.
The following table describes the **Event Viewer** parameters:

**Table 1: Event Viewer Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Displays the source of the event. For example, <strong>Policy Manager UI</strong> or <strong>ClearPass Firmware Update Checker</strong>.</td>
</tr>
</tbody>
</table>
| 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. |
| 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**

To create an Event Viewer report using custom values:

1. Click the **+** icon. A new filter is added. You can add up to four filters.
2. In the **Filter** field, select the element on which you wish to filter:
   - Source
   - Level
   - Category
   - Action
   - Description
3. Specify **equals** or **contains**.
4. In the text field, enter the type of event for which you are searching.
5. (Optional) Create up to three additional filters if needed.
6. (Optional) Change the **Show records** value as desired.
7. Click **Go**. The following figure displays the **Event Viewer** report with custom values:

   **Figure 126**  *Event Viewer Report with Customized Filter*

![Event Viewer Report](image)

**Viewing Report Details**

To display the **System Event Details** page, click a row in the **Event Viewer** page.

**Figure 127**  *System Event Details Page*

![System Event Details](image)
The following table describes the **System Event Details** parameters:

**Table 2: System Event Details Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Displays the source of the event. For example, Admin UI, RADIUS, and SnmpService.</td>
</tr>
</tbody>
</table>
| Level     | Displays the level of the event from the following options:  
- INFO  
- WARN  
- ERROR |
| Category  | Displays the category of the event. For example, **Import, Export, 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 User, Role, Entity, Client IP Address, summary of the event, and when pertinent, 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 100**
- **Syslog Export Filters on page 595**
- **Live Monitoring: Analysis and Trending on page 134**
- **Live Monitoring: Accounting on page 115**

**Preconfigured Data Filters**

Policy Manager is preconfigured with the following data filters:

**Table 1: Access Tracker Edit Page Parameters**

<table>
<thead>
<tr>
<th>Data Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Requests</td>
<td>Shows all RADIUS requests.</td>
</tr>
<tr>
<td>TACACS Requests</td>
<td>Shows all TACACS requests.</td>
</tr>
<tr>
<td>WebAuth Requests</td>
<td>Shows all Web Authentication requests (requests originated from the Guest Portal).</td>
</tr>
<tr>
<td>Data Filter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Requests</td>
<td>Displays all event-based records.</td>
</tr>
<tr>
<td>Failed Requests</td>
<td>Shows all authentication requests that were rejected or failed.</td>
</tr>
<tr>
<td>Successful Requests</td>
<td>Shows all authentication requests that were successful.</td>
</tr>
<tr>
<td>Unhealthy Requests</td>
<td>Shows all requests that were not deemed healthy by Policy Manager.</td>
</tr>
<tr>
<td>Healthy Requests</td>
<td>Shows all requests that were deemed healthy by Policy Manager.</td>
</tr>
<tr>
<td>Guest Access Requests</td>
<td>Shows all requests—RADIUS or Web Authentication—where the user was assigned the built-in role Guest.</td>
</tr>
<tr>
<td>ClearPass Application Requests</td>
<td>Shows all Application session log requests.</td>
</tr>
<tr>
<td>All Requests</td>
<td>Shows all requests (without any rows filtered).</td>
</tr>
</tbody>
</table>

**Accessing the Data Filters Page**

To access the Data Filters page:

1. Navigate to Monitoring > Data Filters.

   The Data Filters page opens.

  **Figure 128 Data Filters Page**

**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 129** shows the Filter dialog when you choose Select Attributes.
2. Specify the Add Data Filters parameters as described in the following table.

**Table 2: Add Data Filters Page > Filter Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the data filter.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of this data filter (recommended).</td>
</tr>
<tr>
<td>Configuration Type</td>
<td>Choose one of the following configuration types:</td>
</tr>
<tr>
<td></td>
<td>- Select Attributes</td>
</tr>
<tr>
<td></td>
<td>- Specify Custom SQL</td>
</tr>
</tbody>
</table>

**Figure 129**  Add Data Filter > Filter Tab > Select Attributes

**Figure 130** shows the Filter dialog when you choose Specify Custom SQL.

**Figure 130**  Add Data Filter > Filter Tab > Specify Custom SQL

The complete Access Tracker query with custom SQL specified is:

```
LEFT OUTER JOIN tps.session_log_details t2 ON t2.session_id = t1.id WHERE t2.type = "" and t2.attr_name = "" and t2.attr_value = ""
```

The configuration details for the query are:

- **Name**: Filter for all RADIUS requests
- **Description**: Filter for all RADIUS requests
- **Configuration Type**: Specify Custom SQL
- **Custom SQL**: The complete Access Tracker query with custom SQL specified is:

```sql
LEFT OUTER JOIN tps.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:

```

AND (T1.stamp BETWEEN "START-TIME-1" AND (T1.stamp + INTERVAL "END-TIME-1"));
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Attributes</td>
<td>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.</td>
</tr>
<tr>
<td>Specify Custom SQL</td>
<td>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. <strong>NOTE:</strong> Aruba does not recommend that you enable this option without first consulting Support (navigate to Administration &gt; Support &gt; Contact Support).</td>
</tr>
</tbody>
</table>

**Rules Tab**

The Rules tab displays when you choose the Select Attributes configuration type on the Filter dialog.

**Figure 131  Add Data Filter > Rules Dialog**

Table 3 describes the Add Filter > Rules tab parameters:

**Table 3: Add Filter > Rules Tab**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Evaluation Algorithm</td>
<td><strong>Select ANY match</strong> is a logical OR operation of all the rules. <strong>Select ALL matches</strong> is a logical AND operation of all the rules.</td>
</tr>
<tr>
<td>Add Rule</td>
<td>Add a rule to the filter.</td>
</tr>
<tr>
<td>Edit Rule</td>
<td>Edit an existing rule.</td>
</tr>
<tr>
<td>Remove Rule</td>
<td>When you select an existing rule and click Remove Rule, the selected Rule is deleted immediately (no confirmation prompt appears).</td>
</tr>
</tbody>
</table>

When you click Add Rule or Edit Rule, the Dashboard Filter Rules Editor dialog opens.

**Figure 132  Dashboard Filters > Rules Editor**
Table 4 describes the **Dashboard Filters > Rules Editor** parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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**.
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.
**Figure 133  Blacklisted Users Page**

<table>
<thead>
<tr>
<th>#</th>
<th>MAC Address</th>
<th>User Name</th>
<th>Authorization Source</th>
<th>Bandwidth Limit</th>
<th>Session Duration</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>F80705B2BDC0</td>
<td>user1</td>
<td>Local User Repository</td>
<td>Exceeded</td>
<td>Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>2</td>
<td>7871EBB37F2D</td>
<td>user2</td>
<td>Guest User Repository</td>
<td>Not Exceeded</td>
<td>Not Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>3</td>
<td>0860C48574F8</td>
<td>user3</td>
<td>Guest Device Repository</td>
<td>Exceeded</td>
<td>Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>4</td>
<td>SF9D2A48E075</td>
<td>user4</td>
<td>Endpoints Repository</td>
<td>Not Exceeded</td>
<td>Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>5</td>
<td>BD2D33311837</td>
<td>user5</td>
<td>Onboard Devices Repository</td>
<td>Exceeded</td>
<td>Not Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>6</td>
<td>FE1A626D6581</td>
<td>user6</td>
<td>Admin User Repository</td>
<td>Not Exceeded</td>
<td>Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>7</td>
<td>0C241D928511</td>
<td>user7</td>
<td>Blacklist User Repository</td>
<td>Exceeded</td>
<td>Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>8</td>
<td>E7C2B90FF82</td>
<td>user8</td>
<td>Insight Repository</td>
<td>Not Exceeded</td>
<td>Not Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>9</td>
<td>FF928B10173</td>
<td>user9</td>
<td>Local User Repository</td>
<td>Not Exceeded</td>
<td>Not Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
<tr>
<td>10</td>
<td>0D9B40910CF3</td>
<td>user10</td>
<td>Guest User Repository</td>
<td>Not Exceeded</td>
<td>Exceeded</td>
<td>Aug 19, 2013 19:20:23 IST</td>
</tr>
</tbody>
</table>

Showing 1-11 of 11

Delete
This section provides the following information:

- Supported Authentication Methods on page 158
- Default Authentication Sources on page 158
- Adding and Modifying Authentication Methods on page 161
- Adding and Configuring Authentication Sources on page 184
- Modifying Authentication Methods or Sources for an Existing Service on page 218

### 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.

ClearPass Policy Manager supports the following authentication methods:

#### Tunneled EAP Authentication Methods

The tunneled EAP authentication methods are:

- 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

The non-tunneled authentication methods are:

- 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

### Default Authentication Sources

The following table describes the predefined ClearPass authentication sources that are part of the ClearPass local SQL database. These local authentication sources appear in brackets in the cannot be copied or deleted.
Table 1: Local Authentication Sources

<table>
<thead>
<tr>
<th>Authentication Source Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Admin User Repository]</td>
<td>Users are authenticated against this Policy Manager admin user database.</td>
</tr>
<tr>
<td>[Blacklist User Repository]</td>
<td>Blacklist database with users who have exceeded bandwidth or session related limits.</td>
</tr>
<tr>
<td>[Endpoints Repository]</td>
<td>Authenticate endpoints against the local Policy Manager database. This database supports the following filter categories: Authentication Status Profile Fingerprint MAC caching</td>
</tr>
<tr>
<td>[Guest Device Repository]</td>
<td>Authenticate guest devices against the local Policy Manager database. This database supports the following filter categories: Authentication Device Role ID</td>
</tr>
<tr>
<td>[Guest User Repository]</td>
<td>Authenticate guest users against the local Policy Manager database. This database supports the following filter categories: Authentication Authorization</td>
</tr>
<tr>
<td>[Insight Repository]</td>
<td>Insight database with session information for users and devices. This database supports the following filter categories: WebAuth check MAC caching Successful login count since midnight Active sessions Online status Daily duration Weekly duration Monthly duration</td>
</tr>
<tr>
<td>[Local User Repository]</td>
<td>Authenticate users against the Policy Manager local user database.</td>
</tr>
<tr>
<td>[Social Login Repository]</td>
<td>Authenticate users against Policy Manager social login database.</td>
</tr>
<tr>
<td>[Time Source]</td>
<td>Authorization source for implementing various time functions</td>
</tr>
</tbody>
</table>

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.

An authentication method is configurable only for some service types. For more information, see Configuring Other Policy Manager Services on page 59. 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 Manager then authenticates this entity against this authentication source. The flow is as follows:

- 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 the following components in sequence:

**Figure 134 Authentication and Authorization Flow of Control**

---

Adding and Modifying 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.
2. Click Add.
   The Add Authentication Method page opens.

3. Enter the name and description of the new authentication method.
4. From the Type drop-down, select the authentication type of authentication type.
5. Configure the Authentication Method of interest as described in the following sections:
   - [Authorize Authentication Method on page 163](#)
   - [CHAP Authentication Method on page 164](#)
   - [EAP-FAST Authentication Method on page 165](#)
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.
3. Modify the selected authentication method as necessary, then click **Save**.

**Figure 137** *Edit Authentication Method Page for EAP-FAST*

Authorize Authentication Method

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

To add the Authorize authentication method:

1. Navigate to **Configuration > Authentication > Methods**. The **Authentication Methods** page opens.
2. Click **Add**. The **Add Authentication Method** configuration dialog opens:
3. Specify the **Authorize Authentication Method** parameters as described in the following table:

**Table 2: Authorize Authentication Method Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the label of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select authentication method type <strong>Authorize</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

**CHAP Authentication Method**

Policy Manager includes the **Challenge-Handshake Authentication Protocol (CHAP)** authentication method. You can create one or more instances of the CHAP authentication method by assigning a customized name to each one. This method can also be associated to a service as an authentication method.

To add the CHAP authentication method:

1. Navigate to **Configuration > Authentication > Methods**. The **Authentication Methods** page opens.
2. Click **Add**. The **Add Authentication Method** configuration dialog opens:

**Figure 139 Adding CHAP Authentication Method**

3. Specify the **CHAP** authentication method parameters as described in the following table:
**Table 1: CHAP Authentication Method Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the CHAP authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select CHAP.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

**EAP-FAST Authentication Method**

EAP-FAST (Flexible Authentication through Secure Tunneling) is an authentication method that encrypts EAP transactions within a TLS (Transport Layer Security) tunnel. Use the **General, Inner Methods, PACs** and **PAC Provisioning** tabs to configure EAP-Fast authentication.

**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 140 Adding the EAP-FAST Authentication Method**

3. Configure the EAP-FAST authentication service as described in **Table 1** then click **Save**.
### Table 1: Specifying the EAP-FAST > General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select EAP-FAST.</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>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.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Caches EAP-FAST sessions on Policy Manager for reuse if the user/end-host reconnects to Policy Manager within the session-timeout interval. 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.</td>
</tr>
<tr>
<td>End-Host Authentication</td>
<td>Specify one of the following end-host authentication methods:</td>
</tr>
<tr>
<td></td>
<td>- Using PACs (Protected Access Credentials)</td>
</tr>
<tr>
<td></td>
<td>- Using Client Certificate</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The PACs and PAC Provisioning tabs are available only when you select Using PACs.</td>
</tr>
<tr>
<td>Certificate Comparison</td>
<td>Specify one of the following Certificate Comparison actions:</td>
</tr>
<tr>
<td></td>
<td>- Do not compare</td>
</tr>
<tr>
<td></td>
<td>- Compare Distinguished Name (DN)</td>
</tr>
<tr>
<td></td>
<td>- Compare Common Name (CN)</td>
</tr>
<tr>
<td></td>
<td>- Compare Subject Alternative Subject Name (SAN)</td>
</tr>
<tr>
<td></td>
<td>- Compare CN or SAN</td>
</tr>
<tr>
<td></td>
<td>- Compare Binary</td>
</tr>
</tbody>
</table>

### Table 2: Specifying the EAP-FAST > General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select EAP-FAST.</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Inner Methods Tab

The following figure displays the **EAP-FAST > Inner Methods** dialog:

**Figure 141  EAP-FAST Authentication Method > Inner Methods Dialog**

In FIPS mode, the EAP-MD5 authentication method is not supported.
Table 3: EAP-FAST > Inner Methods Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Specify inner authentication methods in the preferred order | 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 (Protected Access Credential) Tab

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

Figure 142 EAP_FAST PACs Dialog

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 143**  *EAP_FAST PAC Provisioning Dialog*

1. Configure the PAC Provisioning parameters as described in Table 4.
2. When finished, click **Save**.

**Table 4: EAP_FAST PAC Provisioning Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| 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 the Policy Manager certificate. | |
### EAP-GTC Authentication Method

EAP-GTC (Generic Token Card) 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 144** *Edit EAP-GTC Authentication Method*
3. Specify the **EAP-GTC General** parameters as described in the following table, then click **Save**.

**Table 1: EAP-GTC Authentication Method Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>If necessary, specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>EAP-GTC</strong> is preselected.</td>
</tr>
</tbody>
</table>

**Method Details**

| Challenge | Optionally, specify a password. |

**EAP-MSCHAPv2**

MS-CHAPv2 is an authentication protocol that Microsoft introduced with NT4.0 SP4 and Windows 98. The inner authentication protocol is Microsoft’s CHAP (Challenge Handshake Authentication Protocol), meaning it allows authentication to databases that support the MS-CHAPv2 format, including Microsoft NT and Microsoft Active Directory.

To add the EAP-MSCHAPv2 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:

**Figure 145  Adding the EAP-MSCHAPv2 Authentication Method**

3. Specify the **EAP-MSCHAPv2** parameters as described in the table below, then click **Save**.

**Table 1: EAP-MSCHAPv2 Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>EAP-MSCHAPv2</strong>.</td>
</tr>
</tbody>
</table>
**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.

Use the **General** and **Inner Methods** tabs to configure EAP-PEAP authentication.

**General Tab**

To add the EAP-PEAP 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:

   ![Add Authentication Method Dialog](image)

3. Specify the **EAP-PEAP > General** parameters as described in the following table, then click **Save**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>EAP-PEAP</strong>.</td>
</tr>
</tbody>
</table>

**Table 1: EAP-PEAP > General Parameters**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Resumption</td>
<td>Check the <strong>Session Resumption</strong> check box if you intend to enable <strong>Fast Reconnect</strong>.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Caches EAP-PEAP sessions on the ClearPass server for reuse if the user/client reconnects to the ClearPass server within the session timeout interval. If session timeout value is set to 0, the cached sessions are not purged.</td>
</tr>
<tr>
<td>Fast Reconnect</td>
<td>Enable this check box to allow fast reconnect. When <strong>Fast Reconnect</strong> is enabled, the inner method that takes place inside the server authenticated outer tunnel is also bypassed. This makes the process of reauthentication faster. For <strong>Fast Reconnect</strong> to work, session resumption must be enabled.</td>
</tr>
<tr>
<td>Microsoft NAP Support</td>
<td>Check this check box to enable Network Access Protection (NAP) on this ClearPass server.</td>
</tr>
</tbody>
</table>
| Cryptobinding      | Cryptobinding protects tunnel methods against man-in-the-middle attacks. Cryptographic binding focuses on protecting the server rather than the peer. Specify one of the following cryptobinding options:  
  - None (the default)  
  - Optional  
  - Required |

**Inner Methods Tab**

The tunneled method is frequently referred to as the "inner method." The **Inner Methods** tab controls the inner methods for the **EAP-PEAP** authentication method.

**Figure 147  EAP-PEAP > Inner Methods Tab**

---

**NOTE**

In FIPS mode, the EAP-MD5 authentication method is not supported.
Specify the **EAP-PEAP Inner Methods** parameters as described in the following table:

**Table 2: EAP-PEAP Inner Methods Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Specify inner authentication methods in the preferred order | 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 ClearPass sends in priority order until negotiation succeeds. Select any method available in the current context from the drop-down list. Inner methods available include:  
  - Aruba EAP-GTC  
  - EAP-GTC  
  - EAP-MD5  
  - EAP-MSCHAPv2  
  - EAP-PWD  
  - EAP-TLS with OSCP enabled  
  - EAP-TLS |
| Default | To set an inner method as the default (the method tried first), select it and click **Default**. |
| Remove | To remove an inner method from the displayed list, select the method and click **Remove**. |

**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.

Use the **General** and **Inner Methods** tabs to configure EAP-Peap authentication.

**General**

The **General** tab labels the authentication method and defines session details. To add the EAP-PEAP 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.
3. In the **Type** field, select **EAP-PEAP**.
The following figure is an example of the **EAP-PEAP-Public - General** tab:

**Figure 148  EAP-PEAP-Public - General Tab**

```plaintext
Add Authentication Method

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Specify the type of authentication. In this context, select EAP-PEAP-Public.</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>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.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>
```

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

**Table 1: EAP-PEAP-Public - General Tab Parameters**

```plaintext
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Specify the type of authentication. In this context, select EAP-PEAP-Public.</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>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.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>
```
### 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 149  EAP-PEAP-Public - Inner Methods Tab**

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 2: EAP-PEAP-Public Inner Methods Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 (Password) is an EAP authentication method that 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.

To add the EAP-PWD authentication method:

1. Navigate to **Configuration > Authentication > Methods**. The **Authentication Methods** page opens.
2. Select the **Add** link. The **Add Authentication Method** dialog opens:

   **Figure 150  EAP-PWD Authentication Method Configuration Dialog**

3. Specify the **EAP-PWD** parameters as described in the following table, then click **Save**.
**Table 1: EAP-PWD Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select EAP-PWD.</td>
</tr>
</tbody>
</table>

**Method Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>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).</td>
</tr>
<tr>
<td>Server ID</td>
<td>Specify the string that identifies the ClearPass server to the peer.</td>
</tr>
</tbody>
</table>

**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:

2. Click Add. The Add Authentication Method dialog opens.

**Figure 151 EAP-TLS Authentication Method Dialog**
3. Specify the **Add Authentication Method** parameters as described in the following table, then click **Save**.

**Table 1: EAP_TLS Authentication Method Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method (recommended).</td>
</tr>
<tr>
<td><strong>Method Details</strong></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>EAP_TLS</strong>.</td>
</tr>
<tr>
<td>Session Resumption</td>
<td>Enable this option to cache EAP-TLS sessions on the ClearPass server for reuse if the user or client reconnects to the ClearPass server within the session timeout interval. This option is enabled by default.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Specify the duration in hours for the cached EAP-TLS sessions to be retained. The default is 6 hours.</td>
</tr>
<tr>
<td>Authorization Required</td>
<td>This parameter is enabled by default. Specify whether to perform an authorization check.</td>
</tr>
<tr>
<td>Certificate Comparison</td>
<td>Specify the type of certificate comparison (identity matching) upon presenting Policy Manager with a client certificate:</td>
</tr>
<tr>
<td></td>
<td>- To skip the certificate comparison, choose <strong>Do not compare</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To compare specific attributes, choose <strong>Compare Common Name (CN)</strong>, <strong>Compare Subject Alternate Name (SAN)</strong>, or <strong>Compare CN or SAN</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To perform a binary comparison of the stored (in the client record in Active Directory or another LDAP-compliant directory) and presented certificates, choose <strong>Compare Binary</strong>.</td>
</tr>
<tr>
<td>Verify Certificate using OCSP</td>
<td>- If the certificate is to be verified by the Online Certificate Status Protocol (OCSP), select <strong>Optional</strong> or <strong>Required</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To not verify the certificate, select <strong>None</strong>.</td>
</tr>
<tr>
<td></td>
<td>- If an OCSP server is not accessible to perform certificate validation, you can skip the OCSP check and proceed with the CRL validation result by selecting <strong>Required (CRL fallback)</strong>.</td>
</tr>
<tr>
<td>Override OCSP URL from the Client</td>
<td>Select this option to use a different URL for OCSP. After this option is enabled, you can enter a new URL in the <strong>OCSP URL</strong> field.</td>
</tr>
<tr>
<td>OCSP URL</td>
<td>If the <strong>Override OCSP URL from the Client</strong> field is enabled, enter the replacement URL.</td>
</tr>
</tbody>
</table>

**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.

Use the **General** and **Inner Methods** tabs to configure the **EAP-TTLS** authentication method.

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

1. Navigate to **Configuration > Authentication > Methods**. The **Authentication Methods** page opens.
2. Select the **Add** link. The **Add Authentication Method** dialog opens:

**Figure 152  EAP-TTLS - General Tab**

3. Specify the **EAP-TTLS** parameters as described in the table below, then click **Save**.

**Table 1: EAP-TTLS - General Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of authentication. In this context, select <strong>EAP-TTLS</strong>.</td>
</tr>
<tr>
<td><strong>NOTE</strong>: The EAP-MD5 authentication type is not supported if you use ClearPass Policy Manager in the FIPS (Administration &gt; Server Manager &gt; Server Configuration &gt; FIPS tab) mode.</td>
<td></td>
</tr>
</tbody>
</table>

**Method Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Resumption</td>
<td>Caches EAP-TTLS sessions on Policy Manager for reuse if the user/client reconnects to Policy Manager within the session timeout interval.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Specify the duration in hours for the EAP-TTLS sessions to be cached.</td>
</tr>
</tbody>
</table>

**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 153  EAP_TTLS - Inner Methods Tab**

![Edit Authentication Method](image)

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

**Table 2: EAP-TTLS - Inner Methods Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Specify inner authentication methods in the preferred order | Select any method available in the current context from the drop-down list.  
- 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](image)) 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. To add the MAC-AUTH 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.
3. In the **Type** field, select **MAC-AUTH**.

The following figure is an example of the **MAC-AUTH > General** dialog:

**Figure 154 Adding MAC-AUTH Authentication Method**

![Example of the General tab](image)

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method (recommended).</td>
</tr>
<tr>
<td>Type</td>
<td>Select the <strong>MAC-AUTH</strong> type of authentication.</td>
</tr>
<tr>
<td><strong>Method Details</strong></td>
<td></td>
</tr>
<tr>
<td>Allow Unknown End-Hosts</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

To add the MSCHAP 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.
3. In the **Type** field, select **MSCHAP**.
The following figure is an example of the **MSCHAP - General** tab:

**Figure 155  MSCHAP - General Tab**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication method.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication method.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of authentication. In this context, select <strong>MSCHAP</strong>.</td>
</tr>
</tbody>
</table>

**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.

To add the PAP 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.
3. In the **Type** field, select **PAP**.
displays the Add Authentication Method > PAP dialog.

**Figure 156  Adding the PAP Authentication Method**

| **Table 1** describes the PAP parameters: |
| **Table 1**: PAP 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 PAP as the Type of authentication. |

**Method Details**

| Enable Aruba-SSO | 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**. The Authentication Sources page opens.
2. Click the **Add** link. The **Add** Authentication Sources page opens. Different tabs and fields appear, depending on the authentication source selected.

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

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).
The 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 246.

**Configure Generic LDAP and Active Directory authentication sources**

Use the following tabs to configure new Generic LDAP and Active Directory authentication sources:

**General Configuration**

To add a new Generic LDAP or Active Directory authentication source:

1. Navigate to **Configuration > Authentication > Sources**. The **Authentication Sources** page opens.
2. Click **Add**. The **Add Authentication Sources** dialog opens. In this example, **Type** is set to **Active Directory**.

**Figure 159 Active Directory or Generic LDAP Configuration Dialog**

3. Specify the **Generic Active Directory** or **LDAP > General** parameters as described in the following table.

**Table 1: Active Directory or Generic LDAP Authentication Source> General Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the authentication source.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication source (recommended).</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Active Directory</strong> or <strong>Generic LDAP</strong>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use for Authorization</td>
<td>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 checked (enabled) by default.</td>
</tr>
</tbody>
</table>
| 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          | The Policy Manager server will automatically time out if the Active Directory or LDAP authentication source fails to send a response to an authorization query after 10 seconds. To specify a different duration for the timeout, enter the preferred timeout value in the Server Timeout field.  
|                         | 1. 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 were 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.  
|                         | NOTE: ClearPass logs an alert message in the Event Viewer if the primary Active Directory/LDAP server of an authentication source for RADIUS and TACACS+ authentication fails over to a designated backup server. |

2. Click **Next** to continue to the **Primary** tab.

**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 160**  *Generic LDAP or Active Directory > Primary Tab*

Specify the **Active Directory** or **Generic LDAP > Primary** parameters as described in the following table:

**Table 2: Active Directory or Generic LDAP > Primary Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Specify the hostname or the IPv4/IPv6 address of the LDAP or Active Directory server.</td>
</tr>
</tbody>
</table>
| 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.  
**NOTE:** In a production environment, security is a concern because when ClearPass binds to an LDAP server, it submits the username and password for that account over the network under clear text unless you protect it using Connection Security and set the port to **636**.  
**NOTE:** To ensure successful authentication, be sure to add the CA certificate of the LDAP server to the Certificate Trust List. |
| 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 (Distinguished 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). |
Table 2: Active Directory or Generic LDAP > Primary Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Password</td>
<td>Specify the password for the administrator DN entered in the <strong>Bind DN</strong> field.</td>
</tr>
<tr>
<td>NetBIOS Domain Name</td>
<td>Specify the Active Directory domain name for this server. <strong>Policy Manager</strong> prepends this name to the user ID to authenticate users found in this Active Directory. <strong>NOTE</strong>: This setting is available only for Active Directory.</td>
</tr>
</tbody>
</table>
| 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.  
2. Navigate to the DN that you want to use as the base DN.  
3. To select a node as a base DN, click the preferred node in the tree structure that is displayed.  
**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 Referrals             | 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. |
| User Certificate           | Enter the name of the attribute in the user record from which the 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. |

4. Click **Next** to continue to the **Attributes** tab.

**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** tabs:
The Attributes tab displays the following information for the filters applied to the Generic LDAP Directory or Active Directory authentication source.

**Table 3: Active Directory or Generic LDAP Attributes tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Name of the filter.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Name of the LDAP or Active Directory attributes defined for this filter.</td>
</tr>
<tr>
<td>Alias Name</td>
<td>Alias name for each attribute name selected for the filter.</td>
</tr>
<tr>
<td>Enable As</td>
<td>Indicates 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.</td>
</tr>
</tbody>
</table>

The following table describes the default filters for the Active Directory/Generic LDAP directories.

You can select any filters in the Attributes tab to modify the parameters of that filter. For details, see Modifying Default Filters.
<table>
<thead>
<tr>
<th>Directory</th>
<th>Default Filters</th>
</tr>
</thead>
</table>
| Active Directory   | - **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 attribute can have multiple values.  
  - `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` attribute. 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 on-boarded user.  
  - **Onboard Device Owner Group**: This is the filter 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` attribute. The attribute fetched with this filter query is `cn`, which is the name of the Onboard group.                                                                                                                                                                                                                   |
| Generic LDAP Directory | - **Authentication**: This is the filter used for authentication:  
  `{objectClass=*} (uid=%{Authentication:Username})`  
  When a request arrives, Policy Manager populates `%{Authentication:Username}` with the authenticating user or machine. This filter is also set up to fetch the following attributes based on this filter query:  
  - `dn` (aliased to UserDN): This is an internal attribute that is populated with the user record's DN.  
  - **Group**: This is the filter used for retrieving the name of the groups to which a user belongs.  
    `{objectClass=groupOfNames} (member=%{UserDN})`  
    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`).                                                                                                                                                                                                                     |
<table>
<thead>
<tr>
<th>Directory</th>
<th>Default Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add More Filters</td>
<td>Click this button to open the <strong>Authentication Sources &gt; Add</strong> page to open the <strong>Configure Filter</strong> page. From this page, you can define a filter query and the related attributes to be fetched. For more information, see <a href="#">Generic LDAP and Active Directory</a>.</td>
</tr>
</tbody>
</table>

**Configuration Summary**

Use the **Summary** tab to see a summarized view of the parameters configured in the **General**, **Primary**, and **Attributes** tab.

**Adding and Managing Generic LDAP and Active Directory Filters**

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. The **Filter** tab provides an LDAP browser interface to define the filter search query. 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.

To view or configure filters, navigate to the **Configuration > Authentication > Sources > Add** page, and define an LDAP or Active Directory authentication source according to the procedures described in the previous steps. The **Attributes** tab on the **Configuration > Authentication > Sources > Add** page includes the **Add More Filters** button, which opens the Configure Filters dialog. The four tabs on the **Configure Filter** page allow you to browse the nodes in the Active Directory or LDAP directory, and create and manage filters.

**Browse Tab Settings**

By default, The **Configure Filter** page opens on the **Browse** tab, which allows you to browse the nodes in the Active Directory or LDAP 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.

**Figure 163**  **Configure Filter > Browse** configuration dialog for Active Directory or Generic LDAP authentication sources:
Specify the Active Directory or Generic LDAP Configure **Configure Filter > Browse** tab parameter as described in the following table:

**Table 5: Configure Filter > Browse Actions for Active Directory or Generic LDAP Authentication Sources**

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find Node</td>
<td>To find the node, enter the DN, then click the <strong>Go</strong> button.</td>
</tr>
</tbody>
</table>

**Filters Tab Settings**

Use this tab to view existing filters, or create new ones

**Viewing Existing Filters**

The following figure is an example of the **Configure Filter > Filter** configuration dialog for Active Directory or Generic LDAP authentication sources:

**Figure 164 Configure Filter > Filter configuration dialog for Active Directory or Generic LDAP Authentication Sources**
The following table describes the Configure Filter > Filter tab parameters:

Table 6: Configure Filter > Filter parameters for Active Directory or Generic LDAP Authentication Sources

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find Node</td>
<td>To find a node, enter the DN, then click the Go button.</td>
</tr>
<tr>
<td>Select the attributes for filter</td>
<td>This table has Name and Value columns. You can enter the attribute name in the following ways:</td>
</tr>
<tr>
<td></td>
<td>- By selecting a node, inspecting the attributes, and then manually entering the attribute name by clicking on Click to add... in the table row.</td>
</tr>
<tr>
<td></td>
<td>- By selecting an attribute on the right-hand side of the LDAP browser. The attribute name and value are automatically populated in the table.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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 Tab Settings

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.
The following figure displays the Active Directory or Generic LDAP Configure Filter > Attributes tab:

**Figure 165  Configure Filter > Attributes** Configuration Dialog for Active Directory or Generic LDAP Authentication Sources

![Configure Filter > Attributes Configuration Dialog](image)

Specify the **Active Directory/LDAP Configure Filter Page > Attributes** tab parameters as described in the following table:

**Table 7: Configure Filter > Attributes Settings for Active Directory or Generic LDAP Authentication Sources**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter values for parameters</td>
<td>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 <code>%{Authentication:Username}</code> in the filter query, you are prompted to enter the value for it. You can enter wildcard character (<em>) here to match all entries. <strong>NOTE:</strong> If there are thousands of entries in the directory, entering the wildcard character (</em>) can take a while to fetch all matching entries.</td>
</tr>
<tr>
<td>Execute</td>
<td>1. After entering the values for all dynamic parameters, click <strong>Execute</strong> to execute the filter query. You can see all entries that match the filter query. 2. Click one of the entries (nodes) to view the list of attributes for that node. 3. Click the attribute names that you want to use as role-mapping attributes.</td>
</tr>
<tr>
<td>Name</td>
<td>Specify the name of the attribute.</td>
</tr>
<tr>
<td>Alias Name</td>
<td>Specify the alternative name for the attribute. By default, this is the same as the attribute name.</td>
</tr>
<tr>
<td>Enable As</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Configuration Tab Settings**

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.

**Figure 166 Configure Filter > Configuration Dialog for Active Directory or Generic LDAP Authentication Sources**

![Configure Filter](image)

### Modifying 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.

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 167 Modifying Default filters for Active Directory or Generic LDAP authentication sources:**

![Configure Filter](image)
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.

**Generic SQL DB**

Configure the primary and backup servers, session details, filter query, and role-mapping attributes to fetch the Generic SQL authentication sources. ClearPass Policy Manager can perform MSCHAPv2 and PAP/GTC authentication against any Open Database Connectivity (ODBC)-compliant SQL database such as Microsoft SQL Server, Oracle, or PostgreSQL.

*NOTE* The MySQL database is not supported in ClearPass 6.7.x and later. MySQL has been replaced by Maria-DB Connector.

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

**General Tab**

1. Navigate to the **Configuration > Authentication > Sources**, then click **Add**. The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details.

**Figure 168 Add Generic SQL DB > General Tab**

2. Specify the **Add General SQL DB > General** parameters as described in the following table.
Table 1: Add Generic SQL DB > General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication source.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication source.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Generic SQL DB.</td>
</tr>
<tr>
<td>Use for Authorization</td>
<td>Enable this option to request Policy Manager to fetch role-mapping attributes (or authorization attributes) from this authentication source.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Authorization Sources</td>
<td>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.</td>
</tr>
<tr>
<td>Backup Servers</td>
<td>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.</td>
</tr>
<tr>
<td>Cache Timeout</td>
<td>Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the time period for which the attributes are cached.</td>
</tr>
</tbody>
</table>

Primary Tab

The Primary tab defines the settings for the primary server.

Figure 169 Add Generic SQL DB > Primary Tab
Specify the **Generic SQL DB > Primary** parameters as described in the following table:

**Table 3: Generic SQL DB > Primary Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Enter the Fully Qualified Domain Name (FQDN) or the IPv4/IPv6 address of the database server.</td>
</tr>
<tr>
<td>Port (Optional)</td>
<td>Specify a port value to override the default port.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Enter the name of the database from which records can be retrieved.</td>
</tr>
<tr>
<td>Login Username</td>
<td>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.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the user account entered in the Login Username field.</td>
</tr>
<tr>
<td>Timeout</td>
<td>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).</td>
</tr>
</tbody>
</table>
| ODBC Driver        | Select the ODBC (Open Database Connectivity) driver to connect to the database:  
  - PostgreSQL  
  - Oracle 11g  
  - MariaDB  
  - MSSQL  
  **NOTE:** MySQL is no longer supported for ClearPass 6.7.x and later. MySQL has been replaced by Maria-DB Connector (MariaDB).  
  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 following characters are supported:  
  - Backslash (\)  
  - At-sign (@)  
  - Hyphen  
  - Underscore |
| 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 Algorithm (SHA) hash.  
  - SHA256: Stored with an SHA-256 hash function.  
  - MD5 |

**Attributes Tab**

The **Attributes** tab defines the SQL DB query filters and the attributes to be fetched by using those filters.
Figure 170  *Generic SQL DB > Attributes Tab*

![Generic SQL DB > Attributes Tab](image)

Viewing Existing Filters

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Specifies the name of the filter.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Specifies the name of the SQL DB attributes defined for this filter.</td>
</tr>
<tr>
<td>Alias Name</td>
<td>Specifies an alias name for each attribute name selected for the filter.</td>
</tr>
<tr>
<td>Enabled As</td>
<td>Indicates whether the filter is enabled as a role or attribute type. This can also be blank.</td>
</tr>
<tr>
<td>Add MoreFilters</td>
<td>Click this button to open the <strong>Configure Filter</strong> page. Use this page to define a filter query and the related attributes to be fetched from the SQL DB store. <strong>Figure 171</strong> displays the <strong>Generic SQL DB &gt; Configure Filter</strong> page.</td>
</tr>
</tbody>
</table>

Adding More Filters

To add more filter queries and their related attributes:
1. Click **Add More Filters**. The **Configure Filter** page opens:

Figure 171  *Generic SQL DB > Configure Filter Page*

![Configure Filter Page](image)
2. Select **Click to add**. A new row opens.
3. Specify the **Name** of the filter, **Alias Name**, **Data Type**, and optionally, **Enabled As** attributes.
4. Repeat to add additional filters, then click **Save**.
5. Specify the **Add Generic SQL DB > Configure Filter** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Enter the name of the filter.</td>
</tr>
<tr>
<td>Filter Query</td>
<td>Specify an SQL query to fetch the attributes from the user or device record in DB.</td>
</tr>
<tr>
<td>Name</td>
<td>Specify the name of the attribute.</td>
</tr>
<tr>
<td>Alias Name</td>
<td>Specify the name for the attribute. By default, this is the same as the attribute name.</td>
</tr>
<tr>
<td>Data Type</td>
<td>Specify the data type for this attribute such as String, Integer, or Boolean.</td>
</tr>
<tr>
<td>Enabled As</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Summary Tab**

Use the **Summary** tab to view the Generic SQL DB authentication source configuration.

**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.

To configure an authentication source for an HTTP service:

1. Navigate to **Configuration > Authentication > Sources**. The **Authentication Sources** page opens.
2. Click the **Add** link. The **Add Authentication Sources** page opens.
3. Configure primary and backup servers, session details, filter query, and role mapping attributes to fetch HTTP authentication sources.

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

**Figure 172** HTTP > General Tab

Specify the **HTTP > General** tab parameters as described in the following table:

**Table 1: HTTP > General Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication source.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication source.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of source. In this context, select <strong>HTTP</strong>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use for Authorization</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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. The default authorization sources are as follows:  
  - [Blacklist User Repository] [Local]  
  - [Endpoints Repository] [Local]  
  - [Guest Device Repository] [Local]  
  - [Guest User Repository] [Local]  
  - [Insight Repository] [Local]  
  - [Local User Repository] [Local]  
  - [Multi-Master Cache Repository] [HTTP]  
    This authorization source of type HTTP fetches the store numbers list attribute stored in the Multi-Master Cache against the local host.  
  - [Onboard Devices Repository] [Local]  
  - [Social Login Repository] [Local]  
  - [Time Source] [Local]  
  **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. To remove a backup server, select the server name and click Remove. Select Move Up or Move Down to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.

**Primary Tab**

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

**Figure 173** HTTP > Primary Tab
Specify the **HTTP > Primary** tab parameters as described in the following table:

**Table 6: HTTP > Primary Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base URL</td>
<td>Enter the base URL (host name) or IP address of the HTTP server. For example, http://&lt;hostname&gt; or &lt;fully-qualified domain name&gt;:xxxx, where xxxx is the port to access the HTTP server.</td>
</tr>
<tr>
<td>Login Username</td>
<td>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.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the user account entered in the <strong>Login Username</strong> field.</td>
</tr>
</tbody>
</table>

**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 the **HTTP > Attributes** tab parameters as described in the following table:

**Table 7: HTTP > Attributes tab (Filter List) Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Displays the name of the filter.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Specifies the name of the SQL DB attributes defined for this filter.</td>
</tr>
<tr>
<td>Alias Name</td>
<td>Specifies the name of an alias name for each attribute name selected for the filter.</td>
</tr>
<tr>
<td>Enabled As</td>
<td>Indicates whether an attribute is enabled as a role.</td>
</tr>
<tr>
<td>Add More Filters</td>
<td>Opens the <strong>Configure Filter</strong> page. For more information, see <a href="#">Add More Filters on page 205</a>.</td>
</tr>
</tbody>
</table>
Add More Filters

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

**Figure 175  HTTP Filter Configure Page**

![Configure Filter Page](image)

Specify the **HTTP Configure > Filter** parameters as described in the following table:

**Table 8: HTTP Configure Filter Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Enter the name of the selected filter.</td>
</tr>
<tr>
<td>Filter Query</td>
<td>Specify 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://&lt;hostname or fqdn&gt;:xxxx/abc/def/xyz, where you enter /abc/def/xyz.</td>
</tr>
<tr>
<td>Name</td>
<td>Specify the name of the attribute.</td>
</tr>
<tr>
<td>Alias Name</td>
<td>Specifies the alias name for the attribute. By default, this is the same as the attribute name.</td>
</tr>
<tr>
<td>Data Type</td>
<td>Specifies the data type for this attribute such as String, Integer, and Boolean.</td>
</tr>
<tr>
<td>Enabled As</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Summary Tab**

You can use the **Summary** tab to view configured parameters.

**Kerberos**

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

To configure an authentication source for a Kerberos service:

1. Navigate to **Configuration > Authentication > Sources**. The **Authentication Sources** page opens.
2. Click the **Add** link. The **Add Authentication Sources** page opens.

**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 176  Kerberos > General Tab**

<table>
<thead>
<tr>
<th>Authentication Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Type:</td>
</tr>
<tr>
<td>Use for Authorization:</td>
</tr>
<tr>
<td>Authorization Sources:</td>
</tr>
<tr>
<td>Backup Servers Priority:</td>
</tr>
</tbody>
</table>

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

**Table 1: Kerberos > General Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication source.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication source.</td>
</tr>
<tr>
<td>Type</td>
<td>From the <strong>Type</strong> drop-down, select <strong>Kerberos</strong>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use for Authorization</td>
<td>Leave disabled in this context.</td>
</tr>
<tr>
<td>Authorization Sources</td>
<td>Specify one or more authorization sources from which role-mapping attributes are to be fetched.</td>
</tr>
<tr>
<td></td>
<td>1. Select an authentication source from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add</strong> to add it to the list of authorization sources.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Remove</strong> to remove the selected authentication source from the list.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can specify additional authorization sources at the service level. Policy</td>
</tr>
<tr>
<td></td>
<td>Manager fetches role-mapping attributes irrespective of which authentication source the</td>
</tr>
<tr>
<td></td>
<td>user or device was authenticated against.</td>
</tr>
<tr>
<td>Backup Servers</td>
<td>1. To add a backup Kerberos server, click <strong>Add Backup</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Backup</strong> 1 tab, you can specify connection details for a backup server</td>
</tr>
<tr>
<td></td>
<td>(same fields applicable for primary server specified below).</td>
</tr>
<tr>
<td></td>
<td>▪ To remove a backup server, select the server name and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td></td>
<td>▪ Select <strong>Move Up</strong> or <strong>Move Down</strong> to change the server priority of the backup servers.</td>
</tr>
<tr>
<td></td>
<td>This is the order in which Policy Manager attempts to connect to the backup servers.</td>
</tr>
</tbody>
</table>

**Primary Tab**

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

**Figure 177  Kerberos > Primary Tab**
The following table describes the Kerberos > Primary parameters:

Table 9: Kerberos > Primary Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Specify the name of the host or the IP address of the Kerberos server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port at which the token server listens for kerberos connections. The default port is 88.</td>
</tr>
<tr>
<td>Realm</td>
<td>Specify the Kerberos domain.</td>
</tr>
<tr>
<td>Service Principal Name</td>
<td>Enter the identity of the service principal as configured in the Kerberos server.</td>
</tr>
<tr>
<td>Service Principal Password</td>
<td>Enter the password for the service principal.</td>
</tr>
</tbody>
</table>

Summary Tab

Use the Summary tab to view the authentication source configuration.

Okta

You can use Okta as an authentication source only for servers of the type Aruba Application Authentication.

To configure an authentication source for an Okta service:

1. Navigate to Configuration > Authentication > Sources. The Authentication Sources page opens.
2. Click the Add link. The Add Authentication Sources page opens.

General Tab

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

Figure 178 Okta > General Tab
3. Specify the **Okta > General** parameters as described in the following table:

### Table 1: Okta > General Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication source.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication source.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Okta</strong>.</td>
</tr>
<tr>
<td>Use for Authorization</td>
<td>Enable this check box to request Policy Manager to fetch role mapping attributes (or authorization attributes) from this authentication source.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Specify the duration in number of seconds that Policy Manager waits before considering this server unreachable.</td>
</tr>
<tr>
<td></td>
<td>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 the backup servers in the order in which they are configured.</td>
</tr>
<tr>
<td>Cache Timeout</td>
<td>Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.</td>
</tr>
<tr>
<td>Backup Servers Priority</td>
<td>1. To add a backup serve, click <strong>Add Backup</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Backup 1</strong> tab, you can specify connection details for a backup server (same fields as for primary server that are specified below).</td>
</tr>
<tr>
<td></td>
<td>■ To remove a backup server, select the server name and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ Select <strong>Move Up</strong> or <strong>Move Down</strong> to change the server priority of the backup servers. This is the order in which Policy Manager attempts to connect to the backup servers.</td>
</tr>
</tbody>
</table>

**Primary Tab**

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

**Figure 179  Okta > Primary Tab**
Specify the **Okta > Primary** parameters as described in the following table:

**Table 10: Okta > Primary Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Details</strong></td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>Enter the address of the Okta server.</td>
</tr>
<tr>
<td>Authorization Token</td>
<td>Enter the authorization token provided by Okta support.</td>
</tr>
</tbody>
</table>

**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 180 Okta > Attributes Tab**

Specify the **Okta > Attributes** parameters as described in the following table:

**Table 11: Okta - Attributes Tab Parameters**

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

**Adding Filters**

To add a filter:

1. Click the **Add More Filters** button.

   The **Configure Filter** page opens. This page defines a filter query and the related attributes to be fetched from the SQL DB store.
Specify the **Okta Configure Filter** parameters as described in the following table:

**Table 12: Okta Configure Filter Page**

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

**Summary Tab**

Use the **Summary** tab to view the Okta authentication source configuration.

**RADIUS Server**

You can use the **RADIUS Server** as an authentication source to allow ClearPass to query a third-party **RADIUS Server** for authentication.

To configure an authentication source for a RADIUS service:

1. Navigate to **Configuration > Authentication > Sources**. The **Authentication Sources** page opens.
2. Click the **Add** link. The **Add Authentication Sources** page opens.
The **General** tab labels the authentication source and defines session details, authorization sources, and backup server details.

**Figure 182  RADIUS Server > General Tab**

Specify the **RADIUS Server > General** parameters as described in the following table:

**Table 1: RADIUS Server > General Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the authentication source.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication source.</td>
</tr>
<tr>
<td>Type</td>
<td>From the Type drop-down, select <strong>RADIUS Server</strong>.</td>
</tr>
<tr>
<td>Use for Authorization</td>
<td>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, Policy Manager also fetches role-mapping attributes from the same source if the <strong>Use for Authorization</strong> field is enabled. This check box is enabled by default.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>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 the backup servers in the order in which they are configured.</td>
</tr>
</tbody>
</table>
| Backup Servers Priority    | 1. Click **Add Backup** to add a backup server.  
2. 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.

**Figure 183**  
*RADIUS Server > Primary Tab*

<table>
<thead>
<tr>
<th><strong>Table 13: RADIUS Server - Primary Tab Parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Connection Details</strong></td>
</tr>
<tr>
<td>Server Names</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Secret</td>
</tr>
</tbody>
</table>

**Attributes Tab**

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

**Figure 184**  
*RADIUS Server > Attributes Tab*
Specify the **RADIUS Server > Attributes** parameters as described in the following table:

**Table 14: RADIUS Server > Attributes Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| 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**

Use the **Summary** tab to view the RADIUS Server authentication source configuration.

**Adding a Static Host List as an Authentication Source**

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.

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**.

To add a static host list as an authentication source:

1. Navigate to **Configuration > Authentication > Sources**. The **Authentication Sources** page opens.

**Figure 185 Authentication Sources Page**
2. Click the Add link. The **Add Authentication Sources** dialog opens.

   **Figure 186  Specifying a Static Host List as Authentication Source**

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 opens.
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 187**).

   **Figure 187  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 958.

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

To configure an authentication source for a Token server:

1. Navigate to Configuration > Authentication > Sources. The Authentication Sources page opens.
2. Click the Add link. The Add Authentication Sources page opens.

**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 188** Token Server > General Tab

Specify the Token Server > General parameters as described in the following table:

**Table 1: Token Server > General Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the label of the authentication source.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide the additional information that helps to identify the authentication source.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of authentication. In this context, select Token Server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use for Authorization</td>
<td>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.</td>
</tr>
<tr>
<td>Authorization Sources</td>
<td>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. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>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).</td>
</tr>
<tr>
<td>Backup Servers Priority</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Primary Tab**

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

**Figure 189  Token Server > Primary Tab**

Specify the **Token Server > Primary** parameters as described in the following table:

**Table 15: Token Server > Primary Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Specify the host name or the IP address of the token server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the UDP port at which the token server listens for RADIUS connections. The default port is <strong>1812</strong>.</td>
</tr>
<tr>
<td>Secret</td>
<td>Specify the RADIUS shared secret to connect to the token server.</td>
</tr>
</tbody>
</table>
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.

Figure 190  Token Server > Attributes Tab

For more information, see Configuring a Role and Role-Mapping Policy on page 243.

Specify the Token Server > Attribute parameters as described in the following table:

Table 16: Token Server > Attribute Tab Parameters

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

Summary Tab

Use the Summary tab to see a summarized view of the parameters configured in the General, Primary, and Attributes tab.

Modifying Authentication Methods or Sources for an Existing Service

To add or modify the authentication methods or sources for an existing service:

1. Navigate to the Configuration > Services page.
2. Select the service you want to modify. The Edit Service dialog for the selected service opens.
3. Select the Authentication tab. The Edit Services > Authentication dialog opens:
4. 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 page or the Configuration > Authentication > Sources page.

### Table 1: Authentication Method or Source Configuration for a Service

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration Steps</th>
</tr>
</thead>
</table>
| 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 dialog with the edit page 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 Modifying Authentication Methods on page 161.  
**NOTE:** An authentication method is only configurable for some service types. For more information, refer to Configuring Other Policy Manager Services on page 59. |
| Authentication Sources     | - Select a source, then 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 184. |
| Strip Username Rules       | Select the Enable to specify a comma-separated list of rules to strip usernames check box to preprocess the username and to remove prefixes and suffixes before authenticating it to the authentication source. |
| Service Certificate        | If there is a Service Certificate to associate with this service, select it from the drop-down list.                                                                                                               |
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).

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

### Configuring Single Sign-On

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 logins and Guest Operator logins.

#### SAML Service Provider (SP) Configuration

To configure single sign-on service provider settings:

2. In the Identity Provider (IdP) URL field, enter the URL used to access the IdP.

3. Select the application(s) you want users to access with single sign-on.
   - 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.

4. Create trusted relationships between a Service Provider and Identity Provider clicking the **Select Certificate** drop-down list and selecting 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
   - Validity Status
   - Signature Algorithm
   - Public Key Format
   - Serial Number
   - Enabled

   **Note:** This field only displays certificates that are enabled in the certificate trust list. If you do not specify the Identity Provider Certificate, ClearPass displays the message **Identity Provider (IdP) Certificate is mandatory**. For more information, see also Certificate Trust List on page 705.

5. In the **ClearPass Service Provider (SP) Metadata** field, click **Download** to download and view an XML file containing metadata for the Service ProviderURI (Uniform Resource Identifier). The **Metadata URI** field displays the URI for the Service Provider metadata resource.
To complete this task, you must next define your SAML Identity Provider (IdP) Configuration.

**SAML Identity Provider (IdP) Configuration**

To configure single sign-on identity provider settings:
2. Select the SAML IdP Configuration tab.

![Figure 193 Configuring Single Sign-On > Identity Provider Parameters](image)

3. In the IdP Portal Name field, enter the name of the identity provider portal. To download and view an XML file containing metadata for the Identity Provider URI (Uniform Resource Identifier), click Download. The IdP Metadata URI field displays the URI (Uniform Resource Identifier) for the selected IdP metadata resource.

4. If you upload metadata for SAML service providers, ClearPass can upload the SP metadata for validation during the single-sign on process.
   a. Click Add SP Metadata. The Upload SP Metadata dialog opens.
   b. In the Name field, enter the name of the service provider.
   c. In the Metadata field, browse for the service provider metadata file, then click Upload.

**Managing Local Users**

This section provides the following information:

- Adding a Local User
- Modifying a Local User Account
- Importing and Exporting Local Users
- Setting a 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.
2. Click the **Add** link at the top-right corner the page. The **Add Local User** page opens (see **Figure 195**).

**Figure 195  Adding a Local User**

3. Specify the **Add Local User** parameters as described in the following table, then click **Add**:

**Table 1: Adding a Local User Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Specify the local user's user ID.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the local user’s name.</td>
</tr>
<tr>
<td>Password/ Verify Password</td>
<td>Specify a password for the local user, then verify the password.</td>
</tr>
<tr>
<td>Enable User</td>
<td>You must enable this check box to enable the local user account. Otherwise, the local user account is disabled.</td>
</tr>
<tr>
<td>Change Password</td>
<td>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. <strong>NOTE:</strong> The option to change the password on the next login is applicable for network device administration logins using TACACS+ only.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Role</td>
<td>Select a static role to be assigned to the user from the Role drop-down list.</td>
</tr>
</tbody>
</table>

**Attributes**

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

1. 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.

2. 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 196  Modifying a Local User***

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**.) After selecting one or more user accounts from the list, you can also export specific user accounts by clicking the **Export** button.

The passwords of the local user accounts are not stored in clear text when exported to an XML file.

Setting a 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 197  Account Settings > Password Policy Settings Dialog](image)

3. Specify the **Password Policy** parameters as described in **Table 2**, then click **Save**.
### Table 2: Password Policy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>Specify the minimum length required for the password.</td>
</tr>
<tr>
<td>Complexity</td>
<td>Select the complexity setting from the <strong>Complexity</strong> drop-down list. The complexity settings can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- No password complexity requirement</td>
</tr>
<tr>
<td></td>
<td>- At least one uppercase and one lowercase letter</td>
</tr>
<tr>
<td></td>
<td>- At least one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one letter and one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one of each: uppercase letter, lowercase letter, digit</td>
</tr>
<tr>
<td></td>
<td>- At least one symbol</td>
</tr>
<tr>
<td></td>
<td>- At least one of each: uppercase letter, lowercase letter, digit, and symbol</td>
</tr>
<tr>
<td>Disallowed Characters</td>
<td>Specify the characters not to be allowed in the password. <strong>NOTE:</strong> Password characters validation takes effect for users created or modified after changes are saved.</td>
</tr>
<tr>
<td>Disallowed Words (CSV)</td>
<td>Specify the words not to be allowed in the password. Separate the disallowed words with commas.</td>
</tr>
<tr>
<td>Additional Checks</td>
<td>Select any additional checks, if required. The options are:</td>
</tr>
<tr>
<td></td>
<td>- May not contain User ID or its characters in reversed order.</td>
</tr>
<tr>
<td></td>
<td>- May not contain a repeated character four or more times consecutively.</td>
</tr>
<tr>
<td>Expiry Days</td>
<td>Set the password expiration time for local users. The allowed range is 0 to 500 days. The default value is 0. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>History</td>
<td>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.</td>
</tr>
<tr>
<td>Reminder</td>
<td>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. <strong>NOTE:</strong> The <strong>Reminder</strong> parameter is applicable for TACACS+ authentication only. The other settings are applied to all users.</td>
</tr>
</tbody>
</table>
### Table 3: Password Policy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>Specify the minimum length required for the password.</td>
</tr>
<tr>
<td>Complexity</td>
<td>Select the complexity setting from the Complexity drop-down list. The complexity settings can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- No password complexity requirement</td>
</tr>
<tr>
<td></td>
<td>- At least one uppercase and one lowercase letter</td>
</tr>
<tr>
<td></td>
<td>- At least one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one letter and one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one of each: uppercase letter, lowercase letter, digit</td>
</tr>
<tr>
<td></td>
<td>- At least one symbol</td>
</tr>
<tr>
<td></td>
<td>- At least one of each: uppercase letter, lowercase letter, digit, and symbol</td>
</tr>
<tr>
<td>Disallowed Characters</td>
<td>Specify the characters not to be allowed in the password.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Password characters validation takes effect for users created or modified after changes are saved.</td>
</tr>
<tr>
<td>Disallowed Words (CSV)</td>
<td>Specify the words not to be allowed in the password. Separate the disallowed words with commas.</td>
</tr>
<tr>
<td>Additional Checks</td>
<td>Select any additional checks, if required. The options are:</td>
</tr>
<tr>
<td></td>
<td>- May not contain User ID or its characters in reversed order.</td>
</tr>
<tr>
<td></td>
<td>- May not contain a repeated character four or more times consecutively.</td>
</tr>
<tr>
<td>Expiry Days</td>
<td>Set the password expiration time for local users. The allowed range is 0 to 500 days. The default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>ClearPass alerts users five days before the password expires.</td>
</tr>
<tr>
<td>History</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Valid options are from 1 to 99.</td>
</tr>
<tr>
<td>Reminder</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Reminder parameter is applicable for TACACS+ authentication only. The other settings are applied to all users.</td>
</tr>
</tbody>
</table>

### 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 ClearPassPolicy 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.

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 4). 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) and the Event Viewer (see Event Viewer).

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 198 Disable Accounts Dialog

4. Specify the Disable Accounts parameters as described in Table 4, then click Save.

Table 4: Disable Accounts Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days Exceed</td>
<td>Specify the number of days before the account is disabled. The range is from 1 to 100 days.</td>
</tr>
<tr>
<td>Date Exceeds</td>
<td>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.</td>
</tr>
<tr>
<td>Password not changed for</td>
<td>Specify the number of days allowed before the password must be changed. The range is from 1 to 365 days.</td>
</tr>
</tbody>
</table>
### 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](#)
- [Performing Bulk Deletions 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](#)
- [Adding Vendor-Specific Endpoint Context Servers](#)

### Viewing the List of Authentication Endpoints

ClearPass Policy Manager automatically lists all the endpoints that are authenticated in the **Configuration > Identity > Endpoints** page.

**Figure 199  Endpoints Page**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed attempts count</td>
<td>Specify the number of failed log-in attempts are allowed before the account is disabled. The range is from <strong>1</strong> to <strong>100</strong> attempts.</td>
</tr>
<tr>
<td>Reset failed attempts count</td>
<td>To reset the failed attempts count to zero and reenable those local users who were disabled after exceeding the failed attempts count, click <strong>Reset</strong>.</td>
</tr>
</tbody>
</table>

---

229 | Configuring Identity Settings
Table 1: Endpoint Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td>You can choose to select <strong>ALL matches</strong> or <strong>ANY matches</strong>. Then you can specify from one to three device filters to refine the endpoint information you wish to view.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the MAC address of the endpoint.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Specifies the host name of the endpoint.</td>
</tr>
<tr>
<td>Device Category</td>
<td>Indicates the category of the profiled device. For example, Access Points, Computer, Smart Device, VoIP phone, and so on.</td>
</tr>
<tr>
<td>Device OS Family</td>
<td>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 macOS.</td>
</tr>
</tbody>
</table>
| 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 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 200  Endpoint Authentication Details
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 clicking the corresponding check boxes.
   The Bulk Update button is now enabled.

   In network discovery, when endpoints do not have a MAC address, ClearPass creates MAC addresses for them that include the prefix xa.

2. Click the Bulk Update button.
   The Bulk Update Attributes dialog opens.

   Figure 201 Configuring Bulk Update Attributes

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.
   The multiple attributes that were configured will be updated on all the selected endpoints at once.

Performing Bulk Deletions of Endpoint Attributes

ClearPass supports bulk deletion of endpoint attributes.

To use this feature:

1. Navigate to Configuration > Identity > Endpoints.
   The Endpoints page opens.

   Figure 202 Endpoints Page and Bulk Delete Button
2. Select the check box(es) of an endpoint or endpoints in the list.
3. Click the **Bulk Delete** button.
   The **Bulk Delete Attributes** dialog is displayed.
   
   **Figure 203**  *Endpoints: Bulk Delete Attributes Dialog*

   ![Bulk Delete Attributes](image)

4. To select the endpoint attributes to be deleted, select **Click to add**.
   
   **Figure 204**  *Selecting Endpoint Attributes for Bulk Delete*

   ![Bulk Delete Attributes](image)

5. Select one or more attributes you wish to delete from the specified endpoints, then click **Delete**.
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:

![Endpoints Trigger Server Action Page](image)

3. Specify the **Trigger Server Action** page parameters as described in the following table, then click **Start Action**:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| **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. If you configure custom fingerprints, the custom fingerprint always takes precedence over the dynamically pushed system fingerprint.

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 206).

Figure 206 Update Device Fingerprint Page: Override Fingerprint

![Figure 206](image1.png)

Figure 207 shows the Update Device Fingerprint page when you set the Update Type to Add fingerprint rule.

Figure 207 Update Device Fingerprint Page: Add Fingerprint Rule

![Figure 207](image2.png)

3. Specify the Update Device Fingerprint page parameters as described in the following table, then click Save:
Table 3: Update Device Fingerprint Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Type</td>
<td>Select one of the following update types:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override fingerprint</strong>: Update the device profile details (device category, device OS family, and device name) for the selected endpoint.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Add fingerprint rule</strong>: 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 207.</td>
</tr>
</tbody>
</table>

Specify Device Profile Details

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Category</td>
<td>Select the category the profiled device belongs to.</td>
</tr>
<tr>
<td>Device OS Family</td>
<td>Select the operating system configured on the device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Enter the name of the device. You can select the name of the device from the list.</td>
</tr>
</tbody>
</table>

Manually Adding an Endpoint

To manually add an endpoint:

1. From the Configuration > Identity > Endpoints page, click Add.
   - The Add Endpoint page opens.

   **Figure 208  Add Endpoint Page**

2. Specify the Add Endpoint page parameters as described in the following table, then click Save:

Table 4: Add Endpoint Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Specify the MAC address of the endpoint.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information about the endpoint (recommended).</td>
</tr>
<tr>
<td>Status</td>
<td>Specify the client status as:</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Known client</td>
<td>You can use the Known client and Unknown client status in role-mapping rules by specifying the Authentication:MacAuth attribute.</td>
</tr>
<tr>
<td>Unknown client</td>
<td>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.</td>
</tr>
<tr>
<td>Disabled client</td>
<td></td>
</tr>
</tbody>
</table>

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
- Modifying an Endpoint
- Configuring the Attributes for the Selected Endpoint
- Endpoint Fingerprint Details Page

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 209  Edit Endpoint Page
2. Specify the **Edit Endpoint** page parameters as described in the following table, then click **Save**:

**Table 5: Edit Endpoint Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays the MAC address of the endpoint.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information about the endpoint (recommended).</td>
</tr>
<tr>
<td>Status</td>
<td>Indicate the status of the selected endpoint as:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Known client</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Unknown client</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Disabled client</strong></td>
</tr>
<tr>
<td></td>
<td>- You can use the <strong>Known client</strong> and <strong>Unknown client</strong> status in role-mapping rules by applying the <strong>Authentication:MacAuth</strong> attribute.</td>
</tr>
<tr>
<td></td>
<td>- You can use the <strong>Disabled client</strong> status to block access to a specific endpoint. This status is automatically set when an endpoint is blocked from the Endpoint Profiler.</td>
</tr>
<tr>
<td>MAC Vendor</td>
<td>Displays the MAC OUI (Organizationally Unique Identifier) information for all endpoints even when no other profiling information is available for an endpoint.</td>
</tr>
<tr>
<td>Added by</td>
<td>Displays the name of the ClearPass server that added the endpoint.</td>
</tr>
<tr>
<td>Online Status</td>
<td>Displays the online status of the endpoint:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Online</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Offline</strong></td>
</tr>
<tr>
<td>Connection Type</td>
<td>Indicates the connection type; for example, <strong>Wireless</strong>.</td>
</tr>
<tr>
<td></td>
<td>If the connection type is not known, the connection type is displayed as <strong>Unknown</strong>.</td>
</tr>
<tr>
<td>Access Point</td>
<td>Indicates the access point with which the endpoint device is associated.</td>
</tr>
<tr>
<td>Network SSID</td>
<td>Indicates the SSID of the network in which the endpoint is deployed.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address that is associated with the endpoint.</td>
</tr>
<tr>
<td>Static IP</td>
<td>Indicates whether the IP address of the endpoint is a static IP address (<strong>True</strong> or <strong>False</strong>).</td>
</tr>
<tr>
<td>Hostname</td>
<td>Displays the host name or the IP address of the endpoint.</td>
</tr>
<tr>
<td>Device Category</td>
<td>Select the device category that the endpoint belongs to from the drop-down list.</td>
</tr>
<tr>
<td>Device OS Family</td>
<td>Specify the operating system that the endpoint runs on.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Select the name of the device from the drop-down list.</td>
</tr>
<tr>
<td>Added At</td>
<td>Displays the date and time at which the endpoint was added.</td>
</tr>
<tr>
<td>Updated At</td>
<td>Displays the date and time at which the endpoint was updated.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Profiled At</td>
<td>Displays the date and time at which the endpoint was added to the ClearPass Profile.</td>
</tr>
<tr>
<td><strong>Profile Conflict Details</strong></td>
<td></td>
</tr>
<tr>
<td>Other Category</td>
<td>Specify if this device can be assigned to an alternate device category.</td>
</tr>
<tr>
<td>Other Family</td>
<td>Specify if this device can be assigned to an alternate OS family.</td>
</tr>
<tr>
<td>Other Name</td>
<td>Specify if this device can be assigned to an alternate device name.</td>
</tr>
<tr>
<td>Resolve Conflict</td>
<td>Select one of the following options to be executed in the event of a conflict:</td>
</tr>
<tr>
<td></td>
<td>- Ignore this fingerprint</td>
</tr>
<tr>
<td></td>
<td>- Use this fingerprint</td>
</tr>
<tr>
<td></td>
<td>- Resolve later</td>
</tr>
<tr>
<td><strong>Fingerprints</strong></td>
<td></td>
</tr>
<tr>
<td>Host User Agent</td>
<td>Displays the host user agent of the endpoint. For example, <code>Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Firefox/25.0)</code>.</td>
</tr>
<tr>
<td>DHCP Option60</td>
<td>Defines the VCI (Vendor class identifier) on the DHCP server (for example, <code>MFST 5.0</code>).</td>
</tr>
</tbody>
</table>

### 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 210  Adding Endpoint Attributes

2. To add attributes for the selected endpoint, select **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**.

**About the Airwatch Group ID and Group Name Endpoint Attributes**

The **LocationGroupName** and **LocationGroupID** attributes are fetched from an Airwatch server. These attributes are mapped to the corresponding **GroupName** and **GroupID** Endpoint attributes.

**Figure 211  Airwatch GroupID and GroupName Endpoint Attributes**

**About the Airwatch Compliance Attribute**

The **Compliance** attribute is fetched from an Airwatch server and made available in the Endpoint attributes list. The values for the **Compliance** attribute are:

- **NotAvailable**
- **NonCompliant**
- **Compliant**

**Viewing the Endpoint Fingerprint Details**

The information displayed in the **Edit Endpoint > Fingerprint** page varies depending on what type of device is selected and whether an Nmap-based network discovery scan has been run (see Configuring SNMP, SSH, and WMI Credentials).

As shown in **Figure 212**, the **Endpoint Fingerprint Details** page shows the active and inactive Windows services and processes for the selected Windows endpoint.

**Figure 212  Endpoint Fingerprint Details Page**

**Managing Static Host Lists**

This section provides the following information:

- **About Static Host Lists**
- **Adding a Static Host List**
- **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 Managing Static Host Lists and Adding a Static Host List as an Authentication Source.

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 preconfigured 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.
2. Click **Add**.
   
The **Add Static Host List** dialog opens.

**Figure 214  Adding a Static Host List**

3. For the Host Format of **List**:
   a. Enter the IP or MAC address of the device.
   b. Enter a description of the device.
   c. Click **Save Host**.
      
      The device is added to the Host Entries.
   d. Click **Save**.
   e. Repeat these steps for each entry in the static host list.

4. Specify the parameters to add a static host list as described in **Table 1**, then click **Save**.
Table 1: Add Static Host List Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the static host list.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description that provides additional information about the static host list.</td>
</tr>
<tr>
<td>Host Format</td>
<td>Select a format for expression of the address:</td>
</tr>
<tr>
<td></td>
<td>- Subnet</td>
</tr>
<tr>
<td></td>
<td>- Regular Expression</td>
</tr>
<tr>
<td></td>
<td>- List. For the List Host Format type, you can add a description for each IP address in the static host list (for examples, see Figure 215 below).</td>
</tr>
<tr>
<td>Host Type</td>
<td>Select a host type:</td>
</tr>
<tr>
<td></td>
<td>- IP Address</td>
</tr>
<tr>
<td></td>
<td>- MAC Address</td>
</tr>
<tr>
<td>Subnet</td>
<td>Enter the subnet address.</td>
</tr>
</tbody>
</table>

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.

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 215 Edit Static Host List Dialog
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**.

**Configuring a Role and Role-Mapping Policy**
This section includes the following information:
- **Preconfigured Roles**
- **Adding and Modifying Roles on page 245**
- **Adding and Modifying Role-Mapping Policies on page 246**

After authenticating a request, a Policy Manager service invokes its role-mapping policy, resulting in assignment of a role(s) to the client. This role becomes the identity component of enforcement policy decisions.

---

A service can be configured without a role-mapping policy, but only one role-mapping policy can be configured for each service.

---

**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 ChromeOS device being provisioned.
- [Onboard iOS]: Role for an iOS device being provisioned.
- [Onboard Linux]: Role for a Linux device being provisioned.
- [Onboard macOS]: Role for a macOS 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.
Figure 216 illustrates the role-mapping process and workflow.

Figure 216 Role-Mapping Process

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.

Roles available on this page include roles that are created automatically when an administrator creates a new operator profile in ClearPass Guest. The new role is created with the same name as the operator profile.

If an administrator later wants to rename the role, the role is not replaced—instead, the first role is kept unchanged and another role is created with the new name.

Adding a Role

To add a role:

1. Navigate to **Configuration > Identity > Roles**.
   
   The Roles page opens.

   **Figure 217 Roles Page**

   ![Roles Page](image)

   You can also configure a role from within a role-mapping policy (click the **Add New Role** link).

2. Click **Add**.

   The **Add New Role** page opens.

   **Figure 218 Add New Role Page**

   ![Add New Role Page](image)

3. Define the **Add New Role** parameters as described in the following table, then click **Save**.
Table 1: Add New Role Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the role.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter the description that provides additional information about the new role (recommended).</td>
</tr>
</tbody>
</table>

Modifying a Role

To modify a role:

1. Navigate to Configuration > Identity > Roles.
   The Roles page opens.
2. Click the role Name that you wish to modify.
   The Edit Role page appears.

Figure 219 Edit Role Page

3. Edit the Name and Description as needed, then click Save.

Adding and Modifying Role-Mapping Policies

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

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.
3. Specify the **Role Mappings > Policy** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Enter the name of the role-mapping policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description that provides additional information about the role mapping policy.</td>
</tr>
<tr>
<td>Default Role</td>
<td>Select the role to which Policy Manager will default when the role-mapping policy does not produce a match.</td>
</tr>
<tr>
<td>View Details</td>
<td>To view the details of the default role, click <strong>View Details</strong>.</td>
</tr>
<tr>
<td>Modify</td>
<td>To modify the default role, click <strong>Modify</strong>.</td>
</tr>
<tr>
<td>Add New Role</td>
<td>To add a new role, click <strong>Add New Role</strong>.</td>
</tr>
</tbody>
</table>

**Adding 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**

To add a mapping rule:

1. Click **Add Rule**. The **Rules Editor** page opens.
2. Specify the **Role Mappings Page > Rules Editor** page parameters as described in the following table.

**Table 2: Rules Editor Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| **Type**  | The Rules Editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries, depending on context. (Refer to [Namespaces on page 958](#).) 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 184](#)). 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, see [Operators](#). |
| **Value**  | Depending on attribute data type, this may be a free-form (one or many line) edit box, a drop-down list, or a time/date widget. |

The operator values that display for each type and name are based on the data type specified for the authentication source (from the **Configuration > Authentication > Sources** page). If, for example, you modify the **UserDN Data** type on the authentication sources page to be an integer rather than a string, then the list of operator values here will populate with values that are specific to integers.

---

**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**.
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

**Posture Architecture and Flow**

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 macOS®, 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.

---

A service can 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
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 or 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.

### Creating a New Posture Policy

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 use by Policy Manager as input into an enforcement policy. You can associate one or more posture methods with a single service. ClearPass 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](#).

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 and the plugin version (2.0).

   **Figure 225 Posture Policies Page**

   ![Posture Policies Page](image)

2. Click the **Add** link. The **Posture Policies Add** page opens.
Figure 226  Posture Policies Add Page

   - For information on configuring the Posture policy plug-ins, see Configuring Posture Policy Plug-ins on page 257.
   - For information on configuring Posture Policy Rules, see Configuring Posture Policy Rules on page 335.

Configuring Posture Policy Agents and Hosts

Adding a New Posture Policy

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

2. Click the Add link. The Add Posture Policies page opens.
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.

4. Specify the Add Posture Policy parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Enter the name assigned to the policy by the ClearPass Policy Manager administrator.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify the description that provides additional information about the posture policy.</td>
</tr>
<tr>
<td>Posture Agent</td>
<td>Select the posture agent type. For detailed information on these agents, see <a href="#">Configure NAP Agent Posture Plug-ins</a> and <a href="#">Configure OnGuard Agent Posture Plug-ins</a>.</td>
</tr>
<tr>
<td>Host Operating System</td>
<td>Specify whether the host is using a Windows, Linux, or macOS operating system.</td>
</tr>
</tbody>
</table>
| Restrict by Roles     | Apply the posture policy to the selected roles. To restrict the posture policy by roles:

1. From the Policy tab, click the Select or type role names drop-down. The list of available roles opens.
2. Select the roles you wish to restrict access by, then click Add. The selected roles are added to the Restrict by Roles field. For example, users with access to research data might have a posture policy that does not permit the mounting of USB storage devices. Or users with access to employee or customer personal or health data might have a policy that requires full disk encryption. |
**Configure 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 2**: 

**Table 2: NAP Agent: Windows OS Posture Plug-ins Support**

<table>
<thead>
<tr>
<th>Plug-in</th>
<th>Description/Health Checks</th>
<th>Windows Support</th>
</tr>
</thead>
</table>
| 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:  
- Firewall  
- Virus Protection  
- Automatic Updates  
- 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 |

**Configure 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. MacOS 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 3**)
- MacOS (see **Table 4**)
- Linux (see **Table 5**)

---

255 | Posture Policies and Audit Servers  
---
### Table 3: OnGuard Agent Validator Posture Plug-in Windows OS Support

<table>
<thead>
<tr>
<th>Plug-in</th>
<th>Description/Health Checks</th>
<th>Windows Support</th>
</tr>
</thead>
</table>
| ClearPassWindows Universal System Health Validator | The configurable health checks for this validator are:  
- Services  
- Processes  
- Registry Keys  
- AntiVirus  
- Patch Management  
- Windows HotFixes  
- USB Devices  
- Virtual Machines  
- Network Connections  
- Disk Encryption  
- Installed Applications  
- 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 Server 2016: Yes |
| 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 Server 2016: Yes |
| Windows Security Health Validator             | The configurable health checks for this validator allow you to enable health checks that permit or deny client computers access to your network, subject to checks of the client’s system:  
- Firewall  
- Virus Protection,  
- Automatic Updates  
- Security Updates | - 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 4: OnGuard Agent (Persistent or Dissolvable) Posture Plug-ins for macOS

<table>
<thead>
<tr>
<th>Plug-in Name</th>
<th>Health Checks</th>
</tr>
</thead>
</table>
| ClearPass macOS Universal System Health Validator | The configurable health checks for this health validator are:  
- Services  
- Processes  
- AntiVirus  
- Firewall  
- Patch Management  
- Peer-to-Peer  
- USB Devices  
- Virtual Machines  
- Network Connections  
- Disk Encryption  
- Installed Applications  
- File Check |
### Table 5: OnGuard Agent (Persistent or Dissolvable) Posture Plug-in for Linux

<table>
<thead>
<tr>
<th>Plug-in Name</th>
<th>Health Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClearPass Linux Universal System Health Validator</td>
<td>The configurable health check for this health validator is: <em>Services</em>.</td>
</tr>
</tbody>
</table>

### 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 opens.
   
   **Figure 229 Posture Policies Page**

2. Click **Add**.
   
   The **Add Posture Policies** page opens.
   
   **Figure 230 Adding a Posture Policy**

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 opens.
You can configure the following posture plug-ins in the **Posture Policies** page:

- **ClearPass Windows Universal System Health Validator > OnGuard Agent**
- **Windows System Health Validator: NAP Agent**
- **Windows System Health Validator: OnGuard Agent**
- **Windows Security Health Validator: NAP Agent**

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 macOS operating systems. Refer to the following topics for details on each plugin type:

- **Windows**:
  - **ClearPass Windows Universal System Health Validator > OnGuard Agent** on page 258
  - **Windows System Health Validator: OnGuard Agent** on page 297
  - **Windows Security Health Validator: OnGuard Agent** on page 298
- **Linux**: [ClearPass Linux Universal System Health Validator Plugin on page 299](#)
- **macOS**: [ClearPass macOS Universal System Health Validator: OnGuard Agent on page 304](#)

The following figure displays the **Posture Policies > Posture Plugins** tab:

**Figure 232  Configuring the OnGuard Agent Plugin for macOS**

### 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 233 Adding a Posture Policy**

![Posture Policy Configuration](image)

1. Enter the name and a description of the posture policy.
2. **Posture Agent**: Choose OnGuard Agent (Persistent or Dissolvable).
3. **Host Operating System**: Windows is selected by default.
4. **Plugin Version**: OnGuard plugin version 2.0 (V4 SDK) is set by default.

2. Click **Next**.

   The **Posture Plugins** dialog opens.

**Figure 234 Selecting the Windows Posture Plugin**

![Posture Plugins Configuration](image)

3. In the **Posture Plugins** page, 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. To enable checks for the selected version, click the **Enable checks for Windows Server** check box.
The following list of health checks for the selected version of Windows opens (see Figure 235):

- Services on page 260
- Processes on page 265
- Registry Keys on page 268
- AntiVirus on page 271
- Firewall on page 275
- Peer To Peer on page 277
- Patch Management on page 278
- Windows Hotfixes on page 282
- USB Devices on page 287
- Virtual Machines on page 287
- Network Connections on page 288
- Disk Encryption on page 290
- Installed Applications on page 291
- File Check on page 294

7. When finished, click **Save**.

   You return to the Posture Policies > Posture Plugins page, where the Status column for the ClearPass Windows Universal System Health Validator now shows **Configured**.

**Services**

The **Services** 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 236* displays an example of the **ClearPass Windows Universal System Health Validator > Services** configuration page and highlights examples of the evaluation rule for groups and the evaluation rule for services:

*Figure 236  Specifying Service Groups to Run*

6. Specify the **ClearPass Windows Universal System Health Validator > Services** configuration parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto-remediation for service checks. Enabling this option automatically stops or starts services based on the entries in <strong>Service to Run</strong> and <strong>Services to Stop</strong> configuration. Auto-remediation for the <strong>Services</strong> health class is enabled by default.</td>
</tr>
<tr>
<td>User Notification</td>
<td>When enabled, a remediation message that includes the groups of services to be present or absent is displayed to the end user.</td>
</tr>
</tbody>
</table>
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 237 Specifying the Service Group Evaluation Rule

2. Specify the Add Service Group to Be Present parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Service Group Name</td>
<td>1. Enter the name of the Service Group.</td>
</tr>
<tr>
<td>Service Group Evaluation Rule</td>
<td>2. Select the appropriate Service Group Evaluation Rule:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
</tbody>
</table>

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.
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 239 Add Services to Be Absent Dialog**

2. Specify the Service Groups to Be Absent parameters as described in the following table:
### Table 3: Add Service Group to Be Absent Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Service Group Name</td>
<td>1. Enter the name of the Service Group.</td>
</tr>
<tr>
<td>Service Group Evaluation Rule</td>
<td>2. Select the appropriate Service Group Evaluation Rule:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass All</strong>: Select this evaluation rule if you want all service groups to be stopped. <em>Pass All</em> is the equivalent of an <strong>AND</strong> condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass Any One</strong>: Select this evaluation rule if you want any one of the service groups to be stopped. <em>Pass Any One</em> is the equivalent of an <strong>OR</strong> condition.</td>
</tr>
</tbody>
</table>

3. Click **Add**.
   
   The **Add Services to Stop** dialog opens.

**Figure 240  Specifying the 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 241** shows an example of services configured for Windows Server 2003.
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 242  Processes Configuration Page**

6. Specify the **Processes** configuration parameters as described in the following table:
Table 1: Processes Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto-remediation for processes.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications in the event of process policy violations.</td>
</tr>
</tbody>
</table>

Processes to be Present Parameters

1. In the Processes to be Present section, click Add.
   The Add Processes to be Present page opens.

Figure 243 Add Processes to be Present Page

2. Specify the Processes to be Present parameters as described in the following table, then click Save:

Table 2: Processes to be Present Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Location</td>
<td>Choose from the following locations:</td>
</tr>
<tr>
<td></td>
<td>● System Drive</td>
</tr>
<tr>
<td></td>
<td>● Systemroot</td>
</tr>
<tr>
<td></td>
<td>● Program Files</td>
</tr>
<tr>
<td></td>
<td>● HOMEDRIVE</td>
</tr>
<tr>
<td></td>
<td>● HOMEPATH</td>
</tr>
<tr>
<td></td>
<td>● None</td>
</tr>
<tr>
<td>Enter the Process name</td>
<td>Specify the path name containing the process executable name.</td>
</tr>
<tr>
<td>Enter the Display name</td>
<td>Enter a user-friendly name for the process. This is displayed in end-user facing messages.</td>
</tr>
</tbody>
</table>

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 244 shows the configuration parameters for when you select Process Name and when you select MD5 Sum.
2. Specify the **Processes to be Absent** parameters as described in the following table, then click **Save**:

**Table 3: Processes to be Absent Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Check Type               | 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   | 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 245  Processes Configured

![Processes Configured](image)

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 246  Registry Keys Page (Overview)

![Registry Keys Page](image)

6. Specify the Registry Keys page parameters as described in the following table:
### Table 1: Registry Keys Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable auto remediation for registry checks. Use this page to automatically add or remove registry keys based on the entries in <strong>Registry keys to be present</strong> and <strong>Registry keys to be absent</strong> fields.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable user notifications for registry check policy violations.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Enable this to set the health status of the <strong>Registry Keys</strong> 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.</td>
</tr>
<tr>
<td>Registry keys to be present</td>
<td>To specify a registry key to be added to the <strong>Registry keys to be present</strong> list, click <strong>Add</strong>. If the specified registry key is not present, the remediation message that is added in the <strong>Registry Keys Page (Detail)</strong> window is displayed on <strong>OnGuard Agent</strong>.</td>
</tr>
<tr>
<td>Registry keys to be absent</td>
<td>To add a registry key to the <strong>Registry keys to be absent</strong> list, click <strong>Add</strong>. If the specified registry key is not absent, the remediation message that is added in the <strong>Registry Keys Page (Detail)</strong> window is displayed on <strong>OnGuard Agent</strong>.</td>
</tr>
</tbody>
</table>

7. To configure the **Registry key to Be Present**, click **Add**. The **Edit Registry Key to Be Present** dialog opens.

**Figure 247  Edit Registry Keys to Be Present Parameters**

8. Specify the **Registry Key to be Present** parameters as described in **Table 2**, then click **Save**.
### Table 2: Registry Keys Page (Detail)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the Registry Hive</td>
<td>Specify the registry hive from the following options:</td>
</tr>
<tr>
<td></td>
<td>- HKEY_CLASSES_ROOT</td>
</tr>
<tr>
<td></td>
<td>- HKEY_CURRENT_USER</td>
</tr>
<tr>
<td></td>
<td>- HKEY_LOCAL_MACHINE</td>
</tr>
<tr>
<td></td>
<td>- HKEY_USERS</td>
</tr>
<tr>
<td></td>
<td>- HKEY_CURRENT_CONFIG</td>
</tr>
<tr>
<td>Enter the Registry key</td>
<td>Specify the registry key using the examples given in the GUI.</td>
</tr>
<tr>
<td>Enter the Registry value name</td>
<td>Specify the name of the registry value.</td>
</tr>
<tr>
<td>Select the Registry value data type</td>
<td>Specify the registry value data types. The data type can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>- Multi String</td>
</tr>
<tr>
<td></td>
<td>- String</td>
</tr>
<tr>
<td></td>
<td>- DWORD</td>
</tr>
<tr>
<td></td>
<td>- QWORD</td>
</tr>
<tr>
<td></td>
<td>- Expandable String</td>
</tr>
<tr>
<td>Enter the Registry value data</td>
<td>Specify the registry value.</td>
</tr>
<tr>
<td>Enter Regex pattern for Registry</td>
<td>Enter the Regular Expression (Regex) pattern for the Registry value.</td>
</tr>
<tr>
<td>value</td>
<td>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. <strong>NOTE:</strong> Perl regular expressions are supported.</td>
</tr>
<tr>
<td>Enter Remediation Message</td>
<td>Specify the custom remediation message to be displayed to end users if the registry check fails.</td>
</tr>
</tbody>
</table>

As shown in Figure 248, after you save the registry configuration settings, the remediation message and Regular Expression pattern appears in the Registry page.

**Figure 248** Registry Keys Added
AntiVirus

In the **Antivirus** page, you can turn on an Antivirus application.

To define the Windows Antivirus health class:

1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**.
   
   The Add Posture Policies page opens to the **Policy** tab.

   **Figure 249**  *Creating an Antivirus Posture Policy for Windows*

   ![Posture Policies](image)

   2. From the **Add Posture Policies** page, select the **Posture Plugins** tab.

   3. Select the **ClearPass Windows Universal System Health Validator**.

      **Figure 250**  *Configuring the ClearPass Windows Universal System Health Validator*

      ![Posture Policies](image)

   4. Click **Configure**.

      The configuration page opens. The list of supported Windows operating systems is displayed.

   5. Select the pertinent Windows operating system.

      When you select one of the Windows operating systems, the list of health checks for the selected OS is displayed.
6. Check the **Enable checks for Windows OS**.

7. From the list of health checks, select **Antivirus**.
   
   The **Antivirus** health class configuration page opens.

8. To configure the Antivirus application information, click the **An antivirus application is on** check box.
   
   When enabled, the **Antivirus** detail page opens.
9. To specify product and version-check information, click Add.

Figure 252  Antivirus Health Check Configuration Dialog

10. Specify the Antivirus health class parameters as described in the following table:
### Table 1: Antivirus Health Class Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Antivirus Application is On</td>
<td>Click <strong>Antivirus application is on</strong> to enable testing of health data for configured Antivirus application(s).</td>
</tr>
<tr>
<td>Auto Remediation</td>
<td>Check the <strong>Auto Remediation</strong> check box to enable auto remediation of anti-virus status. This option is enabled by default.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Check the <strong>User Notification</strong> check box to enable user notification of policy violation of anti-virus status. This option is enabled by default.</td>
</tr>
<tr>
<td>Display Update URL</td>
<td>Check the <strong>Display Update URL</strong> check box to show the origination URL of the update. This option is disabled by default.</td>
</tr>
<tr>
<td>Product-specific checks</td>
<td>To configure for product-specific checks, leave the check box checked (the default setting). To allow any Antivirus product, uncheck the check box. All of these checks may not be available for some products. Where checks are not available, they are shown in disabled state.</td>
</tr>
<tr>
<td>Select the antivirus product</td>
<td>Select an antivirus product from the drop-down list.</td>
</tr>
<tr>
<td>Product version check</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Check</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Is Latest</strong>: Requires registration with ClearPass portal.</td>
</tr>
<tr>
<td></td>
<td>- <strong>In Last N Updates</strong>: Requires registration with ClearPass Portal.</td>
</tr>
<tr>
<td>Datafile version check</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Check</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Is Latest</strong>: Requires registration with ClearPass portal.</td>
</tr>
<tr>
<td></td>
<td>- <strong>In Last N Updates</strong>: Requires registration with ClearPass Portal.</td>
</tr>
<tr>
<td>Data file has been updated in</td>
<td>Enter the number, then specify the interval in hours, days, weeks, or months.</td>
</tr>
</tbody>
</table>
### Table 1: Antivirus Health Class Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last scan has been done before</td>
<td>Enter the number, then specify the interval in hours, days, weeks, or months.</td>
</tr>
<tr>
<td>Real-time Protection Status Check</td>
<td><strong>No Check:</strong> ClearPass does not use the Real-time Protection status value for health evaluation. This means that the client is treated as healthy irrespective of the value of its Real-time Protection status.</td>
</tr>
<tr>
<td></td>
<td><strong>On:</strong> Marked as healthy only if the value of Real-time Protection status is On.</td>
</tr>
<tr>
<td>Adaptive Threat Protection</td>
<td>When McAfee Endpoint Security is selected as the antivirus product, the Adaptive Threat Protection option is made available. Status checks for Adaptive Threat Protection are not enabled by default.</td>
</tr>
<tr>
<td></td>
<td>■ To enable checking the status of McAfee Endpoint Security Adaptive Threat Protection, select the On button. Auto-remediation action to enable Adaptive Threat Protection is not supported.</td>
</tr>
<tr>
<td></td>
<td>■ If McAfee Endpoint Security Adaptive Threat Protection is disabled, OnGuard will mark the client as Unhealthy.</td>
</tr>
</tbody>
</table>

After you save your Antivirus configuration, it is listed on the Antivirus page.

**Figure 253** Antivirus Check Configured

![Antivirus Check Configured](image)

Firewall

In the Firewall page, you can specify that a Firewall application must be on and specify information about the Firewall application.

**Figure 254** Firewall Page (Overview Before)

![Firewall Page](image)

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Firewall Application is On</td>
<td>Check the <strong>Firewall Application is On</strong> check box to enable testing of health data for configured firewall application(s).</td>
</tr>
<tr>
<td>Auto Remediation</td>
<td>Check the <strong>Auto Remediation</strong> check box to enable auto remediation of firewall status.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Check the <strong>User Notification</strong> check box to enable user notification of policy violation of firewall status.</td>
</tr>
<tr>
<td>Uncheck to allow any product</td>
<td>To specify Firewall product-specific checks, leave this parameter as is. To specify whether any firewall application (any vendor) is running on the end host, uncheck the <strong>Uncheck to allow any product</strong> check box.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add</td>
<td>To configure firewall application attributes for testing against health data, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Trashcan icon</td>
<td>To remove configured firewall application attributes from the list, click the trashcan icon in that row.</td>
</tr>
</tbody>
</table>
| 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 258  Peer to Peer Page**

The following table describes the **Peer to Peer** parameters:

**Table 1: Peer to Peer Page**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto remediation for service checks (Automatically stop peer-to-peer applications based on the entries in <strong>Applications to stop</strong> configuration).</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for peer to peer application/network check policy violations.</td>
</tr>
<tr>
<td>By Application / By Network</td>
<td>Select the appropriate radio button to select individual peer-to-peer applications or a group of applications that use specific peer-to-peer networks.</td>
</tr>
</tbody>
</table>
| 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 >> to add the applications or networks to the **Applications to stop** pane.  
  - Click the << to remove the applications or networks from the **Applications to stop** pane. |
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 259  ClearPass Windows Universal System Health Validator: Patch Management**

9. Specify the Patch Management parameters as described in the following table.
Table 1: Patch Management Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A patch management application is on</td>
<td>To enable testing of health data for configured Antivirus application(s), check the <strong>A patch management application is on</strong> check box. The Patch Management configuration dialog opens.</td>
</tr>
</tbody>
</table>

Remediation Checks

<table>
<thead>
<tr>
<th>Remediation Checks</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>To enable auto-remediation of patch management status, check the <strong>Auto Remediation</strong> check box.</td>
</tr>
<tr>
<td>User Notification</td>
<td>To enable user notification of policy violation of patch management status, check the <strong>User Notification</strong> check box.</td>
</tr>
</tbody>
</table>

Product Evaluation Rule

<table>
<thead>
<tr>
<th>Product Evaluation Rule</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Evaluation Rule</td>
<td>Select the appropriate <strong>Product Evaluation Rule</strong>:</td>
</tr>
</tbody>
</table>

- **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 260  *Configuration Page for the Patch Management Application*

11. Specify these parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Evaluation Rule</td>
<td>Select the appropriate <strong>Product Evaluation Rule</strong>:</td>
</tr>
</tbody>
</table>

   - **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.

   All checks might not be available for some products. Where checks are not available, they are shown in a disabled.
Table 2: *Patch Management Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product-specific checks</td>
<td>To check whether any patch management application (any vendor) is running on the end host, clear the <strong>Uncheck to allow any product</strong> check box.</td>
</tr>
<tr>
<td>Select Patch Management Product</td>
<td>Select a patch management product vendor. This option is enabled <em>only</em> if the <strong>Product-specific checks</strong> check box is checked.</td>
</tr>
<tr>
<td>Product version is at least</td>
<td>Enter the minimally recommended product version number. This option is enabled <em>only</em> if the <strong>Product-specific checks</strong> check box is checked.</td>
</tr>
</tbody>
</table>
| 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.  
  - **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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Level Check Type</td>
<td>This option is only enabled if the <strong>Product-specific checks</strong> check box is checked. For Microsoft SCCM, selecting <strong>All</strong> will return the full list of all missing patches.</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Check</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All</strong>: Checks for all missing patches and searches for all available patches.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If you select the <strong>Microsoft Windows Update Agent</strong> from the Select Patch Management product list and you select an option from the Install Level Check Type list, the results are as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>All</strong>: Returns the full list of missing patches.</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Check</strong>: Disables the Grace Period and Scan Interval fields.</td>
</tr>
<tr>
<td>Grace Period</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If you selected <strong>No Check</strong> from the Install Level Check Type field, Grace Period is disabled.</td>
</tr>
<tr>
<td>Scan Interval</td>
<td>Specify the Scan Interval by specifying the number of hours, days, weeks, or months. If you selected <strong>No Check</strong> from the Install Level Check Type field, Scan Interval is disabled.</td>
</tr>
</tbody>
</table>

12. Click **Save**.

When you save your patch management configuration, the configuration information is displayed on the Patch Management page:
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 1 for details).
  
  For example, if the status of Group 1 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 2 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:
6. Specify the **Windows Hotfixes** parameters as described in the following table:

**Table 1: Windows Hotfixes Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>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.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications to check for hotfix policy violations.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Click to enable <strong>Monitor Mode</strong>.</td>
</tr>
<tr>
<td>Windows Hotfixes Groups to be Present</td>
<td>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:</td>
</tr>
<tr>
<td>Evaluation Rule</td>
<td>- <strong>Pass All</strong>: Select this evaluation rule to calculate the two group's health status as <em>Group1 AND Group2</em>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass Any One</strong>: Select this evaluation rule to calculate the two group's health status as <em>Group1 OR Group2</em>.</td>
</tr>
</tbody>
</table>

**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 262), click **Add**.
   
The following Hotfixes dialog opens:
2. Specify the Hotfixes Group parameters as described in the following table:

**Table 2: Specifying Hotfixes Group to Be Present Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Windows Hotfixes Group Name</td>
<td>Enter the name of the Hotfixes Group.</td>
</tr>
</tbody>
</table>
| 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 264 opens. |
3. From the first list, specify the criticality of the hotfixes:
   - Critical
   - Important
   - Moderate
   - Low
   - Unspecified
   As shown in Figure 264, 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 264, 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.
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 266  Removing Hotfixes from the Hotfixes to Be Present List

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 267  Summary of Hotfixes Groups Configuration**

USB Devices

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

**Figure 268  USB Devices**

The following table describes the **USB Devices** parameters:

**Table 1: USB Devices**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto remediation for USB mass storage devices attached to the endpoint (Automatically stop or eject the drive).</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for USB devices policy violations.</td>
</tr>
<tr>
<td>Remediation Action for USB Mass Storage Devices</td>
<td>- 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.</td>
</tr>
</tbody>
</table>

**Virtual Machines**

The **Virtual Machines** page provides configuration to Virtual Machines utilized by your network.
The following table describes the **Virtual Machines** parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto remediation for virtual machines connected to the endpoint.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for virtual machine policy violations.</td>
</tr>
<tr>
<td>Allow access to clients running on Virtual Machine</td>
<td>Enable to allow clients that running a VM to be accessed and validated.</td>
</tr>
<tr>
<td>Allow access to clients hosting Virtual Machine</td>
<td>Enable to allow clients that hosting a VM to be accessed and validated.</td>
</tr>
<tr>
<td>Remediation Action for clients hosting Virtual Machines</td>
<td>- No Action - Take no action; do not stop or pause virtual machines.</td>
</tr>
<tr>
<td></td>
<td>- Stop all Virtual Machines running on Host - Stop the VM clients that are running on Host.</td>
</tr>
<tr>
<td></td>
<td>- Pause all Virtual Machines running on Host - Pause the VM clients that are running on Host.</td>
</tr>
</tbody>
</table>

**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.
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 271  Network Connection Types Configuration Page**

6. Specify the **Network Connection Types** configuration parameters as described in the following table:

   **Table 1: Network Connection Type Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Network Connections Type</td>
<td>1. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Allow Only One Network Connection</td>
</tr>
<tr>
<td></td>
<td>- Allow One Network Connection with VPN</td>
</tr>
<tr>
<td></td>
<td>- Allow Multiple Network Connections</td>
</tr>
<tr>
<td>Network Connection Types</td>
<td>2. To add or remove Others, Wired, and Wireless network connection types, click &gt;&gt; or &lt;&lt;.</td>
</tr>
<tr>
<td>Remediation Action for</td>
<td>3. Specify one of the following</td>
</tr>
<tr>
<td></td>
<td>- No Action: Take no action. Do not eject or disable the attached</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Connection Types Not Allowed</td>
<td>devices.</td>
</tr>
<tr>
<td></td>
<td>· Disable Network Connections</td>
</tr>
<tr>
<td></td>
<td>· Disconnect Network Connections</td>
</tr>
</tbody>
</table>

4. Click **Save**.

This returns you to the **Network Connections** configuration page. The following table describes the remaining fields on this page:

**Table 2: Network Connections Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>1. Enable to allow auto-remediation for network connections.</td>
</tr>
<tr>
<td>User Notification</td>
<td>2. Enable to allow user notifications in the event of network connection policy violations.</td>
</tr>
<tr>
<td>Remediation Action for Bridge Network Connection</td>
<td>3. If <strong>Allow Bridge Network Connection</strong> is disabled, then specify whether to take no action when a bridge network connection exists or to disable all bridge network connections.</td>
</tr>
<tr>
<td>Remediation Action for Internet Connection Sharing</td>
<td>4. If <strong>Allow Internet Connection Sharing</strong> is disabled, then specify whether to take no action when Internet connection sharing exists or to disable Internet connection sharing.</td>
</tr>
<tr>
<td>Remediation Action for Adhoc/Hosted Wireless Networks</td>
<td>5. If <strong>Allow Adhoc/Hosted Wireless Networks</strong> is disabled, then specify whether to take no action when an adhoc wireless network exists or to disable all adhoc/hosted wireless networks.</td>
</tr>
</tbody>
</table>

**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.

To configure disk encryption:

1. From the ClearPass macOS Universal System Health Validator page, enable checks for the selected version of Windows.
2. Select **Disk Encryption**.
3. Enable the **A disk encryption application is on** check box to provide the options to specify the remediation checks, auto remediation, or user notification.

The **Disk Encryption** page opens:
4. Specify the Disk Encryption parameters as described in the following table:

**Table 1: Disk Encryption Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for disk encryption policy violations.</td>
</tr>
<tr>
<td>Product-specific checks</td>
<td>If you wish to select a specific disk encryption product, do not change the default setting.</td>
</tr>
<tr>
<td></td>
<td>To allow any encryption product to check disk encryption, select the <strong>Uncheck to allow any product</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Select Disk Encryption product</strong> and <strong>Product Version is at least</strong> fields are disabled after you uncheck the <strong>Uncheck to allow any product</strong> check box.</td>
</tr>
<tr>
<td>Select Disk Encryption product</td>
<td>Select a specific disk encryption product.</td>
</tr>
<tr>
<td>Product Version is at least</td>
<td>Search for the production version of the selected product.</td>
</tr>
<tr>
<td>Locations to Check</td>
<td>Select location to check. The options are:</td>
</tr>
<tr>
<td></td>
<td>■ None</td>
</tr>
<tr>
<td></td>
<td>■ System Root Drive</td>
</tr>
<tr>
<td></td>
<td>■ All Drives</td>
</tr>
<tr>
<td></td>
<td>■ Specific Locations</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**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 273), you can turn on the installed applications check and specify information about which installed applications you want to monitor.

To configure the installed applications for Windows:

1. From the ClearPass Windows Universal System Health Validator page, enable checks for the selected version of Windows.
2. Select **Installed Applications**.
3. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **Installed Application Check is on** check box.

   The **Installed Applications** page opens:

   **Figure 273** Installed Applications for Windows Configuration Page

4. Specify the **Installed Applications Configuration** page parameters as described in the following table:

   **Table 1:** Installed Applications for Windows Configuration Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation checks</td>
<td><strong>Auto-Remediation</strong> for the Installed Applications health class is not supported.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable sending a remediation message with a list of applications to install or uninstall to the user.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Enable <strong>Monitor Mode</strong> to treat all the installed applications as always healthy.</td>
</tr>
<tr>
<td>Applications Allowed (Mandatory)</td>
<td>Specify installed applications to be monitored on a mandatory basis. <strong>NOTE:</strong> Enter the application name as they are shown in Add/Remove Programs.</td>
</tr>
<tr>
<td>Applications Allowed (Optional)</td>
<td>Specify installed applications to be monitored on an optional basis. <strong>NOTE:</strong> Enter the application name as they are shown in Add/Remove Programs.</td>
</tr>
<tr>
<td>Allow only Mandatory and Optional Applications</td>
<td>Specify that only the mandatory and optional applications are monitored. <strong>NOTE:</strong> All applications that are not either mandatory or optional must be removed or uninstalled.</td>
</tr>
</tbody>
</table>

   **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 273).

4. From the desired **Applications Allowed** category, click **Add**.

   The **Add Mandatory Applications** dialog for the selected **Applications Allowed** category opens.

   **Figure 274  Enabling Regular Expression**

![Enable checks for Windows 10](image)

5. Configure the **Add Mandatory Applications** parameters as described in **Table 2**.

**Table 2: Mandatory Applications Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Application Name</td>
<td>Enter the name of the application.</td>
</tr>
<tr>
<td>Enable Regular Expression</td>
<td>Check (enable) this check box to enable the use of regular expressions in the <strong>Application Name</strong>. When this field is enabled, ClearPass treats the <strong>Application Name</strong> as regular expression when comparing application names.</td>
</tr>
<tr>
<td>Remediation Message</td>
<td>Optionally, enter the remediation message that will be displayed to the user in the event of an error. <strong>NOTE:</strong> Remediaiton messages can include reasons for remediation, links to helpful URLs and helpdesk contact information.</td>
</tr>
</tbody>
</table>

6. Click **Save**.

   You return to the **Installed Applications** dialog, where **Regular Expression Enabled** is set to **true** for the specified application (see Figure 275).
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:

The following table describes the File Check Configuration parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation checks</td>
<td>Auto-remediation for the File Check health class is not supported.</td>
</tr>
<tr>
<td>User Notification</td>
<td>1. When enabled, a remediation message that includes the groups of files to be present or absent is displayed to the end user.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>2. To treat all the file check health classes as always healthy, enable Monitor Mode.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Groups to be Present</td>
<td>3. To add the files to be present in the File Check health class, click Add.</td>
</tr>
<tr>
<td>File Groups to be Absent</td>
<td>4. To add the files to be absent in the File Check health class, click Add.</td>
</tr>
</tbody>
</table>

**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:

   ![Image of File Group to Be Present > Add dialog](image)

   The following table describes the **File Group to be Present > Add** parameters:

   **Table 2: File Group to be Present - Add Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the File Group Name</td>
<td>1. Enter the name of the file group.</td>
</tr>
<tr>
<td>File Group Evaluation Rule</td>
<td>2. Select the appropriate File Group Evaluation Rule:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass All</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass Any One</strong>: 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.</td>
</tr>
</tbody>
</table>

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:
The following table describes the **File to be Present > Add** parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Location</td>
<td>1. Select any location of the file from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• SystemDrive</td>
</tr>
<tr>
<td></td>
<td>• Systemroot</td>
</tr>
<tr>
<td></td>
<td>• ProgramFiles</td>
</tr>
<tr>
<td></td>
<td>• ProgramFiles (x86)</td>
</tr>
<tr>
<td></td>
<td>• HOMEDRIVE</td>
</tr>
<tr>
<td></td>
<td>• HOMEPATH</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td>Enter the File Path</td>
<td>2. Enter the file path as described in the examples from the user interface.</td>
</tr>
<tr>
<td>Enter the File Name</td>
<td>3. Enter the name of the file.</td>
</tr>
<tr>
<td>Enter the MD5 Sum</td>
<td>Optionally, specify one or more (comma separated) MD5 checksums of the process executable file.</td>
</tr>
<tr>
<td>Remediation Message</td>
<td>4. Specify the custom remediation message to be displayed to end users if <strong>File check</strong> fails.</td>
</tr>
</tbody>
</table>

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:
Windows System Health Validator: OnGuard Agent

This Windows System Health Validator checks for current Windows Service Packs. The OnGuard Agent also supports Windows Server 2016, as well 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:

2. Click Add.
   - The Add Posture Policies dialog opens.

3. Specify the following:
   a. Policy Name: 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. **Plugin Version**: OnGuard plugin version 2.0 (V4 SDK) is set by default.

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 opens:

   **Figure 280 OnGuard Agent: Windows System Health Validator**

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**.

   You return to the **Posture Policies > Posture Plugins** page, where the Status column for the **Windows System Health Validator** now shows **Configured**.

**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 281** Onguard Agent: Windows Security Health Validator Page

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 OnGuard Dissolvable Agent version of the ClearPass Linux Universal System Health Validator plug-in supports the following health classes:

- **Antivirus** on page 301
- **Services** on page 303

To configure the ClearPass Linux Universal System Health Validator plugin:

1. Navigate to **Configuration > Posture > Posture Policies**.
2. Click **Add**.
   
   The **Add Posture Policies** dialog opens.
3. 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 **Linux**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.

4. Click **Next**.
   The **Posture Plugins** dialog opens.

5. Select the **ClearPass Linux Universal System Health Validator**, then click **Configure** to configure antivirus settings and service types.

The Linux posture plugin configuration dialog opens.
Figure 284  Configuring the ClearPass Linux Universal System Health Validator

6. From the left pane, select the appropriate Linux OS:
   - CentOS
   - Fedora
   - Red Hat Enterprise Linux
   - SUSE Linux Enterprise
   - Ubuntu

7. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the Enable checks for Linux_OS check box.

Antivirus

Use the Antivirus page to turn on an Antivirus application.

1. Select Antivirus.

2. Click An antivirus application is on to configure the Antivirus application information.

   The following figure displays the Antivirus health class configuration page:

   Figure 285  Antivirus Page

3. Specify the Antivirus health class parameters as described in the following table:
Table 1: Antivirus Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation checks</td>
<td>Enable to allow auto-remediation for the Antivirus health class.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications in the event of process policy violations.</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Shows the name of the Antivirus configured. Click Add to specify the name of the Antivirus.</td>
</tr>
<tr>
<td>Prd Version</td>
<td>Shows the version of the Antivirus.</td>
</tr>
<tr>
<td>Eng Version</td>
<td>Shows the Engine version of the Antivirus.</td>
</tr>
<tr>
<td>Dat Version</td>
<td>Shows the version of the data file.</td>
</tr>
</tbody>
</table>

4. To configure the Antivirus product specific checks, click Add.

The values configured in the Antivirus Product configuration dialog will be displayed in the Antivirus page. The following figure is an example of the Antivirus Product configuration dialog:

**Figure 286  Antivirus Product Configuration Dialog**

The following table describes the Antivirus Product configuration parameters:

Table 2: Antivirus Product configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product-specific checks</td>
<td>Select this check box if you want to configure a specific antivirus product. If you want to allow any antivirus product, do not enable this field.</td>
</tr>
<tr>
<td>Select the Antivirus product</td>
<td>Select the Antivirus from the drop-down list.</td>
</tr>
<tr>
<td>Product version check</td>
<td>Select one of the following options to check the product version:</td>
</tr>
<tr>
<td></td>
<td>▬ No Check</td>
</tr>
<tr>
<td></td>
<td>▬ Is Latest</td>
</tr>
<tr>
<td></td>
<td>▬ In Last N Updates.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Engine Version Check</td>
<td>Select one of the following options to check the engine version:</td>
</tr>
<tr>
<td></td>
<td>■ No Check</td>
</tr>
<tr>
<td></td>
<td>■ Is Latest</td>
</tr>
<tr>
<td></td>
<td>■ In Last N Updates.</td>
</tr>
<tr>
<td>Data file version check</td>
<td>Select one of the following options to check the data file version:</td>
</tr>
<tr>
<td></td>
<td>■ No Check</td>
</tr>
<tr>
<td></td>
<td>■ Is Latest</td>
</tr>
<tr>
<td></td>
<td>■ In Last N Updates.</td>
</tr>
</tbody>
</table>

**Services**

The **Services** page provides a set of widgets for specifying services to run or stop.

1. Select **Services**.
   
The **Services** configuration page opens:

   **Figure 287 Services Configuration Page**

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

**Table 3: Services Page**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto remediation for service checks (Automatically stop or start services based on the entries in <strong>Service to run</strong> and <strong>Services to stop</strong> configuration).</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for service check policy violations.</td>
</tr>
<tr>
<td>Available Services</td>
<td>This scrolling list contains a list of services that you can select and move to the <strong>Services to run</strong> or <strong>Services to stop</strong> panels (using their associated widgets). This list varies depending on OS types.</td>
</tr>
<tr>
<td></td>
<td>■ To add the service(s) to the <strong>Services to run</strong> pane, select the service(s) in the <strong>Available Services</strong> pane, then click &gt;&gt; arrows.</td>
</tr>
<tr>
<td></td>
<td>■ To add the service(s) to the <strong>Services to stop</strong> pane, select the service(s) in the <strong>Available Services</strong> pane, then click &gt;&gt; arrows.</td>
</tr>
<tr>
<td></td>
<td>■ To move services from the Services to run or Services to stop panes, select the appropriate services, then click the corresponding &lt;&lt; arrows.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Insert</td>
<td>To add a service to the list of available services, enter its name in the text box adjacent to this button, then click <strong>Insert</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>To remove a service from the list of available services, select it and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

**ClearPass macOS Universal System Health Validator: OnGuard Agent**

To configure the ClearPass Universal System Health Validator for macOS:

1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**.
   
   The **Add Posture Policies** dialog opens.

   **Figure 288 Adding a Universal System Health Validator for a macOS Posture Policy**

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 **macOS**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.

3. Click **Next**.
   
   The **Posture Plugins** dialog opens.

   **Figure 289 Selecting the macOS Universal System Health Validator Posture Plug-in**

4. In the **Posture Plugins** page, click the check box for **ClearPass macOS Universal System Health Validator**.

5. Click **Configure**.
   
   The **ClearPass macOS Universal System Health Validator** configuration page is displayed.

6. To enable checks for mac OS, select the **Enable checks for macOS** check box.
   
   The following configuration page opens:
Figure 290  Configuration Page: macOS Universal System Health Validator

Configuring macOS Health Checks

For details on configuring health checks for macOS, refer to the set of health check configuration pages described in the following sections:

- [Services on page 305](#)
- [Processes on page 307](#)
- [Antivirus on page 310](#)
- [Firewall on page 313](#)
- [Patch Management on page 315](#)
- [USB Devices on page 320](#)
- [Virtual Machine on page 320](#)
- [Network Connections on page 321](#)
- [Disk Encryption on page 323](#)
- [Installed Applications on page 325](#)
- [File Check](#)

Services

From the Services page, you can configure which services to run and which services to stop.

To add or remove specific services on the endpoint:

1. Navigate to Configuration > Posture > Posture Policies, then click Add.

The Add Posture Policies dialog opens.
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 **macOS**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.

3. Click **Next**.
   The **Posture Plugins** dialog opens.

4. Select the **ClearPass macOS Universal System Health Validator**, then click **Configure**.

5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **Enable checks for macOS** check box.

6. Select **Services**.
   The **Services** health class configuration page opens:

   ![Services Health Class Configuration Page](image)

7. Specify the **ClearPass macOS Universal System Health Validator > Services** configuration parameters as described in the following table:
**Table 1: Services Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>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.</td>
</tr>
<tr>
<td>User Notification</td>
<td>When enabled, a remediation message that includes the groups of services to be present or absent is displayed to the end user.</td>
</tr>
</tbody>
</table>

**Specifying the Services to Run**

To specify the services to run:

1. Select one or more of the desired services from the Available Services list.
2. To move the desired services to the Services to Run box, click >>, then click Save.
3. 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.

**Specifying the Services to Stop**

To specify the services to stop:

1. Select one or more of the desired services from the Available Services list.
2. To move the desired services to the Services to Stop box, click >>, then click Save.
3. 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.

**Processes**

The Processes page provides a set of parameters to specify which processes to be explicitly present or absent on the system.

To view and configure processes:

1. Navigate to Configuration > Posture > Posture Policies, then click Add.
   
   The AddPosture Policies dialog opens.

   **Figure 293 Adding a Universal System Health Validator for a macOS Posture Policy**

   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 macOS.
      d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.
3. Click Next. The Posture Plugins dialog opens.
4. Select the ClearPass macOS Universal System Health Validator, then click Configure.
5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the Enable checks for macOS check box.
6. Select Processes. The Processes health class configuration page opens:

**Figure 294** Processes Page for macOS

7. Specify the Processes configuration parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto-remediation for processes.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications in the event of process policy violations.</td>
</tr>
</tbody>
</table>

**Processes to be Present Parameters**

1. In the Processes to be Present section, click Add. The Add Processes to be Present page opens.
2. To open the page with options to configure the name, location, and display name of the processes, click Add. The Process to be Present > Add page opens:
3. Specify the Processes to be Present parameters as described in the following table, then click Save:

**Table 2: Processes to be Present Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Location</td>
<td>Choose from the following locations:</td>
</tr>
<tr>
<td></td>
<td>- Applications</td>
</tr>
<tr>
<td></td>
<td>- UserBin</td>
</tr>
<tr>
<td></td>
<td>- UserLocalBin</td>
</tr>
<tr>
<td></td>
<td>- UserSBin</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td>Enter the Process name</td>
<td>Specify the path name containing the process executable name.</td>
</tr>
<tr>
<td>Enter the Display name</td>
<td>Enter a user-friendly name for the process. This is displayed in end-user facing</td>
</tr>
<tr>
<td></td>
<td>messages.</td>
</tr>
</tbody>
</table>

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 296** shows the configuration parameters for when you select Process Name and when you select MD5 Sum.
2. Specify the **Processes to be Absent** parameters as described in the following table, then click **Save**:

**Table 3: Processes to Be Absent Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Type</td>
<td>Select the type of process check to perform. The agent can look for the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Process Name</strong>: The agent looks for all processes that matches with the given name.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MD5 Sum</strong>: This specifies one or more (comma-separated) MD5 checksums of the process executable file.</td>
</tr>
<tr>
<td></td>
<td>For example, if there are multiple versions of the process executable, you can specify the MD5 sums of all versions here.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Enter the Display name</td>
<td>Enter a user-friendly name for the process. This display name is displayed in end-user facing messages.</td>
</tr>
</tbody>
</table>

You return to the **Processes Configuration** page, which now shows the values for the processes that were configured.

**Antivirus**

In the **Antivirus** page, you can turn on an Antivirus application.
To define the macOS Antivirus health class:

1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**.
   The **AddPosture Policies** dialog opens.

**Figure 297 Adding a Universal System Health Validator for a macOS Posture Policy**

![Image of AddPosture Policies dialog](image)

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 **macOS**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.

3. Click **Next**.
   The **Posture Plugins** dialog opens.

4. Select the **ClearPass macOS Universal System Health Validator**, then click **Configure**.

5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **Enable checks for macOS** check box.

6. Select **Antivirus**.
   The **Antivirus** health class configuration page opens:

**Figure 298 MacOS Antivirus Page**

![Image of MacOS Antivirus Page](image)

7. Configure the initial Antivirus parameters as described in the following table:
**Table 1: Initial Antivirus Health Class Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Antivirus Application is On</td>
<td>To enable testing of health data for configured Antivirus application(s), click <strong>Antivirus application is on</strong>.</td>
</tr>
<tr>
<td>Auto Remediation</td>
<td>To enable auto remediation of anti-virus status, check the <strong>Auto Remediation</strong> check box. This option is enabled by default.</td>
</tr>
<tr>
<td>User Notification</td>
<td>To enable user notification of policy violation of anti-virus status, enable <strong>User Notification</strong>. This option is enabled by default.</td>
</tr>
<tr>
<td>Display Update URL</td>
<td>To show the origination URL of the update, check(able) the <strong>Display Update URL</strong> check box. This option is disabled by default.</td>
</tr>
</tbody>
</table>

8. To specify product and version check information in the antivirus configuration page, click **Add**.

**Figure 299** *MacOS Antivirus Configuration > Add Page*

9. Specify the Add Antivirus health class parameters as described in the following table:

**Table 2: Add Antivirus Health Class Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product-specific checks</td>
<td>To configure for product-specific checks, leave the check box checked (the default setting). To allow any Antivirus product, uncheck the check box. All of these checks may not be available for some products. Where checks are not available, they are shown in the disabled state.</td>
</tr>
<tr>
<td>Select the antivirus product</td>
<td>Select an antivirus product from the drop-down list.</td>
</tr>
</tbody>
</table>
| Product version check    | Select one of the following options:  
  ▪ **No Check** |
Table 2: Add Antivirus Health Class Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Is Latest:</strong> Requires registration with ClearPass portal.</td>
</tr>
<tr>
<td></td>
<td><strong>In Last N Updates:</strong> Requires registration with ClearPass Portal.</td>
</tr>
<tr>
<td>Datafile version check</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>No Check</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Is Latest:</strong> Requires registration with ClearPass portal.</td>
</tr>
<tr>
<td></td>
<td><strong>In Last N Updates:</strong> Requires registration with ClearPass Portal.</td>
</tr>
<tr>
<td>Data file has been updated in</td>
<td>Enter the number, then specify the interval in hours, days, weeks, or months.</td>
</tr>
<tr>
<td>Last scan has been done before</td>
<td>Enter the number, then specify the interval in hours, days, weeks, or months.</td>
</tr>
<tr>
<td>Real-time Protection Status Check</td>
<td><strong>No Check:</strong> ClearPass does not use the Real-time Protection status value for health evaluation. This means that the client is treated as healthy irrespective of the value of its Real-time Protection status.</td>
</tr>
<tr>
<td></td>
<td><strong>On:</strong> Marked as healthy only if the value of Real-time Protection status is On.</td>
</tr>
</tbody>
</table>

10. Click **Save**.

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

**Firewall**

In the **Firewall** page, you can specify that a Firewall application must be on and specify information about the Firewall application.

To view and configure processes:

1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**.

   The **Add Posture Policies** dialog opens.

**Figure 300 Adding a Universal System Health Validator for a macOS Posture Policy**

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 **macOS**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.
3. Click **Next**.
The Posture Plugins dialog opens.

4. Select the ClearPass macOS Universal System Health Validator, then click Configure.

5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the Enable checks for macOS check box.

6. Select Firewall.
   The Firewall health class configuration page opens:

7. To configure the firewall application information, click A Firewall Application is On. The Firewall page opens:

   Figure 301 MacOS Firewall Page

8. Specify the initial Firewall parameters as described in the following table:

   Table 1: Firewall Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Firewall Application is On</td>
<td>Check the Firewall Application is On check box to enable testing of health data for configured firewall application(s).</td>
</tr>
<tr>
<td>Auto Remediation</td>
<td>Check the Auto Remediation check box to enable auto remediation of firewall status.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Check the User Notification check box to enable user notification of policy violation of firewall status.</td>
</tr>
<tr>
<td>Product-specific checks</td>
<td>To specify Firewall product-specific checks, leave this parameter as is. To specify whether any firewall application (any vendor) is running on the end host, uncheck the Uncheck to allow any product check box.</td>
</tr>
</tbody>
</table>

9. To configure different configuration elements specific to the firewall product that you select, from the Firewall page, click Add. The Add macOS Firewall page opens.

   Figure 302 MacOS Firewall > Add Page

10. Specify the parameters as described in the following table:
Table 2: Firewall Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the firewall product</td>
<td>From the drop-down list, select the firewall product.</td>
</tr>
<tr>
<td>Product Version is at least</td>
<td>Optionally, specify the Product Version is at least. Check for the version of the latest product release.</td>
</tr>
</tbody>
</table>

11., Click **Save**.

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

**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.

   **Figure 303  Adding a Universal System Health Validator for a macOS Posture Policy**

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 **macOS**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.

3. Click **Next**.
   
   The **Posture Plugins** dialog opens.

4. Select the **ClearPass macOS Universal System Health Validator**, then click **Configure**.

5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **Enable checks for macOS** check box.

6. Select **Patch Management**.
   
   The **Patch Management** health class configuration page opens:
   
   The initial Patch Management configuration dialog opens.
7. Specify the initial Patch Management parameters as described in the following table.

**Table 1: Patch Management Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A patch management application is on</td>
<td>To enable testing of health data for configured Antivirus application(s), check the <strong>A patch management application is on</strong> check box. The Patch Management configuration dialog opens</td>
</tr>
<tr>
<td>Remediation Checks</td>
<td></td>
</tr>
<tr>
<td>Auto Remediation</td>
<td>To enable auto-remediation of patch management status, check the <strong>Auto Remediation</strong> check box.</td>
</tr>
<tr>
<td>User Notification</td>
<td>To enable user notification of policy violation of patch management status, check the <strong>User Notification</strong> check box.</td>
</tr>
<tr>
<td>Product Evaluation Rule</td>
<td></td>
</tr>
<tr>
<td>Product Evaluation Rule</td>
<td>Select the appropriate <strong>Product Evaluation Rule</strong>:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass All</strong>: Select this product evaluation rule if you want the <strong>Patch Management</strong> health class to be deemed as <strong>healthy</strong> only if all the configured patch management products are present. <strong>Pass All</strong> is the equivalent of an <strong>AND</strong> condition.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pass Any One</strong>: Select this product evaluation rule if you want the <strong>Patch Management</strong> health class to be deemed as <strong>healthy</strong> if any one of the configured patch management products are present. <strong>Pass Any One</strong> is the equivalent of an <strong>OR</strong> condition. <strong>Pass Any One</strong> is the default.</td>
</tr>
</tbody>
</table>

8. To configure the options for the specific patch management product, click **Add**. The **Patch Management > Add** page opens:
9. Specify the Patch Management parameters as described in the following table:

Table 2: Patch Management Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product-specific checks</td>
<td>To configure product-specific checks, leave this option as is. To check whether any patch management application (any vendor) is running on the end host, clear the <strong>Uncheck to allow any product</strong> check box.</td>
</tr>
<tr>
<td>Select Patch Management Product</td>
<td>Select a patch management product vendor. This option is enabled only if the <strong>Product-specific checks</strong> check box is checked.</td>
</tr>
<tr>
<td>Product version is at least</td>
<td>Enter the minimally recommended product version number. This option is enabled only if the <strong>Product-specific checks</strong> check box is checked.</td>
</tr>
<tr>
<td>Status Check Type</td>
<td>Specify the <strong>Status Check Type</strong> 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 <strong>Auto-remediation</strong> is enabled, OnGuard Agent changes the Patch Agent Status on the client to the configured value. Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Check</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Enabled</strong>: Patch Agent is turned on and it automatically updates the client.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disabled</strong>: Patch Agent is disabled and it will not check for missing patches and update the client.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Notify Before Download</strong>: Patch Agent is turned on and it notifies the user before downloading updates.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Notify Before Install</strong>: Patch Agent is turned on and it notifies the user before installing updates.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>The values specific to the selected patch management product are displayed in the <strong>Status Check Type</strong> field. For example, all five values are displayed for Microsoft Windows Automatic Update. For Microsoft System Center Configuration Manager (SCCM), only <strong>No Check</strong>, <strong>Disabled</strong>, and <strong>Notify Before Install</strong> are displayed.</td>
</tr>
</tbody>
</table>
### Parameter | Action/Description
--- | ---
Install Level Check Type  | This option is only enabled if the **Product-specific checks** check box is checked. For Microsoft SCCM, selecting **All** will return the full list of all missing patches.
- **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.
- **All**: Checks for all missing patches and searches for all available 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.
- **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.

10. Click **Save**.
   When you save the patch management configuration, the configuration information is displayed on the **Patch Management** page:

**Peer To Peer**
From the **Peer To Peer** page, you can view and add peer-to-peer applications.
To view and configure processes:
1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**.
   The **Add Posture Policies** dialog opens.

**Figure 306  Adding a Universal System Health Validator for a macOS Posture Policy**

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 **macOS**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.
3. Click Next.
   The Posture Plugins dialog opens.
4. Select the ClearPass macOS Universal System Health Validator, then click Configure.
5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the Enable checks for macOS check box.
6. Select Peer to Peer.
7. To provide configuration options to specify peer-to-peer applications or networks that need to be explicitly stopped, click A Peer to Peer application is on.
   The Peer to Peer health class configuration page opens:

   Figure 307  Peer To Peer Page

8. Specify the Peer to Peer parameters as described in the following table:

   Table 1: Peer-to-Peer-Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto remediation for service checks (Automatically stop peer-to-peer applications based on the entries in Applications to stop configuration).</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for peer-to-peer application/network check policy violations.</td>
</tr>
<tr>
<td>By Application</td>
<td>Select the appropriate radio button to select individual peer-to-peer applications or a group of applications that use specific peer-to-peer networks. When you select a peer-to-peer network, all applications that make use of that network are stopped.</td>
</tr>
<tr>
<td>By Network</td>
<td></td>
</tr>
<tr>
<td>Available Applications</td>
<td>This scrolling list contains a list of applications or networks that you can select and move to the Applications to stop pane.</td>
</tr>
<tr>
<td></td>
<td>Select the applications or networks in the Available Applications pane, then click the &gt;&gt; to add the applications or networks to the Applications to stop pane.</td>
</tr>
<tr>
<td>Applications to Stop</td>
<td>Select the applications or networks in the Applications to stop pane, then click the &lt;&lt; to move the applications or networks to the Available Applications pane.</td>
</tr>
</tbody>
</table>

9. Click Save.
USB Devices

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

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 308**  *USB Devices Page*

![USB Devices Page](image)

The following table describes the **USB Devices** parameters:

**Table 1: MacOS USB Devices Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto remediation for USB mass storage devices attached to the endpoint (automatically stop or eject the drive).</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for USB devices policy violations.</td>
</tr>
</tbody>
</table>
| 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 Machine

The **Virtual Machines** page provides configuration options to virtual machines utilized by the network.

1. Select the **Virtual Machine Detection is on** option to enable the **Auto Remediation** and **User Notification** options.

   The macOS **Virtual Machine** page opens:

**Figure 309**  *Virtual Machine Page*

![Virtual Machine Page](image)

The following table describes the **Virtual Machines** parameters:
### Table 1: Virtual Machines

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>Enable to allow auto remediation for virtual machines connected to the endpoint.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for virtual machine policy violations.</td>
</tr>
<tr>
<td>Allow access to clients running on Virtual Machine</td>
<td>Enable to allow clients that running a VM to be accessed and validated.</td>
</tr>
<tr>
<td>Allow access to clients hosting Virtual Machine</td>
<td>Enable to allow clients that hosting a VM to be accessed and validated.</td>
</tr>
</tbody>
</table>
| 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 the host.  
                                                                  - Pause all virtual machines running on Host: Pause the VM clients that are running on the host. |

2. Click **Save**.

**Network Connections**

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

To configure Network Connections:

1. From the ClearPass macOS Universal System Health Validator page, enable checks for macOS.
2. Select **Network Connections**.
3. Enable the **Network Connection Check is on** check box to provide the options to specify the remediation checks or user notification.
   
   The **Network connections** page opens:
   
   **Figure 310 Network Connections Page**

4. Select the **Check for Network Connection Types** check box.
5. To specify type of network connection, click **Configure**.

   The **Network Connection Types** configuration page opens.
6. Specify the **Network Connection Types** configuration parameters as described in the following table:

**Table 1: Network Connection Type Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Network Connections Type</td>
<td>1. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Allow Only One Network Connection</td>
</tr>
<tr>
<td></td>
<td>- Allow One Network Connection with VPN</td>
</tr>
<tr>
<td></td>
<td>- Allow Multiple Network Connections</td>
</tr>
<tr>
<td>Network Connection Types</td>
<td>2. To add or remove Others, Wired, and Wireless network connection types, click &gt;&gt; or &lt;&lt;.</td>
</tr>
<tr>
<td>Remediation Action for Network Connection Types Not Allowed</td>
<td>3. Specify one of the following:</td>
</tr>
<tr>
<td></td>
<td>- No Action: Take no action. Do not eject or disable the attached devices.</td>
</tr>
<tr>
<td></td>
<td>- Disable Network Connections</td>
</tr>
<tr>
<td></td>
<td>- Disconnect Network Connections</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

This returns you to the **Network Connections** configuration page. The following table describes the remaining fields on this page:

**Table 2: Network Connections Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Remediation</td>
<td>1. Enable to allow auto-remediation for network connections.</td>
</tr>
<tr>
<td>User Notification</td>
<td>2. Enable to allow user notifications in the event of network connection policy violations.</td>
</tr>
<tr>
<td>Remediation Action for Bridge Network Connection</td>
<td>3. If <strong>Allow Bridge Network Connection</strong> is disabled, then specify whether to take no action when a bridge network connection exists or to disable all bridge network connections.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remediation Action for Internet Connection Sharing</td>
<td>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.</td>
</tr>
<tr>
<td>Remediation Action for Adhoc/Hosted Wireless Networks</td>
<td>5. If Allow Adhoc/Hosted Wireless Networks is disabled, then specify whether to take no action when an adhoc wireless network exists or to disable all adhoc/hosted wireless networks.</td>
</tr>
</tbody>
</table>

**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.

To configure disk encryption for macOS:

1. Navigate to **Configuration > Posture > Posture Policies**. The **Posture Policies** page opens.
2. Click the **Add** link. The **Posture Policies > Add** page opens.

**Figure 312 Configuring Disk Encryption for a macOS Posture Policy**

3. 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 **macOS**.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.
4. Click **Next**.
   The **Posture Plugins** dialog opens.
5. Select the check box for the ClearPass macOS Universal System Health Validator, then click the **Configure** button.
6. From the ClearPass macOS Universal System Health Validator page, enable checks for macOS.
7. From the list of macOS health checks, select **Disk Encryption**.
8. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **A disk encryption application is on** check box.

   The **Disk Encryption** page opens:

   *Figure 313  MacOS Disk Encryption Page*

9. To configure the product specific encryption checks, click **Add**.

   The **Disk Encryption > Add** page opens.

   *Figure 314  Disk Encryption Add Page*

10. Specify the macOS **Disk Encryption** health check parameters as described in the following table:
### Table 1: macOS Disk Encryption Health Check Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Notification</td>
<td>Enable to allow user notifications for disk encryption policy violations.</td>
</tr>
<tr>
<td>Product-specific checks</td>
<td>If you wish to select a specific disk encryption product, do not change the default setting. To allow any encryption product to check disk encryption, select the <strong>Uncheck to allow any product</strong> check box. The <strong>Select Disk Encryption product</strong> and <strong>Product Version is at least</strong> fields are disabled after you uncheck the <strong>Uncheck to allow any product</strong> check box.</td>
</tr>
<tr>
<td>Select Disk Encryption product</td>
<td>Select a specific disk encryption product.</td>
</tr>
<tr>
<td>Product Version is at least</td>
<td>Search for the production version of the selected product.</td>
</tr>
</tbody>
</table>
| Locations to Check               | Select the locations to check disk encryption. The options are:  
  ■ None  
  ■ System Root Drive  
  ■ All Drives  
  ■ Specific Locations                                                                                                                               |
| Locations to Exclude             | Specify locations that should be excluded from disk encryption checks. During posture evaluation, ClearPass does not check the encryption state of the drives specified in **Locations to Exclude. Locations to Exclude** is optional and is shown only when **Locations to Check** is set to **All Drives**. This field accepts a list of locations separated by new line; for example:  
  Recovery VM                                                                                                                                           |

11. Click **Save**.

**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.

To configure the installed applications for macOS:

1. Navigate to **Configuration > Posture > Posture Policies**, then click **Add**. The **Add Posture Policies** dialog opens.

**Figure 315** Adding a Universal System Health Validator for a macOS Posture Policy
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 macOS.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.

3. Click **Next**.
   The **Posture Plugins** dialog opens.

4. Select the ClearPass macOS Universal System Health Validator, then click **Configure**.

5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **Enable checks for macOS** check box.

6. Select **Installed Applications**.

7. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **Installed Application Check is on** check box.
   The **Installed Applications** health check configuration page opens:

   **Figure 316 Installed Applications Page for macOS**

8. Specify the **Installed Applications for macOS Configuration** page parameters as described in the following table:
### Table 1: Installed Applications for macOS Configuration Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation checks</td>
<td><strong>Auto-Remediation</strong> for the Installed Applications health class is not supported.</td>
</tr>
<tr>
<td>User Notification</td>
<td>Enable sending a remediation message with a list of applications to install or uninstall to the user.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Enable <strong>Monitor Mode</strong> to treat all the installed applications as always healthy.</td>
</tr>
<tr>
<td>Applications Allowed (Mandatory)</td>
<td>Specify installed applications to be monitored on a mandatory basis. <strong>NOTE:</strong> Enter the application names as they are shown in Add/Remove Programs.</td>
</tr>
<tr>
<td>Applications Allowed (Optional)</td>
<td>Specify installed applications to be monitored on an optional basis. <strong>NOTE:</strong> Enter the application name as they are shown in Add/Remove Programs.</td>
</tr>
<tr>
<td>Allow only Mandatory and Optional Applications</td>
<td>Specify that only the mandatory and optional applications are monitored. <strong>NOTE:</strong> All applications that are not either mandatory or optional must be removed or uninstalled.</td>
</tr>
</tbody>
</table>

9. Click **Save**.

**Enabling Regular Expressions for a macOS Application**

To enable regular expressions for an application:

1. From the **ClearPass macOS Universal System Health Validator > Configure** page (see **ClearPass macOS Universal System Health Validator: OnGuard Agent**), select **Installed Applications**.
2. Click (enable) the **Installed Applications Check is on** check box. The Installed Applications dialog appears (see **Figure 316** above).
3. From the **Applications Allowed (Mandatory)** category, click **Add**. The **Add Mandatory Applications** dialog appears (see **Figure 317**).

**Figure 317 Enabling Regular Expression**

4. Configure the **Add Mandatory Applications** parameters as described in **Table 2**.

---

ClearPass 6.7 Policy Manager | User Guide
Table 2: Add Mandatory Applications Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Application Name</td>
<td>Enter the name of the application.</td>
</tr>
<tr>
<td>Enable Regular Expression</td>
<td>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.</td>
</tr>
<tr>
<td>Remediation Message</td>
<td>Optionally, enter the remediation message that will be displayed to the user in the event of an error. <strong>NOTE</strong>: Remediation messages can include reasons for remediation, links to helpful URLs and helpdesk contact information.</td>
</tr>
</tbody>
</table>

5. Click **Save**. You return to the Installed Applications dialog, where **Regular Expression Enabled** is set to **true** for the specified application.

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.

To configure macOS File Check:

1. Navigate to Configuration > Posture > Posture Policies, then click **Add**. The Add Posture Policies dialog opens.

![Figure 318 Adding a Universal System Health Validator for a macOS Posture Policy](image)

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 macOS.
   d. **Plugin Version**: OnGuard Plugin version 2.0 (V4 SDK) is set by default.
3. Click **Next**. The Posture Plugins dialog opens.
4. Select the **ClearPass macOS Universal System Health Validator**, then click **Configure**.
5. To provide the options to specify the remediation checks, auto remediation, or user notification, enable the **Enable checks for macOS** check box.
6. Select **File Check**.

The **File Check** health class configuration page opens:

The following figure is an example of the **File Check** health class configuration dialog:

**Figure 319**  *MacOS File Check Health Class Configuration*

![File Check Configuration](image)

7. Specify the **File Check Configuration** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation checks</td>
<td>Auto-remediation for the <strong>File Check</strong> health class is not supported.</td>
</tr>
<tr>
<td>User Notification</td>
<td>When enabled, a remediation message that includes the groups of files to be present or absent is displayed to the end user.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>To treat all the file check health classes as always healthy, enable <strong>Monitor Mode</strong>.</td>
</tr>
<tr>
<td>File Groups to be Present</td>
<td>To add the files to be present in the <strong>File Check</strong> health class, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>File Groups to be Absent</td>
<td>To add the files to be absent in the <strong>File Check</strong> health class, click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

8. 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 **File Group to Be Present > Add** dialog opens:
Figure 320  *MacOS File Group to Be Present > Add Dialog*

Specify the **File Group to Be Present > Add** parameters as described in the following table:

**Table 2: File Group to Be Present > Add Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the File Group Name</td>
<td>Enter the name of the file group.</td>
</tr>
</tbody>
</table>
| File Group Evaluation Rule| 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. |

9. 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 **File to Be Present > Add** page opens:

   **Figure 321  File to be Present > Add Dialog**

10. Specify the **File to Be Present > Add** parameters as described in the following table:
Table 3: File to Be Present > Add Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Location</td>
<td>Select any location of the file from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>- Applications</td>
</tr>
<tr>
<td></td>
<td>- UserBin</td>
</tr>
<tr>
<td></td>
<td>- UserLocalBin</td>
</tr>
<tr>
<td></td>
<td>- UserSBin</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td>Enter the File Path</td>
<td>Enter the file path as described in the examples provided.</td>
</tr>
<tr>
<td>Enter the File Name</td>
<td>Enter the name of the file.</td>
</tr>
<tr>
<td>Enter the MD5 Sum</td>
<td>Optionally, you can specify one or more (comma-separated) MD5 checksums of the</td>
</tr>
<tr>
<td></td>
<td>process executable file.</td>
</tr>
<tr>
<td>Remediation Message</td>
<td>Specify the custom remediation message to be displayed to end users if File check</td>
</tr>
<tr>
<td></td>
<td>fails.</td>
</tr>
</tbody>
</table>

11. 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.

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 331
- **Windows Security Health Validator: NAP Agent** on page 333

The following figure displays the **NAP Agent - Posture Plugins** tab:

**Figure 322**  NAP Agent - Posture Plugins Options

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 323  Adding a Windows NAP Agent Posture Policy

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 324  Posture Plugins for Windows Health Validators

5. From the **Posture Plugins** tab, select Windows System Health Validator, then click the **Configure** button.
   The Windows System Health Validator page appears:
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.
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 327 Selecting Posture Plugins for Windows Security Health Validator: NAP Agent**

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 328**.
Figure 328  Windows Security Health Validator

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 plug-ins, you must configure the rules for the posture policy.

To configure posture policy rules:

1. Navigate to **Configuration > Posture > Posture Policies**, then click the **Add** link.
   
   The **Add Posture Policies** dialog opens.

2. Click the **Rules** tab.
   
   The **Posture Policy Rules Editor** opens.

3. Click **Add Rule**.
   
   The **Rules Editor** opens.
4. Specify the Rules Editor configuration parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Plugin Checks</td>
<td>Click select one of the following plugin check types for System Health Validators.:</td>
</tr>
<tr>
<td></td>
<td>- Passes all System Health Validators checks</td>
</tr>
<tr>
<td></td>
<td>- Passes one or more System Health Validators checks</td>
</tr>
<tr>
<td></td>
<td>- Fails all System Health Validators checks</td>
</tr>
<tr>
<td></td>
<td>- Fails one or more System Health Validators checks</td>
</tr>
<tr>
<td>Select Plugins</td>
<td>Select the plug-in to which the plug-in checks should apply.</td>
</tr>
<tr>
<td>Posture Token</td>
<td>Select one of the following posture tokens:</td>
</tr>
<tr>
<td></td>
<td>- HEALTHY (0). This is the default.</td>
</tr>
<tr>
<td></td>
<td>- CHECKUP (10)</td>
</tr>
<tr>
<td></td>
<td>- TRANSITION (15)</td>
</tr>
<tr>
<td></td>
<td>- QUARANTINE (20)</td>
</tr>
<tr>
<td></td>
<td>- INFECTED (30)</td>
</tr>
<tr>
<td></td>
<td>- UNKNOWN (100)</td>
</tr>
</tbody>
</table>

**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 (NAP) 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:

The **Posture Compliance** check box must be selected on the **Service** tab in order for posture to be enabled.

**Figure 330  Posture Features at the Service Level**

You can configure the following components of a posture:

<table>
<thead>
<tr>
<th>Configurable Component</th>
<th>How to Configure</th>
</tr>
</thead>
</table>
| 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 [Creating a New Posture Policy](#).  
- To edit the selected posture policy, click **Modify**. |
| 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. |
**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:
- [Audit Service Flow Control](#)
- [Default Audit Servers](#)
- [Custom Audit Servers](#)
- [Post-Audit Rules](#)

**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 331** Flow of Policy Manager Auditing Control
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 332  Add Services > Audit Dialog

5. Complete the fields in the **Add Services > Audit** tab as described in Table 1, then click **Save**.
Table 1: Add Services > Audit Dialog Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Server</td>
<td>Select a server profile from the list:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Nessus Server</strong>: Performs vulnerability scanning and returns a Healthy/Quarantine result.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Nmap</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>You can click the View Details button to view the Policy Manager Entity Details dialog with the summary of audit server details.</td>
</tr>
<tr>
<td></td>
<td>To view the Summary tab with audit server details, click the Modify button.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Audit Trigger Conditions</td>
<td>Select from the following audit trigger conditions:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Always</strong>: Always perform an audit.</td>
</tr>
<tr>
<td></td>
<td>- <strong>When posture is not available</strong>: Perform audit only when posture credentials are not available in the request.</td>
</tr>
<tr>
<td></td>
<td>- <strong>For MAC Authentication Request</strong>: If you select this option, then Policy Manager presents the following three additional settings:</td>
</tr>
<tr>
<td></td>
<td>- <strong>For known end-hosts only</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>For unknown end-hosts only</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>For all end-hosts</strong>: For both known and unknown end-hosts.</td>
</tr>
<tr>
<td>Action after audit</td>
<td>Select an Action after audit.</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Action</strong>: The audit will not apply policies on the network device after this audit.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Do SNMP bounce</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Trigger RADIUS CoA action</strong>: This option sends a RADIUS CoA command to the network device.</td>
</tr>
</tbody>
</table>

**Modifying Default Audit Servers**

To reconfigure default Policy Manager audit servers:
1. Navigate to **Configuration > Posture > Audit Servers**.

   **Figure 333 Audit Servers Page**

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:

**Audit Tab**

1. Navigate to **Configuration > Posture > Audit Servers**, then click the **Add** link.

   The **Add Audit Servers** dialog opens to the **Audit** tab.
2. Specify the **Nessus Audit Server > Audit** tab parameters as described in Table 1.

**Table 1: Add Nessus Audit Server > Audit Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the audit server.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally (and recommended), enter the description that provides additional information about the audit server.</td>
</tr>
<tr>
<td>Type</td>
<td>Specify the type of audit server: <strong>Nessus</strong>.</td>
</tr>
<tr>
<td>In-Progress Posture Status</td>
<td>Specify the posture status during audit:</td>
</tr>
<tr>
<td></td>
<td>- Healthy (0)</td>
</tr>
<tr>
<td></td>
<td>- Checkup (10)</td>
</tr>
<tr>
<td></td>
<td>- Transition (15). This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>- Quarantine (20)</td>
</tr>
<tr>
<td></td>
<td>- Infected (30)</td>
</tr>
<tr>
<td></td>
<td>- Unknown (100)</td>
</tr>
<tr>
<td>Default Posture Status</td>
<td>Specify the posture status if evaluation does not return a condition or action match. The default setting is <strong>UNKNOWN</strong>.</td>
</tr>
</tbody>
</table>

**Primary Server and Backup Server Tabs**

The **Primary Server** and **Backup Server** tabs specify connection information for the Nessus audit server.
1. Specify the **Nessus Audit Server > Primary Server** tab and **Backup Server** tab parameters as described in Table 2.

**Table 2: Add Nessus Audit Server > Primary and Backup Server Tabs Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup</strong></td>
<td>On the Backup Server dialog: For the backup server to be invoked on primary server failover, check the <strong>Enable to use backup when primary does not respond</strong> check box.</td>
</tr>
<tr>
<td><strong>Nessus Server Name</strong></td>
<td>Enter the name of the Nessus server                                                                ní</td>
</tr>
<tr>
<td><strong>Nessus Server Port</strong></td>
<td>Specify the Nessus Server port. The default is <strong>1241</strong>.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username for the primary and backup Nessus server</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password for the primary and backup Nessus servers.</td>
</tr>
<tr>
<td><strong>Scan Profile</strong></td>
<td>You can accept the default scan profile or select <strong>Add &gt; Edit Scan Profile</strong> to create other profiles and add them to the scan profile list. For details, refer to <a href="#">Nessus Scan Profiles on page 346</a>.</td>
</tr>
<tr>
<td><strong>In-Progress Timeout</strong></td>
<td>Specify the duration (in seconds) before polling for Nmap results. The default is <strong>30 seconds</strong>.</td>
</tr>
</tbody>
</table>

2. 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 336  Selecting a Nessus Audit Server

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 337  Edit Nessus Server > Summary Page

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).
   
   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 or edit scan profiles:

1. Navigate to **Configuration > Posture > Audit Servers**.

2. Select the **Primary Server** tab.

3. From the **Primary Server** tab, click the **Add/Edit Scan Profile** link.
   
   The **Nessus Scan Profile Configuration** page opens.

**Figure 338  Nessus Scan Profile Configuration Page**

4. 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:

   a. 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 339** *Nessus Scan Profile Configuration > Profile Tab*

![Nessus Scan Profile Configuration Profile Tab](image)

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

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

**Figure 340** *Nessus Scan Profile Configuration Profile Tab > Plugin Synopsis*

![Plugin Synopsis](image)
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 341  Nessus Scan Profile Configuration > Selected Plugins Tab**

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 343  Nessus Scan Profile Configuration > Preferences Tab**
After saving the profile, plugin, and preference information for your new (or modified) plugin, you can go to the **Primary/Backup Servers** tabs and select it from the **Scan Profile** drop-down list.

**Adding an Nmap Audit Server**

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.

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.

**Audit Tab**

You can use the **Audit** tab to identify the server and define configuration details.

**Figure 344  NMAP Audit Server > Audit Tab**

Specify the parameters configured in the **Audit** tab as described in the following table:

**Table 17: Audit Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the NMAP audit server.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally (and recommended), enter the description of the Nmap audit server.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>NMAP</strong>.</td>
</tr>
<tr>
<td>In-Progress Posture Status</td>
<td>Specify the posture status during audit:</td>
</tr>
<tr>
<td></td>
<td>- Healthy (0)</td>
</tr>
<tr>
<td></td>
<td>- Checkup (10)</td>
</tr>
<tr>
<td></td>
<td>- Transition (15). This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>- Quarantine (20)</td>
</tr>
<tr>
<td></td>
<td>- Infected (30)</td>
</tr>
<tr>
<td></td>
<td>- Unknown (100)</td>
</tr>
<tr>
<td>Default Posture Status</td>
<td>Select the posture status if evaluation does not return a condition/action match.</td>
</tr>
<tr>
<td></td>
<td>The default setting is <strong>UNKNOWN</strong>.</td>
</tr>
</tbody>
</table>
NMAP Options Tab

You can use the **NMAP Options** tab to specify the type of scan configuration.

**Figure 345  Nmap Server > NMAP Options Tab**

![NMAP Options Tab](image)

**Table 18: NMAP Options Tab**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Scan</td>
<td>Specify the type of TCP (Transmission Control Protocol) scan:</td>
</tr>
<tr>
<td></td>
<td>- TCP SYN scan</td>
</tr>
<tr>
<td></td>
<td>- TCP Connect scan</td>
</tr>
<tr>
<td></td>
<td>- TCP Null Scan</td>
</tr>
<tr>
<td></td>
<td>- TCP FIN scan</td>
</tr>
<tr>
<td></td>
<td>- TCP Xmas scan</td>
</tr>
<tr>
<td></td>
<td>- TCP ACK scan</td>
</tr>
<tr>
<td></td>
<td>- TCP Window scan</td>
</tr>
<tr>
<td></td>
<td>- TCP Maimon scan</td>
</tr>
<tr>
<td>UDP Scan</td>
<td>To enable UDP (User Datagram Protocol) scanning, check the <strong>UDP Scan</strong> check box. Nmap option: <strong>sU</strong>.</td>
</tr>
<tr>
<td>Service Scan</td>
<td>Enable this scan to identify all the services and their versions running on your target application's server. To enable Service scanning, check the <strong>Service Scan</strong> check box. Nmap option: <strong>sV</strong>.</td>
</tr>
<tr>
<td>Detect Host Operating System</td>
<td>To enable host OS detection, check the <strong>Detect Host Operating System</strong> check box. NMAP option: <strong>A</strong>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port Range</td>
<td>Specify the range of ports to scan. Specify the range with a hyphen. For example, to scan ports 25 to 50, you would enter <strong>25-50</strong>. NMAP option: <code>p</code>.</td>
</tr>
<tr>
<td>Host Timeout</td>
<td>Specify the time in seconds for the target host to timeout. Nmap option: <strong>host-timeout</strong></td>
</tr>
<tr>
<td>In-Progress Timeout</td>
<td>Specify the duration (in seconds) before polling for Nmap results.</td>
</tr>
</tbody>
</table>

**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](#).

**Figure 346 Configuring Audit Server Rules**

**Post-Audit Rules**

The **Audit Servers > Rules** dialog specifies rules for post-audit evaluation of the request to assign a role.

**Figure 347 All Audit Server Configurations > Rules Dialog**
Table 1: All Audit Server Configurations > Rules Dialog Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules Evaluation Algorithm</td>
<td>Select first matched rule and return the role or Select all matched rules and return a set of roles.</td>
</tr>
<tr>
<td>Add Rule</td>
<td>When you add a rule, the Rules Editor opens. See below for details.</td>
</tr>
<tr>
<td>Move Up/Down</td>
<td>Reorder the rules as necessary.</td>
</tr>
<tr>
<td>Edit Rule</td>
<td>Opens the selected rule in Edit mode.</td>
</tr>
<tr>
<td>Remove Rule</td>
<td>Removes the selected rule.</td>
</tr>
</tbody>
</table>

Figure 348  All Audit Server Configurations > Rules Editor

Table 2: All Audit Server Configurations > Rules Editor Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions</td>
<td>The Conditions list includes five dictionaries:</td>
</tr>
<tr>
<td></td>
<td>• Audit-Status</td>
</tr>
<tr>
<td></td>
<td>• Device-Type</td>
</tr>
<tr>
<td></td>
<td>• Output-Msgs</td>
</tr>
<tr>
<td></td>
<td>• MAC-Vendor</td>
</tr>
<tr>
<td></td>
<td>• Network-Apps</td>
</tr>
<tr>
<td></td>
<td>• Open-Ports</td>
</tr>
<tr>
<td></td>
<td>• OS-Info</td>
</tr>
<tr>
<td></td>
<td>For more information, refer to Namespaces.</td>
</tr>
<tr>
<td>Actions</td>
<td>The Actions list includes the names of the roles configured in Policy Manager.</td>
</tr>
<tr>
<td>Save</td>
<td>To commit a Condition/Action pairing, click Save.</td>
</tr>
</tbody>
</table>
This chapter describes the following topics:

- Configuring Enforcement Profiles on page 354
- Configuring Enforcement Policies on page 409
- Configuring Deep-Nested Active Directory Queries

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

ClearPass Policy Manager sends these attributes by evaluating an enforcement policy associated with the service.

Each enforcement policy is a rule or set of rules for matching conditions (role, posture, and time) to actions, which are specified in enforcement profiles.

**Configuring Enforcement Profiles**

- 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
- Agent Script Enforcement Profile
- Aruba Downloadable Role Enforcement Profile
- Aruba RADIUS Enforcement Profile
- Cisco Downloadable ACL Enforcement Profile
- Cisco Web Authentication Enforcement Profile
- ClearPass Entity Update Enforcement Profile
- CLI-Based Enforcement Profile
- Filter ID Based Enforcement Profile
- Generic Application Enforcement Profile
- HTTP Based Enforcement Profile on page 393
- RADIUS Based Enforcement Profile
- RADIUS Change of Authorization (CoA) Profile
- Session Restrictions Enforcement Profile
- SNMP-Based Enforcement Profile
- TACACS+ Based Enforcement Profile
- VLAN Enforcement Profile

**Adding an Enforcement Profile**

To add an enforcement profile:

1. Navigate to Configuration > Enforcement > Profiles.
The **Enforcement Profiles** page opens:

**Figure 349  Enforcement Profiles Page**

2. Click the **Add** link.

   The **Add Enforcement Profile** dialog opens.

**Figure 350  Add Enforcement Profile Dialog**

The following table describes the default set of enforcement profiles included with Policy Manager:

**Table 1: Default Enforcement Profiles**

<table>
<thead>
<tr>
<th>Enforcement Profile</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Aerohive - Terminate Session]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disconnect user (Aerohive)</td>
</tr>
<tr>
<td>[AirGroup Personal Device]</td>
<td>RADIUS</td>
<td>System-defined profile for an AirGroup personal device request</td>
</tr>
<tr>
<td>[AirGroup Response]</td>
<td>RADIUS</td>
<td>System-defined profile for any AirGroup request</td>
</tr>
<tr>
<td>[AirGroup Shared Device]</td>
<td>RADIUS</td>
<td>System-defined profile for an AirGroup shared device request</td>
</tr>
<tr>
<td>[Allow Access Profile]</td>
<td>RADIUS</td>
<td>System-defined profile to allow network access</td>
</tr>
<tr>
<td>[Allow Application Access Profile]</td>
<td>Application</td>
<td>System-defined profile to allow access to application</td>
</tr>
<tr>
<td>[Aruba Bounce Host-Port]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to bounce host-port (Aruba)</td>
</tr>
<tr>
<td>[Aruba TACACS read-only Access]</td>
<td>TACACS</td>
<td>System-defined profile for read-only access to Aruba device</td>
</tr>
<tr>
<td>[Aruba TACACS root Access]</td>
<td>TACACS</td>
<td>System-defined profile for root access to Aruba device</td>
</tr>
<tr>
<td>[Aruba Terminate Session]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disconnect user (Aruba)</td>
</tr>
<tr>
<td>Enforcement Profile</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[AirGroup Shared Device]</td>
<td>RADIUS</td>
<td>System-defined profile for an AirGroup shared device request</td>
</tr>
<tr>
<td>[Allow Access Profile]</td>
<td>RADIUS</td>
<td>System-defined profile to allow network access</td>
</tr>
<tr>
<td>[Allow Application Access Profile]</td>
<td>Application</td>
<td>System-defined profile to allow access to an application</td>
</tr>
<tr>
<td>ArubaOS Switching - Bounce Switch Port</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to bounce the switch port on ArubaOS Switching products.</td>
</tr>
<tr>
<td>ArubaOS Switching - Terminate Session</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disconnect the user on ArubaOS Switching, HP ProCurve, and HP UWW (Unified Wired-WLAN) products.</td>
</tr>
<tr>
<td>ArubaOS Wireless - Bounce Switch Port</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to bounce the switch port on ArubaOS Mobility Controllers, Multi-Port APs, and Mobility Access Switches.</td>
</tr>
<tr>
<td>[ArubaOS Wireless - TACACS Read-Only Access]</td>
<td>TACACS</td>
<td>System-defined profile for TACACS read-only access on ArubaOS Mobility Controllers, Aruba Instant APs, and Mobility Access Switches.</td>
</tr>
<tr>
<td>[ArubaOS Wireless - TACACS root Access]</td>
<td>TACACS</td>
<td>System-defined profile for TACACS root access on ArubaOS Mobility Controllers, Aruba Instant APs, and Mobility Access Switches.</td>
</tr>
<tr>
<td>[Aruba Wireless - Terminate Session]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disconnect the user on ArubaOS Mobility Controllers, Aruba Instant APs, and Mobility Access Switches.</td>
</tr>
<tr>
<td>[Cisco - Bounce-Host-Port]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to bounce the host port (Cisco)</td>
</tr>
<tr>
<td>[Cisco - Disable Host-Port]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disable the host port (Cisco)</td>
</tr>
<tr>
<td>[Cisco - Reauthenticate-Session]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to re-authenticate session (Cisco)</td>
</tr>
<tr>
<td>[Cisco - Terminate-Session]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disconnect a user (Cisco)</td>
</tr>
<tr>
<td>[Deny Access Profile]</td>
<td>RADIUS</td>
<td>System-defined profile to deny network access</td>
</tr>
<tr>
<td>[Deny Application Access Profile]</td>
<td>Application</td>
<td>System-defined profile to deny access to an application</td>
</tr>
<tr>
<td>[Drop Access Profile]</td>
<td>RADIUS</td>
<td>System-defined profile to drop the request</td>
</tr>
<tr>
<td>[H3C - Bounce Switch Port]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to bounce the switch port on H3C products (including HPE FlexNetwork/Comware)</td>
</tr>
<tr>
<td>[H3C - Disable Switch Port]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disable the switch port on H3C products (including HPE FlexNetwork/Comware)</td>
</tr>
<tr>
<td>[H3C - Terminate Session]</td>
<td>RADIUS_CoA</td>
<td>System-defined profile to disconnect the user on H3C products (including HPE FlexNetwork/Comware)</td>
</tr>
<tr>
<td>Enforcement Profile</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[Handle AirGroup Time Sharing]</td>
<td>HTTP</td>
<td>System-defined profile to send time-based sharing policy to the AirGroup notification service</td>
</tr>
<tr>
<td>[Juniper Terminate Session]</td>
<td>RADIUS CoA</td>
<td>System-defined profile to disconnect a user (Juniper)</td>
</tr>
<tr>
<td>[Motorola - Terminate Session]</td>
<td>RADIUS CoA</td>
<td>System-defined profile to disconnect a user (Motorola)</td>
</tr>
<tr>
<td>[Operator Login - Admin Users]</td>
<td>Application</td>
<td>Enforcement profile for Guest admin logins</td>
</tr>
<tr>
<td>[Operator Login - Local Users]</td>
<td>Application</td>
<td>Enforcement profile for Guest operator logins</td>
</tr>
<tr>
<td>[TACACS API Admin]</td>
<td>TACACS</td>
<td>API admin access for ClearPass Policy Manager Admin</td>
</tr>
<tr>
<td>[TACACS Deny Profile]</td>
<td>TACACS</td>
<td>System-defined profile to deny network access</td>
</tr>
<tr>
<td>[TACACS Help Desk]</td>
<td>TACACS</td>
<td>Help desk access for ClearPass Policy Manager Admin</td>
</tr>
<tr>
<td>[TACACS Network Admin]</td>
<td>TACACS</td>
<td>Network admin access for ClearPass Policy Manager Admin</td>
</tr>
<tr>
<td>[TACACS Read-only Admin]</td>
<td>TACACS</td>
<td>Read-only admin access for ClearPass Policy Manager Admin</td>
</tr>
<tr>
<td>[TACACS Receptionist]</td>
<td>TACACS</td>
<td>Receptionist access for ClearPass Policy Manager Admin</td>
</tr>
<tr>
<td>[TACACS Super Admin]</td>
<td>TACACS</td>
<td>Super admin access for ClearPass Policy Manager Admin</td>
</tr>
<tr>
<td>[Trapeze - Terminate Session]</td>
<td>RADIUS CoA</td>
<td>System-defined profile to disconnect a user (Trapeze)</td>
</tr>
<tr>
<td>[Update Endpoint Known]</td>
<td>Post-Authentication</td>
<td>System-defined profile to change an Endpoint's status to Known</td>
</tr>
</tbody>
</table>

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 Agent Enforcement > Profile dialog opens.

**Figure 351 Agent Enforcement > Profile Tab**

![Agent Enforcement > Profile Tab](image)

4. Specify the Add Agent Enforcement > Profile parameters as described in the following table:

**Table 1: Add Agent Enforcement > Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the template from the drop-down list. In this context, select Agent Enforcement.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the enforcement profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of the enforcement profile (recommended).</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically with type Agent.</td>
</tr>
<tr>
<td>Action</td>
<td>By default, this field is disabled. It is enabled only when RADIUS type is selected.</td>
</tr>
</tbody>
</table>
| 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.                     |

**Configuring Agent Enforcement Attributes**

Use the Attributes tab to configure the attribute name and attribute value for each attribute you add.

**Figure 352 Agent Enforcement > Attributes Dialog**

![Agent Enforcement > Attributes Dialog](image)
Specify the **Agent Enforcement > Attributes** parameters as described in the following table:

### Table 2: Agent Enforcement > Attributes Tab Parameters

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bounce Client</td>
<td>To bounce the network interface, set the value to <strong>True</strong>.</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the message that needs to be notified on the endpoint.</td>
</tr>
<tr>
<td>Session Timeout (in seconds)</td>
<td>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 <strong>60</strong> to <strong>600</strong> seconds. The default value is <strong>0</strong>. <strong>NOTE:</strong> Setting the lower value for the session timeout interval results in numerous authentication requests in the <strong>Access Tracker</strong> page.</td>
</tr>
</tbody>
</table>
| 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 (see 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:  
  - You can set the Health Check Interval 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 Logout 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.                                                  |
| Show Custom UI for Custom Scripts | Click the check box to set this attribute to **True** and enable the OnGuard Agent Remediation User Interface for Custom Scripts (for related information, refer to the Custom User Interface parameter in Creating OnGuard Custom Web Pages). |
| SDK Type                        | Allows you to specify the V4 OnGuard Detection SDK (for related information, see Upgrading From OnGuard Plugin Version 1.0 to 2.0).               |
| Enable to auto update OnGuard Agent Library | When this option is enabled and a new version of OnGuard Agent Library is available on the ClearPass server, ClearPass OnGuard Agent automatically downloads and installs the new version of OnGuard Agent Library from the ClearPass server. OnGuard modules, including detection libraries for client programs (V4 SDK), can be upgraded without having to upgrade your ClearPass or OnGuard installations (for more information, see OnGuard Agent Library Updates). |
Summary Information
The Summary tab summarizes the parameters configured in the Profile and Attribute tabs.

Figure 353  Agent Enforcement > Summary Tab

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 exits after performing its task.

Mandatory Agent Script Attributes
The following attributes are mandatory when configuring Agent Script Enforcement:
- Path of the Script
- Command to Execute
- Execution Level

Optional Agent Script 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
Progress Message
Description
Download URL
Script Execution Timeout (Seconds)

**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 354  Agent Script Enforcement > Profile Dialog**

3. Specify the **Add Agent Script Enforcement > Profile** parameters as described in the following table:

**Table 1: Add Agent Script Enforcement > Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <strong>Agent Script Enforcement</strong> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the enforcement profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of the enforcement profile (recommended).</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically with type <strong>Agent</strong>.</td>
</tr>
<tr>
<td>Action</td>
<td>This parameter is disabled because it is not applicable to the Agent Script Enforcement Profile.</td>
</tr>
<tr>
<td>Device Group List</td>
<td>This parameter is disabled because it is not applicable to the Agent Script Enforcement Profile.</td>
</tr>
<tr>
<td>Add new Device Group</td>
<td>This parameter is disabled because it is not applicable to the Agent Script Enforcement Profile.</td>
</tr>
</tbody>
</table>
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 355 Agent Script Enforcement > Attributes Dialog

1. Specify the Agent Script Enforcement > Attributes parameters as described in the following table:

Table 2: Agent Script Enforcement > Attributes Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path of the Script</td>
<td>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.</td>
</tr>
<tr>
<td>Command to Execute</td>
<td>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.</td>
</tr>
<tr>
<td>SHA256 Checksum</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success Message</td>
<td>Enter the message to be shown to the end user when the script/program is launched successfully.</td>
</tr>
<tr>
<td>Failure Message</td>
<td>Enter the message to be shown to the end user when execution of the script/program fails.</td>
</tr>
<tr>
<td>Progress Message</td>
<td>This message will be shown on the OnGuard Progress Page (see OnGuard Settings and Agent Library Updates) while OnGuard Agent is executing the custom script and states what action is being performed.</td>
</tr>
<tr>
<td>Description</td>
<td>Provides a description of the custom user interface window or script.</td>
</tr>
</tbody>
</table>
| 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.  
  **NOTE:** OnGuard Agent does not support downloading files from URLs that require credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Script Execution Timeout (Seconds) | Specify the **Script Execution Timeout** attribute value in the number of seconds. The value must be an integer between **60** and **3600**. When this attribute is configured, OnGuard Agent waits for the specified time for the custom script to finish execution. If the custom script does not finish execution within the specified time, OnGuard Agent returns failure for that script.  
  When this attribute is not configured, OnGuard Agent uses varying timeout values, depending upon whether or not custom remediation is enabled.  
  - When Custom Remediation is enabled: the default value is 20 minutes  
  - When Custom Remediation is not enabled: 1 minute  

2. Click **Save**.

**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 356** Agent Script Enforcement > Summary Dialog

---

**Aruba Downloadable Role Enforcement Profile**

- [Profile Configuration on page 364](#)
Profile Configuration

Use the Profile tab to configure the template, type of the profile, and the device group list, as well as specifying the Role Configuration Mode—Standard or Advanced.

- **Standard mode**: User-provided options to configure individual components of a role (for example, Policer Profile, Stateless ACL configuration, etc.). The user role is generated based on components added to the configuration.
- **Advanced mode**: You can enter the entire role configuration as a text under a single attribute.

Events are logged in the Audit Viewer for create, update, and delete operations in the Captive Portal, Policy, and Class configurations. Events are also logged for generated user roles and import/export operations in enforcement profiles.

To configure the Aruba Downloadable Role Enforcement Profile:

1. Navigate to Configuration > Enforcement > Profiles.
   The Enforcement Profiles page opens.
2. Click the Add link.
   The Add Enforcement Profile page opens.
3. From the Template drop-down, select Aruba Downloadable Role Enforcement.

**Figure 357** Aruba Downloadable Role Enforcement > Profile Page (Standard Mode)

4. Specify the Aruba Downloadable Role Enforcement > Profile parameters as described in the following table:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <em>Aruba Downloadable Role Enforcement</em> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the enforcement profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the enforcement profile.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is automatically populated with: <strong>RADIUS</strong>.</td>
</tr>
<tr>
<td>Action</td>
<td>Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong> to define the action taken on the request. The default action is <strong>Accept</strong>.</td>
</tr>
</tbody>
</table>
| Device Group List         | Select a device group from the drop-down list. The list displays all configured device groups. 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](#).                                                                                   |
| Role Configuration Mode  | Select one of the following modes:  
  - Standard (the default)  
  - Advanced                                                                                                                                                                                                     |
| Product                   | Specify one of the following products:  
  - ArubaOS-Switch  
  - Mobility Access Switch (MAS)  
  - Mobility Controller                                                                                                           |
Role Configuration Mode: Standard

When Role Configuration is set to Standard (the default), the Role Configuration tab appears. In Standard mode, the Role Configuration tab includes only the options that are appropriate for the selected product.

Role Configuration Page: Aruba-OS Switch

The fields on the Role Configuration tab vary according to which product you specify. The example below displays the Role Configuration page when you specify the Aruba-OS Switch product. This page provides support for class configuration for the ArubaOS-Switch, and the Role Configuration tab includes a Manage Classes link.

**Figure 358  Role Configuration Page: ArubaOS-Switch**

The following table describes the Role Configuration parameters when the Product parameter is set to Aruba-OS Switch:

**Table 2: Role Configuration Page: ArubaOS-Switch Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captive Portal Profile</td>
<td>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 372.</td>
</tr>
<tr>
<td>Policy</td>
<td>Select the Enforcement Policy from the drop-down list if already configured. Click the Add Policy link to add a new policy. See Policy Configuration Page: Aruba-OS Switch &gt; Rule Configuration for more information.</td>
</tr>
</tbody>
</table>
| Secondary Role Type | Specify one of the following secondary role types:  
  - None  
  - Static: When selected, the Controller Static Role field appears.  
  - Dynamic: When selected, the Controller Downloadable Role field appears. |
| VLAN               | Specify one of the following VLAN identifiers:  
  - None  
  - ID: When selected, the VLAN ID Tagged <number> field appears. Enter the VLAN ID number.  
  - Name: When selected, the VLAN Name field appears. Enter the VLAN name. |
| VLAN Tagged        | Specify one of the following VLAN Tagged identifiers:  
  - None  
  - ID: When selected, the VLAN ID Tagged <number> field appears. Enter the VLAN ID Tagged number.  
  - Name: When selected, the VLAN Name Tagged field appears. Enter the VLAN tagged name. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-Authentication Period</td>
<td>Specify the ArubaOS switch re-authentication period in seconds.</td>
</tr>
<tr>
<td>Class Configuration</td>
<td>Select the Manage Class link to add, edit, or delete Class definitions.</td>
</tr>
<tr>
<td>User Role Configuration</td>
<td>Select the Summary tab to view the generated User Role configuration.</td>
</tr>
</tbody>
</table>

**Policy Configuration Page: Aruba-OS Switch > Rule Configuration**

When you select the **Add Policy** link, the following configuration dialog opens:

![Policy Configuration Page](image)

Enter the appropriate values for each of the fields in the **Policy Configuration > Rule Configuration** dialog, then click **Save Rule**.

**Table 3: Policy Configuration Page: Aruba-OS-Switch Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Enter a number.</td>
</tr>
<tr>
<td>Class</td>
<td>For the packet match, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Ignore</td>
</tr>
<tr>
<td></td>
<td>- Match</td>
</tr>
<tr>
<td>Class Name</td>
<td>Specify the appropriate class name from the drop-down.</td>
</tr>
<tr>
<td>Action</td>
<td>Select the desired action from the drop-down list.</td>
</tr>
<tr>
<td>IP DSCP &lt;0-63&gt;</td>
<td>Enter a number from 0 to 63 to indicate the IP DSCP.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>IP Precedence &lt;0-7&gt;</td>
<td>Specify the IP precedence by entering a number from 0 to 7.</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter a number from 0 to 7 to indicate Priority.</td>
</tr>
<tr>
<td>Rate Limit kpbs</td>
<td>Specify the rate limit in KB per second.</td>
</tr>
</tbody>
</table>

**Role Configuration Page: Aruba-OS Switch > Class Configuration**

You can create and configure traffic classes and you can map the enforcement policy to the traffic classes. When you select the **Manage Classes** link, the following configuration dialog opens:

**Figure 360  ArubaOS Switch Class Configuration Dialog**

Specify the **ArubaOS Switch Class Configuration** parameters as described in the following table.

**Table 4: Class Configuration Page: ArubaOS-Switch Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Class Name</td>
<td>Select the class name from the drop-down list if already configured.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the Class name.</td>
</tr>
<tr>
<td>Traffic</td>
<td>Specify one of the following traffic types:</td>
</tr>
<tr>
<td></td>
<td>IPv4</td>
</tr>
<tr>
<td></td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td>MAC</td>
</tr>
</tbody>
</table>

When you click the **Rule Configuration** tab, the following dialog opens:
Specify the **Rule Configuration** parameters as described in the following table:

**Table 5: Rule Configuration Page: ArubaOS-Switch Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Enter a number.</td>
</tr>
<tr>
<td>Packet Match</td>
<td>For the packet match, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Ignore</td>
</tr>
<tr>
<td></td>
<td>■ Match</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specify the appropriate traffic protocol from the drop-down.</td>
</tr>
<tr>
<td>Source</td>
<td>Select one of the following sources:</td>
</tr>
<tr>
<td></td>
<td>■ Any</td>
</tr>
<tr>
<td></td>
<td>■ Host</td>
</tr>
<tr>
<td></td>
<td>■ IP Subnet. When you select <strong>IP Subnet</strong>, you are prompted for the <strong>Source Value</strong> (the IP subnet address).</td>
</tr>
<tr>
<td>Source Port</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Equal to Port</td>
</tr>
<tr>
<td></td>
<td>■ Greater than Port</td>
</tr>
<tr>
<td></td>
<td>■ Less than Port</td>
</tr>
<tr>
<td></td>
<td>■ Except Port</td>
</tr>
<tr>
<td></td>
<td>■ Port Range &lt;1-65535&gt;</td>
</tr>
<tr>
<td>Source Port Value</td>
<td>Specify the source port value.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select one of the following destinations:</td>
</tr>
<tr>
<td></td>
<td>■ Any</td>
</tr>
<tr>
<td></td>
<td>■ Host</td>
</tr>
<tr>
<td></td>
<td>■ IP Subnet. When you select <strong>IP Subnet</strong>, you are prompted for the <strong>Source Value</strong> (the IP subnet address).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Equal to Port</td>
</tr>
<tr>
<td></td>
<td>- Greater than Port</td>
</tr>
<tr>
<td></td>
<td>- Less than Port</td>
</tr>
<tr>
<td></td>
<td>- Except Port</td>
</tr>
<tr>
<td></td>
<td>- Port Range &lt;1-65535&gt;</td>
</tr>
<tr>
<td>Destination Port Value</td>
<td>Specify the destination port value.</td>
</tr>
<tr>
<td>IP DSCP</td>
<td>Specify the differentiated services code point (DSCP).</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Specify the VLAN ID</td>
</tr>
<tr>
<td>IP Precedence</td>
<td>Specify the IP precedence:</td>
</tr>
<tr>
<td></td>
<td>- Routine</td>
</tr>
<tr>
<td></td>
<td>- Priority</td>
</tr>
<tr>
<td></td>
<td>- Immediate</td>
</tr>
<tr>
<td></td>
<td>- Flash</td>
</tr>
<tr>
<td></td>
<td>- Flash Override</td>
</tr>
<tr>
<td></td>
<td>- Critical</td>
</tr>
<tr>
<td></td>
<td>- Internet</td>
</tr>
<tr>
<td></td>
<td>- Network</td>
</tr>
<tr>
<td>IP Type of Service</td>
<td>Specify one of the following for the type of service:</td>
</tr>
<tr>
<td></td>
<td>- Normal</td>
</tr>
<tr>
<td></td>
<td>- Max Reliability</td>
</tr>
<tr>
<td></td>
<td>- Max Throughput</td>
</tr>
<tr>
<td></td>
<td>- Minimum Delay</td>
</tr>
<tr>
<td>TCP Packets Bit Sets</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Established</td>
</tr>
<tr>
<td></td>
<td>- Fin: The FIN flag indicates the end of data transmission to finish a TCP connection.</td>
</tr>
<tr>
<td></td>
<td>- Rst: Sets the Reset flag.</td>
</tr>
<tr>
<td></td>
<td>- Syn: The SYN flag synchronizes sequence numbers to initiate a TCP connection.</td>
</tr>
</tbody>
</table>
Role Configuration Page: Mobility Access Switch

Many of the fields require you to select a link to launch a new page where you set role configuration profiles and related parameters.

Figure 362  Role Configuration Page > Product: Mobility Access Switch

The following table describes the Role Configuration parameters when the Product parameter is set to Mobility Access Switch:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Action/Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captive Portal Profile</td>
<td>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 372.</td>
</tr>
<tr>
<td>Policer Profile</td>
<td>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 372.</td>
</tr>
<tr>
<td>QoS Profile</td>
<td>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 373.</td>
</tr>
<tr>
<td>VoIP Profile</td>
<td>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 373.</td>
</tr>
<tr>
<td>Reauthentication Interval Time (0-4096)</td>
<td>Enter the number of minutes between reauthentication intervals. You can select the range between 0 to 4096 minutes.</td>
</tr>
<tr>
<td>VLAN To Be Assigned (1-4904)</td>
<td>Enter a number between 1 and 4094 that defines when the VLAN is to be assigned.</td>
</tr>
<tr>
<td>NetService Configuration</td>
<td>Select the Manage NetServices link to add, edit, and delete the NetService definitions. For more information, see NetService Configuration.</td>
</tr>
</tbody>
</table>
Parameters | Action/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 more information, see **NAT Pool 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 the 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 363 Add Captive Portal Configuration Profile**

   ![Add Captive Portal Profile](image)

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 364 Add Policer Configuration 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 365 Add QoS Profile Configuration Profile**

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:
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:

   ![NetService Configuration Profile](image)

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 368  Net Destinations Configuration Profile

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 369  Time Range Configuration Profile

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:
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:

   ![Stateless Access Control List Configuration](image)

   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.
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.

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.
Role Configuration Mode: Advanced

When you set Role Configuration Mode to Advanced, the Enforcement Profile page displays the Attributes tab (see Figure 374 below).

In Advanced mode, the Aruba Downloadable Role Enforcement profile provides two dictionaries and two attributes. The supported dictionaries and their associated attributes are:

- Dictionary: Aruba
  - Attribute: Aruba-CPPM-Role
    The Aruba-CPPM-Role attribute supports Mobility Access Switches.

- Dictionary: Hewlett-Packard Enterprise
  - Attribute: HPE-CPPM-Role
    The HPE-CPPM-Role attribute supports ArubaOS Switches.
  - Attribute: HPE-CPPM-Secondary-Role
    This attribute adds support for a downloadable secondary role that can be used with Per User Tunneled Node (PUTN). When the attribute is added to the enforcement profile, ClearPass can send the controller role for the ArubaOS switch.

You can use only one of the Advanced mode dictionaries at any given time; these dictionaries can't both be used at the same time.

Configuring the Advanced Attributes

To configure the Aruba Downloadable Role Enforcement > Advanced attributes:

1. Navigate to Configuration > Enforcement > Profiles > Add.
2. Select Aruba Downloadable Role Enforcement from the Template drop-down list.
   - The following fields appear:
     a. Role Configuration Mode: Select Advanced.
     b. Product: Select ArubaOS-Switch.

   Figure 374 Downloadable Role Enforcement > Profile Tab (Advanced Mode)

3. Next, select the Attributes tab.
Figure 375  Configuring HPE-CPPM-Role Attribute

The Radius:Hewlett-Packard Enterprise> HPE-CPPM-Role attribute is selected by default.

4. To specify the Hewlett-Packard Enterprise dictionary and attribute:
   a. Type: Hewlett-Packard Enterprise
   b. Name: Select HPE-CPPM-Role (27) or HPE-CPPM-Secondary-Role (28).

In Advanced mode, a validation check is not available for downloadable role names that are greater than 64 characters. This is due to a limitation on the switch. Thus, if a downloadable role name configured on the ClearPass server exceeds 64 characters, the enforcement profile may fail on the switch.

c. Value: Enter the appropriate ArubaOS switch commands.

5. Click Save.

Summary Information
For a profile in Standard Role Configuration Mode, the Summary tab summarizes the parameters configured in the Profile and Role Configuration tabs.
For a profile in Advanced Role Configuration Mode, the Summary tab summarizes the parameters configured in the Profile and Attribute tabs.

Aruba RADIUS Enforcement Profile
This section describes the following Aruba RADIUS Enforcement profile features:

- Profile Configuration on page 379
- Attributes Configuration on page 380
- Summary Information on page 381

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 376  Aruba RADIUS Enforcement > Profile Tab
The following table describes the **Aruba RADIUS Enforcement > Profile** tab parameters:

**Table 1: Aruba RADIUS Enforcement > Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select Aruba RADIUS Enforcement.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed on the Configuration &gt; Enforcement &gt; Profiles page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information about the profile. This description is displayed in on the Configuration &gt; Enforcement &gt; Profiles page.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically.</td>
</tr>
<tr>
<td>Action</td>
<td>Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong> to define the action taken on the request.</td>
</tr>
</tbody>
</table>
| 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. |

**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 377** Aruba RADIUS Enforcement > Attributes Dialog
The following table describes the **Aruba RADIUS Enforcement > Attributes** parameters:

**Table 2: Aruba RADIUS Enforcement > Attributes Parameters**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Type      | Select one of the following attribute types:  
|           | - Radius:Aruba  
|           | - Radius:IETF  
|           | - Radius:Cisco  
|           | - Radius: Hewlett-Packard-Enterprise  
|           | - Radius: Lucent-Alcatel-Enterprise  
|           | - Radius: Microsoft  
|           | - Radius: Avenda  
|           | For more information, see **RADIUS Namespaces on page 967**.  
| 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 378  Aruba RADIUS Enforcement > Summary Tab**

**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 379  Cisco Downloadable ACL Enforcement > Profile Dialog**
Specify the **Cisco Downloadable ACL Enforcement > Profile** parameters as described in the following table:

**Table 1: Cisco Downloadable ACL Enforcement > Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <em>Cisco Downloadable ACL Enforcement</em> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed in the <em>Name</em> column on the <em>Configuration &gt; Enforcement &gt; Profiles</em> page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile. The description is displayed in the <em>Description</em> column on the <em>Configuration &gt; Enforcement &gt; Profiles</em> page.</td>
</tr>
<tr>
<td>Type</td>
<td>The field is populated automatically with Type: <em>RADIUS</em>.</td>
</tr>
<tr>
<td>Action</td>
<td>To define the action to take on the request, click <em>Accept</em>, <em>Reject</em>, or <em>Drop</em>.</td>
</tr>
</tbody>
</table>
| 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 device group, click the *Add New Device Group* link. For more information, see *Adding and Modifying Device Groups*.              |

**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 380  Cisco Downloadable ACL Enforcement > Attributes Dialog**
Specify the **Cisco Downloadable ACL Enforcement > Attributes** parameters as described in the following table:

**Table 2: Cisco Downloadable ACL Enforcement > Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Type      | Select one of the following attribute types:  
|           | • Radius:IETF  
|           | • Radius:Cisco  
|           | • Radius: Hewlett-Packard-Enterprise  
|           | • Radius: Microsoft  
|           | • Radius: Alcatel-Lucent-Enterprise  
|           | • Radius: Aruba  
For more information, see [RADIUS Namespaces on page 967](#). |
| 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 381Cisco Downloadable ACL Enforcement > Summary Tab**

**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 382Cisco Web Authentication Enforcement > Profile Tab**
Specify the **Cisco Web Authentication Enforcement > Profile** tab parameters as described in the following table:

**Table 1: Cisco Web Authentication Enforcement > Profile Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <strong>Cisco Web Authentication Enforcement</strong> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information about the profile (recommended).</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically.</td>
</tr>
<tr>
<td>Action</td>
<td>Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong> to define the action taken on the request.</td>
</tr>
</tbody>
</table>
| Device Group List     | Select a device group from the drop-down list. The list displays all configured device groups. 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](#).                                       |

**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 383  Cisco Web Authentication Enforcement > Attributes Tab**
The following table describes the **Cisco Web Authentication Enforcement > Attributes** parameters:

**Table 2: Cisco Web Authentication Enforcement > Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type      | Select one of the following attribute types:  
- Radius:Aruba  
- Radius:IETF  
- Radius:Cisco  
- Radius: Hewlett-Packard-Enterprise  
- Radius: Lucent-Alcatel-Enterprise  
- Radius: Microsoft  
- Radius: Avenda  
For more information, see [RADIUS Namespaces](#). |
| 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 384  Cisco Web Authentication Enforcement > Summary Tab**

**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 385  ClearPass Entity Update Enforcement > Profile Tab**
Specify the **ClearPass Entity Update Enforcement > Profile** parameters as described in the following table:

### Table 1: ClearPass Entity Update Enforcement > Profile Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the template from the drop-down list. In this context, select ClearPass Entity Update Enforcement.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed in the <strong>Name</strong> column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information about the profile. This description is displayed in the <strong>Description</strong> column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically.</td>
</tr>
<tr>
<td>Action</td>
<td>Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong> to define the action taken on the request.</td>
</tr>
</tbody>
</table>
| 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](#).                                           |

### 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 386** ClearPass Entity Update Enforcement Attributes tab
Specify the **ClearPass Entity Update Enforcement > Attributes** parameters as described in the following table:

### Table 2: ClearPass Entity Update Enforcement > Attributes Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 387  ClearPass Entity Update Enforcement > Summary Tab

**Enforcement Profiles**

- **Profile:** ClearPass Entity Update Enforcement
- **Name:** Ent_Update_Enf
- **Description:**
- **Type:** Post_Authentication
- **Action:** Accept
- **Device Group List:** -

**Attributes:**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Endpoint</td>
<td>Enabled by</td>
</tr>
<tr>
<td>2.</td>
<td>Expire-Time-Update</td>
<td>GuestUser</td>
</tr>
<tr>
<td>3.</td>
<td>GuestUser</td>
<td>Location</td>
</tr>
</tbody>
</table>

### 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 388**
- **Attributes Configuration on page 388**
- **Summary Information on page 389**
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 388 CLI-Based Enforcement > Profile Tab**

Specify the **CLI-Based Enforcement > Profile** tab parameters as described in the following table:

**Table 1: CLI Based Enforcement > Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <strong>CLI Based Enforcement</strong> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information about the profile.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically.</td>
</tr>
<tr>
<td>Action</td>
<td>Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong> to define the action taken on the request.</td>
</tr>
</tbody>
</table>
| 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](#). |

Attributes Configuration

Use the **Attribute** tab to configure the attribute type, name, and value for the enforcement profile.

**Figure 389 CLI Based Enforcement > Attributes Tab**
Specify the **CLI Based Enforcement > Attributes** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Action/Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Select <strong>Command</strong> or <strong>Target Device</strong>.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>Specify the appropriate <strong>Attribute Value</strong>. The options provided for the <strong>Attribute Value</strong> depend on the selected <strong>Attribute Name</strong>.</td>
</tr>
</tbody>
</table>

**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 390 CLI-Based Enforcement > Summary Tab**

**Filter ID Based Enforcement Profile**

This section provides the following information:

- Profile Configuration on page 389
- Attributes Configuration on page 390

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 391 Filter ID Based Enforcement Profile Dialog**
Specify the **Filter ID Based Enforcement Profile** parameters as described in the following table:

**Table 19: Filter ID Based Enforcement > Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <strong>Filter ID Based Enforcement</strong> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed in the Name column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile. The Description is displayed in the Description column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>RADIUS.</strong> The field is populated automatically.</td>
</tr>
<tr>
<td>Action</td>
<td>Enabled. Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong> to define the action taken on the request.</td>
</tr>
</tbody>
</table>
| 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. |

**Attributes Configuration**

The following figure displays the **Filter ID Based Enforcement Profile > Attributes** dialog:

**Figure 392  Filter ID Based Enforcement Profile > Attributes Dialog**
Specify the **Filter ID Based Enforcement > Attributes** parameters as described in the following table:

**Table 1: Filter ID Based Enforcement Profile > Attributes Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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](#). |
| 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 391](#)
- [Attributes Configuration on page 392](#)
- [Summary Information on page 393](#)

**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 393  Generic Application Enforcement > Profile Tab**
Specify the **Generic Application Enforcement > Profile** parameters as described in the following table:

**Table 1: Generic Application Enforcement > Profile Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the template from the drop-down list. In this context, select Generic Application Enforcement.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed in the Name column on the Configuration &gt; Enforcement &gt; Profiles page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information about the profile. This description is displayed in the Description column on the Configuration &gt; Enforcement &gt; Profiles page.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically.</td>
</tr>
<tr>
<td>Action</td>
<td>Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong> to define the action taken on the request.</td>
</tr>
</tbody>
</table>
| 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](#).                                                                |

**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 394  Generic Application Enforcement > Attributes Tab**

Specify the **Generic Application Enforcement > Attributes** parameters as described in the following table:

**Table 20: Generic Application Enforcement > Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Select an attribute name from the drop-down list. The list has multiple names.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>Displays the options for the Attribute Value depend on the selected Attribute Name.</td>
</tr>
</tbody>
</table>
Summary Information

The **Summary** tab summarizes the parameters configured in the **Profile** and **Attributes** tab.

**Figure 395  Generic Application Enforcement > Summary Tab**

**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 396  HTTP Based Enforcement Profile Dialog**

Specify the **HTTP Based Enforcement > Profile** parameters as described in the following table:

**Table 1: HTTP Based Enforcement Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <strong>HTTP Based Enforcement</strong> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed in the <strong>Name</strong> column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile. The description is displayed in the <strong>Description</strong> column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Type</td>
<td>This field is populated automatically with <strong>HTTP</strong>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Action</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
| 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 device group, click the Add New Device Group link and see Adding and Modifying Device Groups. |

**Attributes Configuration**

**Figure 397**  HTTP Based Enforcement Attributes Dialog

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Server</td>
<td>Select the attribute name: Target Server or Action.</td>
</tr>
<tr>
<td>Action</td>
<td>Specify the appropriate value. The options displayed for the Attribute Value depend on the Attribute Name that was selected.</td>
</tr>
</tbody>
</table>

**Table 2: HTTP Based Enforcement Attributes Parameters**

**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 398**  RADIUS Based Enforcement > Profile Tab
Specify the **RADIUS Based Enforcement Profile** parameters as described in the following table:

**Table 1: RADIUS Based Enforcement Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <strong>RADIUS Based Enforcement</strong> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>RADIUS</strong>. This field is populated automatically.</td>
</tr>
<tr>
<td>Action</td>
<td>Enabled. Click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong>.</td>
</tr>
<tr>
<td>Device Group List</td>
<td>Select a Device Group from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>All configured device groups are listed on the <strong>Configuration &gt; Network &gt; Device Groups</strong> page. After you add one or more device group(s), you can select a group and take one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>■ To delete the selected Device Group List entry, click <strong>Remove</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ To see the device group parameters, click <strong>View Details</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ To change the parameters of the selected device group, click <strong>Modify</strong>.</td>
</tr>
<tr>
<td>Add New Device Group</td>
<td>To add a new device group, click the <strong>Add New Device Group</strong> link and see <strong>Adding and Modifying Device Groups</strong></td>
</tr>
</tbody>
</table>

**Attributes Tab**

The following figure displays the **RADIUS Based Enforcement > Attributes** dialog:

**Figure 399**  
*RADIUS Based Enforcement Attributes Dialog*
Specify the **RADIUS Based Enforcement > Attributes** parameters as described in the following table:

**Table 21: RADIUS Based Enforcement > Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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](#). |
| 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 400  RADIUS Change of Authorization (CoA) > Profile Tab**

Specify the **RADIUS Change of Authorization (CoA) > Profile** tab parameters as described in the following table:

**Table 1: RADIUS Change of Authorization (CoA) Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the RADIUS Change of Authorization (CoA) template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of this enforcement profile.</td>
</tr>
<tr>
<td>Type</td>
<td>RADIUS_CoA is automatically populated.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Action</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
| 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 device group, click the Add New Device Group link and see **Adding and Modifying Device Groups**. |

**Attributes Configuration**

The following figure displays the **RADIUS Change of Authorization (CoA) > Attributes** tab:

![Figure 401 RADIUS Change of Authorization (CoA) > Attributes Dialog](image)

The following table describes the **RADIUS Change of Authorization (CoA) > Attributes** parameters:

**Table 2: RADIUS Change of Authorization (CoA) Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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-Packard-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. |
### 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 402 Session Notification Enforcement > Profile Configuration Dialog*

The following table describes the **Session Notification Enforcement > Profile** parameters:

**Table 1: Session Notification Enforcement Profile Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select <strong>Session Notification Enforcement</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile (recommended).</td>
</tr>
<tr>
<td>Type</td>
<td>The field is populated automatically with: <strong>Post_Authentication</strong>.</td>
</tr>
<tr>
<td>Action</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Device Group List</td>
<td>Select a device group from the drop-down list. All configured device groups are</td>
</tr>
<tr>
<td></td>
<td>listed in the <strong>Device Groups Configuration &gt; Network &gt; Device Groups</strong> page.</td>
</tr>
<tr>
<td>Add New Device Group</td>
<td>To add a new device group, click the <strong>Add New Device Group</strong> link. See **Adding</td>
</tr>
<tr>
<td></td>
<td>and Modifying** <strong>Device Groups</strong> for more information.</td>
</tr>
</tbody>
</table>
Attributes Configuration

The following figure displays the **Session Notification Enforcement > Attributes** dialog:

**Figure 403  Session Notification Enforcement > Attributes Configuration Dialog**

Specify the **Session Notification Enforcement > Attributes** parameters as described in the following table:

**Table 22: Session Notification Enforcement > Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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 404  Session Notification Enforcement > Summary Tab**

<table>
<thead>
<tr>
<th>Enforcement Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
</tr>
<tr>
<td><strong>Profile:</strong> Session Notification Enforcement</td>
</tr>
<tr>
<td>Name: SessionNotification</td>
</tr>
<tr>
<td>Description:</td>
</tr>
<tr>
<td>Type: Post_Authentication</td>
</tr>
<tr>
<td>Action: Accept</td>
</tr>
<tr>
<td>Device Group List:</td>
</tr>
<tr>
<td><strong>Attributes:</strong></td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>1. Session-Check</td>
</tr>
<tr>
<td>2. Session Notify</td>
</tr>
</tbody>
</table>

Session Restrictions Enforcement Profile
ClearPass uses Keep-Alive messages to issue Disconnect Messages 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.

- **Enforcement Profile Configuration**
- **Attributes Configuration**
- Examples of Bandwidth-Check Enforcement Profile Configurations
- Examples of Session-Check Enforcement Profile Configurations

**Enforcement Profile Configuration**
To configure Profile and Attributes 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 405  Add Session Restrictions Enforcement > Profile Tab**

4. Specify the Session Restrictions Enforcement > Profile parameters as described in the following table:
### Table 1: Session Restrictions Enforcement Profile Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select <strong>Session Restrictions Enforcement</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the enforcement profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of the enforcement profile (recommended).</td>
</tr>
<tr>
<td>Type</td>
<td><strong>Post-Authentication</strong>. The <strong>Type</strong> field is populated automatically when you select the <strong>Session Restrictions Enforcement</strong> template.</td>
</tr>
<tr>
<td>Action</td>
<td>By default, this field is disabled. It is enabled only when <strong>RADIUS</strong> type is selected.</td>
</tr>
</tbody>
</table>
| 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**. |

**Attributes Configuration**

The following figure displays the **Session Restrictions Enforcement > Attributes** tab:

**Figure 406  Session Restrictions Enforcement Profile > Attributes Dialog**

1. Specify the **Session Restrictions Enforcement > Attributes** parameters as described in **Table 2**:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type      | Select from the following attribute types:  
  - Bandwidth-Check  
  - Expiry-Check  
  - Post-Auth-Check  
  - Session-Check |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The options displayed for the <strong>Name</strong> attribute depend on the <strong>Type</strong> attribute that was selected.</td>
</tr>
</tbody>
</table>

**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**.
- **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 407** SNMP Based Enforcement > Profile Dialog

Specify the SNMP Based Enforcement > Profile parameters as described in the following table:

**Table 1:** SNMP Based Enforcement > Profile Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the SNMP Based Enforcement template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed in the Name column on the Configuration &gt; Enforcement &gt; Profiles page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile (recommended). The description is displayed in the Description column on the Configuration &gt; Enforcement &gt; Profiles page.</td>
</tr>
<tr>
<td>Type</td>
<td>SNMP. This field is populated automatically when you select the SNMP Based Enforcement template.</td>
</tr>
<tr>
<td>Action</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
| 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. |

Attributes Configuration

The following figure displays the SNMP Based Enforcement > Attributes dialog:

**Figure 408** SNMP Based Enforcement > Attributes Dialog
Specify the **SNMP Based Enforcement > Attributes** parameters as described in the following table:

**Table 2: SNMP Based Enforcement Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Select one of the following attributes:</td>
</tr>
<tr>
<td></td>
<td>▪ VLAN ID</td>
</tr>
<tr>
<td></td>
<td>▪ Session Timeout (in seconds)</td>
</tr>
<tr>
<td></td>
<td>▪ Reset Connection (after the settings are applied)</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>The options displayed for the <strong>Attribute Value</strong> depends on the <strong>Attribute Name</strong> that was selected.</td>
</tr>
</tbody>
</table>

**TACACS+ Based Enforcement Profile**

Use this page to configure the TACACS+ Based Enforcement profile.

**Profile Configuration**

To create a TACACS+ Based Enforcement profile:

1. navigate to **Configuration > Enforcement > Profiles**.
2. From the **Enforcement Profiles** page, click **Add**.
   - The **Add Enforcement Profiles** dialog opens.

**Figure 409  Add TACACS+ Based Enforcement Profile Dialog**

Specify the **Add TACACS+ Based Enforcement Profile > Profile** tab parameters as described in the following table:

**Table 1: TACACS+ Based Enforcement > Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the <strong>TACACS+ Based Enforcement</strong> template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile. The name is displayed in the <strong>Name</strong> column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile (recommended). The description is displayed in the <strong>Description</strong> column on the <strong>Configuration &gt; Enforcement &gt; Profiles</strong> page.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>TACACS</strong>. The field is populated automatically.</td>
</tr>
</tbody>
</table>
## Configuring Enforcement Profiles and Policies

### ClearPass 6.7 Policy Manager

### User Guide

#### Parameter Action/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 device group, click the Add New Device Group link. See Adding and Modifying Device Groups.

### Services Configuration

The following figure displays the TACACS+ Based Enforcement > Services dialog:

**Figure 410** TACACS+ Based Enforcement > Services Dialog

Specify the TACACS+ Based Enforcement Profile > Service parameters as described in the following table:

#### Table 2: TACACS+ Based Enforcement > Services Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege Level</td>
<td>Select a level between 0 and 15, with 0 being the minimum privilege level and 15 being the highest.</td>
</tr>
<tr>
<td>Selected Services</td>
<td>Select one or more of the following services:</td>
</tr>
<tr>
<td></td>
<td>- Shell</td>
</tr>
<tr>
<td></td>
<td>- PIX Shell</td>
</tr>
<tr>
<td></td>
<td>- PPP:IP</td>
</tr>
<tr>
<td></td>
<td>- PPP:IPX</td>
</tr>
<tr>
<td></td>
<td>- PPP:LCP</td>
</tr>
<tr>
<td></td>
<td>- ARAP</td>
</tr>
<tr>
<td></td>
<td>- cpass:HTTP</td>
</tr>
<tr>
<td></td>
<td>- Wireless-WCS:HTTP</td>
</tr>
<tr>
<td></td>
<td>- CiscoWLC:Common</td>
</tr>
<tr>
<td></td>
<td>- Aruba:Common</td>
</tr>
<tr>
<td></td>
<td>- AMP:https</td>
</tr>
<tr>
<td></td>
<td>- NCS:HHHP</td>
</tr>
<tr>
<td>Export All TACACS+ Services Dictionaries</td>
<td>Click this link to download the TACACS+ Services dictionary to the local computer.</td>
</tr>
<tr>
<td>Authorize Attribute Status</td>
<td>Select one of the following options:</td>
</tr>
</tbody>
</table>
### Custom Services

To add new TACACS+ services / attributes or upload the modified XML dictionary, click the **Update TACACS+ Services Dictionary** link.

### Service Attributes

**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 411 VLAN Enforcement > Profile Configuration Dialog**

Specify the **VLAN Enforcement > Profile** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select the template from the drop-down list. In this context, select VLAN Enforcement.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the profile.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>RADIUS</strong>. The field is populated automatically.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>To define the action taken on the request, click <strong>Accept</strong>, <strong>Reject</strong>, or <strong>Drop</strong>.</td>
</tr>
</tbody>
</table>
| 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**. |

### Attributes Configuration

The following figure displays the **VLAN Enforcement > Attributes** dialog:

**Figure 412 VLAN Enforcement Attributes Dialog**

![VLAN Enforcement Attributes Dialog](image)

Specify the **RADIUS Based Enforcement > Attributes** parameters as described in the following table:

#### Table 2: VLAN Enforcement Attributes Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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** |
| 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. |

### Configuring Enforcement Policies

- **Adding an Enforcement Policy**
- **Binding SNMP Enforcement for Ingress Events**
Adding an Enforcement Policy

Only one enforcement policy can be associated with each service. Enforcement policies can be added in one of two ways:

- From the Configuration > Services page as part of the flow of the Add Service wizard.
- From Configuration > Enforcement > Enforcement Policies.

The Enforcement Policies page opens:

**Figure 413  Enforcement Policies Page**

1. To add a new enforcement policy from the Enforcement Policies page, navigate to Configuration > Enforcement > Enforcement Policies.
2. Click Add.

   The Add Enforcement Policy page opens to the Enforcement tab:

   **Figure 414  Add Enforcement Policy > Enforcement Tab**

3. Specify the Add Enforcement Policy > Enforcement parameters as described in the following table:

   **Table 1: Add Enforcement Policy > Enforcement Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of this enforcement policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a useful description of this enforcement policy (recommended).</td>
</tr>
<tr>
<td>Enforcement Type</td>
<td>Select one of the following enforcement types:</td>
</tr>
<tr>
<td></td>
<td>RADIUS</td>
</tr>
</tbody>
</table>
4. In the Rules tab, click New Rule to display the Rules Editor:

**Figure 415 Add Enforcement Policy > Rules Editor**

5. Specify the Add Enforcement Policy > Rules tab parameters as described in the following table:

**Table 2: Add Enforcement Policy: Rules Editor**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Rule</td>
<td>Click this button to bring up the Rules Editor.</td>
</tr>
<tr>
<td>Move Up/Down</td>
<td>To reorder the rules in the enforcement policy, select an enforcement policy rule, then click Move Up or Move Down.</td>
</tr>
<tr>
<td>Remove Rule</td>
<td>To delete a rule, select the rule, then click Remove Rule.</td>
</tr>
</tbody>
</table>
Table 3: Add Enforcement Policy: Rules Editor

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 free-form 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 354 for a list of the default profiles. |

**Binding SNMP Enforcement for Ingress Events**

SNMP enforcement profiles can be bound to an event-based enforcement policy, which enables ClearPass to trigger SNMP enforcement based on an Ingress event.

This section demonstrates how ClearPass allows the binding of an SNMP-based enforcement profile to an event-based enforcement policy.

**Figure 416  SNMP-Based Enforcement Profile**

The configuration shown in **Figure 417** demonstrates the binding of an SNMP-based enforcement to an event-based enforcement policy.

**Figure 417  Binding an SNMP-Based Enforcement to an Event-Based Enforcement Policy**
Configuring Deep-Nested Active Directory Queries

This section describes the method for configuring ClearPass deep-nested Active Directory queries. This configuration prevents failed authentications due to lengthy look-up times.

- Configuring the Active Directory Authentication Source
- Using the LDAP Browser to Select the Group Information
- Configuring the Enforcement Policy for Deep-Nested AD Queries

Configuring the Active Directory Authentication Source

The first task in this procedure is to create an Active Directory authentication source and configure a new filter that will then be used in the enforcement policy.

To add a new Active Directory authentication source:

1. Navigate to Configuration > Authentication > Sources.
   The Authentication Sources page opens.
2. Click Add.
   The Add Authentication Sources dialog opens.
3. For Type, select Active Directory.
   For details on configuration for an Active Directory authentication source, refer to Generic LDAP and Active Directory.
4. From the Attributes tab, click Add More Filters.
   The Configure Filter dialog opens.

Figure 418  Configuring a New Filter for the Authentication Source

1. Specify the Authentication Source > Configure Filter parameters as described in the following table:
### Table 1: Authentication Source > Configure Filter Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Enter the name of this authentication source filter.</td>
</tr>
</tbody>
</table>
| Filter Query  | Enter the following filter query: 

\begin{verbatim}
(& (objectClass=user) (sAMAccountName=%{Authentication:Username}))
\end{verbatim}

| Name          | Enter the following name: 

\begin{verbatim}
tokenGroups
\end{verbatim}

<table>
<thead>
<tr>
<th>Attributes</th>
<th></th>
</tr>
</thead>
</table>
| Alias Name    | Enter the following Alias Name: 

\begin{verbatim}
Nested Groups
\end{verbatim}

**NOTE:** Take note of this Alias Name as you will use it when configuring the Rule for the enforcement policy later in this section (see Configuring the Enforcement Policy for Deep-Nested AD Queries). |

| Data Type      | From the drop-down, select String.                                                                                                                    |

6. Click **Save**.

### Using the LDAP Browser to Select the Group Information

Use the LDAP **Browse** page to select the Group Name. Then copy the corresponding **objectSid** value. The **objectSid** value will be used for the Rule Configuration in the enforcement policy (as described in the next section).

To select the group information:

1. From the **Configure Filter** configuration dialog, select the **Browse** tab.
   
   The **Browse** tab shows an LDAP browser from which you can browse the nodes in the Active Directory (or LDAP) directory, starting at the base DN. This is presented in read-only mode.
2. From the panel on the left select the Group Name (for example, CN=Administration).
3. Then, from the panel on the right, locate and copy the corresponding objectSid value.
4. Click Close.

Configuring the Enforcement Policy for Deep-Nested AD Queries

For details on configuring enforcement policies, see Configuring Enforcement Policies.

To configure the enforcement policy for deep-nested queries:

1. Navigate to Configuration > Enforcement > Policies.
   The Enforcement Policies page opens.
2. Click the Add link.
   The Add Enforcement Policies page opens.

Figure 420  Enforcement Policy

3. Specify the Enforcement tab parameters as described in the following table:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of this enforcement policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this enforcement policy</td>
</tr>
<tr>
<td>Enforcement Type</td>
<td>Select RADIUS.</td>
</tr>
<tr>
<td>Default Profile</td>
<td>From the drop-down, select any appropriate enforcement profile.</td>
</tr>
</tbody>
</table>

4. Click **Next** (or click the **Rules** tab).
   The **Rules Editor** opens.

**Figure 421 Configuring the Enforcement Policy Rule**

5. Select conditions for this rule. For each condition, select a matching action (enforcement profile).
6. Specify the **Rules Editor** conditions as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the Active Directory used for authentication.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the <strong>Alias Name</strong> specified for the authentication source (see Configuring the Active Directory Authentication Source).</td>
</tr>
<tr>
<td>Operator</td>
<td>Select the appropriate operator.</td>
</tr>
<tr>
<td>Value</td>
<td>Specify the <strong>objectSid</strong> value copied from the LDAP browser (see Using the LDAP Browser to Select the Group Information).</td>
</tr>
<tr>
<td>Profile Name</td>
<td>From the drop-down, select the appropriate profile name.</td>
</tr>
</tbody>
</table>

7. Click **Save**.
   You return to the **Add Enforcement Policies > Rules** page.
8. Click **Save**.

   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 354](#) for a list of the default profiles.
Adding and Modifying Network Devices

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 423  Network Devices Page**

2. Go to the following sections for Network Access Device configuration information:
   - Adding a Network Device
   - Modifying a Network Device
   - Adding and Modifying Proxy Targets
   - Adding and Modifying Device Groups
   - Configuring the Ingress Event Source

### 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
- Modifying a Network Device

To add a network device:

1. Navigate to the Configuration > Network > Devices page.
   
   The Network Devices page opens.
2. Click the Add link.

The Add Device page opens.

**Device Parameters**

**Figure 425 Add Device > Device Dialog**

3. Enter the Add Device > Device parameters as described in Table 1:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the device.</td>
</tr>
<tr>
<td>IP Address or Subnet</td>
<td>Specify the IPv4 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.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that provides additional information to identify the device.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RADIUS Shared Secret</td>
<td>Enter the RADIUS shared secret.</td>
</tr>
<tr>
<td>TACACS+ Shared Secret</td>
<td>Enter the TACACS+ shared secret.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Specify the name of the vendor to load the dictionary associated with this vendor for this device. This field is optional. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Enable RADIUS CoA</td>
<td>To configure the UDP port on the device to send CoA (Change of Authorization) actions, enable RADIUS CoA for this device. <strong>RADIUS CoA Port:</strong> The default value is 3799.</td>
</tr>
<tr>
<td>Enable RadSec</td>
<td>To enable RadSec, click the Enable Radsec check box. When RadSec is enabled, the RADIUS shared secret is populated with a default shared secret with the string “radsec.” <strong>NOTE:</strong> It is important that the controller is configured with the same shared secret.</td>
</tr>
</tbody>
</table>

**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.

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 426 Add Device > SNMP Read Settings Dialog**

   ![Add Device > SNMP Read Settings Dialog](image)

2. Enter the **SNMP Read Settings** parameters as described in **Table 2**:
### Table 2: *Add Device > SNMP Read Settings Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow SNMP Read</td>
<td>Toggle to enable or disable SNMP Read operations.</td>
</tr>
</tbody>
</table>
| 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 the **Read ARP table on this device** check box on a Layer-3 device if you intend to use the ARP table on this device to discover endpoints in the network.  
  **NOTE:** When this option is selected, all ARP entries read during periodic Network Access Device reads are added to ClearPass endpoints. SNMP, WMI, NMAP, and SSH scans are not used in this process. |
| Username                   | Specify the Admin user name to use for SNMP read operations.  
  **NOTE:** Available in SNMP v3 only.                                                                                                             |
### 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:** This option is 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 427 Add Device > SNMP Write Settings Dialog**

   ![SNMP Write Settings Dialog](image)

2. Enter the **SNMP Write Settings** parameters as described in **Table 3**.

   **Table 3: Add Device > SNMP Write Settings Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow SNMP Write</td>
<td>Toggle to enable or disable SNMP write.</td>
</tr>
<tr>
<td>Default VLAN</td>
<td>Specify the VLAN port setting after the SNMP-enforced session expires.</td>
</tr>
</tbody>
</table>
   | 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 
   - SNMP v3 with no Authentication 
   - SNMP v3 with Authentication using MD5 and no Privacy 
   - SNMP v3 with Authentication using MD5 and with Privacy |
### Parameter Action/Description

- 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community String</td>
<td>Enter the community string for sending the traps.</td>
</tr>
<tr>
<td>Verify</td>
<td>Reenter the community string for sending the traps.</td>
</tr>
</tbody>
</table>

### 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 428** Add Device > CLI Settings Dialog

2. Enter the **CLI Settings** parameters as described in **Table 4**:

   **Table 4:** Add Device > CLI Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow CLI Access</td>
<td>Toggle to enable or disable CLI access.</td>
</tr>
<tr>
<td>Access Type</td>
<td>Select <strong>SSH</strong> or <strong>Telnet</strong>. Policy Manager uses the selected access method to log into the device CLI.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the <strong>SSH</strong> or Telnet <strong>TCP</strong> port number.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to log into the CLI.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to log into the CLI.</td>
</tr>
<tr>
<td>Username Prompt Regex</td>
<td>Specify the regular expression for the username prompt. Policy Manager looks for this pattern to recognize the Telnet username prompt.</td>
</tr>
<tr>
<td>Password Prompt Regex</td>
<td>Specify the regular expression for the password prompt. Policy Manager looks for this pattern to recognize the Telnet password prompt.</td>
</tr>
<tr>
<td>Command Prompt Regex</td>
<td>Specify the regular expression for the command line prompt. Policy Manager looks for this pattern to recognize the Telnet command-line prompt.</td>
</tr>
<tr>
<td>Enable Prompt Regex</td>
<td>Specify the regular expression for the command line in the <strong>enable</strong> prompt. Policy Manager looks for this pattern to recognize the Telnet command-line prompt.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter then reenter the credentials for the <strong>Enable</strong> password in the CLI.</td>
</tr>
</tbody>
</table>

**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:
2. Enter the **OnConnect Enforcement** parameters as described in **Table 5**.

**Table 5: Add Device > OnConnect Enforcement Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Select this check box to enable ClearPass OnConnect on the network access device being added.</td>
</tr>
</tbody>
</table>
| 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 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:** An empty string will enable OnConnect on all ports. ClearPass will attempt to determine the uplink or upstream trunk ports; however, it is recommended to explicitly remove those ports. |
| 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 2** 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 430*.

*Figure 430*  *Querying Ports*

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 431  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 default 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.

Modifying a Network Device

To modify a ClearPass network device:

1. Navigate to the Configuration > Network > Devices page.
   The Network Devices page opens.
2. Select the network device you want to modify.
   The Edit Device Details dialog opens.

3. Modify any device settings as necessary.
   For details about all of the Network Device tabs and parameters, refer to the previous section, Adding a Network Device.

   If you disable RadSec, the shared secret is removed; you will have to reenter the original shared secret.

4. Click Save.

### 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).

**Adding a Device Group**

To add a device group:

1. Navigate to Configuration > Network > Device Groups.
   
The Network Device Groups page opens:

   **Figure 434 Device Groups Page**

2. Click Add.

3. Complete the fields in the Add New Device Group page as described in the following figure:
4. Specify the **Add New Device Group** page parameters as described in the following table:

**Table 1: Add New Device Group Page**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the device group.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter the description that provides additional information about the device group.</td>
</tr>
<tr>
<td>Format</td>
<td>Select the format: Subnet, Regular Expression, or List.</td>
</tr>
</tbody>
</table>
### Parameter | Action/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.
To filter the list based on the text in the associated text box, click Filter.

5. Click **Save**.

### 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 can be 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 Other Policy Manager Services on page 59.

### 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 436 Add Proxy Target Dialog**
3. Specify the **Add Proxy Target** parameters as described in the following table, then click **Save**:

**Table 1: Add Proxy Target Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the proxy target.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description that provides additional information about the proxy target.</td>
</tr>
<tr>
<td>Hostname/Shared Secret</td>
<td>Specify the RADIUS hostname.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret, then verify it.</td>
</tr>
<tr>
<td>Verify Shared Secret</td>
<td><strong>NOTE:</strong> Use the same shared secret that you entered on the proxy target (refer to your RADIUS server configuration).</td>
</tr>
<tr>
<td>RADIUS Authentication Port</td>
<td>Enter the UDP port to send the RADIUS request. The default value for this port is <strong>1812.</strong></td>
</tr>
<tr>
<td>RADIUS Accounting Port</td>
<td>Enter the UDP port to send the RADIUS accounting request. The default value for this port is <strong>1813.</strong></td>
</tr>
</tbody>
</table>

**Configuring the Ingress Event Source**

An event source is a device that sends Syslog events to ClearPass.

Any events sent that are not from configured event sources are ignored.

To configure an Event Source:

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 Event Source** dialog opens.

**Figure 437  Adding an Event Source**

3. Populate the **Add Event Source** parameters as described in **Table 1.**
### Table 1: Configuring the Add Event Source Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name or the IP address of the device that will send Syslog events to ClearPass.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of this Event Source.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the device that will send Syslog events to ClearPass.</td>
</tr>
<tr>
<td>Type</td>
<td>From the drop-down, select <strong>Syslog</strong>.</td>
</tr>
</tbody>
</table>
| Vendor    | From the drop-down, select the event source **Vendor**:  
|           | - Aruba Introspect  
|           | - Check Point  
|           | - Infoblox  
|           | - Juniper Networks  
|           | - Palo Alto Networks |
| Enable    | Select this check box to enable the device as an Event Source. |

4. When finished, click **Add**.

The **Event Sources** page now displays the new Event Sources (see **Figure 438**).

**Figure 438 Event Sources Page**

![Event Sources Page](image)

Note that the IP address displayed in **Figure 438** is the IP address and host name of the Juniper SRX gateway that sends Syslog events to ClearPass.
This chapter provides the following information:

- Configuring SNMP, SSH, and WMI Credentials
- Scheduling Network Scans and Subnet Scans

**Configuring SNMP, SSH, and WMI Credentials**

This section provides the following information:

- About Network Scan
- SNMP Credentials Configuration
- SSH Credentials Configuration
- WMI Credentials Configuration

**About Network Scan**

Network Scan uses a configured *seed network device* (typically a switch, router, or controller) to discover endpoints and network devices. You can schedule network scans and subnet scans (see Scheduling Network Scans and Subnet Scans).

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.
- SSH credentials
  For Linux server or network device discovery, specify SSH configuration credentials. For more information, see SSH Credentials Configuration.
- WMI credentials
  For Windows device discovery, specify WMI (Windows Management Instrumentation) credentials. For more information, see WMI Credentials Configuration.
- 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 Configuring SNMP, SSH, and WMI Credentials.
- ARP table
  ClearPass supports Address Resolution Protocol (ARP) probes for network discovery scans. When the Read ARP Table Info option is enabled, the scan also probes 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 SNMP Read Settings Parameters.
- 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 Monitoring Discovered Devices.

- 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 Scan High-Level Tasks**

Configuring Network Scan consists of these major tasks:

1. Add the configurations (SNMP, SSH, or WMI) needed to query all the devices in the target network.
   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 a network scan or a subnet scan to profile Linux servers and machines (SSH credentials), Windows servers and machines (WMI credentials), and network devices (SNMP).

2. Schedule a network scan or subnet scan (see Scheduling Network Scans and Subnet Scans).

3. Import the discovered network devices into ClearPass (see Importing Network Devices).

4. Review the set of discovered devices and view the connected endpoints and neighbors (see Viewing Details on a Discovered Device).

**SNMP Credentials Configuration**

For querying hosts discovered by a subnet scan, specify **SNMP** configuration. An SNMP-based scan sends an SNMP request to retrieve the network device information.

To add the SNMP configuration for a network scan or subnet scan:

1. Navigate to Configuration > Profile and Network Scan > Profile Settings.
   The **Profile Settings > SNMP Configuration** page opens.

**Figure 439  SNMP Configuration Page**

2. Click the **Add SNMP Configuration** link.
   The **SNMP Configuration** dialog opens.
3. Specify the **SNMP Configuration** parameters as described in [Table 1](#).

**Table 1: SNMP Configuration Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Subnets/IP Addresses</td>
<td>Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas. When you schedule the network scan, ClearPass will use the SNMP configuration to fetch the network device information for discovered devices.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>From the drop-down, select the appropriate SNMP version:</td>
</tr>
<tr>
<td></td>
<td>- SNMP v1 with community strings</td>
</tr>
<tr>
<td></td>
<td>- SNMP v2 with community strings</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with no Authentication</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using MD5 and no privacy</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using MD5 with privacy</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using SHA and no privacy</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using SHA with privacy</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of this SNMP configuration (recommended).</td>
</tr>
<tr>
<td>Community String</td>
<td>Enter the community string, then reenter the community string in the <strong>Verify</strong> field.</td>
</tr>
</tbody>
</table>

4. When finished, click **Save Entry**.
5. Repeat these steps to add additional SNMP credentials per subnet.
6. When finished, click **Save**.
   
   You return to the **SNMP Configuration** tab, where the new SNMP configuration information has been added, and the following message is displayed:
   
   *SNMP configuration added successfully*

**SSH Credentials Configuration**

For Linux servers or network device discovery, specify **SSH** (Secure Shell) configuration credentials. When SSH is found for an IP address or subnet, Network Scan 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 scan or subnet scan:

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 and Network Scan > Profile Settings.
   The Profile Settings page opens.
2. Select the SSH Configuration tab.

**Figure 441 SSH Configuration Tab**

3. Click Add Configuration.
   The SSH Configuration page opens.

**Figure 442 SSH Configuration Page**

4. Specify the parameters in the SSH Configuration dialog as described in the following table, then click Save Entry.
### Table 2: SSH Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Subnets/ IP Addresses</td>
<td>Enter either one or more IP subnets or one or more IP addresses. For multiple entries, separate multiple IP addresses with commas.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the device or subnet specified.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the device or subnet specified.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password, then reenter the password in the Enable Password Verify field.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of this SNMP configuration (recommended).</td>
</tr>
</tbody>
</table>

5. Repeat this procedure for additional entries if needed.

6. 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 443**).

**Figure 443  SSH Configuration Added Successfully**

---

### 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 is a key part of the Windows operating system. It’s 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 scan or subnet scan:

1. Navigate to **Configuration > Profile and Network Scan > Profile Settings**.
   - The **Profile Settings** page opens.
2. Select the **WMI Configuration** tab.
3. Click **Add Configuration**.
   The **WMI Configuration** page opens.

   **Figure 445  WMI Configuration Page**

4. Specify the **WMI Configuration** parameters as described in **Table 3**, then click **Save Entry**.

   **Table 3: WMI Configuration Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
   | IP Subnets/ IP Addresses| 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 scheduled. |
   | Domain                 | Enter the name of the Windows domain for logging into the device(s) that you are scanning. |
   | Username               | Enter the username for the device or subnet specified.                              |
   | Password               | Enter the password for the device or subnet specified.                              |
   | Description            | Optionally, enter a description of this SNMP configuration (recommended).           |

5. Repeat this procedure for additional entries if needed.
6. 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 446**).
Scheduling Network Scans and Subnet Scans

This section provides the following information:

- Network Scan High-Level Tasks
- Scheduling a Network Scan
- Scheduling a Subnet Scan
- Viewing Details About a Subnet Scan
- Configuring Nmap-Based Endpoint Port Scans

Network Scan High-Level Tasks

Configuring Network Scan operations consist of these major tasks:

1. Add the configurations (SNMP, SSH, or WMI) needed to query all the devices in the target network (for details, see Configuring SNMP, SSH, and WMI Credentials).

   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 a network scan or a subnet scan to profile Linux servers and machines (SSH credentials), Windows servers and machines (WMI credentials), and network devices (SNMP).

2. Schedule a network scan or a subnet scan (as described in this section).

3. After running a network scan, import the discovered network devices into ClearPass (see Monitoring Discovered Devices).

4. Review the set of discovered devices and view the connected endpoints and neighbors (see Monitoring Discovered Devices).

Scheduling a Network Scan

Seed devices are the initial IP addresses provided by the network administrator to start the network scan. When you initiate a network 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 1 below).
- You can go to those devices and see their neighbor devices.

Running a network 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 schedule a network scan:

1. Navigate to **Configuration > Profile and Network Scan > Network Scan**.
   
The **Network Scan** page opens.

   **Figure 447  Network Scan Page**

   ![Network Scan Page](image)

2. Click the **Start Scan** link.
   
The **Schedule Scan** dialog opens.

   **Figure 448  Scheduling a Network Scan**

   ![Schedule Scan](image)

   **WARNING:** Performing network scans can be resource intensive and time consuming. For large networks, scans could take more than an hour and ideally should be done on a ClearPass node that is not servicing core authentications, or should be done outside of normal business hours.

3. Specify the **Schedule Scan** parameters as described in **Table 1**.
<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Type</td>
<td>Select <strong>Network Scan</strong>. <strong>NOTE:</strong> For scan operations to be operable, the <strong>Master Server in Zone</strong> parameter must be configured. The master ClearPass server in a zone distributes the load among other ClearPass nodes in the zone. For details, see <strong>Master Server in Zone</strong>.</td>
</tr>
<tr>
<td>Zone</td>
<td>Specify the ClearPass Zone (for more information, see <a href="#">Managing Policy Manager Zones</a>). If a Zone is not configured, accept the default zone. <strong>NOTE:</strong> The primary master server in the zone forwards the scan request to the other ClearPass nodes in the zone, depending on the seed device. Each scan configuration added is distributed by the master to a different node in the zone. If one scan configuration has multiple seed devices, all the seed devices are forwarded to one node.</td>
</tr>
<tr>
<td>Seed Devices</td>
<td>Enter the IP addresses of one or more seed devices from which the network scan should proceed. Separate multiple device IP addresses with commas.</td>
</tr>
</tbody>
</table>
| Frequency of Scan     | Specify the frequency of the network scan:  
  - On Demand  
    This option runs the network scan once, either immediately if no start time is specified, or at the time specified by the **Start Time of Scan** parameter.  
  - Hourly  
  - Daily  
  - Weekly                                                                                                                                 |
| Scan Depth            | 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. |
| Probe ARP entries     | The ARP (Address Resolution Protocol) table provides information about MAC address and IP address associations for endpoints that were discovered by this ClearPass server.  
  The ARP entries for the specified network(s) are read irrespective of whether this check box is enabled.  
  When this option is enabled, ClearPass uses the ARP entries to discover network access devices (NADs), then proceeds to perform a network scan to the configured scan depth. |

4. Click **Save**.  
   You return to the **Network Scan** page, which now indicates the following:  
   - ClearPass Policy Manager Zone specified for the scan  
   - Type of scan: **Network**  
   - IP address(es) of the seed device(s) or subnet(s)  
   - Details such as scan depth and whether ARP probe is enabled or not  
   - Schedule specified for the network scan  
   - If a **Start Time** and **End Time** for the network scan was configured, that information is displayed.  
   - If the scan was set for **On Demand**, the **Schedule** field displays **On Demand**.  
   - The **Status** of the network scan operation, which shows initially as **Running**, and finally, **Completed**. The green status indicator indicates that the scan operation was successful.
To restart a completed scan, click the green **Status** button.

**Figure 449**  *Seed Device Successfully Scanned*

---

**Scheduling a Subnet Scan**

To schedule a subnet scan:

1. **Navigate to** Configuration > Profile and Network Scan > Network Scan.  
   The **Network Scan** page opens.
2. **Click the** Start Scan link.  
   The Schedule Scan dialog opens.

**Figure 450**  *Scheduling a Subnet Scan*

3. **Specify the** Subnet Scan parameters as described in the following table:

**Table 2: Schedule Subnet Scan Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Scan Type  | Select Subnet Scan.  
|            | You can schedule multiple subnet scans per zone.  
|            | To monitor subnet scan progress, navigate to Monitoring > Profiler and Discovery > Network Scan.  
|            | **NOTE:** For scan operations to be operable, Zone Master must be configured. The Zone Master distributes the load among other nodes in the zone. |
| Zone       | Specify the ClearPass Zone.  
|            | If a Zone is not configured, accept the default. |
| IP Subnets | Enter the IP addresses of one or more IP subnets from which the subnet scan should proceed. Separate multiple IP subnets with commas. |
### Field | Action/Description
--- | ---
Frequency of Scan | Specify the frequency of the scan:
- On Demand
  This option runs the subnet scan once, either immediately if no start time is specified, or at the time specified by the *Start Time of Scan* parameter.
- Hourly
- Daily
- Weekly

Start Time of Scan | Select the time for the subnet scan to start.

4. Click **Save**.

You return to the **Network Scan** page, which now indicates the following:

- ClearPass Policy Manager Zone specified for the scan
- Type of scan: **Subnet**
- IP subnet(s) specified for the subnet scan
- Schedule specified for the subnet scan
  - If a **Start Time** and **End Time** for the subnet scan was configured, that information is displayed.
  - If the scan was set for **On Demand**, the **Schedule** field displays *Runs only once On Demand starts at <time specified>*.
- The **Status** of the network scan operation, which shows initially as **Running**, and finally, **Completed**.

The green status indicator indicates that the subnet scan has been scheduled.

**Figure 451  Information Displayed for Scheduled Scans**

---

**Viewing Details About a Subnet Scan**

Additional information is available for the scheduled subnet scans.

To view the details about a subnet scan:

1. Navigate to **Monitoring > Profile and Network Scan > Network Scan**.

  The **Monitoring > Network Scan** page opens.
2. Click anywhere on the line for the subnet scan of interest.

The **Subnet Scan Results** page opens.

**Figure 453  Subnet Scan Results Page**

The **Subnet Scan Results** page provides the following information regarding the selected subnet scan:

**Table 3: Subnet Scan Results: Information Provided**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone</td>
<td>Specifies the ClearPass Policy Manager Zone in which the subnet resides.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the subnet scan started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the subnet scan was completed.</td>
</tr>
<tr>
<td>Active Hosts</td>
<td>Indicates the number of active hosts in the subnet. An active host is a network device that is up in the network.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failed Hosts</td>
<td>Indicates the number of failed hosts in the subnet. A failed host is a host that is not up in the network.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the subnet scan. The possible status states are:</td>
</tr>
<tr>
<td></td>
<td>- Failed</td>
</tr>
<tr>
<td></td>
<td>- Running</td>
</tr>
<tr>
<td></td>
<td>- Completed</td>
</tr>
<tr>
<td>Scan Errors</td>
<td>Displays any errors that occurred during the subnet scan.</td>
</tr>
</tbody>
</table>

**Configuring Nmap-Based Endpoint Port Scans**

The network scan feature supports running an Nmap (Network Mapper)-based scan on a host to detect open ports and also to fingerprint the services running behind those ports. This information is used in the device profile.

To configure endpoint port scans using Nmap:

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.
   c. Set the **Enable Endpoint Port Scans using Nmap** parameter to **TRUE**, then click **Save**.
      For more information, see [Profiler Parameters](#).
      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.

2. Schedule a network scan configuring a seed device with **Probe ARP** entries enabled (see Scheduling a Network Scan).
3. When the network scan is completed, select an endpoint (see Adding and Modifying Endpoints).
   a. Navigate to **Configuration** > **Identity** > **Endpoints**.
b. From the **Endpoints** page, click the endpoint of interest. The **Edit Endpoint** page opens.

**Figure 455** *Edit Endpoint Page*

![Edit Endpoint Page](image)

4. To view the list of host services and the list of open ports returned by the network scan for the selected host or endpoint, select the **Fingerprints** tab (see **Figure 456**).

**Figure 456** *Endpoint Fingerprint Details with Nmap Scan Data Included*

![Endpoint Fingerprint Details with Nmap Scan Data Included](image)
After creating policies, use the **Policy Simulation** feature to evaluate those policies before deployment. The **Policy Simulation** feature applies a set of request parameters as input against a given policy component and displays the outcome.

To configure a policy simulation:

1. Navigate to **Configuration > Policy Simulation**. The **Policy Simulation** page opens.

**Figure 457 Policy Simulation Page**

This chapter describes the following types of policy simulations:

- **Active Directory Authentication Simulation**
- **Application Authentication Simulation**
- **Audit Simulation**
- **Chained Simulation**
- **Enforcement Policy Simulation**
- **RADIUS Authentication Simulation**
- **Role Mapping Simulation**
- **Service Categorization 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 an Active Directory simulation for the authentication test:

1. Navigate to the **Configuration > Policy Simulation > Add** page. The Add Policy Simulation dialog opens.
2. Specify the **Active Directory Authentication > Simulation** tab parameters as described in the following table:

**Table 1: Active Directory Authentication Simulation Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the simulation</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description of this simulation.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>Active Directory Authentication</strong> is specified by default.</td>
</tr>
<tr>
<td><strong>Simulation Details</strong></td>
<td></td>
</tr>
<tr>
<td>Active Directory Domain</td>
<td>Select the Active Directory domain to which the node is joined.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to log in to the domain.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to log in to the domain.</td>
</tr>
</tbody>
</table>

**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 459  Active Directory Authentication Results Tab**
### Table 2: Active Directory Authentication Results Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays the results of the Active Directory Authentication simulation.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status message.</td>
</tr>
</tbody>
</table>

### 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 460  Application Authentication - Simulation Tab**

**Table 1: Application Authentication Simulation Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPPM IP Address/FQDN</td>
<td>Enter the IP Address or FQDN of the domain(s) to which the node is joined.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
</tbody>
</table>

**Attributes Tab**

Enter the attributes of the policy component to be tested. The following figure displays the Application Authentication - Attributes tab:

**Figure 461  Application Authentication - Attributes Tab**
Table 23: Application Authentication - Attributes Tab Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Application or select Application:ClearPass. See Application Namespace</td>
</tr>
<tr>
<td>Name</td>
<td>The options displayed for the Name Attribute depend on the Type Attribute that was selected.</td>
</tr>
<tr>
<td>Value</td>
<td>The options displayed for the Value Attribute depend on the Type Attribute and Name Attribute that were selected.</td>
</tr>
</tbody>
</table>

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 462 Application Authentication Results Tab

Table 2: Application Authentication Results Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays the results of the Active Directory Authentication simulation.</td>
</tr>
<tr>
<td>Application Authentication Output Attributes</td>
<td>Displays the output attributes, such as Super Administrator.</td>
</tr>
</tbody>
</table>

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.

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 463 Audit Simulation - Simulation Tab**

The following table describes the **Audit Simulation - Simulation** tab parameters:

**Table 1: Audit Simulation Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Server</td>
<td>Select [Nessus Server] or [Nmap Audit].</td>
</tr>
<tr>
<td>Audit Host IP Address</td>
<td>Enter the host IP address of the audit host.</td>
</tr>
</tbody>
</table>

**Results Tab**

The following figure displays the **Audit Simulation - Results** tab:

**Figure 464 Audit Simulation Results Tab**

Configuration » Policy Simulation » Edit - audit

**Policy Simulation - audit**

**Summary**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Status</td>
<td>AuditInProgress</td>
</tr>
<tr>
<td>Temporary Status</td>
<td>TRANSITION (15)</td>
</tr>
<tr>
<td>Audit Timeout</td>
<td>60 seconds</td>
</tr>
</tbody>
</table>

**Audit Output Attributes**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avenda:Audit:Audit-Status</td>
<td>AUDIT_INPROGRESS</td>
</tr>
</tbody>
</table>

The following table describes the **Audit Simulation - Results** tab parameters:

**Table 2: Audit Results Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays information about the Audit Status, Temporary Status, and Audit Timeout.</td>
</tr>
<tr>
<td>Audit Output Attributes</td>
<td>Displays the Audit-Status such as AUDIT_INPROGRESS.</td>
</tr>
</tbody>
</table>
**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 465 Chained Simulation Tab**

The following table describes the **Chained Simulation - Results** tab parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Select from:</td>
</tr>
<tr>
<td></td>
<td>• [Policy Manager Admin Network Login Service]</td>
</tr>
<tr>
<td></td>
<td>• [AirGroup Authorization Service]</td>
</tr>
<tr>
<td></td>
<td>• [Aruba Device Access Service]</td>
</tr>
<tr>
<td></td>
<td>• [Guest Operator Logins]</td>
</tr>
<tr>
<td></td>
<td>• Guest Access</td>
</tr>
<tr>
<td></td>
<td>• Guest Access With MAC Caching</td>
</tr>
<tr>
<td>Authentication Source</td>
<td>Default Value = [Local User Repository] if you select:</td>
</tr>
<tr>
<td></td>
<td>• [Policy Manager Admin Network Login Service]</td>
</tr>
<tr>
<td></td>
<td>• [Aruba Device Access Service]</td>
</tr>
<tr>
<td></td>
<td>Default Value = [Guest Device Repository] if you select:</td>
</tr>
<tr>
<td></td>
<td>• [AirGroup Authorization Service]</td>
</tr>
<tr>
<td></td>
<td>• Guest Access</td>
</tr>
<tr>
<td></td>
<td>• Guest Access With MAC Caching</td>
</tr>
<tr>
<td></td>
<td>Values = [Guest Device Repository] or [Local User Repository] if you select [Guest Operator Logins]</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Test Date and Time</td>
<td>Click the calendar icon to select a start date and time for simulation test. For more information, see Date Namespaces</td>
</tr>
</tbody>
</table>

**Attributes Tab**

Enter the attributes of the policy component to be tested.
The following table describes the **Chained Simulation Attributes - Results** tab parameters:

**Table 24: Chained Simulation Attributes tab Parameters**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the type of attributes from the drop-down list.</td>
</tr>
<tr>
<td>Host</td>
<td>See Host Namespaces</td>
</tr>
<tr>
<td>Authentication</td>
<td>See Authentication Namespaces</td>
</tr>
<tr>
<td>Connection</td>
<td>See Connection Namespaces</td>
</tr>
<tr>
<td>Application</td>
<td>See Application Namespace</td>
</tr>
<tr>
<td>Certificate</td>
<td>See Certificate Namespaces on page 963</td>
</tr>
<tr>
<td></td>
<td>See RADIUS Namespaces</td>
</tr>
<tr>
<td>Radius:IETF</td>
<td></td>
</tr>
<tr>
<td>Radius:Cisco</td>
<td></td>
</tr>
<tr>
<td>Radius:Microsoft</td>
<td></td>
</tr>
<tr>
<td>Radius:Avenda</td>
<td></td>
</tr>
<tr>
<td>Radius:Aruba</td>
<td></td>
</tr>
<tr>
<td>Trend:AV</td>
<td></td>
</tr>
<tr>
<td>Cisco: HIPS</td>
<td></td>
</tr>
<tr>
<td>Cisco:HOST</td>
<td></td>
</tr>
<tr>
<td>Cisco:PA</td>
<td></td>
</tr>
<tr>
<td>NAI:AV</td>
<td></td>
</tr>
<tr>
<td>Symantec:AV</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The options displayed for the <strong>Name</strong> attribute depend on the <strong>Type</strong>  attribute that was selected.</td>
</tr>
<tr>
<td>Value</td>
<td>The options displayed for the <strong>Value</strong> attribute depend on the <strong>Type</strong> and <strong>Name</strong> attributes that were selected.</td>
</tr>
</tbody>
</table>
Results Tab

The following figure displays the Chained Simulation - Results tab:

**Figure 467  Chained Simulation Results Tab**

![Chained Simulation Results Tab](image)

<table>
<thead>
<tr>
<th><strong>Summary</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Allow Access</td>
</tr>
<tr>
<td>Roles</td>
<td>[User Authenticated]</td>
</tr>
<tr>
<td>System Posture Status</td>
<td>UNKNOWN (100)</td>
</tr>
<tr>
<td>Enforcement Profiles</td>
<td>[TACACS Deny Profile]</td>
</tr>
</tbody>
</table>

Table 2: Chained Simulation Results Tab Parameters

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| 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 185](#).

To configure an enforcement policy simulation:

1. Navigate to **Configuration > Policy Simulation**.  
The Policy Simulation page opens.
2. Click the **Add** link.  
The Add Policy Simulation page opens to the Simulation tab.
3. Specify the **Policy Simulation** tab parameters as described in the following table:

**Table 1: Enforcement Policy Simulation Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of this policy simulation</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this policy simulation</td>
</tr>
<tr>
<td>Type</td>
<td>From the <strong>Type</strong> drop-down, select <strong>Enforcement Policy</strong>.</td>
</tr>
<tr>
<td>Service</td>
<td>From the <strong>Service</strong> drop-down, select the appropriate service.</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td>Depending on which service you selected, the value for the <strong>Enforcement Policy</strong> will be filled automatically.</td>
</tr>
<tr>
<td>Authentication Source</td>
<td>Value = [Local User Repository] if you select:</td>
</tr>
<tr>
<td></td>
<td>- [Policy Manager Admin Network Login Service]</td>
</tr>
<tr>
<td></td>
<td>- [Aruba Device Access Service]</td>
</tr>
<tr>
<td></td>
<td>Value = [Guest Device Repository] if you select:</td>
</tr>
<tr>
<td></td>
<td>- [AirGroup Authorization Service]</td>
</tr>
<tr>
<td></td>
<td>- Guest Access</td>
</tr>
<tr>
<td></td>
<td>- Guest Access With MAC Caching</td>
</tr>
<tr>
<td></td>
<td>Values = [Local User Repository] or [Guest Device Repository] if you select Guest Operator Logins</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name.</td>
</tr>
</tbody>
</table>
### Parameter | Action/Description
--- | ---
Roles | From the Roles drop-down, select the appropriate role.
Dynamic Roles | To add a role:
1. Enter the name of a dynamic role in the Add Role field.
2. Click the Add Role button to populate the Dynamic Roles list.
To remove a role, highlight the dynamic role of choice, then click Remove Role.
System Posture Status | Select from:
- HEALTHY (0)
- CHECKUP (10)
- TRANSITION (15)
- QUARANTINE (20)
- INFECTED (30)
- UNKNOWN (100)
Test Date and Time | Click the calendar icon to select the start date and time for the simulation test. For more information, see Date Namespaces

**Attributes Tab**
Enter the attributes of the policy component to be tested.

**Table 2: Enforcement Policy Attributes Tab Parameters**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type | Select the type of attribute from the drop-down list.
- Host (for more information, see Host Namespaces).
- Authentication (for more information, see Authentication Namespaces).
- Connection (for more information, see Connection Namespaces).
- Application (for more information, see Application Namespace).
- Radius:IETF
- Radius:Cisco
- Radius:Hewlett-Packard-Enterprise
- Radius:Microsoft
- Radius:Alcatel-Lucent-Enterprise
- Radius:F5
- Radius:Avenda
- Radius:Freeswitch
- Radius:Aruba
  For more information, see RADIUS Namespaces.
| 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 Policy Simulation > Results tab:
**Table 3: Enforcement Policy Results Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny Access</td>
<td>Displays the output of the Deny Access test.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enforcement Profile</td>
<td>Displays the name of the Enforcement Profile that is applied to this policy.</td>
</tr>
</tbody>
</table>

**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 710 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 470 displays the RADIUS Authentication Simulation Details dialog, with the Server parameter set to Remote.
4. Enter the values for each of the **RADIUS Simulation** parameters as described in **Table 1**.

### Table 1: RADIUS Simulation Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>1. Specify <strong>Local</strong> or <strong>Remote</strong>.</td>
</tr>
</tbody>
</table>
| 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](#)). |
| 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                                                                                                                                                           |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7. Enter the client MAC address of the network device to populate the NAS-IP</td>
</tr>
<tr>
<td></td>
<td>address attribute in the RADIUS request.</td>
</tr>
<tr>
<td>Client MAC Address</td>
<td>8. Enter the user name.</td>
</tr>
<tr>
<td>(optional)</td>
<td></td>
</tr>
<tr>
<td>CA Certificate (optional)</td>
<td>9. Click <strong>Browse</strong> and navigate to the optional Root CA certificate. Click <strong>Open</strong></td>
</tr>
<tr>
<td></td>
<td>, then click <strong>Upload</strong>.</td>
</tr>
<tr>
<td>Client Certificate</td>
<td>10. Click <strong>Browse</strong> and navigate to the Client Certificate PKCS12. Click <strong>Open</strong>, then click <strong>Upload</strong>.</td>
</tr>
<tr>
<td>PKCS12 (PFX)*</td>
<td></td>
</tr>
<tr>
<td>Passphrase for PFX file*</td>
<td>11. Enter the pass phrase for the selected PFX file.</td>
</tr>
<tr>
<td>* These fields are</td>
<td></td>
</tr>
<tr>
<td>displayed only if you</td>
<td>select <strong>TTLS</strong> or <strong>PEAP</strong> as the authentication outer method and you select</td>
</tr>
<tr>
<td>select <strong>EAP-TLS</strong> as the</td>
<td>authentication inner method.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12. Click <strong>Save</strong>, or click <strong>Next</strong> to proceed to the <strong>Attributes</strong> tab.</td>
</tr>
</tbody>
</table>

**Setting the Attributes to Be Tested**

The attributes that you can set depend on the **NAS Type** selected on the Policy Simulation page (see Figure 470).

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**.
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 472  Aruba Wireless Controller Type - Attributes**

**Table 2: Aruba Wireless Controller Required - Attribute Settings**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line 1:</td>
<td></td>
</tr>
<tr>
<td>Type = Radius:IETF</td>
<td></td>
</tr>
<tr>
<td>Name = NAS-Port-Type</td>
<td></td>
</tr>
<tr>
<td>Value = Wireless-802.11 (19)</td>
<td></td>
</tr>
</tbody>
</table>

| 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 473 NAS Type: Aruba Wired Switch Controller Attributes Tab*

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Line 1:</th>
<th>Type = Radius:IETF</th>
<th>Name = NAS-Port-Type</th>
<th>Value = Ethernet (15)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Line 2:</th>
<th>Type = Radius:IETF</th>
<th>Name = Service-Type</th>
<th>Value = Login-User (1)</th>
</tr>
</thead>
</table>

**Table 3: NAS Type: Aruba Wired Switch Controller—Required Attribute Settings**

**NAS Type: Cisco Wireless Switch**

*Figure 474 NAS Type: Cisco Wireless Switch Attributes*

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Line 1:</th>
<th>Type = Radius:IETF</th>
<th>Name = NAS-Port-Type</th>
<th>Value = 802.11(19)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Line 2:</th>
<th>Type = Radius:IETF</th>
<th>Name = Service-Type</th>
<th>Value = Framed-User(2)</th>
</tr>
</thead>
</table>

**Table 4: NAS Type: Cisco Wireless Switch Required Attribute Settings**

**Viewing the Simulation Results**

The following figure displays the **Policy Simulation RADIUS - Results** dialog:
Figure 475  Results Tab

Table 5:  RADIUS Authentication Results Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays a summary of the simulation.</td>
</tr>
<tr>
<td>Authentication Result</td>
<td>Displays the outcome of the Authentication test.</td>
</tr>
</tbody>
</table>
| 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 476  Role Mapping Simulation Tab

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |

Attributes Tab

Enter the attributes of the policy component to be tested. The following figure displays the Role Mapping Simulation Attributes tab:
The following table describes the Role Mapping Simulation Attributes tab parameters:

**Table 2: Role Mapping Simulation Attributes Tab Parameters**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the type of attributes from the drop-down list.</td>
</tr>
<tr>
<td>Host</td>
<td>See Host Namespaces</td>
</tr>
<tr>
<td>Authentication</td>
<td>See Authentication Namespaces</td>
</tr>
<tr>
<td>Connection</td>
<td>See Connection Namespaces</td>
</tr>
<tr>
<td>Application</td>
<td>See Application Namespace</td>
</tr>
<tr>
<td>Certificate</td>
<td>See Certificate Namespaces on page 963</td>
</tr>
<tr>
<td>Radius:IETF</td>
<td>See RADIUS Namespaces</td>
</tr>
<tr>
<td>Radius:Cisco</td>
<td></td>
</tr>
<tr>
<td>Radius:Microsoft</td>
<td></td>
</tr>
<tr>
<td>Radius:Avena</td>
<td></td>
</tr>
<tr>
<td>Radius:Aruba</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The options displayed for the Name attribute depend on the Type attribute that was selected.</td>
</tr>
<tr>
<td>Value</td>
<td>The options displayed for the Value attribute depend on the Type and Name attributes that were selected.</td>
</tr>
</tbody>
</table>

**Results Tab**

The following figure displays the Role Mapping Simulation - Results tab:

**Figure 478 Results Tab**

The following table describes the Role Mapping Simulation - Results tab parameters:

**Table 3: Role Mapping Results Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays the results of the simulation.</td>
</tr>
</tbody>
</table>
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:

![Service Categorization Simulation Tab](image)

Table 1: Service Categorization Simulation Tab Parameters

<table>
<thead>
<tr>
<th>Parameter Type</th>
<th>Namespace Details</th>
</tr>
</thead>
</table>
| 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:

![Service Categorization Attributes Tab](image)

Table 2: Service Categorization Simulation Attributes Tab Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the type of attributes from the drop-down list.</td>
</tr>
<tr>
<td>Host</td>
<td>See Host Namespaces</td>
</tr>
<tr>
<td>Authentication</td>
<td>See Authentication Namespaces</td>
</tr>
<tr>
<td>Connection</td>
<td>See Connection Namespaces</td>
</tr>
<tr>
<td>Application</td>
<td>See Application Namespace</td>
</tr>
</tbody>
</table>
### Attribute

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius:IETF</td>
<td>See <a href="#">RADIUS Namespaces</a></td>
</tr>
<tr>
<td>Radius:Cisco</td>
<td></td>
</tr>
<tr>
<td>Radius:Microsoft</td>
<td></td>
</tr>
<tr>
<td>Radius:Aruba</td>
<td></td>
</tr>
</tbody>
</table>

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 481 Results Tab**

---

**Policy Simulation - service_cat**

---

The following table describes the **Service Categorization Simulation Results** tab parameters:

### Table 3: Service Configuration Results Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Gives the name of the service.</td>
</tr>
</tbody>
</table>

---

**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 482 Import Simulations**
Table 1: Import from file page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select file</td>
<td>Browse to select name of simulations to import.</td>
</tr>
<tr>
<td>Enter secret for the file (if any)</td>
<td>If the file was exported with a secret key for encryption, enter the same key here.</td>
</tr>
</tbody>
</table>

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 483  Export Simulations

To export a specific simulation, click Export. In the Save As dialog box, enter the name of the XML file to contain the export data.

Table 2: Export Simulations

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>Select Yes to export the file with password protection.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the secret key in this field.</td>
</tr>
<tr>
<td>Verify Secret</td>
<td>Enter the same secret key to confirm and complete export.</td>
</tr>
</tbody>
</table>
This chapter contains the following information:

- ClearPass Device Profiler Overview
- About the Device Profile
- Endpoint Information Collectors

ClearPass Device Profiler Overview

This section contains the following information:

- About the ClearPass Device Profiler
- Enabling Endpoint Classification
- Viewing Live Endpoint Information for a Specific Device
- Configuring CoA for an Endpoint-Connected Device
- Fingerprint Dictionaries

About the ClearPass Device Profiler

The ClearPass Device Profiler is a ClearPass Policy Manager module that automatically classifies endpoints using attributes obtained from software components called Collectors.

ClearPass Device Profiler 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).

Device 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

To enable endpoint classification, you must configure the Master Server in Zone parameter by specifying the Primary master server and Secondary master server (for more information, see Master Server in Zone). If you don’t specify the primary master server in the zone, ClearPass will automatically select the node in the zone with the lowest UUID (universally unique identifier).

When you enable the ClearPass server for endpoint classification, this associates each endpoint with a specific user or location and secures access for other devices.

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 > Profiler and Discovery > Endpoint Profiler.
   The Endpoint Profiler opens.
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:
   - Monitoring Endpoint Profiler
   - Using the Policy Manager Dashboard

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:
4. Select the **Profiler** tab.
   The **Profiler** page opens.

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).

6. Specify the **Profiler** page parameters as described in **Table 25**:

   **Table 25: Profiler Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Classification</td>
<td>Select one or more endpoint classification items from the drop-down list. You can select a new action, or remove a current action.</td>
</tr>
<tr>
<td>RADIUS CoA Action</td>
<td>Select the RADIUS CoA action from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>- To view the <strong>Policy Manager Entity Details</strong> page with the summary of enforcement profile details, click <strong>View Details</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To view the <strong>Summary</strong> tab with profile details, click <strong>Modify</strong>.</td>
</tr>
<tr>
<td>Add new RADIUS CoA Action</td>
<td>To create a new RADIUS CoA action, click the <strong>Add New RADIUS CoA Action</strong> link.</td>
</tr>
</tbody>
</table>

7. When finished, click **Save**.
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 ClearPass Portal).

To view the contents of the fingerprints dictionary:

1. Navigate to Administration > Dictionaries > Fingerprints.
   
   The Device Fingerprints page opens. This page lists all the device fingerprints recognized by the Device Profiler module.

   **Figure 487  Device Fingerprints Page**

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 488  Device Fingerprint Dictionary Attributes Page**

3. To exit, click Close.
About the Device Profile

The Device Profiler module produces a Device Profile, which is a hierarchical model consisting of three elements that are derived by the endpoint attributes—DeviceCategory, DeviceFamily, and DeviceName.

Table 26: Elements of a Device Profile

<table>
<thead>
<tr>
<th>Endpoint Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceCategory</td>
<td>Denotes the type of the device, for example, Computer, Smart Device, Printer, or Access Point.</td>
</tr>
<tr>
<td>DeviceFamily</td>
<td>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.</td>
</tr>
<tr>
<td>DeviceName</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 indicates when the device was first discovered and last seen

Endpoint Information Collectors

Collectors are the network elements that provide data in order to profile endpoints. This section provides the following information:

- **DHCP Collector**
- **NetFlow Collector**
- **SFlow Collector**
- **ClearPass Onboard Collector**
- **HTTP User-Agent Strings Collector**
- **MAC OUI Collector**
- **ActiveSync Plug-in Collector**
- **ClearPass OnGuard Agent**
- **Subnet Scan Collector**

**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:

```bash
interface <vlan_name>
ip address <ip_addr> <netmask>
ip helper-address <dhcp_server_IP>
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).

**SFlow Collector**

sFlow is a general purpose network-traffic measurement system technology. sFlow is embedded in network devices and provides continuous statistics on any protocol so that all traffic throughout a network can be accurately characterized and monitored.

The main difference between NetFlow and sFlow is that NetFlow is restricted to IP only, whereas sFlow has the ability sample all traffic (that is, it is network-layer independent).

The sFlow Collector has the following characteristics:

- In ClearPass Policy Manager, Sflow listens to UDP port **6343**.

UDP port **6343** must be opened to the firewall. The switch/sFlow source should be configured to send sFlow packets to ClearPass UDP port **6343**.

- Sflow identifies the destination IP/Port from the flow that reaches the ClearPass server and determines whether there is already an IP or MAC address.
- When Sflow finds the corresponding IP/MAC binding, the destination IP/Port is sent to Profiler for further processing in batches of 10 and in one-minute intervals. IP/MAC pairs that are not found do not receive further processing.
- Sflow Collector caches the open port information for a device and only the updated the port information is sent to the Profiler (as a merge request).

**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 collects and sends 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 Scheduling Network Scans and Subnet Scans.
### Table 1: SNMP MIBs Used by the SNMP Collector

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SysDescr</td>
<td>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).</td>
</tr>
<tr>
<td>cdpCacheTable</td>
<td>Provides the cached information obtained via receiving Cisco Discovery Protocol (CDP) messages from CDP-capable devices. This is used to discover neighbor devices connected to the switch or controller configured in ClearPass.</td>
</tr>
<tr>
<td>lldpRemTable</td>
<td>This table contains one or more rows per physical network connection known to this agent read from LLDP (Link Layer Discovery Protocol)-capable devices. This is used to discover and profile neighbor devices connected to the switch or controller configured in ClearPass.</td>
</tr>
<tr>
<td>ARPtable</td>
<td>Address Resolution Protocol (ARP) information is read from the network devices. This is used as a means to discover endpoints in the network.</td>
</tr>
</tbody>
</table>

### 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 489 Specifying SNMP v2 with Community Strings

![Edit Device Details](image)

4. Specify the SNMP Read Settings parameters as described in the following table, then click **Save**.
### Table 2: SNMP Read Settings Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow SNMP Read</td>
<td>If not already enabled, enable the Allow SNMP Read check box. The SNMP Read Settings parameter fields are now enabled for configuration.</td>
</tr>
<tr>
<td>Policy Manager Zone</td>
<td>Select the Policy Manager Zone. If no Policy Manager Zone is configured, select default.</td>
</tr>
<tr>
<td>SNMP Read Setting</td>
<td>Select <strong>SNMPv2 with community strings</strong>.</td>
</tr>
<tr>
<td>Community String</td>
<td>Enter the <strong>Community String</strong> value, then reenter the string to verify it.</td>
</tr>
<tr>
<td>Force Read</td>
<td>Enable the <strong>Force Read</strong> 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 <strong>Force Read</strong> option does not require any trap configuration on the network device.</td>
</tr>
<tr>
<td>Read ARP Table Info</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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.
5. In the **minutes** field, enter the **Device Info Poll Interval**, then click **Save**.

**Subnet Scan Collector**

A network or 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 Manager nodes 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 560.

3. Configure the SNMP, SSH, and WMI credentials required to query for network devices, Linux devices, and Windows devices respectively (for details, see Configuring SNMP, SSH, and WMI Credentials).

4. Schedule a network scan or subnet scan (for details, see Scheduling Network Scans and Subnet Scans).
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 481

**Users and Privileges**
- Managing Admin Users on page 482
- Managing Admin Privileges on page 487

**Server Manager**
- Server Configuration Operations on page 496
- ClearPass Cluster Configuration Options
- Log Configuration on page 572
- Downloading Local Shared Folders on page 576
- License Management on page 576

**External Servers**
- SNMP Trap Receivers on page 589
- Syslog Targets on page 594
- Syslog Export Filters on page 595
- Messaging Setup on page 607
- Endpoint Context Servers on page 609
- Adding Vendor-Specific Endpoint Context Servers
- File Backup Servers on page 684

**Certificates**
- Certificate Store on page 686
- Creating and Installing a Self-Signed Server Certificate
- Creating a Certificate Signing Request
- Importing a Server Certificate
- Exporting a Server Certificate
- Service Certificates
- Associating a RADIUS Service Certificate with a Service
- Certificate Trust List on page 705
- Certificate Revocation Lists on page 707
Dictionaries
- RADIUS Dictionary on page 710
- RADIUS CoA Templates
- TACACS+ Services Dictionary on page 714
- Device Fingerprints Dictionary on page 715
- Dictionary Attributes on page 719
- Applications Dictionaries on page 973
- Configuring Endpoint Context Server Actions on page 723

Agents and Software Updates
- Software Updates
- OnGuard Settings and Agent Library Updates on page 732
- Onguard Agent Installers
- Creating OnGuard Custom Web Pages
- OnGuard Global Agent Settings
- Upgrading From OnGuard Plugin Version 1.0 to 2.0

Cluster Update and Upgrade
- Updating Clusters on page 766
- Upgrading Clusters on page 1

Ingress Events Processing
- Configuring Processing for Ingress Events

Insight Report Tool
- ClearPass Insight Reports

Support Services
- Contacting Support on page 761
- Remote Assistance on page 762
- Accessing ClearPass Documentation on page 765
- Accessing the OnGuard Support Charts

ClearPass Portal
To customize the ClearPass Portal content for your enterprise:
1. Navigate to the Administration > ClearPass Portal page. The ClearPass Portal page opens:
2. Specify the ClearPass Portal parameters as described in the following table, then click **Save**:

**Table 1: ClearPass Portal Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Option</td>
<td>Select the page that the user first sees after logging in to ClearPass:</td>
</tr>
<tr>
<td></td>
<td>- Default Landing Page</td>
</tr>
<tr>
<td></td>
<td>- Application Login Page:</td>
</tr>
<tr>
<td></td>
<td>- Guest Portal</td>
</tr>
<tr>
<td>Page Title</td>
<td>Click and enter the text to appear as the page title in the default landing page.</td>
</tr>
<tr>
<td>Logo Image</td>
<td>Click and browse to select an image for the banner in the default landing page.</td>
</tr>
<tr>
<td>Top section</td>
<td>Click and enter the text to appear as the header in the default landing page.</td>
</tr>
<tr>
<td>Bottom section</td>
<td>Click and enter the text to appear as the footer in the default landing page.</td>
</tr>
<tr>
<td>Copyright</td>
<td>Click and enter the copyright text to appear in the default landing page.</td>
</tr>
</tbody>
</table>

Both the HTTP and HTTPS protocols are supported for ClearPass Portal redirection.

**Managing Admin Users**

This section describes the following topics:

- **About Admin Users**
About Admin Users
ClearPass provides three types of admin users by default:

- **Super Admin**: Allowed read/write access to all configuration elements.
- **API Admin**: Allowed API access to all configuration elements.
- **readonly**: Allowed read-only access to all configuration elements.

In addition, ClearPass allows you to add the following types of admin users:

- **Aruba User Role Download**: This admin role provides access to only download user roles.
- **Help Desk**: Allows the Help Desk to log in to troubleshoot problems reported by end users.
- **Network Administrator**: Allowed to configure all ClearPass policies.
- **Receptionist**: Allowed to access the main monitoring screens.

Select any of the links below to view more information about these procedures.

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 492  Admin Users Page**

In this page, you can view the administrator details such as user ID, user name, and privilege level, as well as whether the admin user type is enabled or disabled. You can also change the admin password, and add, import, export, set password policies for the admin users, and disable admin user accounts 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 493  Changing the Administration User Password

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 494  Adding an Admin User

3. Specify the **Add Admin User** parameters as described in the following table, then click **Save**:

**Table 1: Adding an Admin User Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Specify a user ID for this administrator.</td>
</tr>
<tr>
<td>Name</td>
<td>Specify the name for the admin user.</td>
</tr>
<tr>
<td>Password/Verify Password</td>
<td>Specify a password for the local user, then verify the password.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable User</td>
<td>You must enable this check box to enable the admin user account (is enabled by default). Otherwise, the admin user account is disabled.</td>
</tr>
</tbody>
</table>
| Privilege Level  | From the drop-down list, select one of the following admin user privilege levels:  
|                  |  - API Administrator 
|                  |  - Aruba User Role Download 
|                  |  - 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**.

**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 495  Setting Admin Users Password Policy**

3. Specify the **Password Policy** parameters as described in **Table 2**, then click **Save**.
### Table 2: Password Policy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>Specify the minimum length required for the password.</td>
</tr>
<tr>
<td>Complexity</td>
<td>Select the complexity setting from the <strong>Complexity</strong> drop-down list. The complexity settings can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- No password complexity requirement</td>
</tr>
<tr>
<td></td>
<td>- At least one uppercase and one lowercase letter</td>
</tr>
<tr>
<td></td>
<td>- At least one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one letter and one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one of each: uppercase letter, lowercase letter, digit</td>
</tr>
<tr>
<td></td>
<td>- At least one symbol</td>
</tr>
<tr>
<td></td>
<td>- At least one of each: uppercase letter, lowercase letter, digit, and symbol</td>
</tr>
<tr>
<td>Disallowed Characters</td>
<td>Specify the characters not to be allowed in the password.</td>
</tr>
<tr>
<td>Disallowed Words (CSV)</td>
<td>Specify the words not to be allowed in the password</td>
</tr>
<tr>
<td>Additional Checks</td>
<td>Select any additional checks, if required. The options are:</td>
</tr>
<tr>
<td></td>
<td>- May not contain User ID or its characters in reversed order.</td>
</tr>
<tr>
<td></td>
<td>- May not contain repeated character four or more times consecutively.</td>
</tr>
<tr>
<td>Expiry Days</td>
<td>Set the password expiry time for the local users. The allowed range is <strong>0 to 500</strong> days. The default value is <strong>0</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If the value is set to <strong>0</strong>, 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.</td>
</tr>
</tbody>
</table>

Password Policy settings are effective only for the users created or modified after the changes are saved.

### Disabling Admin User Accounts

The **Disable Account** check occurs every day at midnight. 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.

If the mechanism for logging in to ClearPassPolicy 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 3).
- 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**) and the Event Viewer (see **Event Viewer**).
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 496** *Disable Accounts Dialog*

4. Specify the **Disable Accounts** parameters as described in **Table 3**, then click **Save**.

**Table 3:** *Admin Users > Disable Accounts Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed attempts count</td>
<td>Specify the number of failed log-in attempts are allowed before the account is disabled. The range is from 1 to 100 attempts.</td>
</tr>
<tr>
<td>Reset failed attempts count</td>
<td>To reset the failed attempts count to zero and reenable those admin users who were disabled after exceeding the failed attempts count, click <strong>Reset</strong>.</td>
</tr>
</tbody>
</table>

**Managing Admin Privileges**

ClearPass Policy Manager ships with the following default administrator admin privileges XML files:

**Table 1:** *Default Admin Privileges*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Administrator</td>
<td>An API administrator is only allowed API access to read/write all configuration elements.</td>
</tr>
<tr>
<td>Aruba User Role Download</td>
<td>Privilege level used for Aruba User Role Download API operations.</td>
</tr>
<tr>
<td>Help Desk</td>
<td>The Help Desk person logs in to troubleshoot problems reported by end users.</td>
</tr>
<tr>
<td>Help Desk - ASE</td>
<td>The Help Desk person logs in to troubleshoot problems reported by end users.</td>
</tr>
<tr>
<td>Network Administrator</td>
<td>Allowed to configure all the policies in the ClearPass system.</td>
</tr>
<tr>
<td>Privileged_user</td>
<td>Allowed to add NADs, NAD groups, and edit endpoints along with monitoring operations.</td>
</tr>
<tr>
<td>Read-only Administrator</td>
<td>This administrator is allowed to only read all configuration elements.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Receptionist</td>
<td>The receptionist is allowed access to the main monitoring screens.</td>
</tr>
<tr>
<td>STS-Operations</td>
<td>STS-Operations 7x24 team</td>
</tr>
<tr>
<td>Super Administrator</td>
<td>This administrator is allowed read/write access to all configuration elements.</td>
</tr>
</tbody>
</table>

Each of these default admin privileges define the admin privileges for Policy Manager and ClearPass 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 497 Admin Privileges Page**

   ![Admin Privileges Page](image)

2. Click the Add link.
   
   The Add Admin Privileges dialog opens.
Figure 498  Add Admin Privileges Page: Basic Information Tab

![Add Admin Privileges Page: Basic Information Tab]

3. Specify the parameters in the **Basic Information** tab as described in **Table 27**.

**Table 27: Add Admin Privileges Parameters: Basic Information Tab**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the Admin Privileges administrator.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description of this new admin privileges administrator.</td>
</tr>
<tr>
<td>Access Type</td>
<td>Select one of the following Access Types:</td>
</tr>
<tr>
<td></td>
<td>- Give full access to the Admin</td>
</tr>
<tr>
<td></td>
<td>- Give UI access to the Admin</td>
</tr>
<tr>
<td></td>
<td>- Give API access to the Admin</td>
</tr>
<tr>
<td>Allow Passwords</td>
<td>Select this check box if you want to allow password access.</td>
</tr>
</tbody>
</table>

**Configuring Policy Manager Admin Privileges**

To configure the Policy Manager admin privileges:

1. Select the **Policy Manager** tab.
   
The following dialog opens:
2. Specify the admin privileges for each of the ClearPassPolicy Manager components, then click **Save**.

**Configuring Insight Admin Privileges**

To configure the Insight admin privileges:

1. Select the **Insight** tab.
   
   The following dialog opens:

   ![Specifying Insight Admin Privileges](image)

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
<?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:
```xml
<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:
```xml
<AdminPrivileges>
  <AdminPrivilege name="" description="">
    <AdminTask taskid=""/>
    <AdminTask taskid=""/>
    <AdminTask taskid=""/>
  </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 1: Administrator Privileges and Task IDs

<table>
<thead>
<tr>
<th>Area (ClearPass Policy Manager Menu)</th>
<th>Task ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>dnd</td>
</tr>
<tr>
<td>Monitoring</td>
<td>mon</td>
</tr>
<tr>
<td>Live Monitoring</td>
<td>mon.li</td>
</tr>
<tr>
<td>Access Tracker</td>
<td>mon.li.ad</td>
</tr>
<tr>
<td>Accounting</td>
<td>mon.li.ac</td>
</tr>
<tr>
<td>Onguard Activity</td>
<td>mon.li.ag</td>
</tr>
<tr>
<td>Analysis and Trending</td>
<td>mon.li.sp</td>
</tr>
<tr>
<td>Endpoint Profiles</td>
<td>mon.li.ep</td>
</tr>
<tr>
<td>System Monitor</td>
<td>mon.li.sy</td>
</tr>
<tr>
<td>Audit Viewer</td>
<td>mon.av</td>
</tr>
<tr>
<td>Blacklisted Users</td>
<td>mon.bl</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>mon.ev</td>
</tr>
<tr>
<td>Data Filters</td>
<td>mon.df</td>
</tr>
<tr>
<td>Configuration</td>
<td>con</td>
</tr>
<tr>
<td>Start Here (Services Wizard)</td>
<td>con.sh</td>
</tr>
<tr>
<td>Services</td>
<td>con.se</td>
</tr>
<tr>
<td>Service Templates</td>
<td>con.st</td>
</tr>
<tr>
<td>Authentication</td>
<td>con.au</td>
</tr>
<tr>
<td>Methods</td>
<td>con.au.am</td>
</tr>
<tr>
<td>Sources</td>
<td>con.au.as</td>
</tr>
<tr>
<td>Identity</td>
<td>con.id</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>con.id.sso</td>
</tr>
<tr>
<td>Local Users</td>
<td>con.id.lu</td>
</tr>
<tr>
<td>Endpoints</td>
<td>con.id.ep</td>
</tr>
<tr>
<td>Static Host Lists</td>
<td>con.id.sh</td>
</tr>
<tr>
<td>Roles</td>
<td>con.id.rs</td>
</tr>
<tr>
<td>Role Mappings</td>
<td>con.id.rm</td>
</tr>
<tr>
<td>Area (ClearPass Policy Manager Menu)</td>
<td>Task ID</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Posture</td>
<td></td>
</tr>
<tr>
<td>- Posture Policies</td>
<td>con.pv</td>
</tr>
<tr>
<td>- Posture Servers</td>
<td>con.pv.ex</td>
</tr>
<tr>
<td>- Audit Servers</td>
<td>con.pv.au</td>
</tr>
<tr>
<td>Enforcements</td>
<td></td>
</tr>
<tr>
<td>- Policies</td>
<td>con.en.epo</td>
</tr>
<tr>
<td>- Profiles</td>
<td>con.en.epr</td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>- Devices</td>
<td>con.nw.nd</td>
</tr>
<tr>
<td>- Device Groups</td>
<td>con.nw.ng</td>
</tr>
<tr>
<td>- Proxy Targets</td>
<td>con.nw.pr</td>
</tr>
<tr>
<td>Policy Simulation</td>
<td>con.ps</td>
</tr>
<tr>
<td>Profile Settings</td>
<td>con.prs</td>
</tr>
<tr>
<td>Administration</td>
<td>adm</td>
</tr>
<tr>
<td>User and Privileges</td>
<td>adm.us</td>
</tr>
<tr>
<td>- ClearPass Portal</td>
<td>adm.po.cp</td>
</tr>
<tr>
<td>- Admin Users</td>
<td>adm.us.au</td>
</tr>
<tr>
<td>- Admin Privileges</td>
<td>adm.us.ap</td>
</tr>
<tr>
<td>Server Manager</td>
<td>adm.mg</td>
</tr>
<tr>
<td>- Server Configuration</td>
<td>adm.mg.sc</td>
</tr>
<tr>
<td>- Log Configuration</td>
<td>adm.mg.ls</td>
</tr>
<tr>
<td>- Local Shared Folders</td>
<td>adm.mg.sf</td>
</tr>
<tr>
<td>- Licensing</td>
<td>adm.mg.li</td>
</tr>
<tr>
<td>External Servers</td>
<td>adm.xs</td>
</tr>
<tr>
<td>- SNMP Trap Receivers</td>
<td>adm.xs.st</td>
</tr>
<tr>
<td>- Syslog Targets</td>
<td>adm.xs.es</td>
</tr>
<tr>
<td>- Syslog Export Filters</td>
<td>adm.xs.sx</td>
</tr>
<tr>
<td>- Messaging Setup</td>
<td>adm.xs.me</td>
</tr>
</tbody>
</table>
## Area (ClearPass Policy Manager Menu) | Task ID
--- | ---
- 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
- 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
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0"
<TipsReader 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
<?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
<?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 Manager

This section provides the following information:

- Server Configuration Operations
- Log Configuration
- Downloading Local Shared Folders
- License Management

Server Configuration Operations

You can perform numerous server configuration tasks by navigating to Administration > Server Manager > Server Configuration.

Figure 501 Server Configuration Page

This section describes the following server configuration tasks:

- Configuring the ClearPass Policy Manager Server on page 496
- Cluster-Wide Parameters on page 543
- Synchronizing the Cluster Date and Time with the NTP Server on page 556
- Changing the Cluster-Wide Password on page 559
- Managing Policy Manager Zones on page 560
- Configuring NetEvents Targets on page 562
- Configuring Virtual IP Settings on page 564
- Clearing Machine Authentication Cache on page 563
- Making a Subscriber Node on page 565
- Collecting Logs on page 567
- Backing Up the Policy Manager Database on page 568
- Restoring Policy Manager Configuration Data on page 569
- Performing a System Cleanup
- Shutting Down or Rebooting the Server on page 572

Configuring the ClearPass Policy Manager Server

This section provides the following information:

- ClearPass Server Configuration Tabs
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 502  Server Configuration Page**

2. Click the ClearPass server name of interest.

   The Server Configuration page for the selected server opens:

   **Figure 503  Server Configuration Page for the Selected Server**
ClearPass Server Configuration Tabs
For details on viewing or modifying ClearPass server configuration settings, refer to the following sections:
- System Page on page 500
- Services Control Page on page 510
- Service Parameters Page on page 510
- System Monitoring Page on page 527
- Network Page on page 528
- FIPS Page on page 541

Cluster Configuration Options
For details on the cluster configuration options, see ClearPass Cluster Configuration Options.
- Changing the Cluster Password
- Promoting a ClearPass Subscriber Node to Publisher
- Joining a ClearPass Server Back to the Cluster
For more information, see Server Configuration Operations on page 496.

Changing the Cluster Password
Use the Change 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 Change Cluster Password dialog:
Figure 504 Change Cluster Password Dialog

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:
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.

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.

2. Click the **Join server back to cluster** link.

   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:
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 508  Join Server Back to Cluster Progress Window**

4. For a failed Publisher node, the following message will be displayed in the Dashboard page:

**Figure 509  Publisher Warning Message**

### System Page

- [Management Port Configuration](#)
- [Data/External Port Configuration](#)
- [DNS Settings Configuration](#)
- [Join AD Domain Configuration](#)
- [Adding a Password Server](#)

To configure the Server Configuration > System page parameters:

1. Navigate to Administration > Server Manager > Server Configuration.
2. Select the ClearPass server of interest.
The **Server Configuration** page opens onto the **System** page (see Figure 510).

**Figure 510  Server Configuration > System Page**

![Figure 510](image)

3. Specify the **Server Configuration > System** page parameters as described in the following table, then click **Save**:

**Table 1: Server Configuration > System Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Specify the host name of the Policy Manager server.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> You do not need to enter the fully qualified domain name in this field.</td>
<td></td>
</tr>
<tr>
<td>FQDN</td>
<td>Enter the Fully-Qualified Domain Name (FQDN) of the Policy Manager server.</td>
</tr>
<tr>
<td>Policy Manager Zone</td>
<td>To specify a Policy Manager zone, select a previously configured zone from the drop-down list, then click the Manage Policy Manager Zones link. If you need to add a Policy Manager zone, click the Manage Policy Manager Zones link. For more information on adding zones, see Adding Policy Manager Zones.</td>
</tr>
<tr>
<td>Enable Performance Monitoring Display</td>
<td>To enable the ClearPass Policy Manager server to perform performance monitoring, select the Enable this server for performance monitoring display check box.</td>
</tr>
<tr>
<td>Insight Setting</td>
<td>To enable the Insight reporting tool on this node, select the Enable Insight check box.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>- 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 ClearPass server.</td>
</tr>
<tr>
<td></td>
<td>- When this check box is enabled for other servers in the cluster, they are added as backups for the same authentication source.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>Enable as Insight Master</td>
<td>To specify the current server in the cluster as an Insight Master, select this check box.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is available only when Insight Setting &gt; Enable Insight is enabled.</td>
<td></td>
</tr>
<tr>
<td>Enable Ingress Events Processing</td>
<td>Check this check box to enable ingress events processing on this server. For more information, see Enabling Ingress Events Processing.</td>
</tr>
</tbody>
</table>
| Master Server in Zone                  | Use this option to specify the current ClearPass server as the Primary or Secondary master ClearPass server within a Policy Manager zone. **NOTE:** If no Primary master server for a zone is configured, the ClearPass server
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Primary master ClearPass server in the zone distributes the scan requests to all the nodes in the zone, depending on the number of seed devices (Network Discovery) or the number of networks/subnets (for Subnet Scans) configured.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If the Primary master server goes down, the Secondary master server assumes the role of the Primary master server.</td>
</tr>
<tr>
<td></td>
<td>Each scan configuration that is added is distributed by the Master ClearPass server to a different node in the zone.</td>
</tr>
<tr>
<td></td>
<td>If one scan configuration has multiple seed devices (Network Discovery), scan requests are distributed to other nodes in the zone based on the number of ARP entries received from the seed devices.</td>
</tr>
<tr>
<td></td>
<td>If one scan configuration has multiple subnets configured (Subnet Scan), scan requests are distributed to other nodes in the zone.</td>
</tr>
</tbody>
</table>

**Span Port**

If necessary, select a port for DHCP spanning. On selecting a port, the **Enable TCP/ARP Fingerprinting** check box appears. This field is optional.

**Management Port**

To configure the Management Port parameters, click **Configure**. The **Configure Management Port** dialog opens. For details, see Management Port Configuration.

**Data/External Port**

To configure the Data/External port, click **Configure**. For details, see Data/External Port Configuration.

**DNS Settings**

To configure the DNS settings, click **Configure**. For details, see DNS Settings Configuration.

**AD Domains**

Displays a list of the joined Active Directory domains. To join an active directory domain, click **Join Domain**. For details on joining an AD domain, see Join AD Domain Configuration on page 1.

**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.
2. Specify the **Configure Management Port** parameters for IPv4 as described in the following table:

**Table 2: Configure Management Port Parameters (IPv4)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select IP Version</td>
<td>Select <strong>IPv4</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specify the IPv4 address that is used to access the ClearPass Policy Manager server’s management port.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the management interface subnet mask for an IPv4 address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Specify the default gateway for the management interface. A default gateway serves as an access point or IP router that a networked device uses to send information to a device in another network or the Internet.</td>
</tr>
</tbody>
</table>

**Table 3: Configure Management Port Parameters (IPv4)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select IP Version</td>
<td>Select <strong>IPv4</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specify the IPv4 address that is used to access the ClearPass Policy Manager server’s management port.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the management interface subnet mask for an IPv4 address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Specify the default gateway for the management interface. A default gateway serves as an access point or IP router that a networked device uses to send information to a device in another network or the Internet.</td>
</tr>
</tbody>
</table>

3. Click **Update**.
Figure 512 Configure Management Port Dialog (IPv6)

4. Specify the **Configure Management Port** parameters for IPv6 as described in the following table:

**Table 4: Configure Management Port Parameters (IPv6)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address/Mask</td>
<td>Specify the IPv6 address that is used to access the ClearPass Policy Manager server’s management port. To configure the IPv6 address, specify the IPv6 address with prefix length: <code>&lt;ipv6address&gt;prefixlength</code></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> IPv6 addresses don’t require a netmask as they use Classless Inter-Domain Routing (CIDR).</td>
</tr>
<tr>
<td>IPv6 Default Gateway</td>
<td>Specify the default gateway for the management interface.</td>
</tr>
<tr>
<td></td>
<td>A default gateway serves as an access point or IP router that a networked device uses to send information to a device in another network or the Internet.</td>
</tr>
</tbody>
</table>

**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 513 Configure Data/External Port Dialog (IPv4)

2. Specify the **Configure Data/External Port** parameters for IPv4 as described in the following table:
Table 5: Configure Data/External Port Parameters (IPv4)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select IP Version</td>
<td>Select IPv4.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specify the IPv4 address of the ClearPass server's data interface.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the management interface subnet mask for an IPv4 address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Specify the IPv4 address of the default gateway for the data interface.</td>
</tr>
</tbody>
</table>

3. Click Update.

Figure 514 Configure Data/External Port Dialog (IPv6)

![Configure Data/External Port Dialog (IPv6)](image)

4. Specify the Configure Data/External Port parameters for IPv6 as described in the following table:

Table 6: Configure Data/External Port Parameters (IPv6)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address/Mask</td>
<td>Specify the IPv6 address that is used to access the ClearPass Policy Manager server's data port. To configure the IPv6 address, specify the IPv6address with prefix length: <code>&lt;ipv6address&gt;prefixlength&gt;</code></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> IPv6 addresses don't require a netmask as they use Classless Inter-Domain Routing (CIDR).</td>
</tr>
<tr>
<td>IPv6 Default Gateway</td>
<td>Specify the default gateway for the data/external interface. A default gateway serves as an access point or IP router that a networked device uses to send information to a device in another network or the Internet.</td>
</tr>
</tbody>
</table>

DNS Settings Configuration

To configure the ClearPass server's DNS (Domain Name System) settings:

1. From the **Server Configuration** page > **System** tab > **DNS Settings**, click **Configure**. The **Configure DNS Setting** dialog opens.
2. Specify the **Configure DNS Settings** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Specify the primary DNS server for name look-up. You can specify an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Specify one or more secondary DNS servers for name look-up. You can specify an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>Tertiary</td>
<td>Optionally, in the rare event of both the primary and secondary DNS servers going down, you can configure a tertiary DNS server. You can specify an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The recommended practice is to configure the primary and secondary DNS servers on separate machines, on separate Internet connections, and in separate geographic locations.</td>
</tr>
<tr>
<td>DNS Caching</td>
<td>If enabled, ClearPass Policy Manager will cache DNS entries from the DNS server for the Time to live (TTL) value for each entry, reducing the number of queries to the DNS server. This feature is disabled by default.</td>
</tr>
</tbody>
</table>

3. Click **Update**.

**Join AD Domain Configuration**

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 is not required 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 [Add Password Server](#).
- **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.

For most use cases, if you have multiple nodes in the cluster, you must join each node to the same Active Directory domain.

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 516 Join AD Domain Dialog**

   ![Join AD Domain Dialog](image)

2. Specify the **Join AD Domain** parameters as described in the following table.

   **Table 8: Join AD Domain Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller</td>
<td>Enter the Fully Qualified Domain Name (FQDN) of the domain controller, then press Tab. The following message is displayed: <em>Trying to determine the NetBIOS name...</em> ClearPass searches for the NetBIOS name for the domain.</td>
</tr>
<tr>
<td>NetBIOS name (optional)</td>
<td>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. <strong>NOTE</strong>: 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 <strong>Leave Domain</strong> button (which replaces the <strong>Join Domain</strong> button once you join the domain). After leaving the domain, join again with the correct NetBIOS name.</td>
</tr>
<tr>
<td>Domain Controller name conflict</td>
<td>Specify the action to take in the event of a domain controller name conflict.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Use specified Domain Controller</strong>: Continue to use the domain controller name that you entered.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Use Domain Controller returned by DNS query</strong>: Use the domain controller name returned by the DNS query.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Fail on conflict</strong>: Abort the Join Domain operation.</td>
</tr>
<tr>
<td>Use default domain admin user</td>
<td>Check this box to use the Administrator user name to join the domain.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: 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 Admin username and password in the fields provided.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user ID of the domain administrator account.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: This field is disabled if the Use default domain admin user check box is selected.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the user account that will join ClearPass with the domain (for related information, see Table 9, which displays the characters that are allowed and not allowed for the Active Directory username and password).</td>
</tr>
</tbody>
</table>

**Table 9: Active Directory Username and Password Characters Allowed and Not Allowed**

<table>
<thead>
<tr>
<th>Field</th>
<th>Characters Allowed</th>
<th>Not Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>~ ! @ # $ % ^ _ - + = { } , . &quot; /</td>
<td>` &amp; ( )</td>
</tr>
<tr>
<td>Password</td>
<td>~ ! @ # $ % ^ _ - + = { } , . &quot; /</td>
<td>~ ` [ ] \ ; :</td>
</tr>
</tbody>
</table>

3. **Click** **Save**.
   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 set up as a password server (as described in the next section).

**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.
When an Active Directory password server is updated in the domain server configuration, the RADIUS service is automatically restarted.

To add an Active Directory password server:

1. Navigate to Administration > Server Manager > Server Configuration, then select the ClearPass server of interest.

2. In the AD Domains section of the System page, click the Add Password Server icon: ![Add Password Server Icon](image). This icon appears only after ClearPass joins at least one Active Directory domain (see Figure 517).

**Figure 517  Add Active Directory Password Server Icon**

![Active Directory Password Server Added](image)

The Configure AD Password Servers dialog opens.

**Figure 518  Active Directory Password Server Added**

3. Specify the following:
   - Domain controller
   - NetBIOS name
   - Password server(s)

   You can specify Active Directory password servers with a hostname or an IP address. Use a new line for each entry.

4. To complete adding the Active Directory password servers, click **Save**.
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.

To access the Services Control page:

1. Navigate to Administration > Server Manager > Server Configuration.
   - From the Server Configuration page, select the desired ClearPass server.
2. Click the Services Control tab.
   - The Services Control page opens.

Figure 519 Services Control Page

3. To start a stopped service, click the Start button; to stop a running service, click the Stop button.

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 511
- ClearPass IPsec Service
- ClearPass Network Services Options on page 513
- ClearPass System Services Options on page 516
- Ingress Logger Service Ports
- Policy Server Options on page 519
- RADIUS Server Options
- Stats Collection Service Options on page 524
Async Network Services Options

To configure the parameters for the Async network service:

1. Navigate to the Administration > Server Manager > Server Configuration.
2. Select the ClearPass server.
3. From the Server Configuration page, select the Service Parameters tab.
   
   The Service Parameters > Async network services dialog opens by default:

   Figure 521 Configuring Async Network Services

4. Specify the Service Parameters > Async Network Services parameters as described in Table 1

Table 1: Service Parameters > Async Network Services Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ingress Event</strong></td>
<td></td>
</tr>
<tr>
<td>Batch Processing Interval</td>
<td>Specify the Batch ProcessingInterval for ingress event processing. The default interval is 30 seconds. The range of values is 10 to 300 seconds. <strong>NOTE</strong>: For changes to the Batch Processing Interval to take effect, you must restart the Async Network service.</td>
</tr>
<tr>
<td>Command Control</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CoA Delay</td>
<td>Set the CoA Delay value (in seconds). The default value is 2, and the allowed values are from 0 to 15 seconds.</td>
</tr>
<tr>
<td>Enable SNMP Bounce Action</td>
<td>Set the Enable SNMP Bounce Action value. The default value is FALSE.</td>
</tr>
<tr>
<td>Post Auth</td>
<td></td>
</tr>
<tr>
<td>Number of request processing threads</td>
<td>Set the number of request processing threads. The default value is 20 threads, and the range of values is between 20 and 100.</td>
</tr>
<tr>
<td>Lazy handler polling frequency</td>
<td>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.</td>
</tr>
<tr>
<td>Eager handler polling frequency</td>
<td>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.</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>Set the connection timeout in seconds. The default value is 10, and the range is from 1 to 3600 (one hour).</td>
</tr>
<tr>
<td>Palo Alto User Identification Timeout</td>
<td>Specify the Palo Alto endpoint context server user identification timeout in minutes. The default value is 45; the range is from 1 to 3600.</td>
</tr>
</tbody>
</table>

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) 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:
4. Specify the **Service Parameters > ClearPass IPsec Service** parameters as described in **Table 1**, then click **Save**.

**Table 1: Service Parameters > ClearPass IPsec Service Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCSP URI</td>
<td>In the <strong>Parameter Value</strong> field, specify the HTTP or HTTPS URI (uniform resource</td>
</tr>
<tr>
<td></td>
<td>identifier) for the Online Certificate Status Protocol (OCSP). OCSP enables the</td>
</tr>
<tr>
<td></td>
<td>ClearPass server to determine the revocation state of a certificate presented by</td>
</tr>
<tr>
<td></td>
<td>a peer—for example a network device requesting an IPsec connection to the ClearPass</td>
</tr>
<tr>
<td></td>
<td>server. <strong>NOTE:</strong> When you enter the OCSP URI, ClearPass checks that 1) the URI is</td>
</tr>
<tr>
<td></td>
<td>in the proper format (it must start with HTTP or HTTPS and be syntactically correct),</td>
</tr>
<tr>
<td></td>
<td>and 2) ClearPass checks to see if the specified OCSP server IP address or host name is</td>
</tr>
<tr>
<td></td>
<td>reachable from the ClearPass node. A descriptive error message will be displayed</td>
</tr>
<tr>
<td></td>
<td>in the event of an incorrect OCSP URI.</td>
</tr>
<tr>
<td>Strict CRL Policy</td>
<td>You can enable or disable a strict Certificate Revocation List (CRL) policy. This</td>
</tr>
<tr>
<td></td>
<td>parameter is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>To enable <strong>Strict CRL Policy</strong>, select <strong>Yes</strong> from the <strong>Parameter Value</strong> drop-down.</td>
</tr>
<tr>
<td></td>
<td>When this option is enabled, a fresh Certificate Revocation List must be available in</td>
</tr>
<tr>
<td></td>
<td>order for a peer connection to succeed.</td>
</tr>
<tr>
<td></td>
<td>Whenever <strong>Strict CRL Policy</strong> is modified, existing IPsec tunnels that use Public Key</td>
</tr>
<tr>
<td></td>
<td>Authentication are brought down and then brought up again.</td>
</tr>
</tbody>
</table>

**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

To configure the parameters for ClearPass Network Services:

1. Navigate to the **Administration > Server Manager > Server Configuration**, then select the ClearPass server.
2. From the **Server Configuration** page, select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **ClearPass network services**.

   The **Service Parameters > ClearPass network services** dialog opens:
4. Specify the **ClearPass Network Services** parameters as described in the following table:

**Table 1: Service Parameters > ClearPass Network Services**

<table>
<thead>
<tr>
<th>Service Parameters</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SnmpService</strong></td>
<td></td>
</tr>
<tr>
<td>SNMP Timeout</td>
<td>Specify the seconds to wait for an SNMP response from the network device.</td>
</tr>
<tr>
<td>SNMP Retries</td>
<td>Specify the number of retries for SNMP requests.</td>
</tr>
<tr>
<td>LinkUp Timeout</td>
<td>Specify the seconds to wait before processing link-up traps.</td>
</tr>
<tr>
<td></td>
<td>If a MAC notification trap arrives in this time, the SNMP service does not try to</td>
</tr>
<tr>
<td></td>
<td>poll the switch for MAC addresses behind a port for link-up processing.</td>
</tr>
<tr>
<td>IP Address Cache Timeout</td>
<td>Specify the duration in seconds for which MAC-to-IP lookup response is cached.</td>
</tr>
<tr>
<td>Uplink Port Detection</td>
<td>Specify the limit for the number of MAC addresses found behind a port after which</td>
</tr>
<tr>
<td>Threshold</td>
<td>the port is considered an uplink port and not considered for SNMP lookup and</td>
</tr>
<tr>
<td></td>
<td>enforcement. The default value is <strong>5</strong>, with a range from <strong>0</strong> to <strong>20</strong>.</td>
</tr>
<tr>
<td>Service Parameters</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMP v2c Trap Community</td>
<td>Specify the community string that must be checked in all incoming SNMP v2 traps.</td>
</tr>
<tr>
<td>SNMP v3 Trap Username</td>
<td>Specify the SNMP v3 Username to be used for all incoming traps.</td>
</tr>
<tr>
<td>SNMP v3 Trap Authentication Protocol</td>
<td>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 in FIPS mode.</td>
</tr>
<tr>
<td>SNMP v3 Trap Privacy Protocol</td>
<td>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 in FIPS mode.</td>
</tr>
<tr>
<td>SNMP v3 Trap Authentication Key</td>
<td>Specify the SNMP v3 authentication key and privacy key for incoming traps.</td>
</tr>
<tr>
<td>SNMP v3 Trap Privacy Key</td>
<td></td>
</tr>
<tr>
<td>Device Info Poll Interval</td>
<td>Specify the time (in minutes) between polling for device information.</td>
</tr>
<tr>
<td><strong>Certificate Auth</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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. |
<p>| <strong>PostureService</strong>                |                                                                                                                                                   |
| 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.                  |</p>
<table>
<thead>
<tr>
<th>Service Parameters</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DhcpSnooper</strong></td>
<td></td>
</tr>
<tr>
<td>MAC to IP Request Hold time</td>
<td>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.</td>
</tr>
<tr>
<td>DHCP Request Probation Time</td>
<td>Specify the number of seconds to wait before considering the MAC-to-IP binding received in a DHCP REQUEST 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.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**ClearPass System Services Options**

You can use the ClearPass System Services parameters for PHP (Hypertext Preprocessor) 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.

To configure ClearPass System Services:

1. Navigate to the **Administration > Server Manager > Server Configuration**, then select the ClearPass server.
2. From the **Server Configuration** page, select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **ClearPass system services**.

   The following dialog opens:
4. Specify the **Service Parameters > ClearPass System Services** parameters as described in the following table.

**Table 1: Service Parameters > ClearPass System Services**

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PHP System Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Memory Limit</td>
<td>Specify the maximum memory that can be used by the PHP (Hypertext Preprocessor) applications.</td>
</tr>
<tr>
<td>Form POST Size</td>
<td>Specify the maximum HTTP POST content size that can be sent to the PHP application.</td>
</tr>
<tr>
<td>File Upload Size</td>
<td>Specify the maximum file size that can be uploaded into the PHP application.</td>
</tr>
<tr>
<td>Input Time</td>
<td>Specify the time limit after which the ClearPass server will detect no activity from the user and will take some action.</td>
</tr>
<tr>
<td>Socket Timeout</td>
<td>Specify the maximum time for any socket connections.</td>
</tr>
<tr>
<td>Enable zlib output compression</td>
<td>Specify the setting to compress the output files.</td>
</tr>
<tr>
<td>Service Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include PHP header in web server response</td>
<td>Specify the setting to include PHP header in the HTTP responses.</td>
</tr>
<tr>
<td><strong>TCP Keep Alive Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>Specify a value in seconds from 10 to 86400.</td>
</tr>
<tr>
<td>Keep Alive Interval</td>
<td>Specify a value in seconds from 1 to 3600.</td>
</tr>
<tr>
<td>Keep Alive Probes</td>
<td>Specify a value from 1 to 100 for the number of probes.</td>
</tr>
<tr>
<td><strong>Database Configurations</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum connections</td>
<td>Specify a number between 300 and 2000 for a maximum number of allowed connections.</td>
</tr>
<tr>
<td><strong>Extensions</strong></td>
<td></td>
</tr>
<tr>
<td>Extensions Network Address</td>
<td>You can use the Extensions Network Address parameter to configure the adapter</td>
</tr>
<tr>
<td></td>
<td>interface and change the subnet used for the Extension.</td>
</tr>
<tr>
<td></td>
<td>Specify the bridge IP address used for internal networking with local extensions.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Default</strong>: 172.17.0.1/16</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Format</strong>: IPv4_ADDR/PREFIX_LEN</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Validation</strong>: A valid, non-routable IPv4 address must be supplied. The IPv4</td>
</tr>
<tr>
<td></td>
<td>address must match 10.0.0.0/8, 192.168.0.0/16, or 172.16.0.0/12.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Prefix Length</strong>: A valid prefix length must be supplied: &gt;= 16 and &lt;= 29</td>
</tr>
<tr>
<td><strong>HTTP Proxy</strong></td>
<td></td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specify the hostname or IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: ClearPass Policy Manager supports IPv6 HTTP-proxy addresses for sending</td>
</tr>
<tr>
<td></td>
<td>data to third-party context servers.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port at which the proxy server listens for HTTP traffic.</td>
</tr>
<tr>
<td>Username</td>
<td>Specify the user name to authenticate with the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password to authenticate with the proxy server.</td>
</tr>
<tr>
<td><strong>Web Server Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Timeout</td>
<td>Specify a server timeout value in seconds from 1 to 60.</td>
</tr>
<tr>
<td>Keep Alive</td>
<td>To enable or disable keep-alive for the web server, select <strong>TRUE</strong> or <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>Request Wait</td>
<td>Specify the request wait time in seconds from 1 to 60. The default value is <strong>4</strong></td>
</tr>
<tr>
<td>Enable Host Header check</td>
<td>Specify whether to enable the host header check. The default value is <strong>TRUE</strong>.</td>
</tr>
<tr>
<td>Service Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>- When you set this value to TRUE, the <strong>Host Header Restriction check</strong> is enabled and only the allowed or whitelisted host headers are allowed.</td>
</tr>
<tr>
<td></td>
<td>- When you set this value to FALSE, irrespective of Host Headers in the http packet, ClearPass Policy Manager redirects to https://&lt;ClearPass-server&gt;/tips.</td>
</tr>
<tr>
<td>WhiteList Host Names</td>
<td>When the <strong>Enable Host Header check</strong> 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.</td>
</tr>
<tr>
<td>Maximum Clients</td>
<td>Specify a value from 10 to 20000 for the maximum number of clients allowed.</td>
</tr>
<tr>
<td>Maximum Requests</td>
<td>Specify a number between 0 and 3000 for the maximum number of requests allowed. The default value is 500.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**Ingress Logger Service Ports**

When Ingress Event Processing is enabled and configured on ClearPass (see **Enabling Ingress Events Processing**), 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 525 Ingress Logger Service Dialog**

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**

To configure the Policy Server service:

1. Navigate to the **Administration > Server Manager > Server Configuration**, then select the ClearPass server.
2. From the **Server Configuration** page, select the **Service Parameters** tab.
3. From the Select Service drop-down, select Policy server. The following dialog opens:

**Figure 526  Policy Server Service Parameters**

4. Specify the Service Parameters > Policy Server parameters as described in the following table.

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Authentication Cache Timeout</td>
<td>Specify the time (in hours) for which machine authentication entries are cached by ClearPass Policy Manager. The default is <strong>24 hours</strong>.</td>
</tr>
<tr>
<td>LDAP Primary Retry Interval</td>
<td>After a primary LDAP server is down, the ClearPass server connects to one of the backup servers. Specify how long the ClearPass server waits (in seconds) before it tries to connect to the primary server again.</td>
</tr>
<tr>
<td>Audit SPT Default Timeout</td>
<td>Specify the time (in seconds) for which an Audit success or error response is cached in the Policy server.</td>
</tr>
<tr>
<td>Additional time before session deletion from multi-master cache</td>
<td>Specify the number of seconds the Policy server will wait before deleting the multi-master entry. The default value is <strong>0</strong>. This parameter handles roaming scenarios where an Accounting-Start occurs without an authentication request. If the value for this parameter is <strong>0</strong>, 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.</td>
</tr>
<tr>
<td>Number of request processing threads</td>
<td>Specify the maximum number of threads used to process requests.</td>
</tr>
<tr>
<td>HTTP Thread Pool Size</td>
<td>Specify the number of threads allotted for the HTTP thread pool.</td>
</tr>
<tr>
<td>Authentication Thread Pool Size</td>
<td>Specify the number of threads to use for LDAP/Active Directory and SQL connections.</td>
</tr>
</tbody>
</table>

**RADIUS Server Options**

To configure the RADIUS server service:

1. Navigate to the **Administration > Server Manager > Server Configuration**, then select the ClearPass server.
2. From the **Server Configuration** page, select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **Radius server**.

The following dialog opens:

**Figure 527 RADIUS Server Parameters Dialog**

![RADIUS Server Parameters Dialog](image)

Specify the **Service Parameters > RADIUS server** parameters as described in the following table:

**Table 1: Service Parameters > RADIUS Server Service**

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EAP-FAST</strong></td>
<td></td>
</tr>
<tr>
<td>Master Key Expire Time</td>
<td>Specify the lifetime of a generated EAP-FAST master key.</td>
</tr>
<tr>
<td>Master Key Grace Time</td>
<td>Specify the grace period for an EAP-FAST master key after its lifetime expires.</td>
</tr>
<tr>
<td></td>
<td><strong>The default is 3 weeks.</strong></td>
</tr>
<tr>
<td></td>
<td>If a client presents a PAC (Protected Access Credential) that is encrypted using</td>
</tr>
<tr>
<td></td>
<td>the master key in this period after its TTL (Time-to-Live), it is accepted and a</td>
</tr>
<tr>
<td></td>
<td>new PAC encrypted with the latest master key is provisioned on the client.</td>
</tr>
<tr>
<td>PACs are valid across cluster</td>
<td>If PACs (Protected Access Credentials) generated by this server are valid across</td>
</tr>
<tr>
<td></td>
<td>the cluster, set to <strong>TRUE</strong> (the default setting).</td>
</tr>
<tr>
<td></td>
<td>If not, select <strong>FALSE</strong>.</td>
</tr>
<tr>
<td><strong>Proxy</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum Response Delay</td>
<td>If the target server has not responded, specify the time delay before retrying a</td>
</tr>
<tr>
<td></td>
<td>proxy request. <strong>The default is 5 seconds.</strong></td>
</tr>
<tr>
<td>Maximum Reactivation Time</td>
<td>Specify the time to elapse before retrying a dead proxy server.</td>
</tr>
<tr>
<td><strong>Service Parameter</strong></td>
<td><strong>Action/Description</strong></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Retry Counts</td>
<td>If the target server doesn't respond, specify the maximum number of times to retry a proxy request.</td>
</tr>
<tr>
<td><strong>Accounting</strong></td>
<td></td>
</tr>
<tr>
<td>Log Accounting Interim-Update Packets</td>
<td>To store the Interim-Update packets in session logs, select <strong>TRUE</strong>. <strong>FALSE</strong> is the default setting.</td>
</tr>
<tr>
<td><strong>Thread Pool</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of Threads</td>
<td>Specify the maximum number of threads in the RADIUS server thread pool to process requests.</td>
</tr>
<tr>
<td>Number of Initial Threads</td>
<td>Specify the initial number of threads in the RADIUS server thread pool to process requests.</td>
</tr>
<tr>
<td><strong>Active Directory Errors</strong></td>
<td></td>
</tr>
<tr>
<td>Window Size</td>
<td>Enter a duration during which Active Directory errors are accumulated for possible action. The default is <strong>5 minutes</strong>.</td>
</tr>
<tr>
<td>Number of Errors</td>
<td>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 <strong>150</strong>.</td>
</tr>
</tbody>
</table>
| Recovery Action                             | Select one of the following recovery actions from the drop-down list:  
  - **None**: To not initiate a self-recovery action. This is the default.  
  - **Exit**: To restart the RADIUS server. (The monitoring daemon restarts 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.                                                                                                           |
<p>| <strong>Main</strong>                                     |                                                                                                                                                                                                                                                                                                                                                     |
| Authentication Port                         | Specify the ports on which the RADIUS server listens for authentication requests. Default values are ports <strong>1645</strong> and <strong>1812</strong>. <strong>NOTE</strong>: You can configure the Authentication Port to different values if desired.                                                                                                               |
| Accounting Port                             | Specify the ports on which the RADIUS server listens for accounting requests. The default values are <strong>1646</strong> and <strong>1813</strong>.                                                                                                                                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> You can configure the Accounting Port to different values if desired.</td>
<td></td>
</tr>
<tr>
<td>Maximum Request Time</td>
<td>Specify the maximum time (in seconds) allowed for processing a request after which it is considered timed out. The default is 30 seconds.</td>
</tr>
<tr>
<td>Cleanup Time</td>
<td>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.</td>
</tr>
<tr>
<td>Local DB Authentication Source Connection Count</td>
<td>Specify the maximum number of Local DB connections opened.</td>
</tr>
<tr>
<td>AD/LDAP Authentication Source Connection Count</td>
<td>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.</td>
</tr>
<tr>
<td>SQL DB Authentication Source Connection Count</td>
<td>Specify the maximum number of SQL DB.</td>
</tr>
<tr>
<td>Kerberos Authentication Source Connection Count</td>
<td>Specify the maximum number of Kerberos connections opened.</td>
</tr>
<tr>
<td>EAP-TLS Fragment Size</td>
<td>Specify the maximum allowed size (in bytes) for the EAP-TLS fragment.</td>
</tr>
<tr>
<td>Use Inner Identity in Access-Accept Reply</td>
<td>To use the inner identity in the Access-Accept replies, select <strong>TRUE</strong>. The default setting is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>Reject if OCSP response does not have Nonce</td>
<td>To reject an OCSP response without a nonce, select <strong>TRUE</strong>. Else, select <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>Include Nonce in OCSP request</td>
<td>Specify one of the following:</td>
</tr>
<tr>
<td>- <strong>TRUE</strong>: Select if the OCSP (Online Certificate Status Protocol) request should include the nonce. This is the default value.</td>
<td></td>
</tr>
<tr>
<td>- <strong>FALSE</strong>: To avoid the EAP-TLS authentication failure, select if the OCSP server does not support the nonce.</td>
<td></td>
</tr>
<tr>
<td>Enable signing for OCSP Request</td>
<td>To enable signing for OCSP request, select <strong>TRUE</strong>. This determines whether ClearPass should sign an OCSP request with a RADIUS/EAP server certificate. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>Check the validity of all certificates in the chain against CRLs</td>
<td>To check the validity of all certificates in the chain against Certificate Revocation Lists (CRLs), select <strong>TRUE</strong>. Else, select <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>ECDH Curve</td>
<td>Select one of the following ECDH curve (Elliptic Curve Diffie-Helman) options from the drop-down list:</td>
</tr>
<tr>
<td>- X9.62/SECG curve over a 256-bit prime field</td>
<td></td>
</tr>
<tr>
<td>- NIST/SECG curve over a 384-bit prime field</td>
<td></td>
</tr>
<tr>
<td>Service Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable TLS 1.2</td>
<td>To disable Transport Layer Security 1.2 (TLS 1.2), select <strong>TRUE</strong>. <strong>FALSE</strong> is the default setting—TLS 1.2 is enabled by default.</td>
</tr>
<tr>
<td>Check the validity of intermediary certificates in the chain using OCSP</td>
<td>To check the validity of intermediary certificates in the chain using OCSP (Online Certificate Status Protocol), select <strong>TRUE</strong>. The default setting is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>Maximum Number of AD Authentication Processes</td>
<td>To specify the maximum number of Active Directory authentication processes, enter a number between <strong>1</strong> and <strong>5</strong>. The default is <strong>1</strong>.</td>
</tr>
<tr>
<td>Verify OCSP Signing Purpose</td>
<td>Specify one of the following:&lt;br&gt;  ■ When the value for this parameter is set to <strong>TRUE</strong>, EAP-TLS authentication will fail unless the OCSP signing certificate also has the OCSP signing purpose set.&lt;br&gt;  ■ If this parameter is left at the default setting of <strong>FALSE</strong>, the OCSP signing certificate does not need to have the OCSP signing purpose set.</td>
</tr>
<tr>
<td>Disable CPPM Machine account password expiry in AD</td>
<td>Specify one of the following:&lt;br&gt;  ■ When the value for this parameter is set to <strong>TRUE</strong>, it disables the Samba machine account password timeout setting so that a change to the machine account password will not be made.&lt;br&gt;  ■ If this parameter is left at the default setting of <strong>FALSE</strong>, the Samba machine account password timeout setting remains in effect.</td>
</tr>
<tr>
<td>Skip netevents for IPv6 Accounting Packets</td>
<td>This option is recommended in a dual-stack (IPv4/IPv6) environment when ClearPass is configured to send updates to endpoint servers. Use this option to disable accounting netevents if an IPv6 address is present in the accounting packet.&lt;br&gt;  When you enable this option (that is, set to <strong>TRUE</strong>), ClearPass does not send client IPv6 updates to endpoint servers. The default setting is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>TLS Session Cache Limit</td>
<td>Specify the number of TLS sessions to cache before purging the cache (used in TLS based 802.1X EAP Methods). The range is from <strong>1,000</strong> to <strong>100,000</strong>. The default is <strong>10,000</strong>.</td>
</tr>
</tbody>
</table>

**Stats Collection Service Options**

To configure the Statistics Collection service:

1. Navigate to the **Administration > Server Manager > Server Configuration**, then select the ClearPass server.
2. From the **Server Configuration** page, select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **Stats collection service**.
   The following dialog opens:
4. Specify the **Service Parameters** tab > **Stats Collection Service** parameter as described in the following table:

**Table 1: Service Parameters > Statistics Collection Service**

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Stats Collection</td>
<td>Enable or disable statistics collection and aggregation. The <strong>Statistics Collection Service</strong> 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 administrator attempts to start these services: <strong>Failed to start Stats collection service - Ignoring service start request as Stats Collection option is disabled on the node</strong>. <strong>NOTE:</strong> Enabling or disabling this parameter requires a restart of the <code>cpass-statsd-server</code> and the <code>cpass-carbon-server</code>.</td>
</tr>
</tbody>
</table>

**System Monitor Service Options**

To configure the System Monitor service:

1. Navigate to the **Administration > Server Manager > Server Configuration**, then select the ClearPass server.
2. From the **Server Configuration** page, select the **Service Parameters** tab.
3. From the **Select Service** drop-down, select **System monitor service**.

   The following dialog opens:

**Figure 529 System Monitor Service Dialog**

4. Specify the **Service Parameters > System Monitor Service** parameters as described in the following table:
### Table 1: Services Parameters > System Monitor Service Parameters

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free Disk Space Threshold</td>
<td>This parameter monitors the available disk space on the current ClearPass server node. Specify the <strong>Free Disk Space Threshold</strong> (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.</td>
</tr>
<tr>
<td>1 Min CPU load average Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>5 Min CPU load average Threshold</td>
<td></td>
</tr>
<tr>
<td>15 Min CPU load average Threshold</td>
<td></td>
</tr>
</tbody>
</table>

5. Click **Save**.

**TACACS Server Options**

To configure the TACACS Server service:

1. Navigate to the Administration > Server Manager > Server Configuration, then select the ClearPass server.
2. From the Server Configuration page, select the Service Parameters tab.
3. From the Select Service drop-down, select Tacacs server.

   The following dialog opens:

   **Figure 530 Service Parameters > TACACS+ Server Dialog**

4. Specify the **Service Parameters > TACACS server** parameters as described in the following table:
Table 1: Service Parameters > TACACS Server

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+ Profiles Cache Timeout</td>
<td>Specify the time (in seconds) for which TACACS+ profile result entries are cached by ClearPass Policy Manager. The default is <strong>86400</strong> seconds (24 hours).</td>
</tr>
<tr>
<td>TACACS+ HTTP Thread Pool Size</td>
<td>Specify the maximum number of simultaneous requests the server can handle. The default value is <strong>100</strong>. The range is from 5 to 500. 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.</td>
</tr>
<tr>
<td>TACACS+ Authentication Timeout</td>
<td>Specify the timeout value for the TACACS+ server. The default value is <strong>30</strong> seconds. The range is from 1 to 300 seconds. This parameter specifies the timeout between the TACACS+ server (the ClearPass server) and the Authentication server (such as Active Directory, Token server, or any other authentication method). If the Authentication server does not reply back to ClearPass (TACACS+ server) within the configured TACACS+ Authentication Timeout, then the TACACS+ server (ClearPass) will timeout.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

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 531 System Monitoring Configuration Dialog**

4. Specify the System Monitoring configuration parameters as described in the following table:
Table 1: System Monitoring Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Location</td>
<td>Specify the location of the ClearPass Policy Manager appliance.</td>
</tr>
<tr>
<td>System Contact</td>
<td>Specify the contact information of the ClearPass Policy Manager appliance.</td>
</tr>
<tr>
<td>Engine ID</td>
<td>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.</td>
</tr>
</tbody>
</table>

SNMP Configuration

<table>
<thead>
<tr>
<th>Version</th>
<th>Specify the SNMP version from the options V1, V2C, or V3. The SNMP parameters on this page vary based on the SNMP version selected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community String</td>
<td>V1 and V2C: Enter and reenter the community string for sending traps. This is applicable only for SNMP V1 and V2C versions.</td>
</tr>
<tr>
<td>Username</td>
<td>V3 only: Specify the user name to use for SNMP v3 communication.</td>
</tr>
</tbody>
</table>
| 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.                                                                                                                                                                                                                                          |
| 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 532  Server Configuration > Network Page**

   ![](image)

**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.
5. Specify the **Restrict Access** parameters as described in the following table, then click **Create**:

**Table 1: Restrict Access Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| **Resource Name** | Select the application for which you want to allow or deny access:  
  - OnGuard  
  - ClearPass API  
  - CLI  
  **NOTE:** Restricting CLI access restricts SSH access to the *appadmin* user. The console access is still available through the *appadmin* user account.  
  - Policy Manager  
  - Graphite  
  - Guest Operator  
  - Insight |
| **Access** | Select one of the access control options:  
  - **Allow**: Allows access to the selected application.  
    When you configure the Access option as **Allow**, with a specific set of IP addresses or subnets, this set becomes the white list. This means there is an implicit Deny Access statement for all other IP addresses or subnets in the network.  
  - **Deny**: Denies access to the selected application.  
    When you configure the Access option as **Deny**, with a specific set of IP addresses or subnets, then every other IP address and subnet in the network has access except those specified here. This means there is an implicit Allow Access statement for all other IP addresses or subnets in the network. |
| **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.

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.
4. From the SSH Public Keys option, click Add Public Key. The Add Public Key configuration page opens.

![Figure 534 Adding a Public Key](image)

5. In the SSH Public Key page, copy and paste the SSH public key of the client, then click Save.

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 535  Creating a GRE Tunnel**

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Specify the name for the tunnel interface. This name is used to identify the tunnel in the list of network interfaces.</td>
</tr>
<tr>
<td>Local Inner IP</td>
<td>Enter the local IP address of the tunnel network interface.</td>
</tr>
<tr>
<td>Remote Outer IP</td>
<td>Enter the IP address of the remote tunnel endpoint.</td>
</tr>
<tr>
<td>Remote Inner IP</td>
<td>Enter the remote IP address of the tunnel network interface. Enter a value to automatically create a route to this address through the tunnel.</td>
</tr>
<tr>
<td>Local Outer IP (optional)</td>
<td>Optionally, enter the local IP address of the tunnel endpoint.</td>
</tr>
</tbody>
</table>
```

5. Specify the Create Tunnel parameters as described in the following table, then click Create:

**Table 2: Create Tunnel Parameters**

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 537).

Thus, ClearPass supports adding traffic selectors based on port number and protocol (TCP/UDP) with rule options Bypass, Encrypt, and Drop (see Table 5).

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.
5. Specify the **Create IPsec Tunnel** parameters as described in the following table, then click **Create**:

**Table 3: Create IPSec Tunnel Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| **Local Interface**   | Specify the local Management interface.  
  - IPv6 addresses are available in the drop-down list and can be specified as the remote IP address.  
  - The local interface and remote IP address must either both be IPv4, or both be IPv6.  
  **NOTE:** The IP addresses for the local and remote fields cannot be local link addresses starting with `fe80`. |
| **Remote IP Address** | Specify the IP address of the remote host. The remote IP address can be either IPv4 or IPv6.                                                      |
| **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 |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Action/Description</strong></td>
</tr>
</tbody>
</table>
| Encryption Algorithm            | Select one of the following encryption algorithms:  
  - AES128  
  - AES256                                                                                      |
| 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               | Enter the IKE Shared Secret, then verify the IKE secret key.                                                                                         |
| Verify IKE Shared Secret        | The IKE Shared Secret can be up 128 characters in length.                                                                                           |
| IKE Lifetime                    | Specify the number of minutes for the lifetime of the IKE. The default is 180 minutes.                                                               |
|                                 | The valid range for IKE Lifetime is from 5 to 1440 minutes.                                                                                           |
| Lifetime                        | Specify the lifetime of the IPsec tunnel in minutes. The default is 60 minutes.                                                                   |
|                                 | The valid range for Lifetime is from 5 to 1440 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.                                                                                              |
### Table 4: Create IPSec Tunnel Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Local Interface            | Specify the local Management interface.  
  - IPv6 addresses are available in the drop-down list and can be specified as the remote IP address.  
  - The local interface and remote IP address must either both be IPv4, or both be IPv6.  
  **NOTE:** The IP addresses for the local and remote fields cannot be local link addresses starting with `fe80`. |
| Remote IP Address          | Specify the IP address of the remote host. The remote IP address can be either IPv4 or IPv6.                                                                                                                       |
| 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  
  - Pre-Shared Key |
| Encryption Algorithm       | Select one of the following encryption algorithms:  
  - AES128  
  - AES256                                                                                                                                                                                                          |
| 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                                                                                                                                                                                                   |
<p>| IKE Shared Secret          | Enter the IKE Shared Secret, then verify the IKE secret key. The IKE Shared Secret can be up 128 characters in length.                                                                                               |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify IKE Shared Secret</td>
<td><strong>NOTE:</strong> This option appears only when the Authentication Type is set to <a href="#">Pre-Shared Key</a>.</td>
</tr>
<tr>
<td>IKE Lifetime</td>
<td>Specify the number of minutes for the lifetime of the IKE. The default is 180 minutes. The valid range for <strong>IKE Lifetime</strong> is from 5 to 1440 minutes.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Specify the lifetime of the IPSec tunnel in minutes. The default is 60 minutes. The valid range for <strong>Lifetime</strong> is from 5 to 1440 minutes.</td>
</tr>
<tr>
<td>Peer Certificate Subject DN</td>
<td>When the authentication type is set to <strong>Certificate</strong>, you can configure the <strong>Peer Subject Certificate DN</strong> (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. <strong>NOTE:</strong> Configuring <strong>Peer Certificate Subject DN</strong> is optional. If it is configured, the Distinguished Name should match with the peer certificate DN in order to complete the authentication.</td>
</tr>
<tr>
<td>Enabled</td>
<td>To enable the IPSec tunnel, click the <strong>Enabled</strong> check box.</td>
</tr>
</tbody>
</table>

**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 537  *Create IPsec Tunnel > Traffic Selectors Dialog*

2. Specify the **Traffic Selectors** parameters as described in the following table, then click **Create**.

**Table 5: Create IPsec Tunnel > Traffic Selectors Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt Rules</td>
<td>Displays the IPsec tunnel encryption rules configured for this IPsec tunnel.</td>
</tr>
<tr>
<td>Bypass Rules</td>
<td>Displays the IPsec tunnel bypass rules configured for this IPsec tunnel.</td>
</tr>
<tr>
<td>Drop Rules</td>
<td>Displays the IPsec tunnel drop rules configured for this IPsec tunnel.</td>
</tr>
<tr>
<td>Type</td>
<td>Select one of the following traffic selector types:</td>
</tr>
<tr>
<td></td>
<td>- Bypass</td>
</tr>
<tr>
<td></td>
<td>- Encrypt</td>
</tr>
<tr>
<td></td>
<td>- Drop</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select one of the following protocols:</td>
</tr>
<tr>
<td></td>
<td>- Any</td>
</tr>
<tr>
<td></td>
<td>- TCP</td>
</tr>
<tr>
<td></td>
<td>- UDP</td>
</tr>
<tr>
<td>Port</td>
<td>From the <strong>Port</strong> drop-down list, select the port.</td>
</tr>
<tr>
<td>Reset</td>
<td>To reset the configuration settings to the defaults, click <strong>Reset</strong>.</td>
</tr>
<tr>
<td>Save Rule</td>
<td>To save the current Rule configuration, click <strong>Save Rule</strong>.</td>
</tr>
</tbody>
</table>
### Table 6: Create IPSec Tunnel > Traffic Selectors Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt Rules</td>
<td>Displays the IPSec tunnel encryption rules configured for this IPSec tunnel.</td>
</tr>
<tr>
<td>Bypass Rules</td>
<td>Displays the IPSec tunnel bypass rules configured for this IPSec tunnel.</td>
</tr>
<tr>
<td>Drop Rules</td>
<td>Displays the IPSec tunnel drop rules configured for this IPSec tunnel.</td>
</tr>
<tr>
<td>Type</td>
<td>Select one of the following traffic selector types:</td>
</tr>
<tr>
<td></td>
<td>• Bypass</td>
</tr>
<tr>
<td></td>
<td>• Encrypt</td>
</tr>
<tr>
<td></td>
<td>• Drop</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select one of the following protocols:</td>
</tr>
<tr>
<td></td>
<td>• Any</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td>Port</td>
<td>From the Port drop-down list, select the port.</td>
</tr>
<tr>
<td>Reset</td>
<td>To reset the configuration settings to the defaults, click <strong>Reset</strong>.</td>
</tr>
<tr>
<td>Save Rule</td>
<td>To save the current Rule configuration, click <strong>Save Rule</strong>.</td>
</tr>
</tbody>
</table>

### 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 538 IPsec Tunnel Summary and Action Button to See Tunnel Status

2. To see the current status for an IPSec tunnel, click the **Action** button (see Figure 538).
   - The **IPsec Tunnel Status** window for the selected tunnel opens:
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 540, Phase 1 is complete but Phase 2 is failing. Look at the Audit Viewer events (Monitoring > Audit Viewer) to find the root cause.

Figure 540 IPsec Tunnel Status: Only IKE Phase 1 Complete

Example 2
When the tunnel status displays the information as shown in Figure 541, Phase 2 is also complete.
Figure 541  IPsec Tunnel Status: IKE Phase 1 and Phase 2 Complete

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 542  Creating a VLAN**

5. Specify the Create VLAN parameters as described in the following table, then click Create:

   **Table 7: Server Configuration > Create VLAN Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td>Enter the physical port on which to create the VLAN interface. This is the interface through which the VLAN traffic will be routed. <strong>NOTE:</strong> Make sure your network supports tagged 802.1Q packets on the selected physical interface.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Enter the name for the VLAN interface. This name is used to identify the VLAN in the list of network interfaces.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Parameter | Action/Description
--- | ---
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the VLAN.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the netmask for the VLAN.</td>
</tr>
</tbody>
</table>

### 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](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2577)

### Enabling FIPS Mode Using CLI
1. 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 543 Enabling FIPS Mode**

   ![Figure 543 Enabling FIPS Mode](image)

   The following information has been given:

   India
   
   Therefore TimeZone='Asia/Kolkata' will be used.
   
   Local time is now: Wed May 14 19:31:41 IST 2014.
   
   
   Is the above information OK?
   1. Yes
   2. No
   
   Do you want to enable FIPS Mode? [y/n]: _

2. After enabling FIPS mode using the CLI commands, you can verify whether FIPS mode is enabled or not in the **Configuration Summary** page.
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, then select the server of interest.

   The Server Configuration dialog for the selected server opens.

2. Select the FIPS tab.

   **Figure 545  Server Configuration > FIPS Tab**

**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.

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 546 FIPS Status**

![FIPS Status](image)

You can also view the status of the FIPS mode using the CLI commands. For more information, see Show Commands on page 898.

**ClearPass Cluster Configuration Options**

This section describes the cluster configuration options that are available from the Administration > Server Manager > Server Configuration page.

- **Cluster-Wide Parameters**
- **Synchronizing the Cluster Date and Time with the NTP Server**
- **Changing the Cluster-Wide Password**
- **Managing Policy Manager Zones**
- **Configuring NetEvents Targets**
- **Clearing Machine Authentication Cache**
- **Configuring Virtual IP Settings**
- **Making a Subscriber Node**

**Cluster-Wide Parameters**

This section describes the following Cluster-Wide Parameters features:

- **General Parameters**
- **Cleanup Intervals Parameters**
- **Notifications Parameters**
- **Standby Publisher Parameters**
- Virtual IP Parameter
- Common Criteria Mode Parameter
- Database Parameters
- Profiler Parameters
- TACACS 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 the 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 547  Cluster-Wide Parameters > General Page**
3. Configure the **Cluster-Wide Parameters > General** parameters as described in the following table, then click **Save**.

**Table 1: Cluster-Wide Parameters > General Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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 be used to refresh 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) field. 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 |
<p>| Free disk space threshold value        | Specify the percentage below which disk usage warnings are issued in the Monitoring &gt; 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: <strong>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%</strong> |
| 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.                                                                                                    |
| Syslog Export Interval                 | This parameter provides the ability to configure the Syslog messaging batch interval. The default value is 120 seconds. The supported interval value is between 30 seconds to 120 seconds. <strong>NOTE:</strong> The interval specified for this parameter is applied to all appliances in a cluster and to all the Syslog Export Filters that are in the enabled state. For related information, see Syslog Export Filters. |
| Automatically check for available Software Updates | Specify whether to enable automatic checking for available software updates. The default is <strong>TRUE</strong>. For related information, see Software Updates.                                                                 |
| Automatically download Posture Signature and Windows Hotfixes Updates | Specify whether to automatically download and install Posture Signature and Windows Hotfixes Updates. The default is <strong>FALSE</strong>. For related information, see Software Updates. |
| Automatically download Endpoint Profile Fingerprints | Specify whether to automatically download Endpoint Profile Fingerprints. The default is <strong>FALSE</strong>. For related information, see Software Updates. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Banner Text</td>
<td>Customize the banner text that appears on the ClearPass login screen and CLI access window.</td>
</tr>
</tbody>
</table>
| Allow Concurrent Admin Login      | - When this field is set to **TRUE** (which is the default setting), an Admin user can log in to the same ClearPass server concurrently from either the same device or a different device.  
- When this field is set to **FALSE**, and an Admin user logs into a ClearPass server from one device, and then later logs into the same ClearPass server from either the same device or a different device, the Admin user is logged out of all previous sessions on that ClearPass server. When this occurs, the following message is displayed:  
  *You have been logged out of previous active session(s)*                                                                 |
| 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).                                              |
| CLI Session Idle Timeout          | Specify the maximum idle time permitted for CLI users, beyond which the session times out. The default value is **360 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—the sessions have to be disconnected and reconnected for the updated timeout value to take effect. |
| Console Session Idle Timeout      | Specify the **Console Session Idle Timeout** duration in minutes. The default value is **360 minutes**. The **Console Idle Session Timeout** does not begin counting down until the admin user exits the admin session, or when the admin session has timed out.  
If the user is still logged in to the admin session, the **Console Session Idle Timeout** is not enforced. To impose an automatic logout from the ClearPass server for an admin user connected to the console, you must set the idle timeout for the **Admin Session Idle Timeout** as well as the **Console Session Idle Timeout**.  
**The Console Session Idle Timeout:**  
- Must have a valid integer value (for example, a setting of 10.5 wouldn’t be valid).  
- The range of valid values is from 5 to 1,440 minutes (24 hours).  
- The Audit Viewer captures the details about changes in **Console Session Idle Timeout**.  
| Disable TLSv1.0 support           | To disable Transport Layer Security (TLS) v1.0 support, select one of  
- Admin  
- Network  
- All  
**NOTE:** Operations in Common Criteria require that this value be set to **ALL**. |
| Disable TLSv1.1 support           | To disable Transport Layer Security (TLS) v1.1 support, select one of the following options:  
- None  
- Admin  
- Network  
- All |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content Security Policy (CSP)</strong></td>
<td>When enabled, Content Security Policy (CSP) has significant impact on the way browsers renders pages (e.g., inline JavaScript is disabled by default and must be explicitly allowed in the Content Security Policy). CSP prevents a wide range of attacks, including cross-site scripting and other cross-site injections.</td>
</tr>
<tr>
<td><strong>Performance Monitor Rendering Port</strong></td>
<td>Specify the port for performance monitor rendering. The default value is 80.</td>
</tr>
</tbody>
</table>
| **ICMPv6 Filters**                | - When the ICMPv6 Filters parameter is set to Disable (the default), ClearPass responds to all ICMPv6 (Internet Control Message Protocol) traffic.  
  - When this parameter is set to Enable, the following restrictions are applicable:  
    - ClearPass does not respond to ICMPv6 traffic sent to an anycast or multicast address.  
    - ClearPass does not transmit to ICMPv6 type-3 (Destination Unreachable) messages.                                                                                                                                                                                                                                                                                                                                                     |
| **Multi Master Cache Durability** | For the Multi-Master Cache to survive abrupt shutdowns, set this to Normal or Full. The default value is OFF. **NOTE:** Enabling this feature might result in some performance degradation.                                                                                                                                                                                                                                                                                                                                                                               |
| **Post-Auth v2**                  | When Post-Auth v2 is enabled, it improves ClearPass performance and scaling for post-authentication events when interoperating with third-party systems. To enable Post-Auth v2:  
  1. Set the Post-Auth v2 setting to Enabled.  
  2. Navigate to Administration > Server Manager > Server Configuration and select the appropriate ClearPass server.  
  3. Select the Services Control tab.  
  4. On the Async Network Services row, click Stop, then click Start.  
The following Post-Auth v2 restrictions apply:  
  - Post-Auth v2 does not support ClearPass Proxy.  
  - IPv6 IP addressing is note supported.  
  - When defining a context server action, the following HTTP methods are supported: PATCH, DELETE, POST, GET, and PUT.                                                                                                                                                                                                                                                                                                                                 |
Cleanup Intervals Parameters

The following figure displays the Cluster-Wide Parameters > Cleanup Intervals dialog:

**Figure 548  Cluster-Wide Parameters > Cleanup Intervals Dialog**

1. Specify the Cluster-Wide Parameters > Cleanup Intervals parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</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**. |
| 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**. |
| Known endpoints cleanup interval | Specify the duration in number of days that ClearPass uses to determine when to start deleting known or disabled entries from the Endpoint repository.  
Known entries are deleted based on the last Added At value for each Endpoint. For example, if this value is **7**, then known Endpoints that do not have the Added At value within the last 7 days are deleted.  
The default value is **0 days**. This indicates that no cleanup interval is specified. |
| Unknown endpoints cleanup interval | Specify the duration in number of days that ClearPass uses to determine when to start deleting unknown entries from the Endpoint repository.  
Unknown entries are deleted based on the last Updated At value for each Endpoint.  
For example, if this value is **7**, then unknown endpoints that do not have the Updated At value within the last 7 days (stale endpoints) are deleted. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expired guest accounts cleanup interval</td>
<td>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.</td>
</tr>
<tr>
<td>Profiled Unknown endpoints cleanup interval</td>
<td>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.</td>
</tr>
<tr>
<td>Profiled Known endpoints cleanup option</td>
<td>Specify whether to enable the option to clean up profiled known endpoints. The default value is FALSE.</td>
</tr>
<tr>
<td>Static IP endpoints cleanup option</td>
<td>Specify whether to enable the option to clean up static IP endpoints. The default option is FALSE.</td>
</tr>
</tbody>
</table>

**Notifications Parameters**

The following figure displays the [Cluster-Wide Parameters > Notifications dialog](https://clearpass.dell.com):  

**Figure 549  Cluster-Wide Parameters > Notifications Dialog**
1. Specify the **Cluster-Wide Parameters > Notifications** parameters as described in the following table:

**Table 3: Cluster-Wide Parameters > Notifications Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Alert Level</td>
<td>Specify the alert notifications that are generated for system events logged at this level or higher.</td>
</tr>
<tr>
<td></td>
<td>- <strong>INFO</strong>: Alerts that provide Information, Warnings, and Error messages are generated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>WARN</strong>: Alerts that provide Warnings and Error messages are generated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ERROR</strong>: Alerts that provide Error messages only are generated.</td>
</tr>
<tr>
<td></td>
<td>- The default value is <strong>WARN</strong>.</td>
</tr>
<tr>
<td>Alert Notification Timeout</td>
<td>Specify the timeout in hours that determines how often alert messages are generated and distributed.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Disabled</strong>, alert generation is disabled. The default value is <strong>2 hours</strong>.</td>
</tr>
<tr>
<td>Alert Notification - eMail Address</td>
<td>Enter a comma-separated list of email addresses to which alert messages are sent.</td>
</tr>
<tr>
<td>Alert Notification - SMS Address</td>
<td>Enter a comma-separated list of phone numbers to which alert messages are sent.</td>
</tr>
</tbody>
</table>

**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 550  Cluster-Wide Parameters > Standby Publisher Dialog**
1. Specify the **Cluster-Wide Parameters > Standby Publisher** parameters as described in the following table:

**Table 4: Cluster-Wide Parameters > Standby Publisher Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Publisher Failover</td>
<td>To authorize a node in a cluster on the system to act as a publisher if the primary publisher fails, select <strong>TRUE</strong>. The default value is <strong>FALSE</strong>. <strong>NOTE:</strong> The standby publisher value should be set to <strong>false</strong> before starting a cluster update to avoid false failover triggers.</td>
</tr>
<tr>
<td>Designated Standby Publisher</td>
<td>Select the server in the cluster to act as the standby publisher. The default value is <strong>0</strong>. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Failover Wait Time</td>
<td>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 <strong>10 minutes</strong>. This prevents the secondary node from taking over when the primary node is temporarily unavailable during a restart.</td>
</tr>
</tbody>
</table>

**Virtual IP Parameter**

The following figure displays the **Cluster-Wide Parameters > Virtual IP** dialog:

**Figure 551 Cluster-Wide Parameters > Virtual IP Dialog**

1. Specify the **Cluster-Wide Parameters > Virtual IP** parameter as described in the following table:

**Table 5: Cluster-Wide Parameters > Virtual IP Configuration Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover Wait Time</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 redundancy.
Common Criteria Mode Parameter

The **Mode** tab in the **Cluster-Wide Parameters** page allows you to enable or disable **Common Criteria Mode**.

**Figure 552**  *Cluster-Wide Parameters Page > Common Criteria Mode Parameter*

1. Specify the **Cluster-Wide Parameters > Mode** parameter as described in the following table:

**Table 6: Cluster-Wide Parameters > Mode Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Criteria Mode</td>
<td><strong>Common Criteria Mode</strong> is for specific deployments that require strict compliance to Common Criteria requirements. To enable or disable <strong>Common Criteria Mode</strong>, select <strong>TRUE</strong> or <strong>FALSE</strong>. The default is <strong>FALSE</strong>. When you set <strong>Common Criteria Mode</strong> to <strong>TRUE</strong>, the following Warning message is displayed: <strong>WARNING:</strong> Setting this value to <strong>TRUE</strong> enables strict validation of Certificates and changes to modules in order to comply with Common Criteria requirements.</td>
</tr>
</tbody>
</table>

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.

**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 (see [FIPS Page](#)).
- Server certificates must be updated before you enable **Common Criteria Mode** (see [Certificate Store](#)).
- Only Certificate Authority (CA)-issued certificates can be used for ClearPass server certificates.
- No self-signed certificates are allowed as trusted certificates.
- All X.509 v3 trusted Certificate Authority (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 553  Cluster-Wide Parameters > Database Dialog

1. Configure the Cluster-Wide Parameters > Database parameters as described in the following table:

Table 7: Cluster-Wide Parameters > Database Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto backup configuration options</td>
<td>Select any of the following auto-backup configuration options:</td>
</tr>
<tr>
<td></td>
<td>- Off: Select this to not to perform periodic backups.</td>
</tr>
<tr>
<td></td>
<td>- Select Off before upgrading ClearPass Policy Manager to avoid the interference</td>
</tr>
<tr>
<td></td>
<td>between Auto backup and migration process.</td>
</tr>
<tr>
<td></td>
<td>- Config: Perform a periodic backup of the configuration database only. This is</td>
</tr>
<tr>
<td></td>
<td>the default auto backup configuration option.</td>
</tr>
<tr>
<td></td>
<td>- Config</td>
</tr>
<tr>
<td></td>
<td>session log database.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> It is recommended that you set this option to Off or Config before</td>
</tr>
<tr>
<td></td>
<td>starting an upgrade. This ensures the Auto Backup process does not interfere</td>
</tr>
<tr>
<td></td>
<td>with migration post upgrade. If required, you can change this setting back to</td>
</tr>
<tr>
<td></td>
<td>Config</td>
</tr>
<tr>
<td>Database user &quot;appexternal&quot; password</td>
<td>Enter the password for the appexternal username for this connection to the</td>
</tr>
<tr>
<td></td>
<td>database.</td>
</tr>
<tr>
<td>Replication Batch Interval</td>
<td>Configure the time interval (in seconds) at which the subscribers synchronize with</td>
</tr>
<tr>
<td></td>
<td>the Publisher. The default value is 5 seconds. The allowed range is 1 to 60</td>
</tr>
<tr>
<td></td>
<td>seconds.</td>
</tr>
<tr>
<td>Store Password Hash for MSCHAP authentication</td>
<td>To store passwords for admin and local users to Hash and NTLM hash formats</td>
</tr>
<tr>
<td></td>
<td>(which enables RADIUS MSCHAP authentications against admin or local</td>
</tr>
<tr>
<td></td>
<td>repositories), set this to TRUE.</td>
</tr>
<tr>
<td></td>
<td>If you set this to FALSE, RADIUS MSCHAP authentications are not possible because</td>
</tr>
<tr>
<td></td>
<td>the NTLM hash passwords are removed for all the users.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When you set this value to TRUE, you must reset all the passwords to</td>
</tr>
<tr>
<td></td>
<td>reenable RADIUS MSCHAP authentication against the user repositories.</td>
</tr>
<tr>
<td>Store Local User Passwords using reversible</td>
<td>To enable cleartext password comparison against local users, set this to TRUE.</td>
</tr>
<tr>
<td>encryption</td>
<td>If you set this to FALSE, cleartext password comparison against local users is not</td>
</tr>
<tr>
<td></td>
<td>possible because the reversible passwords for local users are removed.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> After setting this value to TRUE, you must reset all the local user</td>
</tr>
<tr>
<td></td>
<td>passwords to reenable cleartext password comparison against local users.</td>
</tr>
</tbody>
</table>
Profiler Parameters

The following figure displays the Cluster-Wide Parameters > Profiler dialog:

**Figure 554  Cluster-Wide Parameters > Profiler Dialog**

1. Configure the Cluster-Wide Parameters > Profiler parameters as described in the following table:

**Table 8: Cluster-Wide Parameters > Profiler Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiler Scan Ports</td>
<td>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.</td>
</tr>
<tr>
<td>Process wired device information from IF-MAP interface</td>
<td>Choose whether to process wired device information from the IF-MAP interface. The default is FALSE.</td>
</tr>
<tr>
<td>Enable Endpoint Port Scans using Nmap</td>
<td>Set this option to TRUE to enable Endpoint scans using Nmap (Network Mapper). <strong>NOTE:</strong> The Open Ports scanner is disabled when Nmap-based port scanning is enabled. When Nmap scan is enabled, the following warning is displayed: <strong>WARNING:</strong> 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.</td>
</tr>
<tr>
<td>Enable Endpoint Port Scans using WMI</td>
<td>Set this option to TRUE to enable Endpoint scans using WMI (Windows Management Instrumentation).</td>
</tr>
<tr>
<td>Enable NTLMv1 for WMI scans</td>
<td>Set this parameter to TRUE to enable NT LAN Manager v1 for WMI (Windows Management Instrumentation) scans. The default is FALSE. For more information, see WMI Credentials Configuration.</td>
</tr>
<tr>
<td>Netflow/sFlow Reprofile Interval</td>
<td>Specify the interval after which endpoints will be repроfiled. The default value is 24 hours. The minimum value is one hour. For more information about the Netflow and sFlow collectors, see Endpoint Information Collectors on page 474.</td>
</tr>
</tbody>
</table>
**TACACS Parameters**

The following figure displays the **Cluster-Wide Parameters > TACACS** dialog:

![Cluster-Wide Parameters > TACACS Dialog](image)

1. Configure the **Cluster-Wide Parameters > TACACS** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Change Password for TACACS</td>
<td>When logging in for TACACS+ user authentication:</td>
</tr>
<tr>
<td></td>
<td>- If set to <strong>FALSE</strong> (the default setting), after entering a blank password, you are presented with an option to change the TACACS+ user password.</td>
</tr>
<tr>
<td></td>
<td>- If set to <strong>TRUE</strong>, the option to enter the TACACS+ user password is displayed. The option to change the TACACS+ password is <strong>not</strong> displayed.</td>
</tr>
<tr>
<td>TACACS User Prompt Text</td>
<td>You can modify the text to be used for the TACACS+ username prompt as needed. The default TACACS username prompt is as follows: <em>UserName:</em></td>
</tr>
<tr>
<td>TACACS Password Prompt Text</td>
<td>You can modify the text to be used for the TACACS+ password prompt as needed. The default TACACS password prompt is as follows: <em>Password:</em></td>
</tr>
<tr>
<td>TACACS Connection Idle Timeout</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- The default value is <strong>900 seconds</strong> (15 minutes).</td>
</tr>
<tr>
<td></td>
<td>- The minimum allowed value is <strong>60 seconds</strong>.</td>
</tr>
<tr>
<td></td>
<td>- The maximum allowed value is <strong>172800 seconds</strong> (two days).</td>
</tr>
<tr>
<td>Admin UI Login Remote TACACS Server IP</td>
<td>This option is used if you want the ClearPass server to authenticate against a TACACS+ server. In this case, the ClearPass server is acting as a TACACS+ client and talking to the TACACS+ server in order to authenticate users. Specify the IP address for the remote TACACS+ server.</td>
</tr>
<tr>
<td>Admin UI Remote TACACS Server Shared Secret</td>
<td>This option is used if you want the ClearPass server to authenticate against a TACACS+ server. Enter the Shared Secret for the remote TACACS+ server.</td>
</tr>
</tbody>
</table>
Synchronizing the Cluster Date and Time with the NTP Server

- **Restarting ClearPass Services**
- **Specifying the Time Zone on the Publisher Node**

To synchronize the date and time on the nodes in a cluster with an NTP (Network Time Protocol) server:

The option to change the date and time for the ClearPass cluster is available only on the Publisher node. Subscriber nodes in a cluster will synchronize the date and time from the Publisher node.

1. Log in to the Publisher node.
2. Navigate to the Administration > Server Manager > Server Configuration page.
3. Select the Set Date and Time link.
   - The Change Date and Time dialog opens to the Date & Time tab.
   
   **Figure 556**  Change Date and Time > Date & Time Tab

4. Specify the Date & Time parameters as described in the following table, then click Save:
## Table 1: Changing Date and Time Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Synchronize time with NTP server       | To synchronize with a Network Time Protocol (NTP) server, enable this check box (enabled by default).  
**Manually Setting the Date and Time**  
**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:  
![Change Date and Time](image)  
**WARNING:** After command execution, Policy Manager services will be restarted. This may take a few minutes.                                                                                                                                                                                                                                                         |
| Primary Server and Secondary Server   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| NTP Server                             | Specify the IP address or host name for the Primary NTP server and the Secondary NTP server. The IP address can be an IPv4 or IPv6 address.                                                                                                                                                                                                                                                                                 |
| Key Value                              | The **Key Value** is a form of shared secret, which both the client and the ClearPass server use for authenticating NTP messages.  
The **Key Value** can be:  
- Up to 20-character printable ASCII string  
- Up to 40-character hex value  
When entering an ASCII string for the **Key Value**, note that it cannot contain the following characters:  
- & (ampersand)  
- ; (semicolon)  
- ` (grave accent)  
- | (pipe)  
- < (left angle bracket)  
- > (right angle bracket)  
- ( (left parenthesis)  
- ) (right parenthesis)  
The **Key Value** ASCII string must start and end with one of the following characters:  
- - (hyphen)  
- ' (apostrophe)  
- " (quotation mark)  

| Algorithm                               | Select one of the following encryption types:  
- SHA  
- SHA1  
**NOTE:** In FIPS mode, only the SHA1 hashing algorithm is supported.                                                                                                                                                                                                                                                                                                                                                           |
Restarting ClearPass Services

Once you have saved the Date & Time configuration, you must restart ClearPass Policy Manager services.

The Audit Viewer (Monitoring > Audit Viewer) tracks NTP configuration changes.

To restart Policy Manager services:

1. Navigate to Administration > Server Manager > Server Configuration.
2. Select the ClearPass Publisher node.
3. From the Server Configuration page, select the Services Control tab.

Figure 557  Restarting Stopped Services

4. From the Action column, click Start for each service that needs to be restarted.
   For each restarted service, the Start button is changed to Stop.
**Specifying the Time Zone on the Publisher Node**

To specify the time zone on the Publisher node:

1. Click the **Time Zone on Publisher** tab.

**Figure 558  Time Zone on Publisher Dialog**

![Change Date and Time](image)

The time zones are listed in alphabetical order.

2. Select the time zone where the Publisher node resides, then click **Save**.

---

**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.

---

**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 559  Change Cluster Password Dialog**

![Change Cluster Password](image)

**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.

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 to OnGuard Clients

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 a Policy Manager Zone:

1. Navigate to the Administration > Server Manager > Server Configuration page.
2. Click the Manage Policy Manager Zones link.
   The Policy Manager Zones dialog opens:
3. To add a new Policy Manager Zone, click **Click to add...** and enter the name of the Policy Manager Zone to be added.

4. Be sure to click the **Save** icon, then click **Save**.

5. To delete a zone, click the trash can icon (Trash).

**Mapping Policy Manager Zones to OnGuard Clients**

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 the **Policy Manager Zones** link. The **Mappings for Policy Manager Zones to OnGuard Clients** page opens.

**Figure 561  Mappings for Policy Manager Zones to OnGuard Clients Page**

3. Specify the **Mappings for Policy Manager Zones to OnGuard Clients** parameters as described in the following table:
### Table 1: OnGuard Settings > Policy Manager Zones Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Manager Zone</td>
<td>Select the Policy Manager Zone from the drop-down list. If no Policy Manager zone is configured, the default Policy Manager zone is displayed in this field.</td>
</tr>
<tr>
<td>Client Subnets</td>
<td>Displays the client subnet addresses specified for the selected Policy Manager zone.</td>
</tr>
<tr>
<td>Server IPs</td>
<td>Displays the server IP addresses specific to the selected Policy Manager zone.</td>
</tr>
<tr>
<td>Zone Network Details</td>
<td></td>
</tr>
<tr>
<td>Policy Manager Zone</td>
<td>Select the Policy Manager zone from the drop-down list that is created from the Administration &gt; Server Manager &gt; Server Configuration &gt; Manage Policy Manager Zones page.</td>
</tr>
<tr>
<td>Client Subnets</td>
<td>Specify the client subnets that are configured for the selected zone.</td>
</tr>
<tr>
<td>Default ClearPass Server IPs</td>
<td>Specify the IP address of the default ClearPass server.</td>
</tr>
<tr>
<td>Override Server IPs</td>
<td>Optionally, specify the IP addresses or the Fully Qualified Domain Name (FQDN) to which you want the OnGuard agent to send the 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.</td>
</tr>
</tbody>
</table>

4. Click **Save**. The new Policy Manager Zone configuration settings are displayed.

### 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), 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.
2. Click the **NetEvents Targets** link.
   The **NetEvents Targets** configuration dialog opens.

3. Specify the **NetEvents Targets** parameters as described in the following table, then click **Save**:

   **Table 1: NetEvents Targets Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target URL</td>
<td>Enter the HTTP URL for the service that supports posting to the NetEvents target and requires authentication using username and password. To specify an external Insight server, use the following Target URL: https://&lt;ClearPass-IP-address&gt;/netwatch/netevents</td>
</tr>
<tr>
<td>Username/Password</td>
<td>Enter the ClearPass admin credentials configured for authentication for the HTTP service that is provided in the Target URL.</td>
</tr>
<tr>
<td>Reset button</td>
<td>Resets the values entered in this configuration dialog.</td>
</tr>
<tr>
<td>Delete button</td>
<td>Deletes the specified Target URL.</td>
</tr>
</tbody>
</table>

   **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 564  Server Configuration Page > Clear Machine Authentication Cache**

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*

### 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.

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.

   By default, the Virtual IP Settings for IPv4 dialog opens:

   **Figure 565  Virtual IP Settings for IPv4**
3. Specify the Virtual IP Settings parameters as described in the following table, then click Save:

**Table 1: Virtual IPv4 and IPv6 Settings Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select IP Version</td>
<td>Select either the <strong>IPv4</strong> or <strong>IPv6</strong> addressing format.</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Enter the IPv4 or IPv6 address you want to define as the virtual IP address.</td>
</tr>
<tr>
<td>Virtual Host ID</td>
<td>To specify a unique virtual Host for this Virtual IP, enter the virtual router ID (1-255).</td>
</tr>
<tr>
<td>Primary Node</td>
<td>Select the server to use as the primary node.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When IPv6 is selected, the Primary Node and Secondary Node drop-down lists are populated with the corresponding IPv6 addresses for selection.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> To add an IPv6 address as a Virtual IP, it must be in the same subnet as the Primary and Secondary nodes.</td>
</tr>
<tr>
<td>Secondary Node</td>
<td>Select the server to use as the secondary node.</td>
</tr>
<tr>
<td>Interface</td>
<td>When you select the primary node and the secondary node, the Interface field is populated with that node’s management interface IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If the Data/External port is configured, the Interface field is populated with both the management interface IP address and the Data/External port IP address.</td>
</tr>
<tr>
<td>Subnet</td>
<td>The Subnet value for the management interface IP address is automatically populated when you select the primary node and secondary node.</td>
</tr>
<tr>
<td>Enabled</td>
<td>The virtual IP settings configured here are enabled by default.</td>
</tr>
</tbody>
</table>

**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 Aruba Support—navigate to Administration > Support > Contact Support for contact information.

To make a Publisher node a Subscriber node:
1. On a Publisher node, navigate to the Administration > Server Manager > Server Configuration page. The Server Configuration page opens.

   **Figure 567 Make Subscriber Link**

   ![Server Configuration](image)

   2. Click the Make Subscriber link. The Add Subscriber Node page opens:

   **Figure 568 Adding a Subscriber Node**

   ![Add Subscriber Node](image)

   3. Specify the Add Subscriber Node parameters as described in the following table, then click Save:
Table 1: *Add Subscriber Node Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publisher IP</td>
<td>Enter the Publisher node's IP address.</td>
</tr>
<tr>
<td>Publisher Password</td>
<td>Specify the Publisher node's password. <strong>NOTE:</strong> The password specified here is the password for the CLI user <code>appadmin</code>.</td>
</tr>
<tr>
<td>Restore the local log database after this operation</td>
<td>To restore the log database after the Subscriber node has been added, select the check box.</td>
</tr>
<tr>
<td>Do not backup the existing databases before this operation</td>
<td>If you do not require a backup to the existing databases on this node, select the check box.</td>
</tr>
</tbody>
</table>

**Dropping a Subscriber Node**

To drop a Subscriber 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.

**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*).

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.
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
   - Diagnostic dumps from Policy Manager services
   - Back up Policy Manager configuration data
   - Logs from Performance Metrics

   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**.

   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 570  Backup Policy Manager Database Dialog**

3. Specify the Back up Policy Manager Database parameters as described in the following table, then click Start:

**Table 1: Back up Policy Manager Database Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate file name</td>
<td>To enable Policy Manager to generate a filename for the database backup, select this check box. This option is enabled by default.</td>
</tr>
<tr>
<td>File Name</td>
<td>To manually specify the backup file name, clear the Generate file name check box, then enter the desired file name.</td>
</tr>
<tr>
<td>Back up ClearPass configuration data</td>
<td>The option to back up Policy Manager configuration data is enabled by default.</td>
</tr>
<tr>
<td>Back up ClearPass session log data</td>
<td>To enable back up of Policy Manager session log data, select this check box.</td>
</tr>
<tr>
<td>Back up Insight data</td>
<td>To enable back up of ClearPass Insight data, select this check box.</td>
</tr>
<tr>
<td>Do not back up password fields in configuration database</td>
<td>If you don't want to backup the password fields in the configuration database, select this check box.</td>
</tr>
</tbody>
</table>

**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:
3. Specify the **Restore Policy Manager Database** parameters as described in the following table, then click **Start**:

**Table 28: Restore Policy Manager Database Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore file location</td>
<td>Select either <strong>Upload file to server</strong> or <strong>File is on server</strong>.</td>
</tr>
<tr>
<td>Upload file path</td>
<td>Browse to select name of backup file. <strong>NOTE:</strong> This option is available only when the <strong>Upload file to server</strong> option is selected.</td>
</tr>
<tr>
<td>Shared backup files present on the server</td>
<td>If the files is on a server, select a file from the files in the local shared folders. (See <strong>Downloading Local Shared Folders</strong>.) <strong>NOTE:</strong> This is displayed only when the <strong>File on server</strong> option is selected.</td>
</tr>
<tr>
<td>Restore CPPM configuration data (if it exists in the backup)</td>
<td>Select the check box to include an existing configuration data in the restore.</td>
</tr>
<tr>
<td>Restore CPPM session log data (if it exists in the backup)</td>
<td>Select the check box to include the log data in the restore.</td>
</tr>
<tr>
<td>Restore Insight data (if it exists in the backup)</td>
<td>Select the check box to include Insight reporting data in the restore.</td>
</tr>
<tr>
<td>Ignore version mismatch and attempt data migration</td>
<td>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.</td>
</tr>
<tr>
<td>Restore cluster server/node entries from backup.</td>
<td>Select the check box to include the cluster server/node entries in the restore.</td>
</tr>
<tr>
<td>Do not backup the existing databases before this operation.</td>
<td>Select the check box if you do not want to backup the existing databases before performing a restore.</td>
</tr>
</tbody>
</table>
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
- Endpoints
- Stored reports

To perform a system cleanup:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.
2. Select the ClearPass server you wish to clean up.
3. Click the **Cleanup** button.
   
   The **Force Cleanup Files** dialog opens.

**Figure 572  Force Cleanup Files Dialog**

4. Enter the number of days system files can remain before they are removed. The allowed range is 0 to 15 days.

5. To initiate the cleanup process, click **Start**.
   
   The **Force Cleanup Files** status report opens:
Shutting Down or Rebooting the Server

**Shutting Down the Server**

To shut down the current ClearPass server:

1. Navigate to the Administration > Server Manager > Server Configuration page.
2. Click the Shutdown button.
   
   You receive the message:
   
   *Are you sure you want to shut down Policy Manager Server <IP_address>?*

3. To proceed with the shut down operation, click Yes.
   
   You receive the message:
   
   *Shut down of server initiated*
   
   The ClearPass server shuts down in an orderly manner.

4. To cancel the shut down operation, click Cancel.

**Rebooting the Server**

To reboot the current ClearPass server:

1. Navigate to the Administration > Server Manager > Server Configuration page.
2. Click the Reboot button.
   
   You receive the message:
   
   *Are you sure you want to reboot Policy Manager Server <IP_address>?*

3. To proceed with the reboot, click Yes.

4. To cancel the reboot operation, click Cancel.

**Log Configuration**

This section provides the following information:

- [Service Log Configuration](#)
- [System Level Configuration](#)
Service Log Configuration

On the Service Log Configuration tab, you can specify the default log level for each service and its associated modules.

To configure logs for services and system level:

1. Navigate to the Administration > Server Manager > Log Configuration page.
   
   The Service Log Configuration page opens:

   **Figure 574 Log Configuration > Service Log Configuration Tab**

   ![Service Log Configuration Tab](image)

2. Specify the Service Log Configuration parameters as described in the following table:
Table 1: Log Configuration > Service Log Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Select Service                   | Specify the service for which you want to configure logs:  
  - Admin server  
  - AirGroup notification service  
  - Async network service  
  - ClearPass network services  
  - DB change notification server  
  - DB replication service  
  - Micros Fidelio FIAS  
  - Multi-master cache  
  - Policy server  
  - RadSec Service
  
  **NOTE:** When you select the RadSec service and change the Log Level, it takes approximately 8 seconds for the Radsec service to restart. Therefore, Aruba recommends that you wait 8 to 10 seconds after you modify the Log Level before you collect logs (Administration > Server Manager > Server Configuration > click the Collect Logs button).  
  - Radius server  
  - Syslog client service  
  - Tacacs server

| Module Log Level Settings        | 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. Available options include the following:  
  - 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                | 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  
  - WARN  
  - ERROR  
  - FATAL
  
  **NOTE:** Set this option first, and then override any specific modules as necessary.                                                                                                                                                                                                                                                                                           |

| Restore Defaults/Save            | Click Save to save changes. To restore the default settings, click Restore Defaults.                                                                                                                                                                                                                                                                                                                                  |

**System Level Configuration**

On the System Level tab, you can specify the number and size of log files you need to maintain for each service and the server to which they can be sent.

1. From the Log Configuration page, select the System Level tab.
   
   The System Level page opens:
2. Specify the **System Level** tab parameters as described in the following table:

Table 2: Log Configuration > System Level Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server</td>
<td>Specify the server for which you want to configure logs.</td>
</tr>
<tr>
<td>Number of log files</td>
<td>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 <strong>Limit each log file size to</strong>), 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.</td>
</tr>
<tr>
<td>Limit each log file size to</td>
<td>Specify the size of each log file before the log rolls over to the next file. The default value is 50 MB.</td>
</tr>
</tbody>
</table>

**Syslog Settings**

<table>
<thead>
<tr>
<th>Syslog Server</th>
<th>Specify the name of the syslog server. Policy Manager sends the configured module logs to this syslog server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Server Port</td>
<td>Specify the syslog server port number. The default is <strong>514</strong>.</td>
</tr>
<tr>
<td>Enable Syslog</td>
<td>To override the <strong>Syslog Filter Level</strong> for a service, select the <strong>Enable Syslog</strong> check box.</td>
</tr>
<tr>
<td>Syslog Filter Level</td>
<td>If desired, change the <strong>Syslog Filter Level</strong>. The current <strong>Syslog Filter level</strong> is based on the default log level specified on the <strong>Service Log Configuration</strong> tab.</td>
</tr>
<tr>
<td>Restore Defaults/Save</td>
<td>Click <strong>Save</strong> to save your changes. To restore the default settings, click <strong>Restore Defaults</strong>.</td>
</tr>
</tbody>
</table>
**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 567.
- **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 576  Local Shared Folders Page**

3. Select the local shared folder you want to download.
   
   The selected auto-backup file is downloaded to your system's Download folder.

**License Management**

This section describes the following topics:

- Activating the Platform License on a Cluster Node
- Updating a ClearPass Platform License
- Managing Application Licenses
- Adding an Application License
- Activating an Application License
- Updating an Application License
- Refreshing the License Usage Count

**Activating the Platform License on a Cluster Node**

The ClearPass Platform license provides the platform activation code that is installed on all the nodes in a ClearPass cluster. You must have a ClearPass Platform license for every instance of the product.

---

**Note**

You cannot have more than one ClearPass Platform license installed on a ClearPass node.
The ClearPass Platform License is the base-level license. Each device has one ClearPass Platform License for the physical hardware. Virtual devices have a ClearPass Platform License as well on a per-expected device level.

If the Publisher node is added to a cluster without first activating its ClearPass Platform license, the license activation should be done from the Publisher node.

When a Subscriber node is added to the cluster, it already has a ClearPass Platform license. It is not activated by default. This ClearPass Platform license can be activated or not.

- If not activated, the red **Activate** button is shown in the Administration > Licensing > Servers tab.
- If the ClearPass Platform license is already activated, it is shown with a green **Activated** button.

To activate the Platform license on a Publisher or Subscriber node:

1. Navigate to Administration > Server Manager > Licensing.
   - The **Licensing** page opens to the **License Summary** page.
2. Select the Servers tab.
   - The ClearPass Platform license for this ClearPass node is listed. The **Activation Status** column shows a red circle next to the keyword **Activate**.

**Figure 577 ClearPass Platform License Ready to Be Activated**

3. Click **Activate**.
   - The **Activate License** page opens.

**Figure 578 Activate License Page**

4. In the **Online Activation** section, click **Activate Now**.
   - The ClearPass Platform license is now activated. The **Servers** tab > **Activation Status** column shows a green circle next to the keyword **Activated**.
Offline Activation: Creating a Case to Receive the Activation Key

If you are not connected to the Internet, you must submit a case through the HP Enterprise My Networking portal:

1. In the Offline Activation section, click Download to download an activation request token from the Policy Manager server.
2. Go to the My Networking Portal and log in.
3. Click the Support link.
4. Click Open/View Case.
   - This will show all the cases you have submitted to Support.
5. Click Open a New Case.
   - The Case Submission form is displayed.
6. In the Case Submission > Problem Details section, complete all the fields in the Case Submission form as shown in Figure 580.

Figure 580  My Networking > Case Submission Form

7. To attach the activation token from ClearPass, click Browse and select the activation request token.
8. Click Create a case.
9. The Support team will activate the token and send you the activation key.
10. Click Browse to locate the activation key file on your system, then click Upload.

**Updating a ClearPass Platform License**

ClearPass Platform licenses are permanent and do not have an expiry date.

An Evaluation ClearPass Platform License does have an expiry date, after which it must be updated with a permanent Platform license.

In the event that an incorrect Platform license key is entered when activating the license, the ClearPass Platform license would have to be updated.

To update the ClearPass Platform license:
1. Navigate to Administration > Server Manager > Licensing.
   The **Licensing** page opens to the **License Summary** page.
2. Select the Servers tab.
   The ClearPass Platform license for this ClearPass node is listed.

**Figure 582  **ClearPass Platform License to Be Updated

3. Click Activated.
   The **Update License** page opens.
4. Click Update.
   The ClearPass Platform license is now updated.

Managing Application Licenses

- Viewing Existing Application Licenses
- Viewing Application License Details
- Viewing Platform License Information
- Notifications of Application License Usage Exceeded
- Application License Types
- Subscription License Expiry
- License Behavior in a Cluster

Viewing Existing Application Licenses

ClearPass licensing computation is solely based on number of endpoints that successfully connect to the network over a period of time. The Licensing page shows all the licenses that are installed for the ClearPass Policy Manager cluster. There is one entry per server node in the cluster. The License Summary page displays the number and type of purchased licenses, as well as the total license count and the number of licenses being used.

To view the Application licenses that are currently installed for the cluster:

1. Navigate to Administration > Server Manager > Licensing. The Licensing page opens to the License Summary page.

Figure 584 Application License Summary
From the **Licensing** page, you can:

- Add new Application licenses (see [Adding an Application License](#)).
- Refresh the license usage count (see [Refreshing the License Usage Count](#)).

### Viewing Application License Details

The **Licensing > Applications** page displays the ClearPass Policy Manager application license details such as product type (*Access, OnGuard, or Onboard*), license type (*Permanent, Subscription, or Evaluation*), number of endpoints, license duration, license activation status, and the date the application license was added.

The **Applications** tab is activated on adding an application license (*Access, OnGuard, or Onboard*).

![Figure 585 Applications License Details](image)

### Viewing Platform License Information

The **Licensing > Servers** page displays the information for the ClearPass Platform license, including the server IP address, the product (ClearPass Platform), license type (*Permanent*), current duration, license activation status, and the date the Platform license was added.

![Figure 586 Platform License Information](image)

### Notifications of Application License Usage Exceeded

License usage is calculated every 15 minutes. When Application license usage is exceeded, ClearPass sends notifications that are displayed in the ClearPass **Dashboard** and **Event Viewer**.

When the license limit for an Application license (*Access, OnGuard, or Onboard*) has been exceeded, the information banner on the Dashboard page is updated with a license usage exceeded message. The message is removed as soon as license usage falls within the allowed number.

License usage exceeded messages are also posted to the Event Viewer every 15 minutes for each ClearPass application that exceeds its license limit. The Event Viewer displays the number of licenses purchased and the current usage by application. When the appliance falls within the allowed usage, the Event Viewer displays a message to that effect. No banner messages are posted to the Dashboard for CLABV (evaluation) systems or for systems running in Evaluation mode or with Evaluation licenses. For CLABV systems or for applications running under an Evaluation license, messages are posted to the Event Viewer once each night at 11:55 P.M. local time.

### Application License Types

ClearPass Policy Manager supports the following Application license types:
Access License

The Access license accounts for authentications on the system. Guest functionality is embedded in Access licenses.

Without an Access license, ClearPass user interface administration access and cluster operations are allowed. However, the following service operations are disallowed: creation, copy, modification, deletion, and import.

ClearPass endpoints consume Access licenses based on active session counts. The active session is defined as a duration between:
- **RADIUS accounting Start and Stop**

On a ClearPass system with a valid Access license, TACACS+ sessions are not counted towards Access license consumption.

- **OnConnect SNMP MAC address learned and MAC address removed or aged**

If the session can't be identified (due to a lack of accounting), the Access license is consumed based on the MAC address for 24 hours.

The Access license enables various authentication types: 802.1X, MAB, WebAuth, OAuth2, TACACS+, Guest, etc.

The Profiler feature is available after installing an Access license.

WebAuth (non-OnConnect), OAuth2, AppAuth, and API requests are not counted towards Access license consumption.

Regarding Unactivated Access License Expiration

When an Access License that was not activated expires, service creation on that ClearPass server is blocked. For this reason, Aruba recommends that if multiple Access Licenses are installed, activate them as soon as they are installed. This ensures that even if one activated Access License is expired, service configuration will be allowed if the other Access Licenses have not yet reached their expiration dates.

If ClearPass service creation has been blocked due to an Access License that was allowed to expire while it was not activated, do the following:
1. Activate the expired license.
2. Verify whether the other Access Licenses are still within their valid date range.
3. Activate any other Access Licenses that have expired.

OnGuard License

The OnGuard license is responsible for all the activities related to ClearPass OnGuard. The OnGuard license is consumed for all OnGuard deployments (*Persistent* and *Dissolvable*) and any mode of operation (*Authentication with Health Checks, Health Check only, Authentication only*). The OnGuard license is consumed on a device basis for a period of 24 hours.

Onboard License

ClearPass Onboard allows for the self-provisioning of users devices for a secure network, where the user performs the work flow on his or her own. Onboard generates a unique device certificate and pushes the certificate to the user's device, while also performing network configuration. The Onboard license is computed based on the user for the lifetime of certificates.
Manually created devices, certificates, and certificates provisioned through the ClearPass Simple Certificate Enrollment Protocol (SCEP) service for Mobile Device Management systems are also counted towards the Onboard license based on the provisioned user. Devices that received their certificates via Certificates Authorities other than ClearPass, such as Microsoft Enterprise PKI, and not enrolled through ClearPass do not use Onboard licenses. Onboard licenses are returned to the pool when they expire, or are revoked or deleted.

**Subscription License Expiry**

Access licenses are issued as **Permanent or Subscription** types. Subscription licenses can be valid for one, three, or five years. Subscription licenses expire after the specified subscription period. When a Subscription license expires, ClearPass continues to operate normally. However, ClearPass configuration changes cannot be made and updates and upgrades are not operable.

**License Behavior in a Cluster**

The notable aspects of licensing behavior in a ClearPass cluster are as follows:

- All ClearPass license operations are performed on the Publisher node. All license computations are made at the cluster level.
- When a node becomes part of the cluster, the new Subscriber node loses all of its licenses except for the ClearPass Platform License.
- Any Application licenses (Access, Onboard, OnGuard) that were present on the ClearPass server prior to becoming a Subscriber node must be added again to the Publisher.
- When a node is dropped from the cluster, all its licenses are removed except for its ClearPass Platform License.
- When a Subscriber node is manually promoted to Publisher status, all the application licenses must be reactivated.
- When a Subscriber node is automatically promoted to Publisher status, there are no changes to the activation status of its licenses.

**Adding an Application License**

To add an application license:

1. Navigate to **Administration > Server Manager > Licensing**.
   - The **Licensing** page opens.
2. Click the **Add License** link.
   - The **Add License** page opens.
3. Specify the **Add License** parameters as described in the following table:

**Table 1: Add License Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Choose a ClearPass application license to be installed on the Publisher node in a ClearPass cluster.</td>
</tr>
<tr>
<td></td>
<td>- Access</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Guest functionality is included in Access licenses.</td>
</tr>
<tr>
<td></td>
<td>- OnGuard</td>
</tr>
<tr>
<td></td>
<td>- Onboard</td>
</tr>
<tr>
<td></td>
<td>You can install multiple instances of each application license.</td>
</tr>
<tr>
<td>License Key</td>
<td>Enter the license key for the selected application.</td>
</tr>
<tr>
<td>Terms and Conditions</td>
<td>Click the <strong>I agree to the above terms and conditions</strong> check box.</td>
</tr>
</tbody>
</table>

The **Add** button is now enabled.

4. Click **Add**.

You return to the **Licensing > License Summary** page, where the new application license is now listed and the following message is displayed:

*Application name* license added successfully.

When you add an application license, the **Applications** tab is enabled to allow you to activate the application licenses.

**Activating an Application License**

- **Online Activation**
- **Offline Activation: Creating a Case to Receive the Activation Key**

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.

**Online Activation**

To activate the application licenses on the current ClearPass server:
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 588 ClearPass Application Licenses Ready to Be Activated

3. Click Activate.
The Activate License page opens.

Figure 589 Activate License Page

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.

Figure 590 Application License Activated
Offline Activation: Creating a Case to Receive the Activation Key

If you are not connected to the Internet, you must submit a case through the HP Enterprise My Networking portal:

1. In the **Offline Activation** section, click **Download** to download an activation request token from the Policy Manager server.
2. Go to the **My Networking** Portal and log in.
3. Click the **Support** link.
4. Click **Open/View Case**.
   This will show all the cases you have submitted to Support.
5. Click **Open a New Case**.
   The Case Submission form is displayed.
6. In the **Case Submission > Problem Details** section, complete all the fields in the Case Submission form as shown in **Figure 591**.

**Figure 591  My Networking > Case Submission Form**

7. To attach the activation token from ClearPass, click **Browse** and select the activation request token.
8. Click **Create a case**.
9. The Support team will activate the token and send you the activation key.

10. To locate the activation key file on your system, click **Browse**, then click **Upload**.

### 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 of unique endpoints (devices) that can be authenticated.

To update an application license:

1. Navigate to Administration > Server Manager > Licensing.
   
   The **Licensing** page opens.

   **Figure 593 Licensing Page**

2. Select the **Applications** tab.

   **Figure 594 Licensing Applications Tab**

3. Select the application license you need to update.
   
   The **Update License** dialog opens.
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**.
   The selected application license is updated.

**Refreshing the License Usage Count**

To update the latest usage count of all licenses in the ClearPass cluster:

1. Navigate to **Administration > Server Manager > Licensing**.
   The **Licensing** page opens.

**Figure 596  Licensing Page**

2. Click the **Refresh Count** link.
   When you click **Refresh Count**, the license usage count is refreshed immediately. You then receive the following confirmation:
   
   *License count refreshed successfully*

**External Servers**

This section provides the following information:

- SNMP Trap Receivers
- Syslog Targets
SNMP Trap Receivers

This section provides the following information:

- **SNMP Trap Receivers Main Page** on page 589
- **Adding an SNMP Trap Server** on page 590
- **Importing an SNMP Trap Server** on page 591
- **Exporting All SNMP Trap Servers** on page 592
- **Exporting an SNMP Trap Server** on page 593
- **Deleting an SNMP Trap Server** on page 594

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 597  SNMP Trap Receivers Page**

---

**About the ClearPass SNMP Private MIB**
For information about the ClearPass SNMP Private MIB, see [ClearPass SNMP Private MIB](#).

### 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 598](#)). 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](#)).

---

**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 598 Add SNMP Trap Server Dialog**

3. **Specify the Add SNMP Trap Server parameters** as described in the following table, then click **Save**:
### Table 1: Add SNMP Trap Server Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>Enter the trap destination hostname or IP address. <strong>NOTE:</strong> This server must have an SNMP trap receiver or trap viewer installed.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a short description of the SNMP trap server.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>Select one of the following SNMP versions:</td>
</tr>
<tr>
<td></td>
<td>- SNMP v1 with community strings</td>
</tr>
<tr>
<td></td>
<td>- SNMP v2 with community strings</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with no Authentication</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using MD5 and no Privacy</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using MD5 and with Privacy</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using SHA and no Privacy</td>
</tr>
<tr>
<td></td>
<td>- SNMP v3 with Authentication using SHA and with Privacy</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The MD5 authentication type is not supported when you use ClearPass Policy Manager in FIPS mode.</td>
</tr>
<tr>
<td>Username</td>
<td>Specify the Admin user name for SNMP operations. <strong>NOTE:</strong> This parameter is available in SNMP v3 only.</td>
</tr>
<tr>
<td>Type</td>
<td>From the <strong>Type</strong> drop-down, select the type of SNMP notification:</td>
</tr>
<tr>
<td></td>
<td>- Inform</td>
</tr>
<tr>
<td></td>
<td>- Trap</td>
</tr>
<tr>
<td>Authentication Key</td>
<td>Specify the SNMP v3 with authentication option (SHA or MD5). <strong>NOTE:</strong> The EAP-MDS authentication type is not supported if you run ClearPass Policy Manager in FIPS mode.</td>
</tr>
<tr>
<td>Privacy Key</td>
<td>Specify the SNMP v3 with privacy option. <strong>NOTE:</strong> This parameter is available in SNMP v3 only.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>Choose one of the available privacy protocols:</td>
</tr>
<tr>
<td></td>
<td>- DES-CBC</td>
</tr>
<tr>
<td></td>
<td>- AES-128</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This parameter is available in SNMP v3 with Privacy only. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specify the port number for sending the traps. By default, the port number is <strong>162</strong>. <strong>NOTE:</strong> Configure the trap server firewall for traffic on this port.</td>
</tr>
</tbody>
</table>

---

**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 1](#).
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

**Figure 599  Import from file Pop-up**

![Import from file Pop-up](image)

The following table describes the **Import from file** parameters:

**Table 1: Import from file Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select File</td>
<td>Browse to the SNMP Trap Server configuration file to be imported.</td>
</tr>
<tr>
<td>Enter secret for the file (if any)</td>
<td>If the file was exported with a secret key for encryption, enter the secret key here.</td>
</tr>
</tbody>
</table>

**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 1](#).
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 600** Export to file Pop-up

The following table describes the Export to file parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>Choose Yes to export the file with password protection.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the secret key.</td>
</tr>
<tr>
<td>Verify Secret</td>
<td>Re-enter the secret key.</td>
</tr>
</tbody>
</table>

**Table 1: Export to file Parameters**

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 1.
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 601** Export to file Pop-up
The following table describes the Export to file parameters:

**Table 1: Export to file Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>Choose Yes to export the file with password protection.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the secret key.</td>
</tr>
<tr>
<td>Verify Secret</td>
<td>Re-enter the secret key.</td>
</tr>
</tbody>
</table>

**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 100), audit records (see Audit Viewer on page 145) and event records (see Event Viewer on page 148). You can send this information to one or more syslog targets (servers).

**Adding a Syslog Target**

To add a syslog target:

1. Navigate to Administration > External Servers > Syslog Targets.

   The Syslog Targets page opens.

**Figure 602  Syslog Targets Page**

2. Click the Add link.

   The Add Syslog Target dialog opens:
3. Specify the **Add Syslog Target** parameters as described in the following table:

**Table 29: Add Syslog Target Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>Enter the Syslog server hostname or IP address. The IP address can be an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a short description of the Syslog server.</td>
</tr>
</tbody>
</table>
| 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 | The default port number is **514**. If necessary, change the server port number. |

4. Click **Save**.

   The new Syslog Target is now added to the list:

**Figure 604  Syslog Target Added**

---

**Syslog Export Filters**

This section describes the following topics:

- About Syslog Export Filters
- Syslog Export Filters Page on page 596
- Adding a Syslog Export Filter
About Syslog Export Filters

Policy Manager can export session data (see Live Monitoring: Access Tracker on page 100), audit records (see Audit Viewer on page 145), and event records (see Event Viewer on page 148).

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 605 Syslog Export Filters Page

The following table describes the Syslog Export Filters parameters:

Table 1: Syslog Export Filters Page Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the syslog export filter.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description of the syslog export filter.</td>
</tr>
<tr>
<td>Export Template</td>
<td>Displays the name of the Export Template selected in the Add Syslog Export Filter dialog (see Adding a Syslog Export Filter).</td>
</tr>
<tr>
<td>Export Event Format</td>
<td>Displays the Export Event Format Type selected in the Add Syslog Export Filter dialog; for example, LEEF (Log Event Extended Format) and CEF (Common Event Format).</td>
</tr>
</tbody>
</table>
### 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 606 Add Syslog Export Filters Page > General Tab**

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 601**.

The following table describes the **Add Syslog Export Filters > General** tab parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Status    | - A red icon indicates that the syslog export filter is currently disabled. To enable a disabled filter, click the red icon.  
|           | - A green icon indicates that the syslog export filter is currently enabled. To disable an enabled filter, click the green icon. |
| Export    | To export a syslog export filter, select the check box for the appropriate filter, then click **Export**. The **Export to file** dialog opens. For more information, see **Importing and Exporting Information**. |
| Delete    | To delete a syslog export filter, select the check box for the appropriate filter, then click **Delete**. |
### Table 1: Add Syslog Export Filters > General Tab Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the syslog export filter.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description that provides additional information about the syslog export filter (recommended).</td>
</tr>
<tr>
<td>Export Template</td>
<td>Select any one of the templates from the following options:</td>
</tr>
<tr>
<td></td>
<td>- Audit Records</td>
</tr>
<tr>
<td></td>
<td>- Insight Logs</td>
</tr>
<tr>
<td></td>
<td>- Session Logs</td>
</tr>
<tr>
<td></td>
<td>- System Events</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>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 601.</td>
</tr>
<tr>
<td>Export Event Format Type</td>
<td>Select any one of the export event formats from the following options:</td>
</tr>
<tr>
<td></td>
<td>- Standard: Select this event format type to send the event types in raw syslog format. This is the default event format type.</td>
</tr>
<tr>
<td></td>
<td>- LEEF: Select this event format type to send the event types in Log Enhanced Event Format (LEEF).</td>
</tr>
<tr>
<td></td>
<td>- CEF: Select this event format type to send the event types in Common Event Format (CEF). In Syslog Targets, CEF-format field mappings map as many fields as possible for each template. Each template has unique mappings to customstrings, devicecustomdates, and devicecustomnumbers. For sample event format types, see Export Event Format Types—Examples on page 598.</td>
</tr>
<tr>
<td>Syslog Servers</td>
<td>Syslog servers define the receivers of syslog messages sent by servers in the ClearPass cluster.</td>
</tr>
<tr>
<td></td>
<td>To add a ClearPass syslog server, select it from the Select to Add drop-down list.</td>
</tr>
<tr>
<td></td>
<td>To add a new ClearPass syslog server, click the Add New Syslog Target link (for more information, see Adding a Syslog Target on page 594).</td>
</tr>
<tr>
<td></td>
<td>To view details about a syslog server, select the syslog server, then click View Details.</td>
</tr>
<tr>
<td></td>
<td>To change details about a syslog server, select the syslog server, then click Modify. For more information, see Adding a Syslog Target on page 594.</td>
</tr>
<tr>
<td></td>
<td>To remove a syslog server (from receiving syslog messages), select the syslog server, then click Remove.</td>
</tr>
<tr>
<td>ClearPass Servers</td>
<td>You can designate syslog messages to be sent from exactly one server in the ClearPass cluster or from all of them.</td>
</tr>
<tr>
<td></td>
<td>To add a ClearPass server, select it from the Select to Add drop-down list.</td>
</tr>
<tr>
<td></td>
<td>To remove the ClearPass server, select the ClearPass server, then click Remove. <strong>NOTE:</strong> When no servers are listed, syslog messages are sent from all servers in the cluster.</td>
</tr>
</tbody>
</table>

### 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=34a39527af0,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
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=yyyyMMdd-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

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=yyyyMMdd-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=yyyyMMdd-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
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
HH:mm:ss,S,RADIUS.Acct-NAS-Port=0,Common.Username=test1,RADIUS.Acct-Session-Id=testE0F8471A5450-54BEB336C,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 authentications 2 1 0
LEEF Event Format Type > Insight Logs

The following example describes the LEEF event format type for the **Insight Logs** syslog export filter template:


CEF Event Format Type > Insight Logs

The following example describes the CEF event format type for the **Insight Logs** syslog export filter template:


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 userName=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 userName=admin devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z

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-TimestampFormat=MMM dd yyyy HH:mm:ss.SSS 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-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:


**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.

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 607** displays the **Syslog Export Filters > Filter and Columns > Insight Logs**.
As shown in Figure 607, 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 an update on endpoints, syslog events are generated.

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 1: Syslog Export Filters > Filter and Columns > Insight Logs Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Columns Selection</td>
<td>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. <strong>NOTE:</strong> You can add only the Insight reports that are already created in Insight. You cannot create a new data filter for Insight logs.</td>
</tr>
<tr>
<td>Predefined Field Groups</td>
<td>Select the predefined Insight reports that are grouped for addition.</td>
</tr>
<tr>
<td>Selected Columns</td>
<td>After you select an entry from the <strong>Available Columns</strong> list, click <strong>&gt;&gt;</strong> to add the selected entry to the <strong>Selected Columns</strong> list. Click <strong>&lt;&lt;</strong> to remove an entry from the <strong>Selected Columns</strong> list.</td>
</tr>
</tbody>
</table>

**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 608  Syslog Export Filters - Filter and Columns (Session Logs) Tab**

The following table describes the **Syslog Export Filters - Filter and Columns (Session Logs)** parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Filter</td>
<td>Specify the data filter. The data filter limits the type of records sent to the syslog target.</td>
</tr>
<tr>
<td>Modify/Add New Data Filter</td>
<td>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 <a href="#">Adding a Data Filter on page 152</a></td>
</tr>
</tbody>
</table>

**Columns Selection**

- There are predefined field groups, which are column names grouped together for quick addition to the report. For example, *Logged in users* field group has seven predefined columns. When you click *Logged in users* the seven columns automatically appear in the **Selected Columns** list.
- Additional fields are available to add to the reports. You can select the type of attributes (which are the different table columns available in the session database) from the **Available Columns Type** drop down list. Policy Manager populates these column names by extracting the column names from existing sessions in the session database.
- After you select an entry from the **Available Columns** list, click >> to add the selected entry to the **Selected Columns** list.
- Click << to remove an entry from the **Selected Columns** list.

**Custom SQL**

Specify custom SQL query for export. This option is for advanced use cases. **NOTE:** 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 609** *Syslog Export Filters - Summary Tab*

![Figure 609 Syslog Export Filters - Summary Tab](image)

The following table describes the **Syslog Export Filters - Summary** tab parameters:

**Table 1: Syslog Export Filters - Summary Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the syslog export filter.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description that provides additional information about the syslog export filter.</td>
</tr>
<tr>
<td>Export Template</td>
<td>Displays the template selected as the export template.</td>
</tr>
<tr>
<td>Syslog Servers</td>
<td>Displays the IP address of the syslog server selected during configuration.</td>
</tr>
<tr>
<td>ClearPass Servers</td>
<td>Displays the IP address of the ClearPass servers selected during configuration.</td>
</tr>
<tr>
<td><strong>Filter and Columns</strong></td>
<td></td>
</tr>
<tr>
<td>Data Filter</td>
<td>Displays the data filter selected when configuring option 1 in the <strong>Filter and Columns</strong> tab.</td>
</tr>
<tr>
<td>Columns Selection</td>
<td>Displays the predefined field groups and available columns type selected when configuring option 1 in the <strong>Filter and Columns</strong> tab.</td>
</tr>
<tr>
<td>Custom SQL</td>
<td>Displays the SQL query selected when configuring option 2 in the <strong>Filter and Columns</strong> tab.</td>
</tr>
</tbody>
</table>

**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 1](#).
3. Click **Import**.

The following figure displays the **Import from file** pop-up:

**Figure 610 Import from file Pop-up**

The following table describes the **Import from file** parameters:

**Table 1: Import from file Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select File</td>
<td>Browse to the Syslog Filter configuration file to be imported.</td>
</tr>
<tr>
<td>Enter secret for the file (if any)</td>
<td>If the file was exported with a secret key for encryption, enter the same key here.</td>
</tr>
</tbody>
</table>

**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 1](#).
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 611  Export to file Pop-up**

The following table describes the **Export to file** parameters:

**Table 1: Export to file Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>Choose Yes to export the file with password protection.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the secret key.</td>
</tr>
<tr>
<td>Verify Secret</td>
<td>Re-enter the secret key.</td>
</tr>
</tbody>
</table>

**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 1**.
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 612  Export to file Pop-up**
The following table describes the Export to file parameters:

**Table 1: Export to file Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>Choose Yes to export the file with password protection.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the secret key.</td>
</tr>
<tr>
<td>Verify Secret</td>
<td>Re-enter the secret key.</td>
</tr>
</tbody>
</table>

**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
- Resetting the SMTP Settings

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 613  Messaging > SMTP Server Page**

   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 1: Messaging > SMTP Server Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>Enter the Fully Qualified Domain Name (FQDN) or the IP address of the SMTP server.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the username if your email server requires authentication for sending email messages.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the specified username, then verify the password.</td>
</tr>
<tr>
<td>Default From address</td>
<td>Enter the email address that must to be displayed as the sender's address in the message.</td>
</tr>
<tr>
<td>Connection Security</td>
<td>To establish the communication with the SMTP server, select from one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>: Select this option to disable secure communication with the server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SSL</strong>: Select this option to have a Secured Socket Layer communication with the server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Start TLS</strong>: Select this option to have a Transport Layer Security communication with the server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP port number that the SNMP server listens on. The default value of the port is <strong>25</strong>.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Enter the timeout value for connection to the SMTP server (in seconds). The default value is <strong>30</strong> seconds.</td>
</tr>
</tbody>
</table>

**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 614  Send Test Email Dialog**

   ![Send Test Email Dialog](image)

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 615  Send Test SMS Dialog**

   

   ![Send Test SMS Dialog](image)

   

   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**.

Resetting the SMTP Settings
To remove the current SMTP settings specified in the *Messaging* dialog, click **Reset**.

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**
- **Adding Vendor-Specific Endpoint Context Servers**
- **Endpoint Information Collectors**

**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 opens:

**Figure 616  Endpoint Context Servers Page**

The following table describes the **Endpoint Context Servers** categories:

**Table 1: Endpoint Context Server Categories**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Displays the name of the endpoint context server.</td>
</tr>
<tr>
<td>Server Type</td>
<td>Displays the type of the endpoint context server.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the endpoint context server: <strong>Enabled</strong> or <strong>Disabled</strong>. For non-MDM servers, the status is always displayed as <strong>Disabled</strong>.</td>
</tr>
</tbody>
</table>

**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 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 2).
3. In the **Add Endpoint Context Server** dialog, specify the parameters as described in **Table 2**.

4. Click **Save**.

**Table 2** describes the **Add Endpoint Context Server** parameters:

**Table 2: Add Endpoint Context Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose one of the Server Types (endpoint context server vendors) from the following options. The Server Type you select determines the configuration parameters.</td>
</tr>
<tr>
<td></td>
<td>- AirWatch</td>
</tr>
<tr>
<td></td>
<td>- Aruba Activate</td>
</tr>
<tr>
<td></td>
<td>- AirWave</td>
</tr>
<tr>
<td></td>
<td>- Google Admin Console</td>
</tr>
<tr>
<td></td>
<td>- Generic HTTP</td>
</tr>
<tr>
<td></td>
<td>- JAMF</td>
</tr>
<tr>
<td></td>
<td>- Juniper SRX</td>
</tr>
<tr>
<td></td>
<td>- MaaS360</td>
</tr>
<tr>
<td></td>
<td>- MobileIron</td>
</tr>
<tr>
<td></td>
<td>- Palo Alto Networks Firewall</td>
</tr>
<tr>
<td></td>
<td>- Palo Alto Networks Panorama</td>
</tr>
<tr>
<td></td>
<td>- SAP Afaria</td>
</tr>
<tr>
<td></td>
<td>- SOTI</td>
</tr>
<tr>
<td></td>
<td>- XenMobile</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can add more than one endpoint context server of the same type.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter the name of the server or host.</td>
</tr>
</tbody>
</table>
| Server Base URL       | Enter the full URL for the server. The default is the name you entered above with "https://" prepended. You can append a custom port, such as for an MDM server: https://yourservr.yourcompany.com:customerportnumber.
<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Authentication Method | Select one of the following authentication methods:  
  - **Basic**  
  - **OAuth2**: When you select **OAuth2** or **Both**, the following fields are displayed:  
    - OAuth2 Client ID  
    - OAuth2 Client Secret  
    - OAuth2 Resource URL  
    - Validate OAuth2 Credentials: **Validate** button: When you click **Validate**, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.  
  - **Both**: Selecting **Both** allows you to use both Basic and OAuth2 authentication. |
| Username            | Enter the username.                                                                                                                                 |
| Password            | Enter the password of the server or host, then verify the password.                                                                                                                                       |
| API Key             | 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.                                                                |
| Security Details    | Select this check box to enable this endpoint context server to fetch Endpoint Security information.                                                                                                       |
| Validate Server     | 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       | 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        | 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. |

**Add Endpoint Context Server > Actions Tab**

Use the **Actions** tab to view the server actions that can be performed on the specified endpoint context server and their descriptions. The server actions 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 2, "Add Endpoint Context Server Parameters").

For more information about endpoint context server actions configuration, see Configuring Endpoint Context Server Actions.
Figure 618  Example of Default Endpoint Context Server Actions (Airwatch Endpoint Context Server)

![Add Endpoint Context Server](image)

**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 3.
4. Click Import.

Figure 619 displays the Import from File dialog:

![Import from File Dialog](image)

The following table describes the Import from file parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select File</td>
<td>Browse to the Endpoint Context Server configuration file to be imported.</td>
</tr>
<tr>
<td>Enter secret for the file (if any)</td>
<td>If the file was exported with a secret key for encryption, enter the same key here.</td>
</tr>
</tbody>
</table>

**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.
   The Export to File dialog opens.
3. Enter the parameters as described in Table 4.
4. Click Export.
5. Enter the XML file name in the Save As dialog box.
6. Click Save.

Table 4 describes the Export to file parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>To export the file with password protection, choose Yes.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the secret key, then verify it.</td>
</tr>
</tbody>
</table>

**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) listed in Table 2, "Add Endpoint Context Server Parameters."
4. Click Update.

The tabs that appear when you add or modify an endpoint context server vary depending on the type (vendor) of the endpoint context server selected.

**Server Tab**

The following figure displays the Modify Endpoint Context Server > Server dialog:
Modify the **Modify Endpoint Context Server > Server** parameters as described in the following table:

**Table 5: Modify Endpoint Context Server > Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>The <strong>Server Type</strong> cannot be modified.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter the name of the server or host.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the full URL for the server. The default is the name you entered above with &quot;https://&quot; prepended. You can append a custom port, such as for an MDM server: <a href="https://yourserver.yourcompany.com:customerportnumber">https://yourserver.yourcompany.com:customerportnumber</a></td>
</tr>
</tbody>
</table>
| Authentication Method | Select one of the following authentication methods:  
  - **Basic**  
  - **OAuth2**: When you select **OAuth2** or **Both**, the following fields are displayed:  
    - OAuth2 Client ID  
    - OAuth2 Client Secret  
    - OAuth2 Resource URL  
    - Validate OAuth2 Credentials: **Validate** button: When you click **Validate**, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.  
  - **Both**: Selecting **Both** allows you to use both Basic and OAuth2 authentication. |
<p>| Username        | Enter the username of the server or host.                                                                                                       |
| Password        | Enter the password of the server or host, then verify the password.                                                                             |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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.                                                                                                           |
| Validate Server           | 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              | 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 actions that can be performed on the specified endpoint context server and their descriptions. The server actions 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 2, "Add Endpoint Context Server Parameters").

For more information about endpoint context server actions configuration, see Configuring Endpoint Context Server Actions.

The following figure displays an example of the Modify Endpoint Context Server > Actions tab:

**Figure 622  Modify Endpoint Context Server > Actions Tab**
Polling an Endpoint Context Server

To poll an endpoint context server:

- 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 page, click the check box next to the server name entry.

Figure 623  Selecting the Trigger Poll Option

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:

- Configuring Endpoint Context Server Actions
- Filtering an Endpoint Context Server Action Report
- Storing Authentication Attributes in the Multi-Master Cache
- Adding machine-os and host-type Endpoint Attributes

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 Endpoint Context Server Actions page displays a list of all the Context Server Actions that are available by default for each server type that ClearPass supports.

To configure endpoint context server actions:

1. Navigate to Administration > Dictionaries > Context Server Actions.
The **Endpoint Context Server Actions** page opens.

**Figure 624  Endpoint Context Server Actions Page**

2. From the **Endpoint Context Server Actions** page, click a row in the report. The **Endpoint Context Server Details** dialog opens.

**Figure 625  Endpoint Context Server Details Dialog**

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, authentication method, and URL for the endpoint context server action.

Specify the **Endpoint Context Server Details > Action** tab parameters as described in the following table, then click **Save**.

**Table 30: Action Parameters—Endpoint Context Server Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>Specifies the server type configured when the server action was configured. You can select the server type from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Lists the context servers specific to the server type selected in the <strong>Server Type</strong> field. This field is visible only if you selected the service type <strong>Generic HTTP</strong>.</td>
</tr>
<tr>
<td>Action Name</td>
<td>Specifies the name of the action configured.</td>
</tr>
<tr>
<td>Description</td>
<td>Provides additional information about the action specified.</td>
</tr>
<tr>
<td>HTTP Method</td>
<td>Select the HTTP method from the drop-down:</td>
</tr>
<tr>
<td></td>
<td>- DELETE</td>
</tr>
<tr>
<td></td>
<td>- GET</td>
</tr>
<tr>
<td></td>
<td>- POST (the default setting)</td>
</tr>
<tr>
<td></td>
<td>- PUT</td>
</tr>
<tr>
<td></td>
<td>- PATCH</td>
</tr>
<tr>
<td></td>
<td>You can use the HTTP method <strong>PATCH</strong> to append content to existing endpoints/values.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select the authentication method:</td>
</tr>
<tr>
<td></td>
<td>- None: Select <strong>None</strong> to disable the HTTP basic authentication for endpoint context server actions. This exposes the context server attributes to be used in context server actions.</td>
</tr>
<tr>
<td></td>
<td>- Basic</td>
</tr>
<tr>
<td></td>
<td>- OAuth2</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: When associating context server actions with an endpoint context server, be sure to specify the same authentication method that was configured for the endpoint context server.</td>
</tr>
<tr>
<td>URL</td>
<td>Indicates the URL for the selected HTTP method.</td>
</tr>
</tbody>
</table>

**Header Tab Parameters**

Use the **Header** tab to specify the key-value pairs to be included in the HTTP header.

1. From the **Header** tab, select **Click to add**.
2. Specify the **Endpoint Context Server Details—Header** parameters as described in the following table:

**Table 31: Header Parameters—Specifying Key Value Pairs**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header Name</td>
<td>Enter the name of the header to be included in the HTTP header.</td>
</tr>
<tr>
<td>Header Value</td>
<td>Specify the value of the header specific to the name to be included in the HTTP header.</td>
</tr>
</tbody>
</table>

If a ClearPass server is used as an Endpoint context server to update the configuration using the REST API call, add the HTTP header, **Accept: application/json** in the context server action.

3. Repeat these steps for each key-value pairs you need to add.
4. Click **Save**.

**Content Tab**

Use the **Content** tab to specify a content type and add non-default context server attributes (see Figure 627).

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.
Specify the **Endpoint Context Server Details—Content** parameters as described in the following table:

**Table 32: Content Parameters—Endpoint Context Server Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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](#).

**Attributes Tab Parameters**

Use the **Attributes** tab to specify the mapping for attributes used in the content to parameterized values from the request.

**Figure 628 Attributes Tab—Endpoint Context Server Details**
Specify the **Endpoint Context Server Details > Attributes** parameters as described in the following table:

**Table 33: Attributes Parameters—Endpoint Context Server Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Enter attribute names and assign values to those names. These name/value pairs are included in context server actions.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>Enter the value for the selected name in the <strong>Attribute Name</strong> field.</td>
</tr>
</tbody>
</table>

**Figure 629 Adding Endpoint Context Server Attributes**

5. Click **Save**.
   
   You receive the following message:
   
   *Context Server Action "Check Point Login (Generic HTTP)" updated successfully*

**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 opens (see **Figure 624**).

2. From the **Filter** drop-down, select a filter:
   
   - **Server Type**
   - **Action Name**
   - **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**.
Storing Authentication Attributes in the Multi-Master Cache

ClearPass provides a context server action that serves as an example of how to store attributes from an authentication session into Multi-Master Cache for use in policy enforcement during an authentication session. The Administrator can then clone it and customize the context server action to meet their requirements.

To access this context server action:

1. Navigate to **Administration > Dictionaries > Context Server Actions**.

   The **Endpoint Context Server Actions** page opens.

   **Figure 630  Endpoint Context Server Actions Page: Store Attributes in Multi-Master Cache**

2. Scroll down and select the **Store Attributes in Multi-Master Cache** endpoint context server action.

   The **Endpoint Context Server Details** page opens.

   **Figure 631  Endpoint Context Server Details: Store Attributes in Multi-Master Cache**

3. Modify and customize the **Store Attributes in Multi-Master Cache** endpoint context server action as needed.

   At **Configuration > Authentication > Sources**, the **Multi-Master Cache Repository** authentication source will fetch the attributes stored in the Multi-Master Cache and proceed with authentication.
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 opens.
2. Scroll to and select the **Generic HTTP/Check Point Login** server action.

![Figure 632 Selecting the Check Point Login Server Action](image)

The **Endpoint Context Server Details** dialog opens.

3. Select the **Content** tab (see Figure 629).
4. In the **Content** field, add the following attributes (see Figure 629):
   - "machine-os":"%(device_family)"
   - "host-type":"%(device_type)"

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 Generic HTTP Endpoint Context Server
- Adding a Google Admin Console Endpoint Context Server
- Integrating ClearPass with Infoblox Endpoint Context Servers
- Adding a JAMF Endpoint Context Server
- Integrating ClearPass with Juniper Networks SRX Endpoint Context Server
- Adding a MaaS360 Endpoint Context Server
- Adding a MobileIron Endpoint Context Server
- Integrating ClearPass with Palo Alto Networks Firewall Endpoint Context Server
- Adding a Palo Alto Networks Panorama Endpoint Context Server
- Adding a 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 additional 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 opens.
2. Click **Add**.
   The Add Endpoint Context Server page opens. This dialog opens in the Server tab.
3. From the Select Server Type drop-down, select **airwatch**.

**Server Tab**

The Airwatch Add Endpoint Context Server > Server page opens:

*Figure 633  Adding an AirWatch Endpoint Context Server > Server Page*

You can add more than one endpoint context server of the same type.
Specify the **Add Airwatch Endpoint Context Server > Server** parameters as described in the following table:

**Table 1: Adding an Airwatch Endpoint Context Server > Server Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose <strong>AirWatch</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or a hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the full URL for the Airwatch server. You can append a custom port, such as for an MDM server: <strong><a href="https://yourserver.yourcompany.com:customerportnumber">https://yourserver.yourcompany.com:customerportnumber</a></strong></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td>■ Basic</td>
</tr>
<tr>
<td></td>
<td>■ OAuth2: When you select <strong>OAuth2</strong> or <strong>Both</strong>, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>● OAuth2 Client ID</td>
</tr>
<tr>
<td></td>
<td>● OAuth2 Client Secret</td>
</tr>
<tr>
<td></td>
<td>● OAuth2 Resource URL</td>
</tr>
<tr>
<td></td>
<td>● Validate OAuth2 Credentials: <strong>Validate</strong> button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Both</strong>: Selecting <strong>Both</strong> allows you to use both Basic and OAuth2 authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user for the Airwatch endpoint context server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the Airwatch endpoint context server, then verify the password.</td>
</tr>
<tr>
<td>Verify Password</td>
<td></td>
</tr>
<tr>
<td>API Key</td>
<td>Enter the API key that is provided by the vendor.</td>
</tr>
<tr>
<td>Security Details</td>
<td>Enable to fetch endpoint security information.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable to validate the server certificate. Checking this option activates the <strong>Certificate</strong> tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Select the <strong>Enable to fetch endpoints from the server</strong> check box to enable the endpoint context server. By default, this field is disabled. The <strong>Bypass Proxy</strong> field will be enabled only if you enable this field.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>You must enable the <strong>Enable Server</strong> parameter to enable the <strong>Bypass Proxy</strong> parameter. Select the <strong>Enable to bypass proxy server</strong> check box to bypass the proxy server. When this field is enabled, the proxy servers configured in the <strong>Administration &gt; Server Manager &gt; Server Configuration &gt; Service Parameters</strong> tab &gt; <strong>ClearPass system services</strong> 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.</td>
</tr>
</tbody>
</table>
**Actions Tab**

The following figure displays the **Airwatch Add Endpoint Context Server > Actions** page:

**Figure 634** Adding an Airwatch Endpoint Context Server > Actions Page

Specify the **Airwatch Add Endpoint Context Server > Actions** parameters as described in the following table:

**Table 2: Adding an Airwatch Endpoint Context Server > Actions Tab Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Passcode</td>
<td>Reset passcode on the device.</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>Delete only stored corporate information.</td>
</tr>
<tr>
<td>Get Apps</td>
<td>Get application information for the device.</td>
</tr>
<tr>
<td>Lock Device</td>
<td>Lock the associated device.</td>
</tr>
<tr>
<td>Remote Wipe</td>
<td>Delete all stored information.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Send message to the device.</td>
</tr>
<tr>
<td>Send Message (Parameterized)</td>
<td>Send message with parameters to the device.</td>
</tr>
</tbody>
</table>

The **Imei** attribute from an Airwatch server is mapped to the **IMEI** attribute in the ClearPass Endpoint dictionary.

The **ComplianceStatus** attribute from an Airwatch server is mapped to the **Compliance** attribute in the Endpoint dictionary. The available Compliance attributes are: **NotAvailable**, **NonCompliant**, or **Compliant**.
Adding an AirWave Endpoint Context Server

For more information about AirWave, refer to Aruba AirWave documentation.

To add an AirWave Endpoint Context Server:


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 635 Add an AirWave Endpoint Context Server > Server Dialog

   ![Add Endpoint Context Server Dialog](image)

   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 1.

5. When satisfied with the settings, click Save.

Table 1: Adding an AirWave Endpoint Context Server > Server Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>1. Choose AirWave from the Select Server Type drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>2. Enter a valid server name. You can enter an IP address or hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>3. Enter the full URL for the AirWave server. You can append a custom port, such as for an MDM server: <a href="https://yourserver.yourcompany.com:customerportnumber">https://yourserver.yourcompany.com:customerportnumber</a></td>
</tr>
</tbody>
</table>
### Adding an Aruba Activate Endpoint Context Server

To add an Aruba Activate 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** page opens. This dialog opens in the **Server** tab.
3. From the **Select Server Type** drop-down, select **Aruba Activate**.
   - The **Add Aruba Activate Endpoint Context Server** page opens:

   ![Add Aruba Activate Endpoint Context Server](image)

4. Specify the **Aruba Activate Add Endpoint Context Server** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>4. Enter the username for the AirWave server.</td>
</tr>
<tr>
<td>Password</td>
<td>5. Enter the password for the server, then verify the password.</td>
</tr>
<tr>
<td>Verify Password</td>
<td></td>
</tr>
<tr>
<td>Validate Server</td>
<td>6. Enable <strong>Validate Server</strong> to validate the server certificate. Checking this option enables the <strong>Certificate</strong> tab.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>7. Enable <strong>Bypass Proxy</strong> to bypass the proxy server.</td>
</tr>
</tbody>
</table>
Table 1: Adding an Aruba Activate Endpoint Context Server > Server Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose <strong>Aruba Activate</strong> from the <strong>Select Server Type</strong> drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or a hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the complete URL for the Aruba Activate server. You can append a custom port, such as for an MDM server: <a href="https://yourserver.yourcompany.com:customerportnumber">https://yourserver.yourcompany.com:customerportnumber</a></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Basic</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2</strong>: When you select <strong>OAuth2</strong> or <strong>Both</strong>, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Client ID</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Client Secret</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Resource URL</td>
</tr>
<tr>
<td></td>
<td>- Validate OAuth2 Credentials: <strong>Validate</strong> button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Both</strong>: Selecting <strong>Both</strong> allows you to use both Basic and OAuth2 authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the Aruba Activate server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password, then verify the password.</td>
</tr>
<tr>
<td>Device Filter</td>
<td>The <strong>Device Filter</strong> field is populated with a default regular expression to retrieve only the Remote AP (RAP) and Instant AP (IAP) information.</td>
</tr>
<tr>
<td>Folder Filter</td>
<td>Set the value for <strong>Folder Filter</strong> to the Aruba Activate <strong>Folder ID</strong>.</td>
</tr>
<tr>
<td></td>
<td>To locate the <strong>Folder ID</strong> in Aruba Activate:</td>
</tr>
<tr>
<td></td>
<td>1. Log in to Aruba Activate.</td>
</tr>
<tr>
<td></td>
<td>2. Navigate to <strong>Setup</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click the folder.</td>
</tr>
<tr>
<td></td>
<td>A URL is displayed. For example:</td>
</tr>
<tr>
<td></td>
<td><a href="https://activate.arubanetworks.com/registration/#/setup/folder/detail?id=3f1229d8-cef2-4440-add4-7a28309b46ea">https://activate.arubanetworks.com/registration/#/setup/folder/detail?id=3f1229d8-cef2-4440-add4-7a28309b46ea</a></td>
</tr>
<tr>
<td></td>
<td>In this example, the folder ID is: 3f1229d8-cef2-4440-add4-7a28309b46ea</td>
</tr>
<tr>
<td></td>
<td>4. Copy the folder ID from the URL and use it to specify the value for the <strong>Folder Filter</strong> parameter.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Multiple folder IDs can be specified as comma-separated values.</td>
</tr>
<tr>
<td>Disable Stale Endpoints</td>
<td>To disable stale endpoints in the Endpoint database, enable this option.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>To validate the server certificate, enable (check) <strong>Validate Server</strong>. Checking this option enables the <strong>Certificates</strong> tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Enable <strong>Enable Server</strong> to fetch endpoints from the server.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>Enable <strong>Bypass Proxy</strong> to bypass the proxy server.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
Certificates Tab

The following figure displays the Aruba Activate Add Endpoint Context Server > Certificates tab:

Figure 637 Adding an Aruba Activate Endpoint Context Server > Certificates

Adding a Google Admin Console Endpoint Context Server

To add a Google Admin Console 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 page opens.
3. From the Select Server Type drop-down, select Google Admin Console.
   The Add Google Admin Console Endpoint Context Server page opens:

Figure 638 Add Endpoint Context Server > Google Admin Console Page
You can add more than one endpoint context server of the same type.

4. Specify the **Add Endpoint Context Server > Google Admin Console** parameters as described in the following table:

**Table 1: Add Endpoint Context Server > Google Admin Console Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose Google Admin Console from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter the server name.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Enter the client ID.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Enter the client secret.</td>
</tr>
<tr>
<td>Google API Access</td>
<td>Authenticate and authorize ClearPass for access to Google Admin APIs for your domain.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable to validate the server certificate. Checking this option enables the <strong>Certificates</strong> tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Enable this field to enable the server and fetch endpoints from the server. By default, this field is disabled. The <strong>Bypass Proxy</strong> field is enabled when you enable this field.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>To bypass the proxy server, select the Enable to bypass proxy server check box. When this field is enabled, the proxy servers configured in the Administration &gt; Server Manager &gt; Server Configuration &gt; Service Parameters tab &gt; 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.</td>
</tr>
</tbody>
</table>

**Certificates Tab**

The following figure displays the **Add Endpoint Context Server > Google Admin Console** page:

**Figure 639 Add Endpoint Context Server > Certificates > Google Admin Console**
Adding a Generic HTTP Endpoint Context Server

To add a Generic HTTP endpoint context server:

1. Navigate to Administration > External Servers > Endpoint Context Servers. The Endpoint Context Servers page opens. This page lists the server name, server type, and status of the currently configured endpoint context servers.

2. Click the Add link. The Add Endpoint Context Server dialog opens.

3. From the Select Server Type drop-down, select Generic HTTP. The Generic HTTP Add Endpoint Context Server page opens.

Figure 640 Adding a Generic HTTP Endpoint Context Server

![Add Endpoint Context Server dialog](image)

You can add more than one endpoint context server of the same type.

4. Specify the Generic HTTP Add Endpoint Context Server > Server parameters as described in the following table:

Table 1: Add Endpoint Context Server > Server > Generic HTTP Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose Generic HTTP from the Select Server Type drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or a hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the server base URL in the following format: (https://(server_ip)/api/?type=keygen&amp;user={username}&amp;password={password})</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td>- Basic</td>
</tr>
<tr>
<td></td>
<td>- OAuth2: When you select OAuth2 or Both, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Client ID</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>OAuth2 Client Secret</td>
<td>Validate OAuth2 Credentials: Validate button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td>OAuth2 Resource URL</td>
<td>Both: Selecting <strong>Both</strong> allows you to use both Basic and OAuth2 authentication.</td>
</tr>
<tr>
<td>Validate OAuth2 Credentials</td>
<td>Validate button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable <strong>Validate Server</strong> to validate the server certificate. Checking this option enables the <strong>Certificate</strong> tab.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>You must enable the <strong>Enable Server</strong> parameter to enable the <strong>Bypass Proxy</strong> parameter. Select the <strong>Enable to bypass proxy server</strong> check box to bypass the proxy server. When this field is enabled, the proxy servers configured in the Administration &gt; Server Manager &gt; Server Configuration &gt; Service Parameters tab &gt; 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.</td>
</tr>
</tbody>
</table>

5. To save your changes, click **Save**.

**Integrating ClearPass with Infoblox Endpoint Context Servers**

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 Infoblox endpoint context server:

1. Navigate to Administration > External Servers > Endpoint Context Servers.
   The Endpoint Context Servers page opens.

   **Figure 641  Endpoint Context Servers Page**

2. Click Add.
   The Add Endpoint Context Server dialog opens. This dialog opens in the Server page.

   **Figure 642  Adding an Infoblox Endpoint Context 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 opens.

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.

Figure 643  Selecting the Infoblox Server for the Endpoint Context Server Action

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:
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 644**, the following attributes are sent in JSON format to the Infoblox server:
   - Filter name "ClearPass"
   - Username and MAC addresses of the authenticated devices

**Figure 644  Attributes Sent to Infoblox Server**

![JSON attributes](image)

7. Click **Cancel**.

**Creating an Infoblox Enforcement Profile**

This section describes how to create a simple HTTP-based enforcement profile named "Infoblox Notify" that acts against the Infoblox Login action. For additional details on configuring enforcement profiles, see [Configuring Enforcement Profiles](#).

To create an Infoblox enforcement profile:

1. Navigate to **Configuration > Enforcement > Profiles**.

   The **Enforcement Profiles** page opens.

**Figure 645  Enforcement Profiles Page**

![Enforcement Profiles page](image)

2. Click **Add**.
The **Add Enforcement Profiles** dialog opens.

**Figure 646 Adding the Infoblox Enforcement Profile**

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](#).
   b. **Name**: Enter **Infoblox Notify**.
   c. **Description**: Optionally, enter a description of this enforcement profile.
   d. Click **Next**.
      The **Enforcement Profiles Attributes** page opens.

**Figure 647 Specifying the Target Server and Enforcement Action**

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.

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.

To define a RADIUS Enforcement profile:

1. Navigate to Configuration > Enforcement > Profiles.
   The Enforcement Profiles page opens.

2. Click Add.
   The Add Enforcement Profiles dialog opens.

   **Figure 648 Adding a RADIUS-Based Enforcement Profile**

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 649.
Figure 649  Adding Attributes to the RADIUS Enforcement Profile

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius:IETF</td>
<td>Tunnel-Private-Group-Id</td>
<td>data</td>
</tr>
<tr>
<td>Radius:IETF</td>
<td>Session-Timeout</td>
<td>21600</td>
</tr>
<tr>
<td>Radius:IETF</td>
<td>Tunnel-Type</td>
<td>VLAN (13)</td>
</tr>
<tr>
<td>Radius:IETF</td>
<td>Termination-Action</td>
<td>RADIUS-Request (1)</td>
</tr>
</tbody>
</table>

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.

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 opens.

**Figure 650  Adding the Infoblox Enforcement Policy**

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 opens.

4. Click **Add Rule**.
   The **Rules Editor** dialog opens.

**Figure 651  Configuring Infoblox Enforcement Policy Rules**

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**.
You must add the enforcement profiles 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 652** Summary of the Infoblox Enforcement Policy

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 653** Adding an Infoblox Wireless Service
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 654  Specifying Wireless Service Authentication Settings**

   ![Image](image_url)

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 655  Specifying the Enforcement Policy for the Service**

   ![Image](image_url)

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 656  Infoblox Server Initial Page**

2. Select the *Data Management* tab, then select the *DHCP* tab.
   The *DHCP Networks* page opens.

   **Figure 657  Adding an IPv4 Network**

3. To add a new network, click the *Plus* icon.
   The *Add IPv4 Network Wizard* begins.
4. With **Add Network** selected by default, click **Next**. The following screen appears.

**Figure 659  Specifying the Netmask**

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 (as shown in **Figure 659** above).

7. In the **Networks** field, enter the IP address of the network, then click **Next**. The **Members** screen opens.
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 661 Specifying the Lease Time (Session-Timeout Value)**

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**.

   The Lease Time value you enter here must correspond to the **Session-Timeout** value defined under Infoblox RADIUS Enforcement (see **Figure 649**).

   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.
13. Specify when you choose to create the IPv4 network, then click **Save & Close**.

The new network is created.

**Figure 663  New IPv4 Network Created**

---

**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**.

   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**).

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 664** Specifying Lease Time in the IPv4 MAC Address Filter

![Image of Lease Time configuration](image)

The **Lease Time** value entered here must correspond to the **Session-Timeout** value defined under Infoblox RADIUS Enforcement Profile (see **Session-Timeout**).

Step 3 of the IPv4 MAC Address Filter wizard opens.

**Figure 665** Specifying the MAC Address Expiration in the IPv4 MAC Address Filter

![Image of MAC Address Expiration configuration](image)

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 opens.
8. No changes are required for this step, so click **Next**.
   The **Schedule Change** dialog opens.
9. 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 Endpoint Context Server

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 a Juniper Networks SRX endpoint context server 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 endpoint context 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 endpoint context 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 opens.
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 667**).
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 1.

5. When satisfied with the settings, click **Save**.

**Table 1: Specifying Juniper Networks SRX Endpoint Context Server - Server Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose <strong>Juniper Networks SRX</strong>.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or a host name.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the full URL for the server. You can append a custom port, such as for an MDM server: <code>https://yourserver.yourcompany.com:customerportnumber</code></td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and verify the password.</td>
</tr>
<tr>
<td>Verify Password</td>
<td></td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable the <strong>Validate Server</strong> check box to validate the server certificate. Enabling this option activates the <strong>Certificate</strong> tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Enable this option to fetch endpoints from the server. Enabling this option activates the <strong>Poll Status</strong> tab.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>Enable this option to bypass the proxy server.</td>
</tr>
</tbody>
</table>
Adding a Context Server Action to the Juniper SRX Server

Figure 668 displays the Juniper Network SRX Add Endpoint Context Server > Actions page:

**Figure 668** Adding a Juniper Networks SRX Endpoint Context Server > Actions Page

Table 2 describes the endpoint context server actions that are available:

<table>
<thead>
<tr>
<th>Endpoint Context Server Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks SRX Login</td>
<td>Endpoint Context Server action to send a user or device login context to a</td>
</tr>
<tr>
<td></td>
<td>Juniper SRX server.</td>
</tr>
<tr>
<td>Juniper Networks SRX Logout</td>
<td>Endpoint Context Server action to send a user or device logout context to a</td>
</tr>
<tr>
<td></td>
<td>Juniper SRX server.</td>
</tr>
</tbody>
</table>

**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 opens.
2. Select the Juniper Networks SRX endpoint context server action of interest. The Endpoint Context Server Details dialog for the selected action is displayed.
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 670** shows the content of the Juniper Networks SRX Login action:

**Figure 670  Content for the Juniper Networks SRX Login Action**

**Figure 671** shows the content of the Juniper Networks SRX Logout action:
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 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.

To create a Juniper SRX endpoint context server enforcement profile:

1. Navigate to Configuration > Enforcement > Profiles.
   The Enforcement Profiles page opens.

   **Figure 672  Enforcement Profiles Page**

2. Click the Add link.
   The Add Enforcement Profiles dialog opens.
3. Configure the **Add Enforcement Profile** page as follows:

**Table 3: Juniper Networks SRX Endpoint Enforcement Profile Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select <strong>Session Notification Enforcement</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter <strong>Juniper SRX Notify</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally (recommended), enter a brief description of this enforcement profile.</td>
</tr>
<tr>
<td>Type</td>
<td>When you select <strong>Session Notification Enforcement</strong>, the Profile Type is set to <strong>Post-Authentication</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Next**.

   The **Add Enforcement Profiles Attributes** page opens.

   In the following steps, you will add the four Session-Notify Enforcement Profile attributes illustrated in **Figure 674**.

**Figure 674 Adding Attributes to the Enforcement Profile**

5. Select **Click to add**, then specify the **Session-Notify** attributes as described in the following table:
### Table 4: Adding Juniper SRX Endpoint Enforcement Profile Attributes

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-Notify</td>
<td>Server Type</td>
<td>Enter <em>Juniper Networks SRX</em>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Server IP</td>
<td>Enter the IP address of the Juniper Networks SRX endpoint context server.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Login Action</td>
<td>Select <em>Juniper Networks SRX Login</em>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Logout Action</td>
<td>Select <em>Juniper Networks SRX Logout</em>.</td>
</tr>
</tbody>
</table>

6. 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" enforcement profile so that external devices can authenticate against this policy.

For details on configuring enforcement policies, see Configuring Enforcement Policies.

To create a Juniper SRX endpoint context server enforcement policy:

1. Navigate to **Configuration > Enforcement > Policies**.
   
   The **Enforcement Policies** page opens.

2. Click **Add**.
   
   The **Add Enforcement Policies** dialog opens.

**Figure 675 Adding the Juniper SRX Enforcement Policy**

3. Enter the following information:
   
   a. **Name**: Enter *Juniper SRX Enforcement Policy*.
   
   b. **Description**: Optionally, enter a description of this policy.
   
   c. **Enforcement Type**: Set by default to *RADIUS*.
   
   d. **Default Profile**: Select *Deny Access Profile*.
   
   e. Click **Next**.
      
      The **Rules** page opens.

4. Click **Add Rule**.
   
   The **Rules Editor** dialog opens.
Figure 676  Configuring Juniper SRX Enforcement Policy Rules

Specify Conditions
5. In the Conditions panel, select Click to add, then enter the conditions for the rule(s) pertinent to this enforcement policy.

Specify the Enforcement Profile
6. In the Enforcement Profiles panel:
   a. Click Select to Add.
7. Click Save.
8. To view the Juniper SRX enforcement policy summary, click the Summary tab.

Figure 677  Summary of the Juniper SRX Enforcement Policy

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 an 802.1X wireless service named "Juniper SRX Wireless Service" to be applied to the "Juniper SRX Policy."

To create the Juniper SRX wireless service:
1. Navigate to Configuration > Services.
   The Services page opens.
2. Click **Add**.
   
The **Add Services** page opens.

**Figure 678  Adding a Juniper SRX Wireless Service**

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 opens.

**Figure 679  Specifying the Wireless Service Authentication Settings**

4. In the **Authentication** tab, specify the following information:
   
   a. **Authentication Methods**: Select the authentication method of choice.

      If you need an authentication method not provided from the **Select to Add** list, click the **Add new Authentication Method** link.

      This example uses **EAP MSCHAPv2** as the authentication method.

   b. **Authentication Sources**: Click **Select to Add**, then select the authentication source(s).

      This example uses [Local User Repository] [Local SQL DB] as the authentication source.

      If you need an authentication source not provided from the **Select to Add** list, click the **Add new Authentication Source** link.
c. **Strip Username Rules**: Enable this check box to specify a comma-separated list of rules in which the username or suffixes have been stripped. For example, if a username is `username@domain.com` or `domain\username`, you can enable **Strip Username Rules** to strip off `@domain.com` or `domain\`.

d. **Service Certificate**: Optionally, specify the **Service Certificate**. If the **Service Certificate** parameter is left empty, ClearPass picks the Service Certificate from the RADIUS/EAP Server Certificate. For detailed information about the selected Service Certificate, click the **View Certificate Details** link.

5. Select the **Enforcement** tab.

![Figure 680 Specifying the Enforcement Policy for the Juniper SRX Wireless Service](image)

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 you see the following message:

*Service "Juniper SRX Wireless Service" has been added*

**Adding a JAMF Endpoint Context Server**

To add a JAMF endpoint context server:

1. Navigate to **Administration > External Servers > Endpoint Context Servers**.

   The **Endpoint Context Servers** page opens. This page lists the server name, server type, and status of the currently configured endpoint context servers.

2. Click the **Add** link.

   The **Add Endpoint Context Server** dialog opens.

3. From the **Select Server Type** drop-down, select **JAMF**.

   The **Add JAMF Endpoint Context Server** dialog opens:
You can add more than one endpoint context server of the same type.

4. Specify the **Add Endpoint Context Server** > **JAMF** parameters as described in the following table:

**Table 1: Specifying JAMF Endpoint Context Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose <strong>JAMF</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the full URL for the server. You can append a custom port, such as for an MDM server: <code>https://yourserver.yourcompany.com:customerportnumber</code>.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td>Basic</td>
<td></td>
</tr>
<tr>
<td>OAuth2 or Both</td>
<td>When you select <strong>OAuth2</strong> or <strong>Both</strong>, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2 Client ID</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2 Client Secret</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2 Resource URL</strong></td>
</tr>
<tr>
<td></td>
<td>Validate <strong>OAuth2 Credentials</strong>: <strong>Validate</strong> button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the endpoint context server.</td>
</tr>
<tr>
<td>Password, Verify Password</td>
<td>Enter and verify the password for the endpoint context server.</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fetch Computer Records</td>
<td>Enable to fetch computer records from the endpoint context server.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable to validate the server certificate. Checking this option enables the Certificates tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Enable to fetch endpoints from the server. The Bypass Proxy field is enabled when you enable this field.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>Enable to bypass the proxy server. When this field is enabled, the proxy servers configured in the Administration &gt; Server Manager &gt; Server Configuration &gt; Service Parameters tab &gt; 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.</td>
</tr>
</tbody>
</table>

5. To save your changes, click **Save**.

**Adding a MaaS360 Endpoint Context Server**

To add a MaaS360 endpoint context server:

1. Navigate to Administration > External Servers > Endpoint Context Servers.
   - The Endpoint Context Servers page opens. This page lists the server name, server type, and status of the currently configured endpoint context servers.

2. Click the **Add** link.
   - The Add Endpoint Context Server dialog opens.

3. From the **Select Server Type** drop-down, select MaaS360.
   - The Add MaaS360 Endpoint Context Server dialog opens:

   ![Add MaaS360 Endpoint Context Server Dialog](image)

   You can add more than one endpoint context server of the same type.

---

ClearPass 6.7 Policy Manager | User Guide
Administration | 660
4. Specify the **Add MaaS360 Endpoint Context Server** parameters as described in the following table:

**Table 1: Add MaaS360 Endpoint Context Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose <strong>MaaS360</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the full URL for the server. You can append a custom port, such as for an MDM server: <a href="https://yourserver.yourcompany.com:customerportnumber">https://yourserver.yourcompany.com:customerportnumber</a>.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Basic</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2</strong>: When you select <strong>OAuth2</strong> or <strong>Both</strong>, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2 Client ID</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2 Client Secret</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>OAuth2 Resource URL</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Validate OAuth2 Credentials</strong> button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the endpoint context server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and verify the password for the endpoint context server.</td>
</tr>
<tr>
<td>Verify Password</td>
<td></td>
</tr>
<tr>
<td>Application Access Key</td>
<td>Enter the application access key (API key), then verify it.</td>
</tr>
<tr>
<td>Application ID</td>
<td>Enter the application ID.</td>
</tr>
<tr>
<td>Application Version</td>
<td>Enter the application version number.</td>
</tr>
<tr>
<td>Platform ID</td>
<td>Enter the Platform ID.</td>
</tr>
<tr>
<td>Billing ID</td>
<td>Enter the Billing ID.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable to validate the server certificate. Checking this option enables the <strong>Certificates</strong> tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Enable to fetch endpoints from the server.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>Enable to bypass the proxy server.</td>
</tr>
</tbody>
</table>
Actions Page

The following figure displays the MaaS360 Endpoint Context Server Actions page:

**Figure 683** MaaS360 Endpoint Context Server Actions Page

The following table shows the MaaS360 Endpoint Context Server Actions:

**Table 2: MaaS360 Endpoint Context Server Actions**

<table>
<thead>
<tr>
<th>Endpoint Context Server Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve Device in Messaging System</td>
<td>Approve the device in Messaging System.</td>
</tr>
<tr>
<td>Block Device in Messaging System</td>
<td>Block the device in Messaging System.</td>
</tr>
<tr>
<td>Cancel Pending Wipe</td>
<td>Cancel outstanding Remote Wipe sent to the device.</td>
</tr>
<tr>
<td>Change Device Policy</td>
<td>Assign a given policy to a device.</td>
</tr>
<tr>
<td>Check Action Status</td>
<td>Check the status of a prior executed action.</td>
</tr>
<tr>
<td>Locate Device</td>
<td>Get current or last know location of the device.</td>
</tr>
<tr>
<td>Lock Device</td>
<td>Lock the device.</td>
</tr>
<tr>
<td>Refresh Device</td>
<td>Create a request to refresh the device information.</td>
</tr>
<tr>
<td>Remove Device</td>
<td>Mark the device as inactive.</td>
</tr>
<tr>
<td>Reset Device Passcode</td>
<td>Reset the pass code on the device.</td>
</tr>
<tr>
<td>Revoke Selective Wipe</td>
<td>Cancel Selective Wipe executed on the device.</td>
</tr>
<tr>
<td>Endpoint Context Server Actions</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Search Action History</td>
<td>Search action history by Device ID.</td>
</tr>
<tr>
<td>Selective Wipe Device</td>
<td>Execute a Selective Wipe on a device.</td>
</tr>
<tr>
<td>Wipe Device</td>
<td>Delete all information stored on a device.</td>
</tr>
</tbody>
</table>

### 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:

2. Click Add.
3. The Add Endpoint Context Server dialog opens to the Server tab.
4. From the Select Server Type drop-down, select MobileIron.

#### Server Page

The following figure displays the MobileIron Add Endpoint Context Server > Server page:

**Figure 684 Adding a MobileIron Endpoint Context Server > Server Page**

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 1.
Table 1: Adding a MobileIron Endpoint Context Server > Server Page Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose MobileIron from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or host name.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the full URL for the server. You can append a custom port, such as for an MDM server: <a href="https://yourserver.yourcompany.com:customerportnumber">https://yourserver.yourcompany.com:customerportnumber</a></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td>- Basic</td>
</tr>
<tr>
<td></td>
<td>- OAuth2: When you select OAuth2 or Both, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Client ID</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Client Secret</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Resource URL</td>
</tr>
<tr>
<td></td>
<td>- Validate OAuth2 Credentials: Validate button: When you click Validate, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td></td>
<td>- Both: Selecting Both allows you to use both Basic and OAuth2 authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the MobileIron endpoint context server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the MobileIron endpoint context server, then verify the password.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable to validate the server certificate. Checking this option enables the Certificate tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>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 is enabled when you enable this field.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>You must enable the Enable Server parameter to enable the Bypass Proxy parameter. 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 &gt; Server Manager &gt; Server Configuration &gt; Service Parameters tab &gt; 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.</td>
</tr>
</tbody>
</table>

5. When satisfied with the settings, click Save.
**Actions Page**

The following figure displays the MobileIron Add Endpoint Context Server > Actions page:

**Figure 685** Adding a MobileIron Endpoint Context Server > Actions Page

![Add Endpoint Context Server](image)

Table 2 describes the Endpoint Context Server Actions that are available:

**Table 2: Adding a MobileIron Endpoint Context Server > Actions**

<table>
<thead>
<tr>
<th>Actions</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Label to Device</td>
<td>Applies label to identify when devices have attached to corporate Wi-Fi and apply corresponding policies.</td>
</tr>
<tr>
<td>Get Labels</td>
<td>Gets labels information of the device.</td>
</tr>
<tr>
<td>Lock Device</td>
<td>Locks the device.</td>
</tr>
<tr>
<td>Remote Wipe</td>
<td>Deletes all information stored on the device.</td>
</tr>
<tr>
<td>Remove Label from Device</td>
<td>Removes label and corresponding policies.</td>
</tr>
<tr>
<td>Retire/Enterprise Wipe (Device MAC Address)</td>
<td>Deletes only corporate information stored and remove device from MDM management.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Sends message to the device.</td>
</tr>
<tr>
<td>Send Push Notification (UUID)</td>
<td>Sends Push Notification message using UUID:</td>
</tr>
<tr>
<td></td>
<td>- APNs for Apple iOS</td>
</tr>
<tr>
<td></td>
<td>- C2DM GCM for Google Android</td>
</tr>
<tr>
<td></td>
<td>- WNS for Windows 8.1</td>
</tr>
</tbody>
</table>
### Actions

<table>
<thead>
<tr>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send SMS (UUID)</td>
</tr>
<tr>
<td>Sends SMS Message (cellular devices only) using UUID</td>
</tr>
<tr>
<td>Unlock Device</td>
</tr>
<tr>
<td>Unlocks the device.</td>
</tr>
<tr>
<td>Wake-up Device (Device MAC Address)</td>
</tr>
<tr>
<td>Sends wake-up to device, request check-in.</td>
</tr>
<tr>
<td>Wake-up Device (UUID)</td>
</tr>
<tr>
<td>Sends wake-up to device, request check-in.</td>
</tr>
</tbody>
</table>

6. **Click** Save.

Endpoints fetched from a MobileIron MDM server will have the `Compliance` attribute set to **True** if the device is compliant. If the device is not compliant, the `Compliance` attribute is set to **False**.

### Integrating ClearPass with Palo Alto Networks Firewall Endpoint Context Server

This feature provides admins with the ability to customize the context server action content for Palo Alto Networks Firewall endpoint context servers.

Integrating ClearPass with Palo Alto Networks Firewall endpoint context servers 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 Palo Alto Networks Firewall endpoint context 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 Palo Alto Networks Firewall endpoint context server.

This section provides the following information:

- Adding a Palo Alto Networks Firewall Endpoint Context Server
- Creating a Palo Alto Networks Firewall Enforcement Profile
- Creating a Palo Alto Networks Firewall Enforcement Policy
- Defining a Palo Alto Networks Firewall Wireless Service

**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. This page lists the server name, server type, and status of the currently configured endpoint context servers.
2. Click the **Add** link. 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 686).
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 1.
5. When satisfied with the settings, click Save.

Table 1: Add Endpoint Context Server > Palo Alto Networks Firewall Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose Palo Alto Networks Firewall from the drop-down.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter the IPv4 or IPv6 address/hostname of the Palo Alto Networks server.</td>
</tr>
</tbody>
</table>
| Server Base URL                        | Enter the server base URL in the following format:  
  https://{server_ip}/api/?type=keygen&user={username}&password={password}          |
<p>| Authentication Method                   | Select one of the following authentication methods:                                |
|                                        | Basic                                                                             |
|                                        | OAuth2: When you select OAuth2 or Both, the following fields are displayed:       |
|                                        |   OAuth2 Client ID                                                                |
|                                        |   OAuth2 Client Secret                                                            |
|                                        |   OAuth2 Resource URL                                                             |
|                                        |   Validate OAuth2 Credentials: Validate button: When you click Validate, ClearPass|
|                                        |     retrieves a bearer token in order to validate whether the OAuth token server  |
|                                        |     is reachable and the credentials are correct. If the credentials are not     |
|                                        |     correct, an error message is displayed.                                       |
|                                        | Both: Selecting Both allows you to use both Basic and OAuth2 authentication.      |
| Username                               | Enter the username.                                                               |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Verify Password</td>
<td>Enter the password, then verify the password.</td>
</tr>
<tr>
<td>Username Transformation</td>
<td>Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>: Do not use any username transformation.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Prefix NetBIOS name</strong>: Use the Prefix NetBIOS name in UID updates.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Use Full Username</strong>: Use the full username in UID updates.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Select this check box to validate the server certificate. Checking this option enables the Certificate tab.</td>
</tr>
</tbody>
</table>

**Add Endpoint Context Server > Actions Page**

When you select the **Add Endpoint Context Server > Actions** tab, the **Actions** page lists the set of server actions that can be performed on the Palo Alto Networks Firewall endpoint context server. The server actions that are displayed in the **Actions** page vary depending on which **Server Type** you select.

**Figure 687** Default Palo Alto Networks Firewall Endpoint Context Server Actions

The following table describes the endpoint context server actions that are available for the Palo Alto Networks Firewall endpoint context server:

**Table 2**: Palo Alto Networks Firewall Endpoint Context Server Actions

<table>
<thead>
<tr>
<th>Endpoint Context Server Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register Device</td>
<td>Registers device category information.</td>
</tr>
<tr>
<td>Unregister Device</td>
<td>Unregisters device category information.</td>
</tr>
<tr>
<td>Register Posture</td>
<td>Registers posture status for the endpoint.</td>
</tr>
<tr>
<td>Endpoint Context Server Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Unregister Posture</strong></td>
<td>Unregisters posture status for the endpoint.</td>
</tr>
<tr>
<td><strong>Register Role</strong></td>
<td>Registers Role information for the user.</td>
</tr>
<tr>
<td><strong>Unregister Role</strong></td>
<td>Unregisters Role information for the user.</td>
</tr>
<tr>
<td><strong>Send HIP Report (Global Protect)</strong></td>
<td>Sends HIP (Host Information Profiles) report data for the user enabled by the GlobalProtect feature on the Palo Alto Networks Firewall endpoint context server. <strong>NOTE:</strong> You must enable the GlobalProtect license on the firewall for this to be operable.</td>
</tr>
<tr>
<td><strong>Send Login Info</strong></td>
<td>Sends login Information for the user.</td>
</tr>
<tr>
<td><strong>Send Logout Info</strong></td>
<td>Sends logout Information for the user,</td>
</tr>
</tbody>
</table>

**Adding the Endpoint Repository as an Authorization Source**

For this feature to work properly, the Endpoint Repository must be added as an authorization source and one of the Profile attributes must be enabled as *Role*.

To add the Endpoint Repository as an authorization source:

1. Navigate to **Configuration > Authentication > Sources**. The Authentication Sources page is displayed.
2. Select *Endpoints Repository*.
3. From the Authentication Sources - [Endpoints Repository] page, select the Attributes tab.

---

**NOTE:** The Register Posture endpoint context server action requires that the Eager handler polling frequency parameter must be 120 seconds or more.

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. From the list of ClearPass server, select the Publisher node, then select the Service Parameters tab.
3. From the Select Service drop-down, select the Async network services service (which is selected by default).
4. In the Post Auth section, set the Eager handler polling frequency parameter to a value 120 seconds or more, then click Save.
Creating a Palo Alto Networks Firewall Enforcement Profile

This section describes how to create a session-notification enforcement profile named "Palo Alto Networks Firewall Notify."

For details on configuring enforcement profiles, see Configuring Enforcement Profiles.

To create a Palo Alto Networks Firewall enforcement profile:

1. Navigate to Configuration > Enforcement > Profiles.
   The Enforcement Profiles page opens.
2. Click the **Add** link. The **Add Enforcement Profiles** dialog opens.

**Figure 689 Enforcement Profiles Page**

![Enforcement Profiles Page](image)

3. Configure the **Add Enforcement Profile** page as follows:

**Table 3: Palo Alto Networks Endpoint Enforcement Profile Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select <strong>Session Notification Enforcement</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter <strong>Palo Alto Networks Firewall Notify Profile</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally (recommended), enter a brief description of this enforcement profile.</td>
</tr>
<tr>
<td>Type</td>
<td>When you select <strong>Session Notification Enforcement</strong>, the Profile Type is set to <strong>Post-Authentication</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Next**. The **Add Enforcement Profiles Attributes** page opens. In the following steps, you will add the **Session-Notify** Enforcement Profile attributes illustrated in **Table 4**.
5. Select **Click to add**, then specify the **Session-Notify** attributes as described in **Table 4**:

**Table 4: Adding Palo Alto Networks Firewall Endpoint Enforcement Profile Attributes**

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-Notify</td>
<td>Server Type</td>
<td>Enter <strong>Palo Alto Networks Firewall</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Server IP</td>
<td>Enter the IP address of the Palo Alto Networks endpoint context server.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Login Action</td>
<td>Select <strong>Send Login Info</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Login Action</td>
<td>Select <strong>Register Device</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Login Action</td>
<td>Select <strong>Send HIP Report (Global Protect)</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Login Action</td>
<td>Select <strong>Register Role</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Login Action</td>
<td>Select <strong>Register Posture</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Logout Action</td>
<td>Select <strong>Unregister Role</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Logout Action</td>
<td>Select <strong>Unregister Device</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Logout Action</td>
<td>Select <strong>Unregister Posture</strong>.</td>
</tr>
<tr>
<td>Session-Notify</td>
<td>Logout Action</td>
<td>Select <strong>Send Logout Info</strong>.</td>
</tr>
</tbody>
</table>

**Figure 691**  *Palo Alto Networks Firewall Enforcement Profile Attributes Entered into Profile*

6. Click **Save**.

You return to the **Enforcement Profiles** page, where the new Palo Alto Networks Notify enforcement profile is now listed.
Creating a Palo Alto Networks Firewall Enforcement Policy

This section describes how to create an enforcement policy to act against the "Palo Alto Networks Firewall Notify" enforcement profile so that external devices can authenticate against this policy.

For details on configuring enforcement policies, see Configuring Enforcement Policies.

To create a Palo Alto Networks Firewall endpoint context server enforcement policy:

1. Navigate to Configuration > Enforcement > Policies.
   The Enforcement Policies page opens.

2. Click the Add link.
   The Add Enforcement Policies dialog opens.

   **Figure 692 Adding the Palo Alto Networks Firewall Enforcement Policy**

3. Enter the following information:
   a. Name: Enter Palo Alto Networks Firewall Enforcement Policy.
   b. Description: Optionally, enter a description of this policy.
   c. Enforcement Type: Set by default to RADIUS.
   d. Default Profile: Select Deny Access Profile.
   e. Click Next.
      The Rules page opens.

4. Click Add Rule.
   The Rules Editor dialog opens.

   **Figure 693 Specifying the Enforcement Profile**

5. In the Conditions panel, select Click to add, then enter the conditions for the rule(s) pertinent to this enforcement policy.
6. In the Enforcement Profiles panel:
   a. Click Select to Add.
7. Click Save.
8. To view the enforcement policy summary, click the Summary tab.

**Figure 694  Summary of the Enforcement Policy**

**Defining a Palo Alto Networks Firewall Wireless Service**

This section describes how to create an 802.1X wireless service named "Palo Alto Networks Wireless Service" to be applied to the "Palo Alto Networks Firewall Enforcement Policy."

To create the Palo Alto Networks wireless service:

1. Navigate to Configuration > Services.
   The Services page opens.
2. Click the Add link.
   The Add Services page opens.

**Figure 695  Adding a Palo Alto Networks Wireless Service**

3. In the Service tab, specify the following information:
   a. **Type**: Select 802.1X Wireless.
   b. **Name**: Enter Palo Alto Networks 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 opens.

**Figure 696  Specifying the Wireless Service Authentication Settings**

![Authentication Settings](image)

4. In the **Authentication** tab, specify the following information:
   a. **Authentication Methods**: Select the authentication method of choice.
      If you need an authentication method not provided from the **Select to Add** list, click the **Add new Authentication Method** link.
      This example uses **EAP MSCHAPv2** as the authentication method.
   b. **Authentication Sources**: Click **Select to Add**, then select the authentication source(s).
      This example uses **[Local User Repository] [Local SQL DB]** as the authentication source.
      If you need an authentication source not provided from the **Select to Add** list, click the **Add new Authentication Source** link.
   c. **Strip Username Rules**: Enable this check box to specify a comma-separated list of rules in which the username or suffixes have been stripped. For example, if a username is `username@domain.com` or `domain\username`, you can enable **Strip Username Rules** to strip off `@domain.com` or `domain\`.
   d. **Service Certificate**: Optionally, specify the **Service Certificate**. If the **Service Certificate** parameter is left empty, ClearPass picks the Service Certificate from the RADIUS Server/EAP Certificate.
      For detailed information about the selected Service Certificate, click the **View Certificate Details** link.

5. Select the **Enforcement** tab.

**Figure 697  Specifying the Enforcement Policy for the Palo Alto Networks Wireless Service**

![Enforcement Policy](image)
6. From the Enforcement Policy drop-down, select Palo Alto Networks Enforcement Policy, then click Next.

The Palo Alto Networks Wireless Service Summary is displayed.

Figure 698  Summary of the Palo Alto Networks Wireless Service

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 you see the following message:

Service "Palo Alto Networks Wireless Service" has been added

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:
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 1.
5. When satisfied with the settings, click Save.

Table 1: Add Endpoint Context Server > Palo Alto Networks Panorama Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose Palo Alto Networks Panorama from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the server base URL in the following format: https://{server_ip}/api/?type=keygen&amp;user={username}&amp;password={password}</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter and verify the password.</td>
</tr>
<tr>
<td>Verify Password</td>
<td></td>
</tr>
<tr>
<td>Username Transformation</td>
<td>Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong>: Do not use any username transformation.</td>
</tr>
<tr>
<td></td>
<td><strong>Prefix NETBIOS name</strong>: Prefix NetBIOS name in UID updates.</td>
</tr>
<tr>
<td></td>
<td><strong>Use Full Username</strong>: Use full username in UID updates.</td>
</tr>
<tr>
<td>GlobalProtect</td>
<td>Enable to send HIP report to firewall. GlobalProtect license should be enabled on firewall for this to work.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ClearPass Profiler</td>
<td>Select this check box to enable sending of endpoint profile information. This parameter is enabled by default.</td>
</tr>
<tr>
<td>ClearPass Role</td>
<td>Select this check box to enable sending of the applicable role information.</td>
</tr>
<tr>
<td>Palo Alto Firewall Serial Numbers</td>
<td>Enter the Palo Alto firewall serial numbers.</td>
</tr>
<tr>
<td>UserID Post URL</td>
<td>Enter the user ID post URL in the following format: https://[server_ip]/api/?type=user-id&amp;action=set&amp;key={key}&amp;cmd={cmd}</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable to validate the server certificate. Checking this option enables the Certificate tab.</td>
</tr>
</tbody>
</table>

**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 SAP Afaria Endpoint Context Server**

Consult SAP Afaria's documentation for additional information about the parameters that you must enter to configure this endpoint.

To add a SAP Afaria 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 to the Server tab.

3. From the Select Server Type drop-down, select SAP Afaria.
**Server Tab**

The following figure displays the **Add Endpoint Context Server > Server** page:

**Figure 700  Add Endpoint Context Server > Server Page**

---

**Note:**
You can add more than one endpoint context server of the same type.

---

The following table describes the **Add SAP Afaria Endpoint Context Server** parameters:

**Table 1: Add SAP Afaria Endpoint Context Server > Server Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose <strong>SAP Afaria</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or a hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the full URL for the server. You can append a custom port, such as for an MDM server: <code>https://yourserver.yourcompany.com:customerportnumber</code>.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td><strong>Basic</strong></td>
</tr>
<tr>
<td></td>
<td><strong>OAuth2</strong>: When you select <strong>OAuth2</strong> or <strong>Both</strong>, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Client ID</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Client Secret</td>
</tr>
<tr>
<td></td>
<td>- OAuth2 Resource URL</td>
</tr>
<tr>
<td></td>
<td>Validate OAuth2 Credentials: <strong>Validate</strong> button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Both</strong>: Selecting <strong>Both</strong> allows you to use both Basic and OAuth2 authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the server password, then verify the password.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Enable to validate the server certificate. Checking this option enables the Certificate tab.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable this parameter to fetch endpoints from the server. When you enable the Enable Server parameter, you enable the Bypass Proxy parameter.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>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 &gt; Server Manager &gt; Server Configuration &gt; Service Parameters tab &gt; 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.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td></td>
</tr>
</tbody>
</table>

**Actions Tab**

The following figure displays the Add SAP Afaria Endpoint Context Server > Actions page:

**Figure 701 Add SAP Afaria Endpoint Context Server > Actions Page**

The following table describes the Add SAP Afaria Endpoint Context Server > Actions:

**Table 2: Add SAP Afaria Endpoint Context Server > Actions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Wipe</td>
<td>Deletes only corporate information.</td>
</tr>
<tr>
<td>Lock Device</td>
<td>Locks the associated device.</td>
</tr>
<tr>
<td>Remote Wipe</td>
<td>Deletes all stored information.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Sends a message to the device.</td>
</tr>
</tbody>
</table>

**Adding a SOTI Endpoint Context Server**

Consult the SOTI MobiControl endpoint documentation for additional information about the parameters that you must enter to configure this endpoint.

To add a SOTI Endpoint Context server:

2. Click Add. The Add Endpoint Context Server dialog opens.

3. From the Select Server Type drop-down, select SOTI. The SOTI Add Endpoint Context Server dialog opens:

   **Figure 702 Adding a SOTI Endpoint Context Server**

   ![Add Endpoint Context Server Dialog](image)

   You can add more than one endpoint context server of the same type.

4. Specify the SOTI Add Endpoint Context Server parameters as described in the following table:

   **Table 1: Adding a SOTI Endpoint Context Server > Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose SOTI from the Select Server Type drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or a hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the complete URL for the SOTI server. You can append a custom port, such as for an MDM server: <code>https://yourserver.yourcompany.com:customerportnumber</code></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td>▪ Basic</td>
</tr>
<tr>
<td></td>
<td>▪ OAuth2: When you select OAuth2 or Both, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>▪ OAuth2 Client ID</td>
</tr>
<tr>
<td></td>
<td>▪ OAuth2 Client Secret</td>
</tr>
<tr>
<td></td>
<td>▪ OAuth2 Resource URL</td>
</tr>
<tr>
<td></td>
<td>▪ Validate OAuth2 Credentials: Validate button: When you click Validate, ClearPass retrieves a bearer token in order to validate whether the OAuth</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td></td>
<td>■ Both: Selecting Both allows you to use both Basic and OAuth2 authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the SOTI server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the SOTI server, then verify it.</td>
</tr>
<tr>
<td>Group ID</td>
<td>Optionally, enter the group ID.</td>
</tr>
<tr>
<td>Validate Server</td>
<td>To validate the server certificate, enable Validate Server. Enabling this option enables the Certificate tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>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 is enabled when you enable this field.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>You must enable the Enable Server parameter to enable the Bypass Proxy parameter. 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 &gt; Server Manager &gt; Server Configuration &gt; Service Parameters tab &gt; 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.</td>
</tr>
</tbody>
</table>

5. 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.

To add a XenMobile 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 **XenMobile**. The **XenMobile Add Endpoint Context Server > Server** page opens:
Figure 703  Add XenMobile Endpoint Context Server Page

You can add more than one endpoint context server of the same type.

4. Specify the **Add Endpoint Context Server** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Type</td>
<td>Choose <em>XenMobile</em> from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a valid server name. You can enter an IP address or hostname.</td>
</tr>
<tr>
<td>Server Base URL</td>
<td>Enter the server base URL in the following format: https://(server_ip)/api/?type=keygen&amp;user=(username)&amp;password=(password)</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select one of the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td><strong>Basic</strong></td>
</tr>
<tr>
<td></td>
<td><strong>OAuth2</strong>: When you select <strong>OAuth2</strong> or <strong>Both</strong>, the following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>● OAuth2 Client ID</td>
</tr>
<tr>
<td></td>
<td>● OAuth2 Client Secret</td>
</tr>
<tr>
<td></td>
<td>● OAuth2 Resource URL</td>
</tr>
<tr>
<td></td>
<td>Validate OAuth2 Credentials: <strong>Validate</strong> button: When you click <strong>Validate</strong>, ClearPass retrieves a bearer token in order to validate whether the OAuth token server is reachable and the credentials are correct. If the credentials are not correct, an error message is displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Both</strong>: Selecting <strong>Both</strong> allows you to use both Basic and OAuth2 authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to log in to the XenMobile server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to the XenMobile server, then verify the password.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Validate Server</td>
<td>Enable to validate the server certificate. Checking this option enables the Certificate tab.</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Select the <strong>Enable to fetch endpoints from the server</strong> check box to enable the endpoint context server. By default, this field is disabled. The <strong>Bypass Proxy</strong> field is enabled when you enable this field.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>You must enable the <strong>Enable Server</strong> parameter to enable the <strong>Bypass Proxy</strong> parameter. Select the <strong>Enable to bypass proxy server</strong> check box to bypass the proxy server. When this field is enabled, the proxy servers configured in the Administration &gt; Server Manager &gt; Server Configuration &gt; Service Parameters tab &gt; 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.</td>
</tr>
</tbody>
</table>

**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 704  File Backup Servers - Add File Backup Server Page**

The following table describes the **Add File Backup Server** page parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the name or IP address of the host.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description that provides additional information about the File Backup server.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specify the protocol to be used to upload the generated reports to an external server. You can select from the following protocols: <strong>SFTP (SSH File Transfer Protocol)</strong>, <strong>SCP (Session Control Protocol)</strong></td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port number. The default port is 22.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name and password of the host server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the user name of the host server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Enter the password of the host server.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specify the timeout value in seconds. The default value is 30 seconds.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>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 <strong>ClearPass Servers</strong> field.</td>
</tr>
<tr>
<td>ClearPass Servers</td>
<td>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 <strong>Select to Add</strong> drop-down list.</td>
</tr>
</tbody>
</table>

**Certificate Store**

This section describes the following topics:

- **About the Certificate Store**
- **Viewing the Server Certificates**
- **Creating and Installing a Self-Signed Server Certificate**
- **Creating a Certificate Signing Request**
- **Importing a Server Certificate**
- **Exporting a Server Certificate**
- **Service Certificates**

**About the Certificate Store**

ClearPass Policy Manager supports multiple RADIUS server certificates. You can tie different server certificates to different ClearPass services (for example, Service A can use RADIUS/EAP server certificate A, while Service B can use RadSec server certificate B).

The Certificate Store allows you to view the Server Certificates, create, modify, delete, and view Certificate Signing Requests (CSRs), as well as import and export CSRs.

A root certificate is a public key certificate that identifies a root certificate authority (CA). A root certificate is the top-most certificate of the certificate tree structure.

**Viewing the Server Certificates**

- **RADIUS/EAP Server Certificate**
- **HTTPS Server Certificate**
- **RadSec Server Certificate**

The **Server Certificates** page displays the parameters configured when a self-signed certificate has been created and installed on a ClearPass server. The **RADIUS/EAP Server Certificate** is selected by default.

The ClearPass Certificate Store provides three types of server certificates.

- **RADIUS/EAP Server Certificate**
- **HTTPS Server Certificate**
- **RadSec Server Certificate**

The availability of three certificate types (internally signed and publicly signed) provides deployment flexibility.
To view the Server Certificates available for the current ClearPass server:

1. Navigate to **Administration > Certificates > Certificate Store**.

   The **Certificate Store** page opens to the **Server Certificate** tab:

   **Figure 705 Certificate Store > Server Certificates Page**

---

### RADIUS/EAP Server Certificate

The following table provides a summary of the **RADIUS/EAP Server Certificate** parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server</td>
<td>Select a ClearPass server in the cluster for server certificate operations.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> From the Publisher node, you can select the Publisher or any of the Subscriber nodes.</td>
<td></td>
</tr>
<tr>
<td>Select Type</td>
<td>Select <strong>RADIUS/EAP Server Certificate</strong>.</td>
</tr>
<tr>
<td>Subject</td>
<td>Displays the Organization and Common Name.</td>
</tr>
<tr>
<td>Issued by</td>
<td>Displays the Organization and Common Name that issued this certificate.</td>
</tr>
<tr>
<td>Issue Date</td>
<td>Displays the date the self-signed certificate is installed.</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>Displays the date (in days) when the self-signed certificate expires.</td>
</tr>
<tr>
<td>Validity Status</td>
<td>Displays the validity status of the self-signed certificate: Valid or Invalid.</td>
</tr>
</tbody>
</table>

**Viewing Server Certificate Details**

Click the **View Details** button to view details about the certificate, such as signature algorithm, subject public key Info, etc.

To view the Server Certificate details:

1. Navigate to **Administration > Certificates > Certificate Store**.
The Server Certificate summary information is displayed.

2. Click **View Details**.
   
The **Certificate Details** window opens.

**Figure 706 Server Certificate Details**

3. When finished viewing the information, click **Close**.

**HTTPS Server Certificate**

The **HTTPS Server Certificate** page displays the parameters configured after a self-signed certificate with an HTTPS Server Certificate has been created and installed.

With an HTTPS connection, all communications are securely encrypted. The major benefits of an HTTPS certificate are:

- Customer information (such as credit card numbers) is encrypted and cannot be intercepted.
- Visitors can verify you are a registered business and that you own the domain.
- Customers are more likely to trust and complete transactions from sites that use HTTPS.

To access the HTTPS Server Certificate:

1. Navigate to the **Administration > Certificate Store > Server Certificates** tab.
2. From the **Select Type** drop-down, choose **HTTPS Server Certificate**.
   
The **HTTPS Server Certificate** page opens.
The following table describes the HTTPS Server Certificate parameters:

**Table 2: HTTPS Server Certificate Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server</td>
<td>Select a ClearPass server in the cluster for server certificate operations.</td>
</tr>
<tr>
<td>Select Type</td>
<td>Select HTTPS Server Certificate.</td>
</tr>
<tr>
<td>Subject</td>
<td>Displays the Organization and Common Name.</td>
</tr>
<tr>
<td>Issued by</td>
<td>Displays the Organization and Common Name that issued the server certificate.</td>
</tr>
<tr>
<td>Issue Date</td>
<td>Displays the date the self-signed certificate is installed.</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>Displays the date when the self-signed certificate expires.</td>
</tr>
<tr>
<td>Validity Status</td>
<td>Displays the validity status of the self-signed certificate.</td>
</tr>
<tr>
<td>Details</td>
<td>To view details about the certificate, such as Signature Algorithm and Subject Public Key Info, click the View Details button.</td>
</tr>
</tbody>
</table>

**RadSec Server Certificate**

RADIOS-over-TLS (Transport Layer Security), or RadSec, employs a TLS tunnel to enable secure communication between the controller and a ClearPass server.

Employing RADIOS communication over TLS increases the level of security for authentication. When configured, the RadSec protocol is used to safely transmit authentication and accounting data across the network.

To access the RadSec Server Certificate:

1. Navigate to the Administration > Certificate Store > Server Certificates tab.
2. From the Select Type drop-down, choose RadSec Server Certificate.

The RadSec Server Certificate page opens.
The following table describes the **RadSec Server Certificate** parameters:

**Table 3: Summary of RadSec Server Certificate Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server</td>
<td>Select a ClearPass server in the cluster for server certificate operations.</td>
</tr>
<tr>
<td>Select Type</td>
<td>Select <strong>RadSec Server Certificate</strong>.</td>
</tr>
<tr>
<td>Subject</td>
<td>Displays the Organization and Common Name.</td>
</tr>
<tr>
<td>Issued by</td>
<td>Displays the Organization and Common Name that issued this certificate.</td>
</tr>
<tr>
<td>Issue Date</td>
<td>Displays the date the self-signed certificate is installed.</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>Displays the date (in days) when the self-signed certificate expires.</td>
</tr>
<tr>
<td>Validity Status</td>
<td>Displays the validity status of the self-signed certificate: <em>Valid</em> or <em>Invalid</em>.</td>
</tr>
</tbody>
</table>

### Creating and Installing a Self-Signed Server Certificate

After you select a server and a certificate type, you can create and install a self-signed server certificate.

When Common Criteria mode is enabled, the **Create-Self Signed Certificate** option for both HTTPS and RADIUS certificates is not available from the **Certificate Store** page (for more information, see [Common Criteria Mode Parameter](#)).

### Creating a Self-Signed Server Certificate

To create a self-signed server certificate:

1. Navigate to **Administration > Certificates > Certificate Store**.
2. Select a server.
3. Click the **Create Self-Signed Certificate** link.

The **Create Self-Signed Certificate** dialog opens.
Figure 709 Creating a Self-Signed Server Certificate

4. Configure the **Create Self-Signed Certificate** parameters as described in **Table 1**.

**Table 1: Specifying Self-Signed Server Certificate Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Type</td>
<td>Select <strong>Server Certificate</strong>.</td>
</tr>
<tr>
<td>Server</td>
<td>Displays the name of the selected ClearPass server on the <strong>Certificate Store</strong> page.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the selected certificate type for the server on the <strong>Certificate Store</strong> page.</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>Enter the name associated with this entity. This can be a host name, IP address, or other meaningful name. This field is mandatory.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Enter the name of the organization. This field is optional.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Enter the name of the department, division, section, or other meaningful name. This field is optional.</td>
</tr>
<tr>
<td>Location (L)</td>
<td>Enter the name of the location, state, country, and/or other meaningful location information. These fields are optional.</td>
</tr>
<tr>
<td>State (ST)</td>
<td></td>
</tr>
<tr>
<td>Country (C)</td>
<td></td>
</tr>
<tr>
<td>Subject Alternate Name (SAN)</td>
<td>Enter the alternative name for the specified Common Name. This field is optional. Enter the Subject Alternate Name in one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>- email: email_address</td>
</tr>
<tr>
<td></td>
<td>- URI: uri</td>
</tr>
<tr>
<td></td>
<td>- IP: ip_address</td>
</tr>
<tr>
<td></td>
<td>- dns: dns_name</td>
</tr>
<tr>
<td></td>
<td>- rid: id</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Private Key Password</td>
<td>Enter the Private Key password, then verify the password.</td>
</tr>
<tr>
<td>Private Key Type</td>
<td>Select the length for the generated private key types from the following options:</td>
</tr>
<tr>
<td></td>
<td>• 1024-bit RSA</td>
</tr>
<tr>
<td></td>
<td>• 2048-bit RSA</td>
</tr>
<tr>
<td></td>
<td>• 4096-bit RSA</td>
</tr>
<tr>
<td></td>
<td>• X9.62/SECG curve over a 256 bit prime field</td>
</tr>
<tr>
<td></td>
<td>• NIST/SECG curve over a 384 bit prime field</td>
</tr>
<tr>
<td></td>
<td>The default private key type is <strong>2048-bit RSA</strong>.</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>Select the message digest algorithm from the following options:</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td></td>
<td>• SHA-1</td>
</tr>
<tr>
<td></td>
<td>• SHA-224</td>
</tr>
<tr>
<td></td>
<td>• SHA-256</td>
</tr>
<tr>
<td></td>
<td>• SHA-384</td>
</tr>
<tr>
<td></td>
<td>• SHA-512</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The <strong>MD5</strong> algorithm is not available in <strong>FIPS</strong> mode.</td>
</tr>
<tr>
<td>Valid for</td>
<td>Enter the certificate duration in number of days. The default is <strong>180</strong> days.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

   The **Create Self-Signed Certificate** dialog opens (as shown in **Figure 710** below).

**Installing a Self-Signed Server Certificate**

This page displays a summary of the values specified in the **Create Self-Signed Certificate** page and provides the **Install** button to install the self-signed certificate.

1. Check the summary values for the Self-Signed Server Certificate.

**Figure 710 Create Self-Signed Certificate Page**

2. Click **Install**.
After you click Install, you return to the Certificate Store page and Policy Manager generates a message about the status of the certificate installation.

If the installation is successful, the page displays the message:

*Server Certificate updated successfully.*

**Figure 711 Server Certificate Successfully Updated**

3. Because all services are restarted after a successful certificate installation, you must click the Logout link, then log in to the ClearPass client to continue.

**Creating a Certificate Signing Request**

After you select a certificate type (Server Certificate or Service Certificate), you can create a certificate signing request (CSR).

When you generate certificate signing request, the Private Key is automatically stored on the current ClearPass server. Thus, you can then upload (import) the certificate alone, without having to include the Private Key in the import process.

To create a certificate signing request:

1. Navigate to Administration > Certificates > Certificate Store.
   
   The Server Certificates tab is selected.

2. Click the Create Certificate Signing Request link.
   
   The Create Certificate Signing Request dialog opens:

   **Figure 712 Create Certificate Signing Request Dialog**
3. Specify the **Create Certificate Signing Request** parameters as described in **Table 1**, then click **Submit**.

**Table 1: Create Certificate Signing Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>Enter the name associated with this entity. This field is mandatory. This can be a host name, IP address, or other name. The default is the fully-qualified domain name (FQDN).</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Optionally, enter the name of the organization.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Optionally, enter the name of the department, division, section, or other meaningful name.</td>
</tr>
<tr>
<td>Location (L)</td>
<td>Optionally, enter the name of the location, state, country.</td>
</tr>
<tr>
<td>State (ST)</td>
<td></td>
</tr>
<tr>
<td>Country (C)</td>
<td></td>
</tr>
<tr>
<td>Subject Alternate Name (SAN)</td>
<td>Optionally, enter the alternative names for the specified Common Name in one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• email: email_address</td>
</tr>
<tr>
<td></td>
<td>• URI: uri</td>
</tr>
<tr>
<td></td>
<td>• IP: ip_address</td>
</tr>
<tr>
<td></td>
<td>• dns: dns_name</td>
</tr>
<tr>
<td></td>
<td>• rid: id</td>
</tr>
<tr>
<td>Private Key Password</td>
<td>Enter the private key password, then verify it.</td>
</tr>
<tr>
<td>Verify Private Key Password</td>
<td></td>
</tr>
<tr>
<td>Private Key Type</td>
<td>Select the length for the generated private key types from the following options:</td>
</tr>
<tr>
<td></td>
<td>• 1024-bit RSA</td>
</tr>
<tr>
<td></td>
<td>• <strong>2048-bit RSA</strong>. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• 4096-bit RSA</td>
</tr>
<tr>
<td></td>
<td>• X9.62/SECG curve over a 256 bit prime field</td>
</tr>
<tr>
<td></td>
<td>• NIST/SECG curve over a 384 bit prime field</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>Select the message digest algorithm from the following options:</td>
</tr>
<tr>
<td></td>
<td>• SHA-1</td>
</tr>
<tr>
<td></td>
<td>• SHA-224</td>
</tr>
<tr>
<td></td>
<td>• SHA-256</td>
</tr>
<tr>
<td></td>
<td>• SHA-384</td>
</tr>
<tr>
<td></td>
<td>• <strong>SHA-512</strong>. This is the default.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

The generated certificate signing request is displayed.
Note that the Private Key is automatically stored on the current ClearPass server. You can then upload (import) the certificate without having to include the Private Key as part of the import process (for related information, see Importing a Server Certificate).

5. Copy the certificate signing request content and paste it into the Web form as part of the enrollment process.

6. To save and download the Certificate Signing Request file, click Download CSR.

**Importing a Server Certificate**

When you import the server certificate, you are provided with three upload options:

- **Upload Certificate and Use Saved Private Key**: This option allows the admin to upload only the certificate. The server certificate is then matched against the private key saved on the ClearPass server.

- **Upload PKCS#12 Certificate (.pfx or .p12 only)**: With this option, the admin uploads the PKCS#12 file and provides a pass phrase.

- **Upload Certificate and Private Key Files**: The admin can choose to upload the private key file and password along with the server certificate file.

To import a server certificate into the current ClearPass server:

1. Navigate to **Administration > Certificates > Certificate Store**.
2. From the **Server Certificates** tab, click the **Import Certificate** link. The **Import Certificate** dialog opens:
For security reasons, certificates signed using SHA1RSA are not recommended. Importing certificates signed with stronger keys, such as RSA with a length of more than 1024 bits, is recommended.

ClearPass does not support importing the HTTPS Server Certificate chain or RADIUS/EAP Server Certificate chain in P7b Base64 format. A P7B file contains only certificates and chain certificates (intermediate certificate authorities), not the private key.

3. Specify the **Import Certificate** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Type</td>
<td>Select <strong>Server Certificate</strong> (selected by default).</td>
</tr>
<tr>
<td>Server</td>
<td>Select the name of the ClearPass server that the server certificate will be imported into. <strong>NOTE:</strong> When importing a certificate to a Subscriber node from the Publisher node, in the Server field, select the Subscriber node.</td>
</tr>
<tr>
<td>Type</td>
<td>Select one of the following server certificate types:</td>
</tr>
<tr>
<td></td>
<td>- RADIUS/EAP Server Certificate</td>
</tr>
<tr>
<td></td>
<td>- HTTPS Server Certificate</td>
</tr>
<tr>
<td></td>
<td>- RadSec Server Certificate</td>
</tr>
<tr>
<td>Upload Method</td>
<td>Select one of the following methods to upload the certificate:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Upload Certificate and Use Saved Private Key</strong></td>
</tr>
<tr>
<td></td>
<td>This option allows the administrator to upload only the certificate. The certificate is then matched against the private key saved on the ClearPass server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Upload PKCS#12 Certificate (.pfx or .p12 only)</strong></td>
</tr>
<tr>
<td></td>
<td>With this option, the administrator uploads the PKCS#12 file and provides a pass phrase.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Upload Certificate and Private Key Files</strong></td>
</tr>
<tr>
<td></td>
<td>The administrator can choose to upload the private key file and password</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certificate File</td>
<td>Browse to the certificate file to be imported. <strong>NOTE:</strong> Both certificates with a</td>
</tr>
<tr>
<td></td>
<td>wild card as the common name and Extended Validation certificates are not</td>
</tr>
<tr>
<td></td>
<td>recommended for use as the RADIUS/EAP server certificate. Some clients may</td>
</tr>
<tr>
<td></td>
<td>be unable to authenticate when these types of certificates are used.</td>
</tr>
</tbody>
</table>

4. Click **Import**.

**Exporting a Server Certificate**

To export a server certificate from the current ClearPass server:

1. Navigate to **Administration > Certificates > Certificate Store**.
   The **Certificate Store** page opens.

   **Figure 715 Certificate Store Page**

   2. Click the **Export** link.
      The **Export to File** dialog opens.

   **Figure 716 Export to File Dialog**

   3. Specify the **Export to File** parameters as described in the following table.
Table 1: Export to File Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>Select <strong>Yes</strong> (the default) or <strong>No</strong> to specify whether you want to require password protection.</td>
</tr>
<tr>
<td>Secret Key Verify Secret</td>
<td>Enter the secret key, then reenter the secret key to verify.</td>
</tr>
</tbody>
</table>

4. Click **Export**.

Upon clicking **Export**, the certificate is exported in **PKCS#12** format.

The PKCS#12 (or PFX) format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file.

**Service Certificates**

This section describes the following topics:

- Adding Service Certificates
- Creating a Self-Signed Service Certificate
- Creating a Service Certificate Signing Request
- Importing a Service Certificate

**Adding Service Certificates**

The **Service Certificates** feature allows you to create multiple service certificates, each of which can be associated with a specific ClearPass service. For details, see [Associating a RADIUS Service Certificate with a Service](#).

You can also create a server certificate to replace the current server certificate.

---

**NOTE**

Service Certificates must always be RADIUS certificates.

---

To view the **Service Certificates** page:

1. Navigate to **Administration** > **Certificates** > **Certificate Store**.
2. Select the **Service Certificates** tab.

**Figure 717 Service Certificates Tab**

**Creating a Self-Signed Service Certificate**

This task creates a self-signed certificate to be signed by a CA (Certificate Authority).
To create a Self-Signed Service Certificate:

1. From the **Certificate Store > Service Certificates** page, click the **Create Self-Signed Certificate** link. The **Create Self-Signed Certificate** dialog opens.

2. Specify the parameters for the Self-Signed Service Certificate as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Type</td>
<td>Select <strong>Service Certificate</strong>.</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>Enter the name associated with this entity. This can be a host name, IP address, or other meaningful name. This field is mandatory.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Optionally, enter the name of the organization. This field is optional.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Enter the name of the department, division, section, or other meaningful name. This field is optional.</td>
</tr>
<tr>
<td>Location (L)</td>
<td>Enter the name of the location, state, country, and/or other meaningful name. These fields are optional.</td>
</tr>
<tr>
<td>State (ST)</td>
<td></td>
</tr>
<tr>
<td>Country (C)</td>
<td></td>
</tr>
<tr>
<td>Subject Alternate Name (SAN)</td>
<td>Enter the alternative name for the specified Common Name.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Entries for Subject Alternate Name in one of the following formats:</td>
<td></td>
</tr>
<tr>
<td>- email: email_address</td>
<td></td>
</tr>
<tr>
<td>- URI: uri</td>
<td></td>
</tr>
<tr>
<td>- IP: ip_address</td>
<td></td>
</tr>
<tr>
<td>- dns: dns_name</td>
<td></td>
</tr>
<tr>
<td>- rid: id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This field is optional.</td>
</tr>
</tbody>
</table>
### Parameter | Action/Description
---|---
Private Key Password | Enter the Private Key password, then verify the password.
Verify Private Key Password | 
Private Key Type | Select the length for the generated private key types from the following options:
- 1024-bit RSA
- 2048-bit RSA
- 4096-bit RSA
- X9.62/SECG curve over a 256 bit prime field
- NIST/SECG curve over a 384 bit prime field
The default private key type is **2048-bit RSA**.
Digest Algorithm | Select the message digest algorithm from the following options:
- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512
**NOTE:** The MD5 algorithm is not available in **FIPS** mode.
Valid for | Enter the certificate duration in number of days. The default is **180** days.

3. Click **Submit**.

The new self-signed service certificate is added.

**Figure 718  Self-Signed Service Certificate Added**

4. Repeat these steps to add as many self-signed service certificates as required.

**Creating a Service Certificate Signing Request**

After you select a server and a certificate type, you can create a certificate signing request.

To create a certificate signing request:

1. Navigate to **Administration > Certificates > Certificate Store**.
   The **Server Certificates** tab is selected.
2. Click the **Create Certificate Signing Request** link.
   The **Create Certificate Signing Request** dialog opens:
Figure 719  *Create Certificate Signing Request Dialog*

![Create Certificate Signing Request Dialog](image)

3. Specify the **Create Certificate Signing Request** parameters as described in the following table.

**Table 2: Create Service Certificate Signing Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>Enter the name associated with this entity. This field is mandatory. This can be a host name, IP address, or other name. The default is the fully-qualified domain name (FQDN).</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Optionally, enter the name of the organization.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Optionally, enter the name of the department, division, section, or other meaningful name.</td>
</tr>
<tr>
<td>Location (L)</td>
<td>Optionally, enter the name of the location, state, country.</td>
</tr>
<tr>
<td>State (ST)</td>
<td></td>
</tr>
<tr>
<td>Country (C)</td>
<td></td>
</tr>
<tr>
<td>Subject Alternate Name (SAN)</td>
<td>Optionally, enter the alternative names for the specified Common Name in one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>email: email_address</td>
</tr>
<tr>
<td></td>
<td>URI: uri</td>
</tr>
<tr>
<td></td>
<td>IP: ip_address</td>
</tr>
<tr>
<td></td>
<td>dns: dns_name</td>
</tr>
<tr>
<td></td>
<td>rid: id</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Private Key Password Verify Private Key Password</td>
<td>Enter the private key password, then verify it.</td>
</tr>
<tr>
<td>Private Key Type</td>
<td>Select the length for the generated private key types from the following options:</td>
</tr>
<tr>
<td></td>
<td>1024-bit RSA</td>
</tr>
<tr>
<td></td>
<td><strong>2048-bit RSA</strong>. This is the default.</td>
</tr>
<tr>
<td></td>
<td>4096-bit RSA</td>
</tr>
<tr>
<td></td>
<td>X9.62/SECG curve over a 256 bit prime field</td>
</tr>
<tr>
<td></td>
<td>NIST/SECG curve over a 384 bit prime field</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>Select the message digest algorithm from the following options:</td>
</tr>
<tr>
<td></td>
<td>SHA-1</td>
</tr>
<tr>
<td></td>
<td>SHA-224</td>
</tr>
<tr>
<td></td>
<td>SHA-256</td>
</tr>
<tr>
<td></td>
<td>SHA-384</td>
</tr>
<tr>
<td></td>
<td><strong>SHA-512. This is the default.</strong></td>
</tr>
</tbody>
</table>

4. Click **Submit**.
   The generated certificate signing request is displayed.

   **Figure 720 Certificate Signing Request Generated**

   ![Certificate Signing Request](image)

5. Copy the certificate signing request content and paste it into the Web form as part of the enrollment process.

6. To save and download the Certificate Signing Request file, click **Download CSR**.

**Importing a Service Certificate**

To import a service certificate into the current ClearPass server:

1. Navigate to **Administration > Certificates > Certificate Store**.
2. From the **Server Certificates** tab, click the **Import Certificate** link.
   The **Import Certificate** dialog opens:
For security reasons, certificates signed using SHA1RSA are not recommended. Importing certificates signed with stronger keys, such as RSA with a length of more than 1024 bits, is recommended.

ClearPass does not support importing the HTTPS Server Certificate chain or RADIUS Server Certificate chain in P7b Base64 format. A P7b file contains only certificates and chain certificates (intermediate certificate authorities), not the private key.

3. Specify the **Import Certificate** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Type</td>
<td>Select <strong>Service Certificate</strong>.</td>
</tr>
<tr>
<td>Upload Method</td>
<td>Select one of the following upload methods:</td>
</tr>
<tr>
<td></td>
<td>- Upload Certificate and Use Saved Private Key</td>
</tr>
<tr>
<td></td>
<td>- Upload PKCS#12 Certificate (.pfx or .p12 only)</td>
</tr>
<tr>
<td></td>
<td>- Upload Certificate and Private Key Files</td>
</tr>
</tbody>
</table>
| Certificate File   | Click **Browse** to specify the certificate file to be imported. **NOTE:** Both certificates with a wildcard as the common name and Extended Validation certificates are not recommended for use as the RADIUS/EAP server certificate. Some clients may be unable to authenticate when these types of certificates are used.

4. Click **Import**.

**Associating a RADIUS Service Certificate with a Service**

The **Service Certificates** feature allows you to create multiple RADIUS service certificates (for details, see **Service Certificates on page 698**). Once you create the RADIUS service certificates you need, you can associate a service certificate with a specific ClearPass service. This creates a virtual mapping between a ClearPass service and a RADIUS service certificate.

To associate a service certificate with a specific ClearPass service:

1. Navigate to **Configuration > Services**.
   The **Services** page opens.
2. From the **Services** page, click **Add**.
   
   The **Add Services** page opens.

3. From the **Type** drop-down, select the type of service you want to add.
4. Enter the name of the new service.
5. Select the **Authentication** tab.
   
   The **Add Services > Authentication** tab opens.

6. Select the **Authentication Method**.
7. Specify the **Authentication Source**.
8. Select the **Service Certificate** you want to associate with this service.
9. To view the details, click **View Certificate Details**.
   
   The **View Certificate Details** window opens.
10. Click **Close**, then click **Save**.
   You return to the **Services** page. The following message is displayed:
   
   *Service "<service_name>" has been added.*

11. Repeat this procedure for each service with which you want to associate a service certificate.

### 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 Page on page 705
- Adding a Certificate on page 706
- Enabling a Certificate on page 707
- Deleting a Certificate on page 707

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 Page

To display a list of trusted Certificate Authorities (CA):

1. Navigate to **Administration > Certificates > Trust List**.
   
   The **Certificate Trust List** page opens:
The Certificate Trust List (Administration > Certificates > Trust List) page can include the following certificates:

- **DoD (Department of Defense) certificates**: A DoD certificate allows a browser to trust web sites whose secure communications are authenticated by a DoD agency. These certificates are disabled by default.

- **Alcatel root certificate**: An Alcatel root certificate allows Alcatel Lucent IP phones to authenticate using EAP-TLS. These certificates are disabled by default.

The following table describes the information provided on Certificate Trust List:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Displays the Distinguished Name (DN) of the subject field in the certificate.</td>
</tr>
<tr>
<td>Validity</td>
<td>Indicates whether the CA certificate is valid or expired.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the CA certificate is enabled or disabled.</td>
</tr>
</tbody>
</table>

### Adding a Certificate

To add a certificate to the Certificate Trust List:

1. Navigate to **Administration > Certificates > Trust List**.
2. Click the **Add** link.
   - The **Add Certificate** dialog opens.

### Figure 727 Adding a Certificate

3. To browse to the certificate file, click **Choose File**.
4. Select the file, then click **Add Certificate**.
The selected certificate is added to the Certificate Trust List.

**Enabling a Certificate**

When you enable a CA certificate, Policy Manager considers the entity whose certificate is signed by this CA to be trusted.

To enable a certificate that is currently disabled:

1. Select the desired entry from the Certificate Trust List. The **View Certificate Details** page opens.

   **Figure 728**  *Viewing the Certificate Details*

   ![View Certificate Details](image)

2. Click the **Enable** button. The following message is displayed:  
   
   *Certificate is enabled successfully*

**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 729   Certificate Revocation Lists Page**

   ![Certificate Revocation Lists Page](image)

2. Click the Add link on the top-right section of the page.
   The Add Certificate Revocation List dialog opens:
3. Configure the **Add Certificate Revocation List** parameters as described in **Table 34**, then click **Save**.

**Table 34: Add Certificate Revocation List Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Enable the <strong>File</strong> button to use a distribution file as the Certificate Revocation List distribution point. <em>File</em> is enabled by default.</td>
</tr>
<tr>
<td>Distribution File</td>
<td>To select the distribution file to fetch the certificate revocation list, click <strong>Browse</strong> and select the CRL distribution file.</td>
</tr>
<tr>
<td>URL</td>
<td>Enable the <strong>URL</strong> button to use a URL as the CRL distribution point. Selecting <strong>URL</strong> enables the <strong>Distribution URL</strong> option.</td>
</tr>
<tr>
<td>Distribution URL</td>
<td>Specify the distribution URL to fetch the certificate revocation list.</td>
</tr>
<tr>
<td>Auto Update</td>
<td>- To update the CRL at intervals specified in the list, select <strong>Update whenever CRL is updated</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To check periodically and at the specified frequency (in hours), select <strong>Periodically update every _____ hour(s)</strong>.</td>
</tr>
<tr>
<td>Bypass Proxy</td>
<td>To bypass the proxy server, click the <strong>Enable to bypass proxy server</strong> option.</td>
</tr>
</tbody>
</table>

**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**.
Using ClearPass Dictionaries

This section provides the following information:

- **RADIUS Dictionary**
- **RADIUS CoA Templates**
- **TACACS+ Services Dictionary**
- **Device Fingerprints Dictionary**
- **Dictionary Attributes**
- **Applications Dictionaries**
- **Configuring Endpoint Context Server Actions**
- **Enabling Ingress Event Dictionaries**

**RADIUS Dictionary**

This page includes the list of available vendor dictionaries.

To configure RADIUS dictionaries:

1. Navigate to **Administration > Dictionaries > RADIUS**. The **RADIUS Dictionaries** page opens.

**Figure 731  RADIUS Dictionaries**

![RADIUS Dictionaries](image)

2. To view the dictionary attributes, enable a dictionary, or export the dictionary, click on the row of interest. For example, click on vendor **3com** to see all its attributes and their data type. The following figure displays the RADIUS 3Com dictionary attributes page:
Enabling a RADIUS Dictionary

To enable a RADIUS dictionary:
1. From the RADIUS Dictionaries page, select the dictionary of interest.
2. Click the Enable button.
   You return to the RADIUS Dictionaries page. The following message is displayed:
   Dictionary has been successfully enabled.

Exporting a RADIUS Dictionary

To export a RADIUS dictionary:
1. From the RADIUS Dictionaries page, select the dictionary of interest.
2. Click the Export button.
3. Open or save the XML file.
4. You can make modifications to the dictionary and import the file back into Policy Manager as needed.

Importing a RADIUS Dictionary

You can add additional dictionaries using the Import option. To add a new vendor dictionary:
1. Navigate to Administration > Dictionaries > RADIUS.
2. Click the Import link.
   The Import from file dialog opens:
3. Specify the **Import from file** parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select File</td>
<td>If the file that you want to import is password protected, enter the secret here.</td>
</tr>
</tbody>
</table>

**Editing an Existing RADIUS Dictionary**

To edit an existing dictionary:

1. Export an existing dictionary.
2. Edit the exported XML file.
3. Then import the dictionary.

**RADIUS CoA Templates**

The RADIUS CoA Templates allows users to add or update custom Change of Authorization (CoA) and Disconnect Message (DM) dictionaries for specific vendor IDs.

There is no user interface method for creating a RADIUS CoA Template—an existing template must be exported, modified, and then reimported.

To access the RADIUS CoA Templates:

1. Navigate to **Administration > Dictionaries > RADIUS CoA Templates**.
   
   The **RADIUS CoA Templates** page opens.

2. To enable or disable a template, and to export the template, click the desired row.
The RADIUS CoA Template Attributes page opens.

**Figure 735  RADIUS CoA Template Attributes**

---

The following table describes the RADIUS COA Template Attributes action buttons:

**Table 1: RADIUS Dictionary Attributes Action Buttons**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Click the Export button to save the template file in XML format. You can make modifications to the template and import the file back into Policy Manager.</td>
</tr>
<tr>
<td>Enable/Disable</td>
<td>Enable or disable this CoA template. Enabling a template makes it appear in the Policy Manager Rules Editors (Service rules, Role mapping rules, etc.).</td>
</tr>
</tbody>
</table>

**Importing a RADIUS CoA Template**

To add additional templates:

1. From the RADIUS CoA Templates page, click the Import button.
   
   The Import from File dialog opens.

   **Figure 736  Import from File Dialog**

2. Browse to the template file you wish to import.
3. Enter the secret for the file if required.
4. Click Import.
**Editing a RADIUS CoA Template**
To edit an existing CoA Template:

1. From the **RADIUS CoA Templates** page, select the CoA template you wish to modify, then click the **Export** button.
   
   The selected CoA template is converted to XML format.

2. Edit the exported XML file as necessary.

3. Then import the RADIUS CoA template back into the ClearPass server.

**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 737 TACACS+ Services Dictionaries Page**

The following table describes the **TACACS+ Services Dictionaries** parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Click to open the <strong>Import Dictionary</strong> pop up. Import the dictionary (XML file).</td>
</tr>
<tr>
<td>Export All</td>
<td>Export all TACACS+ services into one XML file containing multiple dictionaries.</td>
</tr>
</tbody>
</table>

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 738  TACACS+ Service Dictionary Attributes Pop-up**

---

**Device Fingerprints Dictionary**

- **Viewing the Contents of a Device Fingerprints Dictionary**
- **Importing and Exporting Custom Fingerprints**

Device fingerprints are composed of information collected about an online computing device for the purpose of unique identification of the device on subsequent visits. A device fingerprint can fully or partially identify individual users or devices even when cookies and other tracking data are turned off.

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 Updates Portal (see **Software Updates** for more information).

Custom device fingerprints can be added and updated between ClearPass servers.

---

**NOTE**

If custom fingerprints are configured, the custom rules are evaluated before the default rules are evaluated.

---

**Viewing the Contents of a Device Fingerprints Dictionary**

To view the contents of the Device Fingerprints Dictionary:

1. Navigate to **Administration > Dictionaries > Fingerprints**.

   The **Device Fingerprints** page opens.
2. To drill down and view additional details about the category, click on a line in the Device Fingerprints list.

The **Device Fingerprint Dictionary Attributes** page opens.

### Importing and Exporting Custom Fingerprints

When you click **Import Custom Fingerprints** or **Export Custom Fingerprints**, the standard Import from File and Export to File dialogs are displayed.

You are not required to provide a new selection of rules when they are exported. All the associated rules for the Custom Created Fingerprints are exported.

When imported on a node that does not have these details, the exported rules are associated with the Custom Fingerprints present in the Import File.

#### Importing Custom Fingerprints

To import custom fingerprints:

1. From the **Device Fingerprints** page, click **Import Custom Fingerprints**.

   The **Import from file** dialog box opens.
2. Browse to the Fingerprint Dictionary file that you want to import.
   - Be sure to select an XML file that is in the correct format.

   *NOTE* See Appendix B, "Using the ClearPass Configuration API" in the *ClearPass Deployment Guide* for more information about the format and contents of XML files.

3. **Enter secret for the file (if any):** If you entered a secret key to encrypt the exported file, enter the same secret key to import the device into this ClearPass server.

4. Click Import.
   
The **Update Device Fingerprints** dialog opens:

   *Figure 742 Update Device Fingerprints Dialog*

5. Modify the **Category**, **Family**, or **Name** device fingerprinting attributes as desired, then click **Update**.

**Exporting Custom Fingerprints**

ClearPassPolicy Manager allows you to export configuration and administration-related information from the current ClearPass server to an XML file. You can set this file to be password protected.

To export custom fingerprints:

1. From the **Device Fingerprints** page, click **Export Custom Fingerprints**.
   
The **Export to file** dialog opens.
Specify the **Export to file** parameters as described in Table 1:

**Table 1: Export to File Dialog Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>To export the file with password protection, choose Yes.</td>
</tr>
<tr>
<td>Secret Key/Verify Secret</td>
<td>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. Enter the secret key. Then reenter the secret key.</td>
</tr>
</tbody>
</table>

3. Click **Export**.

   The following figure shows ClearPass an example of the exported custom fingerprints file:

**Figure 744  Exported XML File**

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContent xmlns="http://www.avendassys.com/tipsapirefs/1.0">
 <TipsHeader exportTime="2017-05-24 11:15:00Z" version="6.7"/>
 <DeviceFingerprint>
   <DeviceFingerprint category="Spidey" family="super" name="bat">
     <FingerprintRule>
       <FingerprintRule match-conditions="ALL">
         <RuleCondition name="fingerprint" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="vendor" operator=""contains"" value="Super Micro Computer, Inc."/>
         <RuleCondition name="family" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="device" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="os" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="type" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
         <RuleCondition name="product" operator=""contains"" value="Spiderman, Inc."/>
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 745 Dictionary Attributes Page**

   ![Dictionary Attributes Page](image)

   Table 1 describes the dictionary Attributes parameters:

   **Table 1: Dictionary Attributes Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Use the Filter drop-down list to create a search based on the Name, Entity, Data Type, Is Mandatory, or Allow Multiple settings.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the attribute.</td>
</tr>
<tr>
<td>Entity</td>
<td>Indicates whether the attribute applies to a Local User, Guest User, Device, or Endpoint.</td>
</tr>
<tr>
<td>Data Type</td>
<td>Indicates whether the data type is String, Integer, Boolean, List, Text, Date, MAC address, or IPv4 address.</td>
</tr>
<tr>
<td>Is Mandatory</td>
<td>Indicates whether the attribute is required for a specific entity.</td>
</tr>
<tr>
<td>Allow Multiple</td>
<td>Indicates whether multiple attributes are allowed for an entity.</td>
</tr>
</tbody>
</table>
Adding a Dictionary Attribute

To add a dictionary attribute:

1. From the Attributes page, click Add.
   - The Add Attribute dialog appears.

**Figure 746 Add Attribute Dialog**

2. Specify the Add Attribute parameters as described in the following table, then click Add.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity</td>
<td>Specify whether the attribute applies to a Device, Endpoint, Guest User, Local User, or Onboard.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique ID for this dictionary attribute.</td>
</tr>
<tr>
<td>Data Type</td>
<td>From the drop-down, specify the data type.</td>
</tr>
<tr>
<td>Is Mandatory</td>
<td>Specify whether the attribute is required for a specific entity.</td>
</tr>
<tr>
<td>Allow Multiple</td>
<td>Specify whether multiple attributes are allowed for an entity.</td>
</tr>
<tr>
<td>Default Value</td>
<td>Optionally, specify whether the default value is true or false.</td>
</tr>
</tbody>
</table>

**NOTE:** Multiple attributes are not permitted if Is Mandatory is specified as Yes.

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 747 Importing Dictionary Attributes**

![Import from File Dialog](image)

2. Enter the **Import from File** parameters as described in Table 3.

**Table 3: Import From File Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select File</td>
<td>Browse to select the file that you want to import.</td>
</tr>
<tr>
<td>Enter secret for the file (if any)</td>
<td>If the file that you want to import is password protected, enter the secret here.</td>
</tr>
</tbody>
</table>

3. When finished, click **Import**.

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 748 Exporting Dictionary Attributes**

![Export to File Dialog](image)

2. Specify the **Export to File** parameters as described in Table 4.
Table 4: *Export to File Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export file with password protection</td>
<td>The <em>Yes</em> option is enabled by default. If you wish to disable password protection when exporting a file, select <strong>No</strong>.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>If the file that you want to import is password protected, enter the secret here. Then verify the secret key.</td>
</tr>
</tbody>
</table>

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 4.
   - When finished, click **Export**.
   - The *TagDictionary.xml* file is created.
4. 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 opens.
2. To see the application attributes, click the name of an application. The **Application Attributes** dialog box opens.

**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.

**Configuring Endpoint Context Server Actions**

This section contains the following information:
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 **Endpoint Context Server Actions** page displays a list of all the Context Server Actions that are available by default for each server type that ClearPass supports.

To configure endpoint context server actions:

1. Navigate to *Administration > Dictionaries > Context Server Actions*.
   
   The **Endpoint Context Server Actions** page opens.

   **Figure 751  Endpoint Context Server Actions Page**

2. From the **Endpoint Context Server Actions** page, click a row in the report.
   
   The **Endpoint Content Server Details** dialog opens.
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, authentication method, and URL for the endpoint context server action.

Specify the Endpoint Context Server Details > Action tab parameters as described in the following table, then click Save.

**Table 35: Action Parameters—Endpoint Context Server Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>Specifies the server type configured when the server action was configured. You can select the server type from the drop-down list.</td>
</tr>
<tr>
<td>Server Name</td>
<td>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.</td>
</tr>
<tr>
<td>Action Name</td>
<td>Specifies the name of the action configured.</td>
</tr>
<tr>
<td>Description</td>
<td>Provides additional information about the action specified.</td>
</tr>
<tr>
<td>HTTP Method</td>
<td>Select the HTTP method from the drop-down:</td>
</tr>
<tr>
<td></td>
<td>• DELETE</td>
</tr>
<tr>
<td></td>
<td>• GET</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>POST</td>
<td>The default setting</td>
</tr>
<tr>
<td>PUT</td>
<td>You can use the HTTP method PATCH to append content to existing endpoints/values.</td>
</tr>
<tr>
<td>PATCH</td>
<td></td>
</tr>
</tbody>
</table>

**Authentication Method**

Select the authentication method:
- **None**: Select None to disable the HTTP basic authentication for endpoint context server actions. This exposes the context server attributes to be used in context server actions.
- **Basic**
- **OAuth2**

**NOTE**: When associating context server actions with an endpoint context server, be sure to specify the same authentication method that was configured for the endpoint context server.

**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.

1. From the **Header** tab, select **Click to add**.

**Figure 753  Header Tab—Endpoint Context Server Details**

2. Specify the **Endpoint Context Server Details—Header** parameters as described in the following table:

**Table 36: Header Parameters—Specifying Key Value Pairs**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header Name</td>
<td>Enter the name of the header to be included in the HTTP header.</td>
</tr>
<tr>
<td>Header Value</td>
<td>Specify the value of the header specific to the name to be included in the HTTP header.</td>
</tr>
</tbody>
</table>

**NOTE**: If a ClearPass server is used as an Endpoint context server to update the configuration using the REST API call, add the HTTP header, **Accept: application/json** in the context server action.

3. Repeat these steps for each key-value pairs you need to add.
4. Click **Save**.
**Content Tab**

Use the **Content** tab to specify a content type and add non-default context server attributes (see Figure 754).

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 754**  **Content Tab**—**Endpoint Context Server Details**

Specify the **Endpoint Context Server Details**—**Content** parameters as described in the following table: **Table 37: Content Parameters**—**Endpoint Context Server Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| 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](#).
Attributes Tab Parameters

Use the Attributes tab to specify the mapping for attributes used in the content to parameterized values from the request.

Figure 755 Attributes Tab—Endpoint Context Server Details

Specify the Endpoint Context Server Details > Attributes parameters as described in the following table:

Table 38: Attributes Parameters—Endpoint Context Server Details

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Enter attribute names and assign values to those names. These name/value pairs are included in context server actions.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>Enter the value for the selected name in the Attribute Name field.</td>
</tr>
</tbody>
</table>

Figure 756 Adding Endpoint Context Server Attributes

5. Click Save.

You receive the following message:

Context Server Action "Check Point Login (Generic HTTP)" updated successfully

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 opens (see **Figure 751**).

2. From the **Filter** drop-down, select a filter:
   - **ServerType**
   - **Action Name**
   - **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**.

### Storing Authentication Attributes in the Multi-Master Cache

ClearPass provides a context server action that serves as an example of how to store attributes from an authentication session into Multi-Master Cache for use in policy enforcement during an authentication session. The Administrator can then clone it and customize the context server action to meet their requirements.

To access this context server action:

1. **Navigate to Administration > Dictionaries > Context Server Actions.**
   - The **Endpoint Context Server Actions** page opens.

**Figure 757  Endpoint Context Server Actions Page: Store Attributes in Multi-Master Cache**

2. Scroll down and select the **Store Attributes in Multi-Master Cache** endpoint context server action.
   - The **Endpoint Context Server Details** page opens.
3. Modify and customize the **Store Attributes in Multi-Master Cache** endpoint context server action as needed.

   At **Configuration > Authentication > Sources**, the **Multi-Master Cache Repository** authentication source will fetch the attributes stored in the Multi-Master Cache and proceed with authentication.

**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 opens.
2. Scroll to and select the **Generic HTTP/Check Point Login** server action.
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. The set of ingress event dictionaries are displayed. By default, they are disabled.

   **Figure 760** Viewing Ingress Event Dictionaries

2. To enable a dictionary, select the disabled Ingress Events Dictionary for the appropriate vendor.

   The Events Attributes dialog opens.
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** (see **Figure 762**).

**Figure 762  Ingress Events Dictionary Enabled**

---

**OnGuard Settings and Agent Library Updates**

This section provides the following information:

- **Introduction**
- **Configuring OnGuard Settings**
- **OnGuard Agent Library Updates**
- **Certificate-Based Authentication Using OnGuard**
- **Installing Standalone VIA 3.2.x with OnGuard Agent**

**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, macOS, and Ubuntu 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 or download the agent deployment packages to another location.

To view the OnGuard Support Charts, see [Accessing the OnGuard Support Charts](#).

## Configuring OnGuard Settings

To configure the OnGuard settings:

1. Navigate to **Administration > Agents and Software Updates > OnGuard Settings**.
   
The **OnGuard Settings** page opens to the **Settings** tab:

   **Figure 763  OnGuard Settings Page > Settings Tab**

2. Configure the **OnGuard Settings** parameters as described in [Table 1](#), then click **Save**.

   **Table 1: OnGuard Settings Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Agent Settings</td>
<td>Click the <strong>Global Agent Settings</strong> link to configure the global agent settings for OnGuard agents. For more information, see <a href="#">OnGuard Global Agent Settings</a>.</td>
</tr>
<tr>
<td>Policy Manager Zones</td>
<td>Click the <strong>Policy Manager Zones</strong> link to configure the client subnets that comprise the Policy Manager Zone. For more information on configuring Policy Manager zones, see <a href="#">Managing Policy Manager Zones</a>.</td>
</tr>
<tr>
<td>Agent Version</td>
<td>Indicates the current version of the OnGuard agent.</td>
</tr>
</tbody>
</table>
### Parameter | Action/Description
--- | ---
Agent Library Version | Indicates the version of the OnGuard Agent Library. OnGuard Agent uses this library for health collection and auto-remediation.

**Installer Mode**
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**
  - **NOTE:** Selecting this option will automatically remove any existing and installed Aruba VIA client software.
- **Install and enable Aruba VIA component**
  - **NOTE:** Selecting this option will automatically upgrade any existing and installed Aruba VIA client software.
  - **NOTE:** For related information, see [Installing Standalone VIA 3.2.x with OnGuard Agent](#).

**Agent Customization**

**Managed Interfaces**
Select the type(s) of interfaces that OnGuard will manage on the endpoint. Select from the following options:
- Wired
- Wireless
- VPN
- Other

**Mode**
Select one of the following options:
- **Authenticate with health checks:** OnGuard collects the username and password and also performs health checks on the endpoint. This is the default setting.
- **Authenticate - no health checks:** OnGuard collects the username and password but does not perform health checks on the endpoint.
- **Check health - no authentication:** OnGuard does not collect the username and password.
- **Authentication type:** OnGuard provides *username and password authentication* and *certificate-based authentication*:
  - **Username & Password:** Select this option for standard username and password authentication.
  - **Certificate:** The *Certificate* option is available only when you specify *Authenticate with health checks* or *Authenticate - no health checks*. When you select *Certificate*, the *Certificate Filter Criteria* option appears to allow you to show or select certificates based on specific criteria.

```
<table>
<thead>
<tr>
<th>Authenticate with health checks</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Certificate</td>
</tr>
</tbody>
</table>
```

The *Certificate Filter Criteria* setting is used by the OnGuard client. The OnGuard client applies this filter to the list of installed user certificates on the client machine prior to using them for authentication.

*ClearPass* OnGuard Agent supports certificates that are stored under the personal certificate store of the user's system (for example, under *Certificates - Current User on Windows*) and smart cards. For details, refer to [Certificate-Based Authentication Using OnGuard](#).

- **Username/Password Text:**
  - If desired, change the label for the *Username* and *Password* fields on the OnGuard agent.
  - **NOTE:** This setting is not valid for the *Check health - no authentication* mode.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Agent action when an update is available      | Determines what the ClearPass OnGuard Agent does when an update of OnGuard Agent Library is available. Select one of the following options:  
  ■ Ignore: ClearPass OnGuard Agent ignores the available OnGuard Agent Library update.  
  ■ Notify User: ClearPass OnGuard Agent notifies the user that a new version of OnGuard Agent Library is available on the ClearPass server.  
  ■ Download and Install: When this option is selected and a new version of OnGuard Agent Library is available on the ClearPass server, ClearPass OnGuard Agent automatically downloads and installs the new version of OnGuard Agent Library from the ClearPass server. |

### Agent Remediation User Interface Customization

| Custom User Interface                          | When you select the Configure check box, the Agent Remediation User Interface Customization dialog opens.  
  ■ Web Pages: To create the OnGuard custom web pages and define the properties for the web page, click the Create link for the corresponding web page (for details, see Creating OnGuard Custom Web Pages). |

### Native Dissolvable Agent Customization

| Managed Interfaces                             | The Native Dissolvable Agent performs health checks for one of the selected interfaces. This feature ensures that, if both wired and wireless interfaces are connected, the OnGuard Agent will send health requests through the correct interface. Select the type(s) of managed interfaces that are supported for the Native Dissolvable Agent.  
  Select from the following options:  
  ■ Wired  
  ■ Wireless  
  ■ VPN  
  ■ Other |

### OnGuard Agent Library Updates

OnGuard modules, including detection libraries for client programs (V4 SDK), can be upgraded without having to upgrade your ClearPass or OnGuard installations.

To support this feature, OnGuard Agent Library update patches with new versions of the detection library/SDK will be released periodically. When they are released, the OnGuard Agent Library update patches will be available on the Software Updates page under Firmware & Patch Updates (see Software Updates Page).

When a new version of an OnGuard Agent Library patch is installed, it is immediately available in OnGuard Settings. OnGuard Agents can be configured to install the update automatically, or administrators may install them manually instead. The OnGuard Agent Library update patches are also available on the Aruba Support Center for offline updates through the CLI.

OnGuard Agent Library update patch versions are independent of ClearPass and OnGuard versions, so newer versions of OnGuard Agent Library update patches can be installed on older versions of ClearPass. This feature is available for both the persistent and dissolvable agents, and for Windows, macOS, and Ubuntu operating systems.

As OnGuard Agent Library update files become available, the files for the various operating systems are listed on the new OnGuard Settings > Installers tab. Administrators can download these files for manual installation or to push via Patch Management applications such as Microsoft System Center Configuration Manager (SCCM).
While auto-remediation or ClearPassUSHAREmediate.exe is running, the OnGuard Agent Library update will fail on Windows OS. Once auto-remediation has completed, you can install the OnGuard Agent Library update.

**Important Points**

Please note the following important points:

1. On a ClearPass server, new versions of an OnGuard Agent Library Update patch must be installed manually from the **Software Updates** page.

2. OnGuard Agent Library Update patches are independent from ClearPass server versions (for example, the same patch will be available for all 6.7.x versions).

3. The OnGuard Agent Library version is different than the ClearPass server and OnGuard Agent versions. The currently installed version of OnGuard Agent Library is shown at **Administration > Agents and Software Updates > OnGuard Settings**.

**Figure 764 OnGuard Settings > Agent Library Version**
4. The current version of OnGuard Agent Library installed on the client is shown in the OnGuard Agent About box:

**Figure 765  Agent Library Version and the OnGuard Agent About Box**

5. On a ClearPass server, the *Software Updates* page shows only those patches that have versions higher than the currently installed version. Installing a patch that is a lower version (that is, downgrading the version) on a ClearPass server is not supported.

6. OnGuard Agent Library Updates are supported for both Persistent and Native Dissolvable Agents on the Windows, macOS, and Ubuntu operating systems.

7. Auto-updating OnGuard Agent Library is supported on Ubuntu clients having ClearPass OnGuard Agent version 6.7.1 and higher.

8. Installing OnGuard Agent Library Update on clients having ClearPass OnGuard version 6.7.1 or higher will restart OnGuard Agent and Services. Thirty to 60 seconds after installing OnGuard Agent Library Update, ClearPass OnGuard Agent will be restarted.

9. OnGuard Agent Library Update patches will include only Library Update installers.

10. Installing a new version of the OnGuard Agent Library installs the new version of the V4 SDK library files.

11. While automatically updating the OnGuard Agent library, OnGuard Agent supports installing newer (higher) versions on clients only. If the ClearPass server has a lower version than the version installed on the client, OnGuard Agent does not automatically downgrade the OnGuard Agent library.

12. Downgrading the OnGuard Agent Library version on a client is supported via manual installation; that is, an administrator can manually install a lower version of the OnGuard Agent Library on a client.

13. If auto-update of the OnGuard Agent Library is enabled and a new version of OnGuard Agent Library is available on the ClearPass server, OnGuard Agent installs the new version after performing health checks as OnGuard Agent performs enforcement actions (such as applying the Agent Enforcement profile).

14. After successful installation of a new version of OnGuard Agent Library Update, OnGuard Agent performs health checks again, using the new version of the V4 SDK. This is applicable for both automatic and manual installations.
15. OnGuard Agent sends the installed version of OnGuard Agent Library update to the ClearPass server in a WebAuth request. This information is available in **Access Tracker > Input > Computed Attributes > Host:AgentLibraryVersion**. This attribute is available in Service Rules and Role Mapping.

16. Third-party support charts under **Administration > Support > Documentation** will also get updated when a new version of the OnGuard Agent Library Update patch is installed on the ClearPass server.

17. On Windows clients, installing the OnGuard Agent Library manually restarts OnGuard Agent and Services. Also, if multiple users are logged in at the time of installation, OnGuard Agent is launched only for the current active user. For other, non-active users, OnGuard Agent must be restarted manually.

18. Uninstalling OnGuard Agent also uninstalls OnGuard Agent Library Update from the client. Reinstalling OnGuard Agent does not install the new version OnGuard Agent Library update automatically, as the new version of Library Update is not part of OnGuard Installer. If **Enable to auto update OnGuard Agent Library** is set to **True** in the Agent Enforcement profile (see [Configuring Agent Enforcement Attributes](#)), OnGuard Agent will install it again; otherwise, it must be installed manually.

**Certificate-Based Authentication Using OnGuard**

For certificate-based authentication, OnGuard agent uses the client certificate during the SSL handshake (the private key can be obtained from OS store/TPM/smart card). The ClearPass server verifies the client certificate against the configured trusted CA list.

On successful certificate verification, the client is authenticated. Additionally, ClearPass can perform user-lookup for the identity fetched from the client certificate with the configured authentication source and display an alert in Access Tracker if lookup fails.

**Configuration**

To configure certificate-based authentication:

1. Navigate to **Administration > Agent and Software Updates > OnGuard Settings**. The **OnGuard Settings** page opens.
2. Under **Agent Customization** specify the **Authentication Type** as **Certificate**. The **Certificate Filter Criteria** field is displayed.
The **Configure Filter Criteria** parameter supports regular expressions with an exception of * (asterisk).

**Figure 767 Asterisk (*) Specified as Certificate Filter Criteria**

When * is configured for the certificate filter criteria, OnGuard Agent shows all the certificates that are stored under the personal certificate store of the user's system (for example, under Certificates - Current User on Windows) and smart cards in the Certificate Selection dialog:
Certificate Filter Criteria Example

If **Certificate Filter Criteria** is configured as "organizationalUnitName=ARUBA;organizationName=HPE"
OnGuard Agent selects the certificate that matches both the conditions:

**Figure 769  Example of Certificate Filter Criteria with Two Conditions**

If only one certificate is present in the personal certificate store of the user's system that matches the filter criteria, OnGuard Agent uses that certificate without prompting the Certificate Selection dialog.

**Table 2: Certificate Filter Criteria: Supported Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>commonName</td>
<td>2.5.4.3</td>
</tr>
<tr>
<td>organizationalUnitName</td>
<td>2.5.4.11</td>
</tr>
<tr>
<td>organizationName</td>
<td>2.5.4.10</td>
</tr>
<tr>
<td>Attribute</td>
<td>OID</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>certificateIssuer</td>
<td>2.5.29.29</td>
</tr>
<tr>
<td>userPrincipalName</td>
<td>1.3.6.1.4.1.311.20.2.3</td>
</tr>
<tr>
<td>emailAddress</td>
<td>1.2.840.113549.1.9.1</td>
</tr>
<tr>
<td>friendlyName</td>
<td>1.2.840.113549.1.9.2</td>
</tr>
</tbody>
</table>

**OnGuard Agent Behavior for Certificate-Based Authentication**

When Certificate-based Authentication Mode is selected:

- OnGuard Agent prompts for the Certificate Selection dialog.
- OnGuard Agent shows the information of the selected certificate in Diagnostic logs.
- If a smart card is used for authentication, OnGuard Agent prompts for the PIN dialog:

**Figure 770**  *PIN Dialog When a Smart Card is Used for Authentication*

During reconnect from the same running instance of the OnGuard Agent, the PIN may not be required again due to internal caching supported by the operating system and the smart card provider.
OnGuard caches the certificate selection and PIN if the **Save Credential** setting is ON in the OnGuard Agent Preferences.

**Host:AuthType Attribute**

In the WebAuth request, OnGuard Agent sends a new attribute—**Host:AuthType**.

**Host:AuthType** has two values:

- **Certificate**: For Certificate-based authentication.
- **Password**: For username and password-based authentication.
This attribute is available in Service Rules and Role Mapping.

**Important Points**

Please note the following important points:

1. Certificate-based authentication is supported for Persistent Agent on the Windows operating system.
2. If the ClearPass Policy Manager version is 6.7.5 and the OnGuard agent is older than 6.7.5, OnGuard Agent continues to work with user name password-based authentication.
3. Certificates that are installed in the machine store are not displayed in the Certificate Selection dialog.
4. OnGuard Agent discards expired certificates.
5. The user's certificates that don't include the private key are displayed in the OnGuard Agent dialog, but these certificates don't work when used for authentication.
6. ClearPass does not support SubjectAltName (SAN) in Certificate Filter Criteria. However, you can use values inside the SAN as certificate filter criteria (for example email, IP, dns).

**Installing Standalone VIA 3.2.x with OnGuard Agent**

ClearPass supports standalone installation of both VIA 3.2.x and the OnGuard Agent. This allows administrators to use VIA 3.2.x functionality that is not yet available in the Unified Agent in conjunction with the OnGuard Agent. This feature is supported by OnGuard 6.7.2 and higher and by VIA 3.2.2 and higher. This feature is available only on Windows OS.

To use this feature, OnGuard must be installed by passing the AllowBothVIAAndOnGuard flag to the installer in the following format:

```
ClearPassOnGuardInstall.exe /AllowBothVIAAndOnGuard=1
msiexec /i ClearPassOnGuardInstall.msi ALLOWBOTHVIAANDONGUARD=1
```

Both OnGuard and VIA must be installed with this flag in order for them to co-exist on the same system. If either of them is installed without this flag, the other cannot be installed.

In addition, VIA must be installed with the AllowBothVIAAndOnGuard flag in the following format:

```
msiexec /i Aruba-VIA-3.2.0.0.XXXXX-64(86).msi ALLOWBOTHVIAANDONGUARD=1
```

If the ClearPass OnGuard Unified Agent is installed with AllowBothVIAAndOnGuard=1, the Unified Agent will not
enable the VPN component, even if it is enabled in the ClearPass user interface, i.e., the ClearPass OnGuard Unified agent will run in OnGuard-only mode even if the Administration > Agents and Software Updates > OnGuard Settings > Installer Mode option is set to Install and enable Aruba VIA component.

# OnGuard Agent Installers

To access the OnGuard Agent Installers:

1. Navigate to Administration > Agents and Software Updates > OnGuard Settings.
2. From the OnGuard Settings page, select the Installers tab.

   The Installers tab provides all available installer files for OnGuard and for library updates.

   For each OS (Windows, macOS, and Ubuntu), you have the option of initiating a full installation or an update only, which installs only the OnGuard Agent for OPSWAT OESIS framework for the selected OS.

---

![OnGuard Settings Page > Installers Tab](image_url)

---

**Table 1: OnGuard Settings > Installers Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| Windows   | Select the appropriate download link to download OnGuard Agent for Windows.  
   - The ClearPassOnGuardInstall binary file is provided in .exe and .msi formats.  
   - The ClearPassOnGuardLibraryUpdate file updates only the OnGuard Agent Library for Windows without requiring reinstallation of OnGuard Agent. |
| macOS     | Select the appropriate download link to download OnGuard Agent for macOS.  
   - The ClearPassOnGuardInstall binary file is provided in .DMG format.  
   - The ClearPassOnGuardLibraryUpdate file updates only the OnGuard Agent Library for macOS without requiring reinstallation of OnGuard Agent. |
<p>| Ubuntu    | Select the appropriate download link to download OnGuard Ubuntu Agent for Linux. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
|           | - The ClearPass OnGuardInstall binary file and the ClearPass OnGuardUpdate file are provided in .tar.gz format.  
|           | - The ClearPassOnGuardLibraryUpdate file updates only the OnGuard Ubuntu Agent for Linux without requiring reinstallation of OnGuard Agent.  
| Native Dissolvable Agent Apps |   |
| Windows   | - Click the OnGuard Windows Health Checker URL to install the Native Dissolvable Agent for Windows.  
|           | - Click the OnGuard Windows Health Checker Library Update URL to update only the Native Dissolvable Agent for Windows without requiring reinstallation of OnGuard Agent.  
| macOS     | - Click the OnGuard Mac Health Checker URL to download Native Dissolvable Agent for macOS.  
|           | - Click the OnGuard Mac Checker Library Update URL to update only the Native Dissolvable Agent for macOS without requiring reinstallation of OnGuard Agent.  
| Ubuntu    | - Click the OnGuard Ubuntu Health Checker URL to download Native Dissolvable Agent for macOS.  
|           | - Click the OnGuard Ubuntu Checker Library Update URL to update only the Native Dissolvable Agent for Ubuntu without requiring reinstallation of OnGuard Agent.  
| NOTE:     | You can download the .tar.gz files specific to 32-bit (indicated by x86 in the filename) and 64-bit systems. |

**Manually Installing a New Version of the OnGuard Agent Library**

You can use the installers available on the OnGuard Settings > Installers page for offline or manual installation of OnGuard Agent Library updates on clients.

To manually install a new version of the OnGuard Agent Library:

1. Download the applicable installer from the OnGuard Settings > Installers page.
2. Copy the installer file on the client and run it.
3. Wait for the installation to complete.
4. When the installation is complete:
   a. On Windows clients, OnGuard Agent will be restarted.
   b. On Ubuntu and macOS clients, OnGuard Agent will perform health checks.

**Automatically Updating New Versions of OnGuard Agent Library from a ClearPass Server**

This feature is supported by ClearPass OnGuard Agent for Windows and macOS. This feature is not supported for the Ubuntu OS in ClearPass Policy Manager 6.7.0.

ClearPass OnGuard Agents support automatically downloading and installing new versions of the OnGuard Agent Library from a ClearPass server when a new version is available.

While auto-remediation or ClearPassUSHARemEDIATE.exe is running, the OnGuard Agent Library update will fail on Windows OS. Once auto-remediation has completed, you can install the OnGuard Agent Library update.
To enable automatic updates of the OnGuard Agent Library:

1. Navigate to **Configuration > Enforcement > Profiles**.
2. Configure a new Agent Enforcement profile or edit an existing Agent Enforcement profile.
3. Set the attribute **Enable to auto update OnGuard Agent Library** to **True** (for details, see Configuring Agent Enforcement Attributes).

### OnGuard Global Agent Settings

This section provides the following information:

- **About Global Agent Settings**
- **Global Agent 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.
   
   The **Configure Global Agent Settings** page opens.

**Figure 774 Configure Global Agent Settings Page**

3. To add additional Global Agent Settings parameters, select **Click to add**.
   
   a. **Name**: Select the desired Global Agent Setting (see **Table 1**).
   
   b. **Value**: Specify the appropriate value.

4. Repeat these steps as necessary for each additional parameter, then click **Save**.
Global Agent Settings Parameters for OnGuard Agents

*Table 1* describes the **Global Agent Settings** parameters for OnGuard agents:

<table>
<thead>
<tr>
<th>Name Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Credentials Interval (in days)</td>
<td>Select the number of days the user credentials should be cached on OnGuard agents.</td>
</tr>
<tr>
<td>Delay to bounce after Logout (in minutes)</td>
<td>Specify the number of minutes that should elapse before OnGuard bounces the interface if OnGuard remains disconnected.</td>
</tr>
<tr>
<td>Enable OnGuard requests load-balancing</td>
<td>Enable this option to balance the load of OnGuard authentication requests across ClearPass Policy Manager servers in a cluster.</td>
</tr>
<tr>
<td>Enable access over Remote Desktop Session</td>
<td>Enable this option to allow OnGuard access through a Remote Desktop session.</td>
</tr>
<tr>
<td>Enable to hide Logout button</td>
<td>Enable this option to hide the <strong>Logout</strong> button on OnGuard agent.</td>
</tr>
<tr>
<td>Enable to install VPN component</td>
<td>Enable this option to install the OnGuard VPN component.</td>
</tr>
<tr>
<td>Enable to use Windows Single-Sign On</td>
<td>Enable this option to allow use of a user’s Windows credentials for authentication.</td>
</tr>
<tr>
<td>Keep-alive Interval (in seconds)</td>
<td>Specify a keep-alive interval for OnGuard agents.</td>
</tr>
<tr>
<td>OnGuard Health Check Interval (in hours)</td>
<td>The connected OnGuard Agents periodically send heart-beat (Keep-Alive) messages to ClearPass Policy Manager. This interval is defined by the <strong>Keep-Alive Interval (in seconds)</strong> parameter. The default value is 60 seconds. ClearPass uses Keep-Alive messages to:</td>
</tr>
<tr>
<td></td>
<td>▪ Update the status of OnGuard Agents regarding OnGuard Activity.</td>
</tr>
<tr>
<td></td>
<td>▪ Issue CoA (Change of Authorization) for a Session Restrictions Enforcement Profile if OnGuard Agent is disconnected:</td>
</tr>
<tr>
<td></td>
<td>▪ Session-Check &gt; Agent-Connection = Down</td>
</tr>
<tr>
<td></td>
<td>▪ Post-Auth-Check &gt; Action = Disconnect</td>
</tr>
<tr>
<td></td>
<td>For related information, see <a href="https://www.clearpass.com">Session Restrictions Enforcement Profile</a>.</td>
</tr>
<tr>
<td>OnGuard Health Check Interval (in hours)</td>
<td>Specify the number of hours that OnGuard will skip health checks for healthy clients.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Note the following information when you set the <strong>OnGuard Health Check Interval</strong> parameter:</td>
</tr>
<tr>
<td></td>
<td>▪ Set this parameter if OnGuard mode is set to <em>health</em> only.</td>
</tr>
<tr>
<td></td>
<td>▪ This parameter is valid only for wired and wireless interface types.</td>
</tr>
<tr>
<td></td>
<td>▪ This parameter is not applicable for the <em>OnGuard Dissolvable Agent, VPN, and Other</em> interface types.</td>
</tr>
<tr>
<td></td>
<td>You can also specify the health-check interval in the <strong>Agent Enforcement</strong> profile (<a href="https://www.clearpass.com">Configuration &gt; Enforcement &gt; Profiles &gt; Add</a>) to create different Agent Enforcement Profiles for different users.</td>
</tr>
<tr>
<td>Run OnGuard As</td>
<td>For details, see the next section, <a href="https://www.clearpass.com">Global Agent Settings: Run OnGuard As Parameter</a>.</td>
</tr>
<tr>
<td>Server Certificate Validation</td>
<td>Enables the ClearPass OnGuard Unified Agent to validate the ClearPass Server Certificate when it sends a WebAuth health request to ClearPass.</td>
</tr>
<tr>
<td>Server Communication Mode</td>
<td>Based on the value of this attribute, OnGuard Agent will use the <em>IP address, HostName, or FQDN</em> (Fully Qualified Domain Name) to communicate with the ClearPass server.</td>
</tr>
<tr>
<td></td>
<td>Select one of the following values:</td>
</tr>
</tbody>
</table>

---

747 | Administration

ClearPass 6.7 Policy Manager | User Guide
<table>
<thead>
<tr>
<th>Name Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support Team Email Address</strong></td>
<td>Enter an email address that automatically populates the To field in the user’s email client when they send logs.</td>
</tr>
<tr>
<td><strong>Use active Username in Health Only mode</strong></td>
<td>When this option is enabled (set to True) and the OnGuard Agent is running in Health Only mode, instead of using the MAC address as the username, OnGuard Agent sends the currently active user’s username as the username in the WebAuth request.</td>
</tr>
<tr>
<td>■ Username format on Windows:</td>
<td>• Local users: <code>&lt;host_name&gt;</code>\ <code>&lt;username&gt;</code>  \ Domain users: <code>&lt;domain_name&gt;</code>\ <code>&lt;username&gt;</code>  \ Username format on macOS and Ubuntu: \ Local users and Domain users: <code>&lt;username&gt;</code>  \ <strong>NOTE:</strong> when this option is enabled, OnGuard Persistent Agent sends the attribute Host:ActiveUserName in the WebAuth request. This attribute is available in both Service Rules and Role Mapping.  \ <strong>NOTE:</strong> This option is not applicable for Native Dissolvable Agent and OnGuard running as Service.</td>
</tr>
<tr>
<td>■ Username format on macOS and Ubuntu:</td>
<td></td>
</tr>
<tr>
<td><strong>Use Current OS Language (Windows Only)</strong></td>
<td>Enables ClearPass OnGuard Agent to use the current user’s display language, if supported, overriding the language selected at installation time. This parameter applies only to Windows clients.</td>
</tr>
<tr>
<td><strong>VPN Device Names (Windows)</strong></td>
<td>This parameter lets you specify a VPN adapter (device) name and categorize the network interface as a VPN on Windows.  \  \  \ 1. Enter a Windows device name as a <strong>Value</strong>. If OnGuard Agent finds a network interface with a matching device name, it classifies it as a VPN interface. Admins can specify multiple names by using a comma separator and adding each name in double quotes. For example: &quot;VPN&quot;, &quot;F5&quot;, &quot;Checkpoint&quot;. \ Admins can also use an asterisk (*) as a wild-card character in this field. For example:  \ ■ <strong>VPN</strong>: Specifies that any interface having <strong>VPN</strong> in its device name will be set as a VPN interface.  \ ■ <strong>F5</strong>: Specifies that any interface that has a device name starting with <strong>F5</strong> will be set as a VPN interface. \ ■ <strong>Checkpoint</strong>: Specifies that any interface name that ends with <strong>Checkpoint</strong> will be set as a VPN interface. All the string comparisons are case-insensitive.</td>
</tr>
<tr>
<td><strong>VPN Device Names (macOS)</strong></td>
<td>This parameter lets you specify a VPN adapter (device) name and categorize the network interface as a VPN on macOS.  \  \  \ 1. Enter a macOS device name as a <strong>Value</strong>. Refer to the description of <strong>VPN Device Names (Windows)</strong> above for functionality details.</td>
</tr>
</tbody>
</table>

---

**NOTE:**
- When specifying device names, ensure they are unique and accurately reflect the network interfaces. Failure to do so can lead to misclassification and incorrect network access.
- Use the asterisk (*) wildcard to include device names with similar prefixes.
- Be cautious with case sensitivity, as specified in the OnGuard configuration.
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 opens.
2. Click Global Agent Settings.
   The Global Agent Settings dialog opens.

Figure 775  Global Agent Settings Dialog

3. Click Click to add....
   a. Name: Select Run OnGuard As.
   b. Value: Select the appropriate option as described in Table 2.
      Table 2 describes the available values for the Run OnGuard As parameter.
4. Click Save.

Table 2: Global Agent Settings: Run OnGuard As Parameters

<table>
<thead>
<tr>
<th>Run OnGuard As Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Health checks are performed by the OnGuard Agent after the user logs in to the client.</td>
</tr>
<tr>
<td>Service</td>
<td>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.</td>
</tr>
<tr>
<td>BothServiceAndAgent</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 the 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.

### Creating OnGuard Custom Web Pages

This section provides the following information:

- About the OnGuard Custom Interface and the Remediation Process
- Creating OnGuard Custom Web Pages
- HTML Content for OnGuard Custom Web Pages
- **Important Points**
- OnGuard Custom Script Exit Codes

### About the OnGuard Custom Interface and the Remediation Process

OnGuard provides the ability to show end users a custom interface, or wizard, that guides them through the remediation process if their device is quarantined.

When this feature is enabled and OnGuard needs to run a custom remediation script, the wizard tells the user why the device was denied network access, describes the tasks that are required to fix the problem, and lets the user choose whether to execute the remedial script or not. While the script is being executed and new health checks are run, progress messages are displayed.

The pages of the wizard are created using ClearPass Guest’s Web Pages configuration forms, and can be customized with logo, text, and images (for details, refer to the **Custom User Interface** parameter in Table 1).

### Configuring the Show Custom User Interface for Custom Scripts Attribute

To configure the **Show Custom UI for Custom Scripts** attribute:

1. Navigate to **Configuration > Enforcement > Profiles**, then select the **Agent Script Enforcement** profile.

2. Specify the **Success Message**, **Failure Message**, **Progress Message**, and **Description** attributes, as well as other script-related attributes (for details, see Configuring Agent Script Enforcement Attributes).

### Creating OnGuard Custom Web Pages

To create the OnGuard custom web pages:

1. Navigate to **Administration > Agents and Software Updates > OnGuard Settings**.

   The **OnGuard Settings** page opens.

2. Scroll down to the **Agent Remediation User Interface Customization** section.
3. To enable the **Custom User Interface** configuration dialog, click (enable) the **Configure** check box.

4. Click the **Create** link for the OnGuard custom web page you want to create. For details, see [HTML Content for OnGuard Custom Web Pages](#).

   The **Create Web Page (New) > Web Page Settings** configuration dialog opens.
5. Specify the required parameters (Name, Page Name, and Skin, as well as Title if desired), then click Create Page.

The OnGuard custom web page is created.

6. **Window Behavior:**
   
   - **Always on Top:** The custom user interface window will always be on top of any other windows present.
   
   - **Allow Minimize:** When set to True, the custom user interface window can be minimized.
   
   - **Allow Close:** Prevents users from closing the custom user interface window. If set to True, users will be allowed to close the custom custom user interface window; however, the execution of custom scripts will continue in the background.

   Even if the **Allow Close** option is enabled, OnGuard Agent disables the **Close** button of the custom custom user interface while it is loading a page.

7. **Window Size:** Specify the window height and width, as well as whether the window size should be a percentage of the the client's screen or defined by the size in pixels.
HTML Content for OnGuard Custom Web Pages

The following information is provided in this section:

- **OnGuard Start Page**
- **OnGuard Progress Page**
- **OnGuard Finish Success Page**
- **OnGuard Finish Error Page**
- **OnGuard Finish Reboot Page**

This section provides the required names for each OnGuard custom web page as well as the recommended HTML content.

Be sure to use the **Page Names** specified here as ClearPass Policy Manager and OnGuard Agent look for pages with these names. Text in *italics* should not be changed.

**OnGuard Start Page**

The OnGuard Start Page is the initial web page shown to the end user when script execution begins. This page might include a **Next** button.

**Page Name:** onguard_start

**HTML:**

```html
<p>Your device does not meet Minimum Specifications, which is required before you can connect to the Network.</p>
<p>The following is required:</p>
<div id="tasks_list">
</div>

<p>Please click the **Next** button below to start the remediation needed.</p>

<p>You will be connected to the Network after verification that your device meets all Minimum Security Specifications.</p>

<p><button id="next_button" type="button" onclick=""/>Next</button></p>
```

---

**Note:** If the **Next** button is missing on the OnGuard Start Page, OnGuard Agent will move to the OnGuard Progress Page after 30 seconds. This time duration is not configurable.

**OnGuard Progress Page**

The OnGuard Progress Page shows the progress and status of custom scripts that are being executed.

**Page Name:** onguard_progress

**HTML:**

```html
<p>Please do not disconnect your device.</p>

<div id="task_progress_list">
</div>
```
OnGuard Finish Success Page
The OnGuard Finish Success Page is shown after all the scripts have executed successfully and a system reboot is not necessary. This page includes a Close button.

Page Name: onguard_finish_success

HTML:
<p>We will now rescan your system to verify that it meets Minimum Security Specifications and then connect you to the Network.</p>
<p>If you are not connected in five minutes, please contact <b>12334</b> or click here.</p>
<p><button id="close_button" type="button" onclick="/">Close</button></p>

OnGuard Finish Error Page
The OnGuard Finish Error Page is shown if at least one of the scripts returns Failure and a reboot is not required. This page includes a Close button.

Page Name: onguard_finish_error

HTML:
<p>Remediating your device to meet Minimum Security Specifications was unsuccessful because:</p>
<div id="failed_tasks"></div>
<p>Please visit this Support Page to get assistance.</p>
<p>You are not yet connected to the Network.</p>
<p><button id="close_button" type="button" onclick="/">Close</button></p>

OnGuard Finish Reboot Page
The OnGuard Reboot Page is shown after all the scripts have executed successfully and a system reboot is necessary. This page includes a Reboot button.

HTML:
<p>We will now rescan your system to verify that it meets Minimum Security Specifications and reboot your system, then connect you to the Intel Network.</p>
<p>If you are not connected in five minutes, please contact <b>12334</b> or visit this Support Page to get assistance.</p>
<p><button id="reboot_button" type="button" onclick="/">Reboot</button></p>

Important Points
This section provides important notes regarding OnGuard Agent behavior when using the Custom User Interface for Custom Scripts.

---

In ClearPass Policy Manager 6.6.7, this feature is supported for Windows Persistent Agent only.

1. OnGuard Agent checks the custom script’s exit code to compute the custom scripts status.
2. OnGuard Agent determines the final page based on the script's exit codes and the client's health status. For details, see the next section, OnGuard Custom Script Exit Codes.

3. This feature is not supported when OnGuard is running as a service.

4. The custom user interface loads a fresh web page from ClearPass Guest every time. It does not cache the pages.

5. If the user closes the custom user interface while the script is executing, OnGuard Agent continues executing scripts without the custom user interface.

6. Administrators will have to refresh or open the OnGuard Settings page again after creating web pages in ClearPass Guest (Administration > Agents and Software Updates > OnGuard Settings).

7. If the ClearPass Server Certificate is not validated when ClearPass loads the web page for the first time, the custom user interface displays the following security alert:

   **Figure 779 Server Certificate Not Validated Security Alert**

   ![Security Alert](image)

8. A new option, Server Communication Mode, has been added in Global Agent Settings that you can configure to avoid receiving a Server Certificate security alert (see the Server Communication Mode parameter description in Global Agent Settings Parameters for OnGuard Agents).

### OnGuard Custom Script Exit Codes

The OnGuard custom script exit codes are comprised of Success Codes and Failure Codes as described below:

#### Success Codes (0 to 63)

The range available to Administrators to define their own Success Codes = 3 (0x03) to 63 (0x3F).

- Script executed successfully = 0 (0x00)
- Reboot (Reboot is required) = 2 (0x02)

#### Failure Codes (65 to 255)

The range available to Administrators to define their own Failure Codes = 65 (0x41) to 255 (0xFF).

- Script executed successfully but its exit code indicates failure = 64 (0x40)
OnGuard Agent Codes (256 onwards):

- Unknown error = 256 (0x100)
- Timeout: Script did not finish execution in expected time = 257 (0x101)
- Failed to read exit code of script = 258 (0x102)
- OnGuard failed to execute script = 259 (0x103)
- Script file not found = 260 (0x104)
- Script file did not pass validation checks = 261 (0x105)
- Failed to download script file = 262 (0x106)
- Execution level is set to “User” but the user is not logged on, so OnGuard was not able to launch the script = 263 (0x107)

Software Updates

This section provides the following information:

- About Software Updates
- Software Updates Page on page 757
- Install Update Dialog Box on page 759
- Reinstalling a Patch on page 760
- Uninstalling a Skin on page 761

About Software Updates

This section describes the ClearPass Policy Manager server software update process.

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 (depending on the Cluster-Wide Parameter settings for those parameters). Use the Software Updates page to register for and receive live updates for:

- Posture Signature updates
  These updates include AntiVirus version updates. The ClearPass server uses these updates to check if the versions of the AntiVirus and the DAT file are the latest version.

- Windows Hotfixes updates
  These updates include a list of available Windows Hotfixes for supported Windows operating systems. The ClearPass server uses these updates to show a list of the available hotfixes in the Windows Hotfixes health class.

- Endpoint Profile Fingerprints updates
  These updates include fingerprints and are used by ClearPass in profiling endpoints.

Automatic download and installation for these three types of updates are not enabled by default (see General Parameters for more information).

You can also:

- Reinstall a patch in the event the previous installation attempt fails.
- Uninstall a skin.
Software Updates Page

To update the software on the current ClearPass server:

1. Navigate to Administration > Agents and Software Updates > Software Updates.

Figure 780 displays the Software Updates page:

**Figure 780** Software Updates Page

To update the software on the current ClearPass server:

1. Navigate to Administration > Agents and Software Updates > Software Updates.

Figure 780 displays the Software Updates page:

**Figure 780** Software Updates Page

Table 1 describes the Software Updates parameters

**Table 1: Software Updates Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
</table>
| HPE Passport Credentials      | Enter the HPE Passport Credentials provided to you. This text box is enabled only on a Publisher node. The first time the HPE Passport Credentials are saved, the ClearPass server performs the following operations:  
  - Contacts the Webservice server to download the latest Posture & Profile Data updates (depending on the Cluster-Wide Parameter settings for those parameters).  
  - Checks for any available firmware and patch updates.                                      |
| Import Updates                | To download the Posture and Profile Data Updates to the client (for example, a Windows laptop):  
  1. From the client device, log in to the Aruba Support Center.                                |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Select the <strong>Download Software</strong> tab, then navigate to <strong>ClearPass &gt; Tools &gt; Posture &amp; Profile Data Updates</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click the desired update(s) (which are in zip file format) and save the file.</td>
</tr>
<tr>
<td></td>
<td>4. From ClearPass, click the <strong>Posture and Profile Data Updates &gt; Import Updates</strong> button to import the downloaded file into ClearPass.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>In a ClearPass cluster, the <strong>Import Updates</strong> option is available on the Publisher node only.</td>
</tr>
<tr>
<td></td>
<td>By default, updates for <strong>Posture Signature, Windows Hotfixes</strong>, and <strong>Endpoint Profile Fingerprints</strong> are <em>not</em> automatically downloaded and installed. To set these updates to be automatic, you must set the following Cluster-Wide Parameters to <strong>TRUE</strong>:</td>
</tr>
<tr>
<td></td>
<td><strong>Automatically download Posture Signature and Windows Hotfixes Updates</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Automatically download Endpoint Profile Fingerprints</strong></td>
</tr>
<tr>
<td></td>
<td>For details, refer to <strong>General Parameters</strong>.</td>
</tr>
</tbody>
</table>

**Firmware & Patch Updates**

**NOTE:** The Firmware & Patch Updates table shows only the data that is known to Webservice or imported using the **Import Updates** button.

**NOTE:** Patch residual files under */var/avenda/platform/backup, */var/avenda/platform/patches*, and */var/avenda/platform/store/updates* seven days old and older are automatically deleted daily.

**Import Updates**

If the server is not able to reach the Webservice server, click **Import Updates** to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server.

These patch binaries will appear in the table and can be installed by clicking 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. 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**

Click **Re-Install** to reinstall a patch in the event the previous attempt to install fails.

Reinstalling a patch is available only for the last installed patch.

**Uninstall**

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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Error</td>
<td>This link appears when an update install encounters an error. Clicking this link displays the <strong>Install Update</strong> dialog box, which shows the log messages generated during the install.</td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>Check Status Now</td>
<td>Click this button to perform an on-demand check for available updates. <strong>Check Status Now</strong> applies to updates only on a Publisher node, as well as Firmware &amp; Patch Updates.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use this option to delete a downloaded update.</td>
</tr>
</tbody>
</table>

**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 following methods:

- While the installation is in progress, click the **Install in progress...** link.
- Click the **Installed > Install Error** link.
- When the installation is completed, click the **Needs Restart** link.

The following figure displays the **Install Update** dialog box:

**Figure 781  Install Update Dialog Box**
Specify the **Install Update** parameters as described in the following table:

**Table 2: Install Update Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot</td>
<td>To initiate a reboot of the server, click <strong>Reboot</strong>. The <strong>Reboot</strong> button appears only for updates that require a reboot to complete the installation.</td>
</tr>
<tr>
<td>Clear &amp; Close</td>
<td>To delete the log messages and close the dialog, click <strong>Clear &amp; Close</strong>. <strong>Clear &amp; Close</strong> also removes the corresponding row from the Firmware &amp; Patch Updates table. To delete the log messages from a failed installation, click <strong>Clear &amp; Close</strong>. After the log messages are cleared, attempt the installation again.</td>
</tr>
<tr>
<td>Close</td>
<td>To close the dialog box, click <strong>Close</strong>.</td>
</tr>
</tbody>
</table>

**Webservice Operations**

System Events (as seen on the **Monitoring > Event Viewer** page) shows records for events, such as communication failures with Webservice, successful or failed update downloads, and successful or failed update installations.

The **ClearPass** 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. The Webservice server is refreshed with the Antivirus data hourly and with Windows Updates daily. Fingerprint data and Firmware & Patches are refreshed as soon as new ones are available.

A new list of firmware and update patches that are available for download and installation are noted by the Policy Manager server automatically and shown in the user interface. 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 782**  Viewing the Installed Link for a Skin

3. Click the **Installed** link.
   The **Install Update** dialog opens.

**Figure 783**  Install Update Dialog

4. To uninstall the skin, click **Uninstall**.
   The **Install Update** screen closes and the software is uninstalled.

Support Services

The Administration > Contact Support page provide information for contacting Support, setting up a Remote Assistance session, and viewing ClearPass Policy Manager documentation:

- [Contacting Support on page 761](#)
- [Remote Assistance on page 762](#)
- [Accessing ClearPass Documentation on page 765](#)

Contacting Support

The Administration > Support > Contact Support page provides you with information on how to contact ArubaCare.
Remote Assistance
This section provides the following information:

- Remote Assistance Process
- Setting Up a Remote Assistance Session

The Remote Assistance feature allows a Support engineer to log in remotely using Secured Shell (SSH) to a customer’s ClearPass Policy Manager server and perform the following tasks:

- View and operate the ClearPass Policy Manager user interface to debug any issues the customer is experiencing.
- Perform proactive monitoring of the ClearPass server.

Remote Assistance Process
The Remote Assistance process is as follows:

1. The Administrator sets up a Remote Assistance session.
2. The Support contact receives an email with instructions and credentials to log in to the remote system.
3. The Remote Assistance session is terminated at the end of the specified duration.

You can terminate a session before its stipulated duration.

4. If the ClearPass Policy Manager user interface at the customer site is inaccessible, you can configure a Remote Assistance session through the ClearPass CLI. For details, refer to the following System Commands.
   - `system start-rasession`
   - `system status-rasession`
   - `system terminate-rasession`

Setting Up a Remote Assistance Session
You can set up a Remote Assistance session on a ClearPass Policy Manager server in either a single node or cluster setup.

Sessions can be saved and deleted only from the Publisher node. Sessions can be terminated from Publisher and Subscriber nodes.
To set up a Remote Assistance session:

1. Prior to setting up a Remote Assistance session, you must enter valid **HPE Passport Credentials**. To do so, navigate to **Administration > Agents and Software Updates > Software Updates**.

   The **Software Updates** page opens.

   **Figure 785  Software Updates Page**

   ![Software Updates Page](image)

2. Enter the **HPE Passport Credentials**, then click **Save**.

3. Navigate to **Administration > Support > Remote Assistance**.

   The **Remote Assistance** page opens.

4. Click the **Add Session** link.

   The **Add Session** dialog opens:

   **Figure 786  Remote Assistance > Add Session Dialog**

   ![Add Session Dialog](image)

5. Specify the **Add Session** parameters as described in **Table 1**, then click **Save**.
**Table 1: Add Session Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Name</td>
<td>Enter the name of the Remote Assistance session.</td>
</tr>
</tbody>
</table>
| Session Type         | Specify the **Session Type**:  
  - **One Time Now**: Initiates a session at a specified date and time.  
  - **One Time Future**: Initiates a session on a specified weekday at the selected time.  
  - **Weekly**: Initiates a session on a specified day of every month at the selected time.  
| Duration             | Specify the duration of the Remote Assistance session in hours and minutes. The "session begin" time is the time relative to the ClearPass server's time, and is specified in a 24-hour format. |
| Status               | Indicates the session state. Available states are:  
  - Saving  
  - Scheduled  
  - Initiated  
  - Running  
  - Terminated  
  - Failed |
| HPE Support Contact  | Enter the email ID of the Hewlett Packard Enterprise (HPE) Support contact.                                                                                                                                       |

You return to the **Remote Assistance** page where the new session has been added:

**Figure 787  Remote Assistance Session Added**

The following table describes the information provided for configured Remote Assistance sessions:

**Table 2: Remote Assistance Page Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the session.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates if the session is a one-time session or a periodic session. To view the schedule of the session, move the cursor over the entry.</td>
</tr>
<tr>
<td>Support Contact</td>
<td>The email address of the support contact.</td>
</tr>
<tr>
<td>Status</td>
<td>Provides the session state. Available states are:</td>
</tr>
</tbody>
</table>
### Parameter | Description
--- | ---
- Saving
- Scheduled
- Initiated
- Running
- Terminated
- Failed

**NOTE:** You can edit and save a session in **Scheduled**, **Terminated**, and **Failed** states.
- To terminate a session in **Running** state, select that session and click **Terminate**.
- To delete a session in **Scheduled**, **Terminated**, or **Failed** states, select that session and click **Delete**.
- If a session fails, the Event Viewer indicates the cause of the failure.

**Timestamp** Displays the server time when the Remote Assistance session status was last updated.

## Accessing ClearPass Documentation
The ClearPass Policy Manager **Documentation** page includes links to frequently-used sections of the ClearPass Policy Manager Online Help system.

For example, to view documentation for the CLI, click the **Command Line Interface** button.

This page also provides links to the PDF version of the **ClearPass Policy Manager User Guide** and the **OnGuard Agent Support Charts for Plugin Version 1.0 (V3 SDK) and 2.0 (V4 SDK)**.

To access the **Documentation** page, navigate to **Administration > Support > Documentation**.

**Figure 788  ClearPass Policy Manager Documentation Page**
This chapter covers the following topics:

- Updating Clusters
- Upgrading Clusters

**Updating Clusters**

This section includes the following information:

- Cluster Update Overview
- Before Updating the Cluster
- Updating the Cluster
- Viewing Update Status

**Cluster Update Overview**

The Cluster Update page automates the process of updating the ClearPass cluster with Patch and Skin releases. The cluster Publisher is updated first. You can select one or more Subscribers 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 Subscribers have been updated.

The Cluster Update performs the following actions:

- Copies the update image to the selected Subscribers.
  - Subscribers copy the update image over an HTTPS connection from the Publisher.
  - If you want to avoid the copy on one or more Subscribers:
    1. Log in to the Subscriber node.
    2. Trigger a download of the update image in the Software Update page.
    3. Alternatively, upload the update image through the Software Update page 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 Cluster Update page is accessible again to review progress and log messages.
- The Cluster Update is now initiated on the selected Subscribers; after completion, the Subscribers are rebooted (reboot is initiated only if it is mandatory).
- Where possible, multiple Subscribers are updated in parallel.
- After all selected Subscribers have been updated, you can select and trigger a Cluster Update for any additional Subscribers.

**Time Required for Subscriber Update**

The time required for a Subscriber update depends on the following factors:

- Hardware or virtual appliance model. In the case of virtual machine installations, update times vary significantly based on the I/O per second performance of your virtual machine infrastructure.
- For Subscribers, bandwidth and latency of the network link between the Subscriber and Publisher.
Before Updating the Cluster

Before updating the ClearPass cluster, complete the following tasks:


2. Confirm that Relevant Patch updates are available under the **Firmware & Patch Updates** area of the **Software Updates** page before starting the cluster update. Please download the patches by clicking the **Download** button next to the patches on the **Software Updates** page or load them directly by clicking the **Import Updates** button on the **Software Updates** page.

   Only patches listed under **Software Updates** page are shown in the **Cluster Update** page.

3. Confirm that your Cluster sync and replications are fine before starting the Cluster Update.

4. When a particular Subscribers version information is set to "UNKNOWN," it means the Publisher is not able to contact the remote Subscriber. (If a Subscriber has been disabled and gone out of sync, the Cluster Update page might not detect the disabled status until the patch failure has occurred, after which the failed/inaccessible Subscriber is marked as *UNKNOWN*). Confirm the status of the cluster sync and service status of Async Network Services in such cases (for details, see *Async Network Services Options*).

5. In virtual machine environments, ClearPass Policy Manager Virtual appliance host date and time settings should be in sync with that of the VMware vSphere or Microsoft Hyper-V server that is hosting the instance. Otherwise, you might see inconsistent data in **Time Taken** columns of the **Cluster Update** page.

Updating the Cluster

To update the cluster:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.

2. Click the **Cluster Update** link.

   The **Cluster Update** page opens.

3. Select the **Update Image Name** from the drop-down list.

**Figure 789  Cluster Update Page**

This page includes the information described below in **Table 1**.
Table 1: Information on the Cluster Update Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Info</td>
<td>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.</td>
</tr>
<tr>
<td>Database Info</td>
<td>Shows the size of the Configuration database.</td>
</tr>
<tr>
<td>Publisher Details</td>
<td>Information for the publisher and for all subscribers in the cluster. Information includes the management IP address, version number, zone, Insight database size, last update step completed, and update status.</td>
</tr>
<tr>
<td>Subscriber Details</td>
<td></td>
</tr>
<tr>
<td>Current/Previous Update Steps</td>
<td>During the cluster update, this area displays the status of each stage in the process. As each stage completes, it displays how long it took to complete.</td>
</tr>
<tr>
<td>View Logs</td>
<td>In each publisher and subscriber row, this button when clicked opens the Logs page which provides detailed status and log messages for each update stage.</td>
</tr>
</tbody>
</table>

When the update is available locally and all subscribers have been patched, the Start Update link is available in the upper-right corner of the page.

4. Click Start Update.

The Start Cluster Update page opens.

Figure 790  The Start Cluster Update Page

You can update the entire cluster or just a subset of subscribers.

5. In the Start Cluster Update page, use the check boxes to select the Subscriber nodes to update.
6. To force the update, select Force install patch update under the Install Option area.
7. Click Update.

This initiates the automated update process. No further manual steps are required until all selected subscribers have been updated. The publisher is always updated and rebooted first.

The Cluster Update page is not 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.

The page provides two ways to monitor the progress of the update:

1. On the Cluster Update page, progress indicators in the Current/Previous Update Steps area display the status of some of the main steps.
   Indicators in the Publisher Details and Subscriber Details areas also display when the Publisher or each Subscriber is in progress or completed.
   When the update completes successfully, these areas display a successful update status for the Publisher and every Subscriber.
2. For detailed progress information, click the View Logs button for a Publisher or Subscriber row.
   The Logs page opens. This page includes tabs for the Download, Update, Reboot, and Onboot logs.
   You can view detailed status in these logs during and after the update.
   This button is not available while the Publisher is rebooted and data migration is in progress. It is available again when the Publisher update is complete.

Upgrading Clusters

This section includes the following information:

- Cluster Upgrade Overview
- Sample Times Required for Upgrade
- Before You Upgrade
- Upgrading the Cluster
- Viewing Upgrade Status
- Steps in the Cluster Upgrade Automated Workflow
- Troubleshooting Tips

Cluster Upgrade Overview

The Cluster Upgrade page automates the upgrade procedure for a ClearPass cluster. When the upgrade is initiated, no manual actions are required until the Publisher and all selected Subscriber nodes have been upgraded.

The Cluster Upgrade page can be used to upgrade ClearPass 6.5.3, 6.5.7, and 6.6.x systems to ClearPass 6.7. 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 high-level cluster upgrade process:

1. Download the upgrade image from the Software Updates page.
2. Initiate the Upgrade procedure (see Upgrading the Cluster).
   The Cluster Upgrade tool automatically performs the upgrade.
3. 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).
Cloning a virtual machine to facilitate a ClearPass deployment is not recommended or supported.

Steps in the Cluster Upgrade Automated Workflow

This section describes the steps that are automatically completed by the Cluster Upgrade.

1. To prepare the Subscriber nodes for upgrade, a patch that provides required API support is automatically installed by the Cluster Upgrade on every Subscriber. The Cluster Upgrade uses remote API calls to control and monitor upgrade progress on the Subscribers.

   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 Subscribers copy the upgrade image over an HTTPS connection from the Publisher.

   If the upgrade image is already present on a Subscriber node (assuming you have downloaded it from the **Software Updates** page, or uploaded it in the **Software Updates** page), the existing upgrade image on the Subscriber is used for the upgrade.

3. If the Standby Publisher settings were configured, they are temporarily disabled. This setting is restored after all Subscribers 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** page to review log messages.

6. When the Publisher upgrade is complete, upgrade is initiated on each selected Subscriber. When possible, multiple Subscribers are upgraded in parallel. When each Subscriber is complete, the Subscriber node is rebooted.

7. During the parallel upgrade process, upgrade of the first Subscriber begins five minutes after the Publisher upgrade is completed.

8. Upgrade of the second Subscriber 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 Subscribers have been upgraded, you can select and trigger the upgrade operation for any additional Subscriber nodes.

11. When all the Subscribers in the cluster have been upgraded, the Standby Publisher settings are restored. Detailed information for each of these steps is available in the **Logs** page during and after upgrade.

Sample Times Required for Upgrade

To help you estimate how much time the upgrade might take, **Table 1** displays 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 appliance installations, upgrade times vary significantly based on the I/O per second performance of your virtual appliance infrastructure.

- The size of the configuration database to be migrated.

- For ClearPass Insight appliances, the size of the Insight database.
For Subscribers, the bandwidth and latency of the network link between the Subscriber and the Publisher.

For the most current information about times required for upgrade, refer to the "Before Upgrade" section of the ClearPass 6.7 Release Notes.

Table 1: Sample Times Required for Upgrade

<table>
<thead>
<tr>
<th>Hardware Model</th>
<th>Config DB Size</th>
<th>Insight DB Size</th>
<th>Publisher Upgrade Time</th>
<th>Subscriber Upgrade Time</th>
<th>Insight Restoration Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1000</td>
<td>100 MB</td>
<td>5 GB</td>
<td>50 minutes</td>
<td>50 minutes</td>
<td>20 minutes</td>
</tr>
<tr>
<td></td>
<td>200 MB</td>
<td>5 GB</td>
<td>60 minutes</td>
<td>60 minutes</td>
<td>20 minutes</td>
</tr>
<tr>
<td>C2000</td>
<td>100 MB</td>
<td>5 GB</td>
<td>50 minutes</td>
<td>50 minutes</td>
<td>15 minutes</td>
</tr>
<tr>
<td></td>
<td>200 MB</td>
<td>5 GB</td>
<td>60 minutes</td>
<td>60 minutes</td>
<td>15 minutes</td>
</tr>
<tr>
<td>C3000</td>
<td>200 MB</td>
<td>5 GB</td>
<td>30 minutes</td>
<td>30 minutes</td>
<td>15 minutes</td>
</tr>
<tr>
<td></td>
<td>500 MB</td>
<td>10 GB</td>
<td>40 minutes</td>
<td>40 minutes</td>
<td>20 minutes</td>
</tr>
</tbody>
</table>

Before You Upgrade

Before you begin the cluster upgrade process, ensure that the following tasks have been completed:

2. Plan for adequate downtime for the upgrade. Use the upgrade time estimates in Table 1 as a guide.
3. 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.
4. HTTP, HTTPS, and SSH port traffic must be allowed between the cluster appliances. This is required for the Cluster Upgrade to be able to communicate between appliances.
   Verify that the following ports are in an open state between the cluster appliances:
   - Port 80 (HTTP)
   - Port 443 (HTTPS)
   - Port 22 (SSH)
5. Confirm that the Publisher and all Subscriber nodes in the cluster are in sync before starting the upgrade.
6. On the Software Updates page, enter the HPE Passport Credentials.
7. On the Publisher, download the ClearPass 6.7 upgrade image from the Software Updates page (see Software Updates).
   The Cluster Upgrade page automates the process of copying over the upgrade image to the selected Subscriber nodes in the cluster.
8. 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 Contacting Support), 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 (for more information, see Service Commands).

9. When a particular Subscriber version information is set to "UNKNOWN," it means the Publisher is not able to contact the remote Subscriber.

If a Subscriber has been disabled and gone out of sync, the Cluster Upgrade page might not detect the status until the patch failure has occurred, after which the failed or inaccessible subscriber is marked as **UNKNOWN**.

In such cases, confirm the status of the cluster sync and the service status of **Async network services** (for details, see Async Network Services Options).

a. In virtual machine environments, ClearPass Policy Manager virtual machine host date and time settings should be in sync with that of the VMware vSphere Hypervisor server or Microsoft Hyper-V server that is hosting the instance. Otherwise, you might see inconsistent data in **Time Taken** columns of the **Cluster Upgrade** page.

**Upgrading the Cluster**

To upgrade the ClearPass cluster:

1. Navigate to **Administration > Agents and Software Updates > Software Updates**.
2. Click the **Cluster Upgrade** link.

   The **Cluster Upgrade** page opens.

**Figure 791 Cluster Upgrade Page**

This page includes the information described below in **Table 1**.

**Table 1: Information on the Cluster Upgrade Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Info</td>
<td>Describes the upgrade image's name and size, and includes release-specific comments.</td>
</tr>
<tr>
<td>Database Info</td>
<td>Shows the size of the Configuration database.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Publisher Details</td>
<td>Provides information for the Publisher and for all Subscribers in the cluster. Information includes the management IP address, version number, zone, Insight database size, last upgrade step completed, and upgrade status.</td>
</tr>
<tr>
<td>Upgrade Steps</td>
<td>During the cluster upgrade, this area displays the status of each stage in the process. As each stage completes, it displays how long it took to complete.</td>
</tr>
<tr>
<td>View Logs</td>
<td>In each Publisher and Subscriber row, clicking this button opens the Logs page which provides detailed status and log messages for each upgrade stage.</td>
</tr>
</tbody>
</table>

When you open the **Cluster Upgrade** page, it immediately prepares the Subscriber nodes 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 displayed during this stage.

To install the patch for API support on subscribers, these subscribers 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 6.7 upgrade image is available locally and all subscribers have been patched, the **Start Upgrade** link is available.

3. Click **Start Upgrade**.

The **Start Cluster Upgrade** page opens.

**Figure 792 The Start Cluster Upgrade Page**

You can upgrade the entire cluster or just a subset of Subscribers.
4. In the **Start Cluster Upgrade** window, use the check boxes to select the Subscribers to upgrade.

5. In the **LogDB backup and restore options** drop-down list, select one of these options:
   a. **Access tracker records are backed up but will not be restored**: Select if you need a backup of the access tracker records to potentially restore after upgrade.
      This option increases the overall upgrade time.
   b. **Do not backup access tracker records**: Select if you do not need a backup of the access tracker records.

6. Click **Upgrade**.
   The Cluster Upgrade 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 Cluster Upgrade Automated Workflow](#).
   The Publisher is always upgraded and rebooted first. The **Cluster Upgrade** page is not available while the Publisher is rebooted and data migration is in progress.

7. When the Publisher upgrade is complete, navigate to the **Cluster Upgrade** page to monitor upgrade progress, as described in [Viewing Upgrade Status](#).

8. After a successful upgrade, confirm that all the Subscriber nodes in the cluster are back in sync and all the services are accessible.

9. 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**.

This feature provides two ways to monitor the progress of the upgrade:

1. On the **Cluster Upgrade** page, progress indicators in the **Upgrade Steps** area display the status of some of the main steps.
   Indicators in the **Publisher Details** and **Subscriber Details** areas also display when the Publisher or each Subscriber node is in progress or completed.
   When the upgrade is complete, these areas display a successful upgrade status for the Publisher and every Subscriber node.

2. For detailed progress information, click the **View Logs** button for the publisher or subscriber row.
   The **Logs** page opens. This page includes tabs for the **Patch, Download, Upgrade, Reboot, and Onboot** logs.
   You can view detailed status in these logs during and after the upgrade.

---

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.

### Troubleshooting Tips

Here are a couple of troubleshooting tips when upgrading a cluster:

- If you encounter errors while upgrading a Subscriber node, 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 (see [Cluster Commands](#)).
Be aware that all status and progress information is reset when the Publisher is reverted to a previous version. You can initiate the upgrade again from the Cluster Upgrade page.
This chapter includes the following information:
- Enabling Ingress Event Dictionaries
- Configuring the Ingress Event Source
- Configuring an Event-Based Enforcement Service
- Configuring the Ingress Receiving Ports
- Enabling Ingress Events Processing

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 the defined enforcement policies and services.

**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. The set of ingress event dictionaries are displayed. By default, they are disabled.

   **Figure 793  Viewing Ingress Event Dictionaries**

2. To enable a dictionary, select the disabled Ingress Events Dictionary for the appropriate vendor.

   The Events Attributes dialog opens.

   ```
   Administration > Dictionaries > Ingress Events
   Ingress Events Dictionaries
   Filter: Vendor   
   Selection:  
   Profile:  
   #   Vendor   
   1. Check Point   
   2. Infoblox   
   3. Juniper Networks   
   4. Juniper Networks   
   5. Juniper Networks   
   6. Juniper Networks   
   7. Juniper Networks   
   8. Juniper Networks   
   9. Park IoT Networks   
   Vendor:  
   Filter:  
   Profile:  
   #   Vendor   
   1. Check Point   
   2. Infoblox   
   3. Juniper Networks   
   4. Juniper Networks   
   5. Juniper Networks   
   6. Juniper Networks   
   7. Juniper Networks   
   8. Juniper Networks   
   9. Park IoT Networks   
   Show 10 | All records
   ```
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** (see **Figure 795**).

**Figure 795  Ingress Events Dictionary Enabled**

---

**Configuring the Ingress Event Source**

An event source is a device that sends Syslog events to ClearPass.

---

Any events sent that are not from configured event sources are ignored.

---

To configure an Event Source:

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 Event Source** dialog opens.
Figure 796  Adding an Event Source

3. Populate the **Add Event Source** parameters as described in Table 1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name or the IP address of the device that will send Syslog events to ClearPass.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description of this Event Source.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the device that will send Syslog events to ClearPass.</td>
</tr>
<tr>
<td>Type</td>
<td>From the drop-down, select <strong>Syslog</strong>.</td>
</tr>
<tr>
<td>Vendor</td>
<td>From the drop-down, select the event source <strong>Vendor</strong>:</td>
</tr>
<tr>
<td></td>
<td>- Aruba Introspect</td>
</tr>
<tr>
<td></td>
<td>- Check Point</td>
</tr>
<tr>
<td></td>
<td>- Infoblox</td>
</tr>
<tr>
<td></td>
<td>- Juniper Networks</td>
</tr>
<tr>
<td></td>
<td>- Palo Alto Networks</td>
</tr>
<tr>
<td>Enable</td>
<td>Select this check box to enable the device as an Event Source.</td>
</tr>
</tbody>
</table>

4. When finished, click **Add**.

The **Event Sources** page now displays the new Event Sources (see Figure 797).

Figure 797  Event Sources Page

Note that the IP address displayed in Figure 797 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 ingress-related events.

By default, the ingress receiving port is 514 for both TCP and UDP. You can modify the ingress receiving ports with 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 (see Figure 798).

**Figure 798  Selecting the Ingress Syslog Service**

As you can see in Figure 798, 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 port numbers 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 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.
2. To add the service, click Add.
The **Add Services** dialog opens.

3. From the **Type** drop-down list, select **Event-based Enforcement** (see Figure 799).

**Figure 799** Specifying Event-Based Enforcement

4. Specify the **Service** tab parameters for this service as described in the following table:

**Table 1: Event-Based Enforcement > Service Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select <strong>Event-based Enforcement</strong>.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter the name or label for the service you want to create.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter the description that provides additional information to identify the service. This field is optional but recommended.</td>
</tr>
<tr>
<td><strong>Monitor Mode</strong></td>
<td>Optionally, check <strong>Enable to monitor network access without enforcement</strong> to allow authentication and health validation exchanges to take place between the endpoint and Policy Manager, but without enforcement. In <strong>Monitor Mode</strong>, no enforcement profiles (and associated attributes) are sent to the network device.</td>
</tr>
</tbody>
</table>

**Service Rule**

<table>
<thead>
<tr>
<th>Matches</th>
<th>Select one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANY</strong></td>
<td>Matches one of the configured conditions.</td>
</tr>
<tr>
<td><strong>ALL</strong></td>
<td>Specifies to match all of the configured conditions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Type</strong></th>
<th>Select the type of data filter:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date</strong></td>
<td><strong>Event</strong></td>
</tr>
<tr>
<td></td>
<td>Then configure the <strong>Name</strong>, <strong>Operator</strong>, and <strong>Value</strong> for the selected type accordingly.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Select the name of the attribute. The <strong>Name</strong> list varies according to which <strong>Type</strong> you selected.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operator</strong></td>
<td>Select any subset of string data type operators from the <strong>Operator</strong> drop-down list.</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>Enter or select the value of the attribute.</td>
</tr>
</tbody>
</table>
Associating the Service with an Enforcement Policy

After you create the event-based enforcement service, you must associate the service with an enforcement policy.

1. From the Add Services > Service page, click Next.
   The Services > Enforcement page opens.

   **Figure 800 Selecting the Ingress Events Enforcement Policy**

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

2. Specify the Add Services > Enforcement parameters as described in the following table, then click Save.

   **Table 2: Add Service > Enforcement Page Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Cached Results</td>
<td>Select this check box to use cached roles and posture attributes from previous sessions.</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td>From the drop-down list, select the preconfigured enforcement policy. This is mandatory. If you do not have any preconfigured enforcement policies, click the Add New Enforcement Policy link to create a new enforcement policy.</td>
</tr>
</tbody>
</table>

   **Enforcement Policy Details**

   | Description            | Displays additional information about the selected enforcement policy.                                                                                   |
   | Default Profile        | Displays the name of the profile applied by the selection of the enforcement policy.                                                                    |
   | Rules Evaluation Algorithm | Shows the first matched rule and returns the role; or selects all matched rules and return a set of roles.                        |
   | Conditions             | Displays the conditions configured for the selected enforcement policy rules configuration.                                                              |
   | Enforcement Profiles   | Displays the enforcement profile(s) specified in the selected enforcement policy.                                                                      |

   **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 opens to the System tab.

**Figure 801  Enabling Ingress Event Processing**

3. 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 802  Warning Dialog for Enabling Ingress Events Processing**

4. To proceed with ingress events processing on this server, click Yes.
   For details on the Server Configuration > System Tab parameters, see System Page.
This chapter includes the following information:

- **Introduction**
- **Authentication in Guest Web Login Using OnGuard Native Dissolvable Agent**
- **Accessing the OnGuard Support Charts**
- **Unified Agent System Tray Status Icons**
- **Upgrading From OnGuard Plugin Version 1.0 to 2.0**
- **Native Agents Only Mode**
- **Configuring Web Agent Flow—Native Agent**

### 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 to be unsecure, which is accomplished by running an extensive posture assessment.

The OnGuard Agent is supported by Windows, Linux, and MacOS devices. For information on the supported browsers for OnGuard Native agent, refer to the ClearPass Release Notes.

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 Native Agents Only mode.

The 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 (for details, see Native Agents Only Mode).

### Authentication in Guest Web Login Using OnGuard Native Dissolvable Agent

- **Creating a Guest Web Login Page for Native Dissolvable Agent**
- **Creating a RADIUS Service in ClearPass for VPN Authentication**
- **Configuring the Guest Access - Web Login Service Template**
- **Configuring a Web-Based Health Check Only Service**
- **Enabling the VPN Interface**
- **Access Tracker Requests Reflect Credentials**

This section describes how to enable application authentication in Guest Web Login pages while using the OnGuard Native Dissolvable Agent to also identify the username.

---

**NOTE**

The Dissolvable Agent, by default, does not perform end-user authentication.

---

The OnGuard Dissolvable Agent can be supported with VPN interfaces when:
The same username is used to identify the client in both RADIUS VPN authentication and application authentication.

- **Pre-Auth Check** is configured using one of the following values (refer to Table 1 for details):
  - App Authentication
  - Local
  - RADIUS
  - Single Sign On

### Creating a Guest Web Login Page for Native Dissolvable Agent

To create a Guest Web Login page for Native Dissolvable Agent:

1. Log in to ClearPass Guest, then navigate to **Configuration > Pages > Web Logins**. The Web Logins page opens.
2. Click the Create a new web login page link. The Guest Web Login Editor opens.

### Figure 803 Guest Web Login Editor

3. Specify the **Web Login Editor** parameters as described in the following table:
For details about all the settings available in the Web Login Editor, see the "Creating and Editing Web Login Page" section in the ClearPass 6.7 Guest User Guide.

**Table 1: Web Login Editor Properties for Native Dissolvable Agent Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name for the page.</td>
</tr>
<tr>
<td>Page Name</td>
<td>Enter the Identifier page name that will appear in the URL—for example, &quot;/guest/page_name.php&quot;. The Page Name must consist of letters, numbers, underscore ( _ ), or dash ( - ).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter additional information or comments about the page.</td>
</tr>
</tbody>
</table>
| Vendor Settings        | (Required) Specifies vendor-specific settings for network configuration. This drop-down list includes a list of vendors you can select from and a list of Other settings.  
  - Select Aruba Networks. |
| Login Method           | Specifies how the user's network login should be handled.                           
  - Select Policy Initiated—An enforcement policy will control a change of authorization.  
  This option should be selected if you are using OnGuard health checks. |
| **Page Redirect**      |                                                                                     |
| Security Hash          | Specifies the level of checking to apply to URL parameters passed to the Web Login page.  
  - Select Do not check — login will always be permitted |
| **Login Form**         |                                                                                     |
| Authentication         | Specifies the authentication requirement method to use.                             
  - Select Credentials — Require a username and password |
| Prevent CNA            | If selected, this option enables bypassing the Apple Captive Network Assistant (CNA). The CNA is the pop-up browser shown when joining a network that has a captive portal.  
  - Click this check box to enable the Prevent CNA option. |
| Pre-Auth Check         | Specifies how the username and password should be checked before authentication.     
  - Select App Authentication — check using Aruba Application Authentication.  
  When App Authentication is not enabled, Native Dissolvable Agent uses the MAC address as the user name.  
  When App Authentication is enabled (with Health Check also enabled), instead of using the MAC address as the username in the WebAuth Request, Native Dissolvable Agent sends the username specified in the App Authentication option.  
  If Pre-Auth Check has one of the following values, Native Dissolvable Agent sends the username specified in App Authentication:  
  - App Authentication: Check using Aruba Application Authentication.  
  - Local: Match a local account.  
  - RADIUS: Check using a RADIUS request.  
  - Single Sign On: Enable SSO for this web login. |
| Terms                  | Select this check box to require the user to mark a check box to accept a Terms and Conditions agreement. |
| **Default Destination**|                                                                                     |
### Field | Action/Description
--- | ---
Default URL | (Required) Specify the default URL for the redirect page. For external domains, this must include the `http://` prefix.
Override Destination | Select this check box to force the default destination for all clients, overriding any default value already set on the client.

#### Post-Authentication

<table>
<thead>
<tr>
<th>Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Check</td>
<td>Select this check box to require the guest to pass a health check before they can access the network. The health check is done automatically through the OnGuard Dissolvable Agent.</td>
</tr>
</tbody>
</table>

4. Click **Save Changes**.
   You return to the **Web Logins** page, where the name of the new page is now displayed.

**Figure 804**  
*New Guest Web Login Page Added*

---

**Creating a RADIUS Service in ClearPass for VPN Authentication**

To create a RADIUS service in ClearPass for VPN Authentication:

1. In ClearPass, navigate to **Configuration > Services**.
   The **Services** page opens.
2. Click **Add**.
   The **Add Services** dialog opens.
3. From the **Type** drop-down, select **RADIUS Enforcement (Generic)**.
   The **RADIUS Enforcement (Generic)** service configuration dialog opens:
4. Proceed to configure the RADIUS Enforcement service to match the service settings displayed in **Figure 806**.

**Figure 806  Summary of the RADIUS Enforcement Service**

For details on configuring RADIUS Enforcement Services (Generic), refer to [RADIUS Enforcement (Generic) Service](#) on page 73.

5. Specify the RADIUS Enforcement Service (Generic) service parameters as described in the table below.
### Table 2: Aruba RADIUS Enforcement (Generic) Service Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>RADIUS Enforcement (Generic)</strong>.</td>
</tr>
<tr>
<td>Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>More Options</td>
<td>Not required.</td>
</tr>
<tr>
<td><strong>Authentications</strong></td>
<td></td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>Specify the following authentication methods:</td>
</tr>
<tr>
<td></td>
<td>- EAP-MSCHAPV2</td>
</tr>
<tr>
<td></td>
<td>- MSCHAPV2</td>
</tr>
<tr>
<td></td>
<td>- EAP-PEAP</td>
</tr>
<tr>
<td></td>
<td>Add additional authentication methods as needed for this service.</td>
</tr>
<tr>
<td>Authentication Sources</td>
<td>Select the following authentication sources:</td>
</tr>
<tr>
<td></td>
<td>- [Local User Repository] [Local SQL DB]</td>
</tr>
<tr>
<td></td>
<td>- [Guest User Repository] [Local SQL DB]</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can also add Active Directory (AD) as an authentication source.</td>
</tr>
<tr>
<td>Strip Username Rules</td>
<td>Not required.</td>
</tr>
<tr>
<td>Service Certificate</td>
<td>Not required.</td>
</tr>
<tr>
<td><strong>Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Role Mapping Policy</td>
<td>Not required.</td>
</tr>
<tr>
<td><strong>Enforcement</strong></td>
<td></td>
</tr>
<tr>
<td>User Cached Results</td>
<td>Select this check box to use cached roles and posture attributes from previous sessions.</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td>Select [Sample Allow Access Policy].</td>
</tr>
</tbody>
</table>

6. Click **Save**.

**Configuring the Guest Access - Web Login Service Template**

In this web login service, you associate the **Guest Web Login page for Native Dissolvable Agent** created earlier (see [Creating a Guest Web Login Page for Native Dissolvable Agent](#) above) with the **Guest Access - Web Login** service.
To configure the **Guest Access - Web Login** service:

1. Navigate to **Configuration > Service Templates & Wizards**.
   The list of ClearPass Service Templates and Wizards opens.
2. Select **Guest Access - Web Login**.
   The **Guest Access Web Login** service template opens:

   **Figure 807**  *Guest Access- Web Login Service Template*

3. In the **Name Prefix** field, enter the prefix.
   This prefix is appended to services that use the Guest Access - Web Login template.
4. Click Next.
   The **Service Rule** dialog opens.

   **Figure 808**  *Guest Access - Web Login Service Rule Configuration*

5. Select the **Guest Access Restrictions** tab to specify the days of the week that guest users are allowed network access.
6. Click **Add Service**.
   You return to the **Services** page. The following message is displayed:

   *Added 1 Enforcement Policies*
   *Added 1 Service(s)*

**Configuring a Web-Based Health Check Only Service**

To create a Web-Based Health Check Only service:

1. Navigate to Configuration > Services, then click the **Add** link.
   The Add Services dialog opens.
2. From the **Type** drop-down, select **Web-based Health Check Only**.
   The **Web-based Health Check Only** service configuration dialog opens:
3. Proceed to configure the Web-based Health Check Only service to match the service settings displayed in Figure 810.

**Figure 810 Summary of Web-based Health Check Only Service**

4. Specify the Web-based Health Check Only service parameters as described in the following table.

**Table 3: Web-based Check Only Service Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide additional information that helps to identify the service.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Web-based Health Check Only</strong>.</td>
</tr>
<tr>
<td>Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Parameter</td>
<td>Action/Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>More Options</td>
<td>Click the check box for <strong>Posture Compliance</strong>. The <strong>Posture</strong> tab is added.</td>
</tr>
<tr>
<td><strong>Service Rule</strong></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Host</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Select <strong>CheckType</strong>.</td>
</tr>
<tr>
<td>Operator</td>
<td>Select <strong>MATCHES_ALL</strong>.</td>
</tr>
<tr>
<td>Value</td>
<td>Select Health.</td>
</tr>
<tr>
<td><strong>Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Role Mapping Policy</td>
<td>Not required.</td>
</tr>
<tr>
<td><strong>Posture</strong></td>
<td></td>
</tr>
<tr>
<td>Posture Policies</td>
<td>Select <strong>Posture_Compliance</strong>.</td>
</tr>
<tr>
<td>Default Posture Token</td>
<td><strong>HEALTHY</strong></td>
</tr>
<tr>
<td>Remediate End-Hosts</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remediation URL</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Enforcement</strong></td>
<td></td>
</tr>
<tr>
<td>User Cached Results</td>
<td>Disabled</td>
</tr>
<tr>
<td>Enforcement Policy</td>
<td>Select [<strong>RADIUS CoA Terminate Session</strong>].</td>
</tr>
</tbody>
</table>

5. Click **Save**.
For details on configuring a Web-based Health Only service, refer to [Web-based Health Check Only Service](#).
Enabling the VPN Interface
To enable the VPN interface in the set of managed interfaces:

1. Navigate to Administration > Agents and Software Updates > OnGuard Settings.
   The OnGuard Settings page opens.

Figure 811  Enabling the VPN Managed Interface

2. In the Native Dissolvable Agent Customization > Managed Interfaces section, check (enable) the VPN check box. (The Wired and Wireless interfaces are enabled by default.)

3. Click Save.

Access Tracker Requests Reflect Credentials
As shown in Figure 812, the ClearPass Access Tracker shows that the credentials configured in the RADIUS Enforcement service are the same credentials used in the Guest Web Login and the Webauth service.

Figure 812  Access Tracker Information

- The RADIUS request is obtained when connected to a VPN.
- The Application authentication is obtained when logged into Guest Web Login.
- The Webauth request is obtained after health checks have been performed.

Accessing the OnGuard 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
There are two sets of support charts provided:

- OnGuard Agent Support Charts for Plugin Version 1.0 (OnGuard Detection V3 SDK)
- OnGuard Agent Support Charts for Plugin Version 2.0 (OnGuard Detection V4 SDK)
The plugin version 2.0 support charts pertain to the V4 SDK.

**Figure 813  OnGuard Agent Support Charts for Plugin Versions 1.0 and 2.0**

---

**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 1* describes that icons that indicate the possible states for the Unified Agent.
<table>
<thead>
<tr>
<th>OnGuard Status</th>
<th>Network Type</th>
<th>VPN Status</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthy</td>
<td>Trusted</td>
<td>Connected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Healthy</td>
<td>Trusted</td>
<td>Disconnected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>Trusted</td>
<td>Connected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>Trusted</td>
<td>Disconnected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Healthy</td>
<td>Untrusted</td>
<td>Connected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Healthy</td>
<td>Untrusted</td>
<td>Disconnected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>Untrusted</td>
<td>Connected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>Untrusted</td>
<td>Disconnected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Healthy</td>
<td>N/A</td>
<td>Error</td>
<td>![Red Icon]</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>N/A</td>
<td>Error</td>
<td>![Red Icon]</td>
</tr>
<tr>
<td>Logged Out: No Health Status</td>
<td>N/A</td>
<td>Error</td>
<td>![Red Icon]</td>
</tr>
<tr>
<td>Error</td>
<td>Trusted</td>
<td>Connected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Error</td>
<td>Trusted</td>
<td>Disconnected</td>
<td>![Red Icon]</td>
</tr>
<tr>
<td>Error</td>
<td>Untrusted</td>
<td>Connected</td>
<td>![Green Icon]</td>
</tr>
<tr>
<td>Error</td>
<td>Untrusted</td>
<td>Disconnected</td>
<td>![Red Icon]</td>
</tr>
<tr>
<td>Error</td>
<td>No Profile</td>
<td>N/A</td>
<td>![Yellow Icon]</td>
</tr>
<tr>
<td>Error</td>
<td>N/A</td>
<td>Error</td>
<td>![Red Icon]</td>
</tr>
<tr>
<td>OnGuard Status</td>
<td>Network Type</td>
<td>VPN Status</td>
<td>Icon</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>Healthy</td>
<td>No Profile</td>
<td>N/A</td>
<td>🟢</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>No Profile</td>
<td>N/A</td>
<td>🔴</td>
</tr>
<tr>
<td>Logged Out: No Health Status</td>
<td>No Profile</td>
<td>N/A</td>
<td>🟢</td>
</tr>
<tr>
<td>Logged Out: No Health Status</td>
<td>Trusted</td>
<td>Connected</td>
<td>🟢</td>
</tr>
<tr>
<td>Logged Out: No Health Status</td>
<td>Untrusted</td>
<td>Disconnected</td>
<td>🟢</td>
</tr>
</tbody>
</table>

### OnGuard-Only System Tray Icons

Table 2 describes that icons that indicate the possible states for OnGuard-only.

<table>
<thead>
<tr>
<th>OnGuard Status</th>
<th>Network Type</th>
<th>VPN Status</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthy</td>
<td>N/A</td>
<td>N/A</td>
<td>🟢</td>
</tr>
<tr>
<td>Unhealthy</td>
<td>N/A</td>
<td>N/A</td>
<td>🔴</td>
</tr>
<tr>
<td>Logged Out: No Health Status</td>
<td>N/A</td>
<td>N/A</td>
<td>🟢</td>
</tr>
<tr>
<td>Error</td>
<td>N/A</td>
<td>N/A</td>
<td>🟢</td>
</tr>
</tbody>
</table>

### Upgrading From OnGuard Plugin Version 1.0 to 2.0

This section contains the following information:

- **Overview**
- Creating a New Enforcement Profile to Set the SDK Type
- Modifying an Existing Enforcement Policy for OnGuard Plugin v2.0
- Creating a New Posture Policy for OnGuard Plugin v2.0 Agents
- Creating a WebAuth Service for OnGuard Plugin v2.0 Agents
- Important Points
Overview
The ClearPass OnGuard Agents for Windows and macOS support OnGuard plugin version 2.0, which provides enhanced product detection.

The new OnGuard plugin version 2.0 is based on the OESIS V4 SDK, while the earlier plugin version 1.0 is based on the OESIS V3 SDK. OnGuard continues to use plugin version 1.0 and your existing V3 SDK policies until you explicitly upgrade to plugin version 2.0, as described in this section.

Customers who use ClearPass OnGuard must upgrade to the OnGuard Plugin version 2.0 (V4 SDK) in order to maintain application signature and virus definition updates. As of May 1, 2018, the V3 SDK and AV Updates for V3 SDK are no longer supported by OPSWAT. Since virus definitions are updated at least once a day, and sometimes several times a day, it is important to maintain regular automatic updates.

To upgrade to plugin version 2.0, you will first upgrade the OnGuard agents, after which you create a new enforcement profile, enforcement policy, and a Web Auth service. Finally, you will need to modify any existing V3 SDK enforcement policies to use the V4 SDK.

Creating a New Enforcement Profile to Set the SDK Type
The first task in upgrading to the OnGuard plugin version 2.0 is to create a new enforcement profile where you set the attribute SDK Type to V4.

To create the OnGuard plugin version 2.0 enforcement profile:

1. Navigate to Configuration > Enforcement > Profiles.
   The Enforcement Profiles page opens.
2. Click the Add link.
   The Add Enforcement Profile dialog opens.

Figure 814 Adding a V4 Agent Enforcement Profile

3. Specify the Add V4 Agent Enforcement Profile parameters as described in the following table:
**Table 1: Add V4 Agent Enforcement Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Select <em>Agent Enforcement</em>.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for this enforcement profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally (but recommended), add a description of this enforcement profile.</td>
</tr>
<tr>
<td>Type</td>
<td>When you select the <em>Agent Enforcement</em> template, the enforcement profile <strong>Type</strong> is set automatically to <em>Agent</em>.</td>
</tr>
<tr>
<td>Action</td>
<td>Keep the default action: <strong>Accept</strong>.</td>
</tr>
<tr>
<td>Device Group List</td>
<td>The <strong>Device Group List</strong> is no longer pertinent and this option is grayed out.</td>
</tr>
</tbody>
</table>

4. Click **Next**.  
   The **Attributes** dialog opens.  

*Figure 815*  **Specifying the SDK Type Attribute to V4**

5. Optionally (but recommended), specify a message in the **Message** attribute.  
6. Select **Click to add**, then make the following selections:  
   - Attribute Name: **SDK Type**  
   - Attribute Value: **V4**  
7. Click **Save**.  
   The new enforcement profile is added.

**Modifying an Existing Enforcement Policy for OnGuard Plugin v2.0**

If you have an existing enforcement policy of the WebAuth service that is being used for OnGuard plugin version 1.0: V3 SDK, you must modify the enforcement policy to support OnGuard plugin version 2.0.

To modify an existing enforcement policy to support OnGuard plugin version 2.0:

1. Navigate to **Configuration > Enforcement > Policies**.  
   The **Enforcement Policies** page opens.
2. Select the enforcement policy of the WebAuth service that is being used for the OnGuard plugin version 1.0.

   The Edit Enforcement Policies page opens.

3. Select the Enforcement tab.

4. Update the Name and Description if necessary.

5. Click Modify.

6. Select the Attributes tab.

7. Change the SDK Type > Attribute Value to V4, then click Save.

   The Enforcement Policy has been updated to support the OnGuard plugin version 2.0: V4 SDK. When the agent next performs a health check, it picks OnGuard plugin version 2.0.

**Creating a New Posture Policy for OnGuard Plugin v2.0 Agents**

The supported posture policy for the OnGuard plugin version 2.0 is required because many third-party products that were not supported by OnGuard plugin version 1.0 are supported by OnGuard plugin version
2.0. Also, the names of some of the antivirus products that are recognized by the OnGuard plugin version 1.0 are changed in OnGuard plugin version 2.0.

When you create a new posture policy, by default the new posture policy uses V4 support charts (see Accessing the OnGuard Support Charts).

To create a posture policy for OnGuard plugin version 2.0 V4 SDK agents:


**Figure 819 Creating a Posture Policy for OnGuard Plugin Version 2.0 V4 SDK Agents**

2. Specify the Add V4 Posture Policy parameters as described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Enter the name of this posture policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally (but recommended), add a description of this posture policy.</td>
</tr>
<tr>
<td>Posture Agent</td>
<td>Specify OnGuard Agent (the default).</td>
</tr>
<tr>
<td>Host Operating System</td>
<td>Specify Windows (the default).</td>
</tr>
<tr>
<td>Plugin Version</td>
<td>Plugin version <strong>2.0</strong> is specified by default. This is the plugin version required by the V4 SDK.</td>
</tr>
<tr>
<td>Restrict by Roles</td>
<td>Configure the roles as required by your installation. For more information on role configuration, see Adding and Modifying Roles.</td>
</tr>
</tbody>
</table>

3. Click Next. The Posture Plugins page opens.
Figure 820  Selecting the Posture Plugin

4. Click the check box for the **ClearPass Windows Universal System Health Validator**, then click **Configure**:  

Figure 821  Configuring the V4 Posture Plugin

5. Specify the **ClearPass Windows Universal System Health Validator** parameters as described in the following table:

**Table 3: Add V4 Posture Plugin Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows OS list</td>
<td>Select the Windows version of choice.</td>
</tr>
<tr>
<td>Enable checks for Windows &lt;version&gt;</td>
<td>Select the check box for <strong>Enable checks</strong> for the selected version of Windows.</td>
</tr>
<tr>
<td>Firewall</td>
<td>From the list of Windows checks, select <strong>Firewall</strong>.</td>
</tr>
<tr>
<td>Firewall application</td>
<td>Select the check box for <strong>A firewall application is on</strong>.</td>
</tr>
<tr>
<td>Product-specific checks</td>
<td>To allow any firewall product, uncheck <strong>Product-specific checks</strong>.</td>
</tr>
</tbody>
</table>

6. Click **Save**.
Once you have defined the posture hosts, agents, and plugins, you must configure the rules for the posture policy.

7. Select the Rules tab, then click Add Rule.
   The Rules Editor opens.

**Figure 822 Configuring OnGuard Plugin Version 2.0 Posture Policy Rules**

8. Specify the Rules Editor parameters as described in the following table, then click Save:

**Table 4: Rules Editor Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Conditions</strong></td>
<td></td>
</tr>
<tr>
<td>Select Plugin Checks</td>
<td>Select <strong>Passes all SHV</strong> checks (the default setting). The following plugin check types are available for System Health Validators (SHVs):</td>
</tr>
<tr>
<td></td>
<td>■ Passes all SHV checks</td>
</tr>
<tr>
<td></td>
<td>■ Passes one or more SHV checks</td>
</tr>
<tr>
<td></td>
<td>■ Fails all SHV checks</td>
</tr>
<tr>
<td></td>
<td>■ Fails one or more SHV checks</td>
</tr>
<tr>
<td>Select Plugins</td>
<td>Select the plugin to which the plugin checks should apply. In this case, the <strong>ClearPass Windows Universal System Health Validator</strong> plugin has been automatically selected.</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td></td>
</tr>
<tr>
<td>Posture Token</td>
<td>Select <strong>HEALTHY (0)</strong> (the default setting). The following Posture Token settings are available:</td>
</tr>
<tr>
<td></td>
<td>■ HEALTHY (0)</td>
</tr>
<tr>
<td></td>
<td>■ CHECKUP (10)</td>
</tr>
<tr>
<td></td>
<td>■ TRANSITION (15)</td>
</tr>
<tr>
<td></td>
<td>■ QUARANTINE (20)</td>
</tr>
<tr>
<td></td>
<td>■ INFECTED (30)</td>
</tr>
<tr>
<td></td>
<td>■ UNKNOWN (100)</td>
</tr>
</tbody>
</table>

The following figure displays a summary of all the settings for this posture policy:
Figure 823  Summary of V4 SDK Agents Posture Policy

Creating a WebAuth Service for OnGuard Plugin v2.0 Agents

The final task is to create a WebAuth service for OnGuard plugin version 2.0 V4 SDK Agents. To do so:

1. Navigate to Configuration > Services.
2. Click Add.
   
   The Add Services page opens.

Figure 824  Adding a Web-Based Authentication Service

3. Type: Select Web-based Authentication.
4. Name: Enter the name for this service.
5. Service Rule:
   a. Matches: Leave the default setting, ALL of the following conditions.
   b. Select Click to add... and specify the following attributes:
   c. Type: Select Host.
   d. Name: Select SDKType.
   e. Operator: Select EQUALS.
6. Select the Authentication tab and specify the authentication source(s).
7. Select the Enforcement tab and select the enforcement policy created in the previous section.
8. Click Save.
9. From the Services page, click Reorder, then place the service for the V4 SDK before the service for the V3 SDK.

This ensures that WebAuth requests with the V4 SDK are evaluated by the service configured for the V4 SDK.

**Important Points**

This section provides the important points to keep in mind and, in some cases, follow up on, when upgrading to OnGuard plugin version 2.0.

1. After installing ClearPass 6.7.0, OnGuard Agent is configured to use the OnGuard plugin version 2.0: OESIS V4 SDK by default. Thus, to fully configure the OnGuard plugin version 2.0, you must follow the procedure described above in Creating a WebAuth Service for OnGuard Plugin v2.0 Agents.

2. To locate the support charts for OnGuard plugin version 2.0, navigate to Administration > Support > Documentation > OnGuard Agent Support Charts for Plugin Version 2.0.

3. The Plugin Version field in the Posture Policy > Summary tab indicates the version and related SDK as follows (see Figure 823):
   - Plugin Version 1.0: OESIS V3 SDK
   - Plugin Version 2.0: OESIS V4 SDK

4. The names of some of the third-party products (for example, AntiVirus, Firewall, and Patch Management) have changed in the OnGuard plugin version 2.0, so be sure to test the OnGuard plugin version 2.0 Service and Posture policies in your lab before applying them in a production environment.

5. In OnGuard plugin version 2.0 Posture Policy for Windows and macOS, AntiVirus and AntiSpyware health classes are merged into the AntiVirus health class.

6. The following features/checks are not supported with the OnGuard plugin version 2.0:
   - **AntiVirus health class**: Engine Version Check, Display Update URL, Disable RTP Check (see AntiVirus on page 271).
   - **Patch Management health class**: Selected On Server and Security options in the Install Level Check Type (see Patch Management).

7. Note that new posture policies created on ClearPass Policy Manager 6.7.0 and later will be for OnGuard plugin version 2.0: OESIS V4 SDK.

8. ClearPass Policy Manager 6.7.0 and later does not allow creating a new Posture Policy for OnGuard plugin version 1.0: OESIS V4 SDK. However, you can import a Posture Policy for OnGuard plugin version 1.0 from the previously released versions of ClearPass.

9. Make sure that the Agent Enforcement profile has the required SDK Type configured—V3 or V4 (see Modifying an Existing Enforcement Policy for OnGuard Plugin v2.0).

10. Make sure to use the posture policy having Plugin Version 2.0, if V4 SDK is enabled. Similarly for V3 SDK, use the posture policy with Plugin Version 1.0 (see Creating a New Posture Policy for OnGuard Plugin v2.0 Agents).

11. You can change the SDK Type from V4 to V3 by modifying the Agent Enforcement profile to have V3 as the SDK Type. In this case, be sure to configure the service posture policy is set to Plugin Version 1.0 (see Creating a New Enforcement Profile to Set the SDK Type).

12. OnGuard Agent sends two WebAuth requests when the SDK Type is changed on a client. The first request uses the previously configured SDK Type, and the second request is for the new SDK Type.

13. If an Agent Enforcement Profile without the SDK Type attribute is applied, it will not reset the SDK Type on the client; that is, once the SDK Type is changed on the client by the Agent Enforcement profile, it will not change until a new Agent Enforcement profile having a different SDK Type is applied.
14. If the **Host:SDK Type** attribute is missing in WebAuth Requests, it indicates that OnGuard Agent is using the V3 SDK as versions prior to OnGuard Agents version 6.7.0 do not send the **Host:SDK Type** attribute.

15. You can check the value of the **Host:SDKType** attribute in Monitoring > Access Tracker > Input > Computed Attributes.

**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>
<thead>
<tr>
<th>Table 1: Supported Operating Systems and Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OS</strong></td>
</tr>
<tr>
<td>Windows</td>
</tr>
<tr>
<td>macOS</td>
</tr>
<tr>
<td>Linux</td>
</tr>
</tbody>
</table>

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:
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.

3. Select the **Native agents only** mode in the **Client Agents** field:

**Figure 826  Native Agents Only Mode**

### End-to-End Flow in Native Agents Only Mode

The following steps describe the end-to-end flow of the OnGuard Dissolvable Agent running on 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 827 Native Dissolvable Agent - Login Page

Please login to the network using your username and password.

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 828 Native Dissolvable Agent Installer Prompt

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 829 Native Dissolvable Agent Binary Downloader
5. To download the OnGuard agent, click **Save File**.
6. To install the OnGuard agent, click **Run**.

**Figure 830  Native Dissolvable Agent Installation**

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.

If you are running macOS, 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**.
The following progress screen appears and shows the progress:

**Figure 832** *Native Dissolvable Agent Installation Progress*

After the successful installation, the health check scanning is initiated. The following figure shows an example of the progress indicator:

**Figure 833** *Health Check Progress*

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:
9. 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.

10. You can track the events with the end-to-end flow in the **Access Tracker** page.

The following figure shows an example of the **Access Tracker** page with the Native Dissolvable Agent flow:

**Figure 835  Access Tracker Page**

<table>
<thead>
<tr>
<th>#</th>
<th>Source</th>
<th>Destination</th>
<th>Mode</th>
<th>Result</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Radius</td>
<td>sunbibab</td>
<td>EX-Wireless</td>
<td>ACCEPT</td>
<td>2014/07/10 16:07:12</td>
</tr>
<tr>
<td>10.2</td>
<td>WEBAUTH</td>
<td>7cd1c373c4e4</td>
<td>Health-only</td>
<td>ACCEPT</td>
<td>2014/07/10 16:07:03</td>
</tr>
<tr>
<td>10.3</td>
<td>Radius</td>
<td>sunbibab</td>
<td>EX-Wireless</td>
<td>ACCEPT</td>
<td>2014/07/10 16:06:30</td>
</tr>
</tbody>
</table>

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 macOS, the Native dissolvable agent flow logs are available at:

```
~/Library/Logs/ClearPassOnGuardTemp/logs.
```

**Configuring Web Agent Flow—Native Agent**

You can configure a new web agent flow in two different applications (ClearPass Policy Manager and ClearPass Guest) to perform health scans on endpoints.
Configuring Web Agent Flow in ClearPass Policy Manager

To configure a new web agent flow in ClearPass Policy Manager:

1. Create an 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 > Enforcement page:

   **Figure 836** Web Agent Flow - 802.1X Service

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 > Enforcement page:

   **Figure 837** Web Agent Flow - Health Only Service

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 > Authentication page:

   **Figure 838** Web Agent Flow - Services Web Auth
Configuring Web Agent Flow in ClearPass Guest

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 user interface.

   The following figure shows an example of the **Web Login Editor** page:

   **Figure 839 Web Login Editor**

   Web Login (new)

   Use this form to create a new Web Login.

   ![Web Login Editor](image)

   **Figure 840 Web Login - Login Form**

   ![Login Form](image)

2. **Authentication**: Select the **Anonymous - Do not require a username or password** option from the drop-down.

3. **Prevent CNA**: Check the **Enable bypassing the Apple Captive Network Assistant** option.
4. **Pre-Auth Check**: Select the **Local - match a local account** option.

5. **Terms**: Check the **Require Terms and Conditions confirmation** option.

6. **Default destination**: Specify the destination URL to which the client must be redirected after health checks.

7. **Post Authentication**: Select the **Local - match a local account** option.

   The following figure shows an example of the **Web Login - Post-Authentication** page:

   **Figure 841**  *Web Login - Post-Authentication*

   The following figure shows an example of the final web agent flow:

   For more information, refer to ClearPass Guest Online Help.
Chapter 16
ClearPass Insight Reports

This chapter describes how to use the ClearPass 6.7 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**
- **Insight Inventory**
- **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**
- **Special Characters Supported in Passwords for All ClearPass Modules**

### 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 supports the following features:

- Customizable dashboard "widgets" allow you view the specific kinds of information you need to monitor and understand what is occurring on the network. You can create customized dashboards to track detailed authentication records, audit trails, and details on network-access trends (see **About the Insight Dashboard**).
- The Insight Search feature allows you to search for clients, users, ClearPass servers, and network access devices (see **Searching the Insight Database**).
- Customized reports analyze authentication information, device profiling, client health, licensing and posture data, as well as guest and BYOD use cases (for details, see **Creating Reports** and **Insight Report Categories**).
- Alerts allow you to receive near-real-time messages regarding anomalous network activity. Alerts can be delivered via SMS or email notification to multiple recipients. Monitor a user watchlist (a list of VIPs, executives or devices that warrant special tracking) for authentication failures or other key events (see **Creating Alerts**).
This chapter also provides information on how to configure operational elements about file transfers, as well as database and report data retention (see Administration Operations).

**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.

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 842 Server Configuration > System Page**

![Server Configuration > System Page](image)

   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.

   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 843).
   - Point the browser to https://<ClearPass-host-name>/insight.

2. Enter the default username and password, then click **Login** to launch Insight.

*Figure 843*  *ClearPass Access Page*

![Figure 843](image_url)

Special Characters Supported in Passwords for All ClearPass Modules

The special characters that are supported in passwords for all ClearPass modules (Policy Manager, ClearPass Guest, ClearPass OnGuard, ClearPass Onboard, and ClearPass Insight) are described in the following table:

<table>
<thead>
<tr>
<th>Special Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Plus sign</td>
</tr>
<tr>
<td>,</td>
<td>Comma</td>
</tr>
<tr>
<td>-</td>
<td>Hyphen</td>
</tr>
<tr>
<td>.</td>
<td>Period</td>
</tr>
<tr>
<td>;</td>
<td>Semicolon</td>
</tr>
<tr>
<td>=</td>
<td>Equal sign</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
</tr>
<tr>
<td>_</td>
<td>Underscore</td>
</tr>
</tbody>
</table>
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
- Licensing Dashboard
- Network Dashboard
- Posture 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. The Insight header statistics at the top of the dashboard display authentication, endpoints and user statistics collected over the previous 24 hours. You can click any of these values to display a dashboard page with additional information.

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.

Figure 844 Insight Header Statistics

<table>
<thead>
<tr>
<th>TOTAL AUTH</th>
<th>FAILED AUTH</th>
<th>UNIQUE ENDPOINTS</th>
<th>UNIQUE USERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>120</td>
<td>5</td>
<td>80</td>
<td>65</td>
</tr>
</tbody>
</table>

The following report widgets are included by default on the Dashboard Landing page:

- Authentication Trend
- Authentication Distribution
- Authentication Status
- Authentication Service
- Top 10 MAC Address Authentications
- Top 20 NAD Authentications
- Top 10 Authentication Errors
- Latest 10 Authentication Alerts
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 Monitor Dashboard, the **Top 10 Restarted Services** widget would be present in both the Dashboard Landing page and the System Monitor 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 846).
   That report widget will appear when you return to the Dashboard Landing page.

Figure 846  **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 847).

**Figure 847  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 **Create 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 **Create Alerts** wizard from the Dashboard, click the down-arrow icon in the widget title bar and select **Create Alert**.
Figure 848  Opening the Reports or Alerts Wizard from the Dashboard

For detailed procedures to create reports and alerts, see Creating Reports and Creating Alerts.

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 849.
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 850  Authentication Dashboard**

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.

**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 851  Endpoints Dashboard**

The following widgets are included by default on the Endpoints Dashboard:

- Endpoint Unique Trend
- Endpoint Device Profiling
- Endpoint Device Categories
- Endpoint Device Families
- Endpoint Device Names
- Top 20 Bandwidth Users

For more information about the Authentication reports and the widgets provided for each report, see Endpoint Category Reports.
**Guest Dashboard**

To access the Guest Dashboard, navigate to Dashboard > Guest.

**Figure 852  Guest Dashboard**

The following widgets are included by default on the **Guest Dashboard**:

- Guests Authentication Trend
- Unique Guest Authentication
- Guests Provisioned
- Guest Device Category
- Guest Device Families
- Guest Device Names
- Top 20 Bandwidth Guest Users

For more information about the Guest reports and the widgets provided for each report, see [Guest Authentication Category Reports](#).
Licensing Dashboard

To access the Licensing dashboard, navigate to Dashboard > Licensing.

**Figure 853  Licensing Dashboard**

The following widgets are included by default on the Guest Licensing:

- Current License Usage
- License Usage in the Last 24 Hours
- Maximum License Usage

This page displays the current Access, OnGuard and Onboard license usage over the previous 15 minutes and previous 24 hour interval, and the maximum usage for each of these license types in the previous day, week or month. For more information, see Licensing Reports.
Network Dashboard

To access the Network Dashboard, navigate to Dashboard > Network.

Figure 854  Network Dashboard: NAD Vendor Distribution

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.

Posture Dashboard

The Posture Dashboard widgets focus on device health status and device profiles. To access the Posture Dashboard, navigate to Dashboard > Posture.

Figure 855  Posture Dashboard

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.

**System Monitor Dashboard**

The System Monitor Dashboard widgets focus on health, including Authentication health, processing time, and CPU, memory, and disk usage.

You cannot pin System Monitor widgets to the Dashboard.

To access the System Monitor Dashboard, navigate to Dashboard > System Monitor.

**Figure 856  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  
- Top 10 Restarted Services  
- Insight Disk usage

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.
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 PM.
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.

The Insight Search window is always available at the top of every page.

Search works on all pages except the Report Configuration and Alert Configuration pages.
Search Example

Let’s take the example of searching for an endpoint hostname:

1. Start entering the endpoint hostname into the Search window.
   
   As you type in the endpoint hostname, Insight Search may discover that there are multiple entities with the same initial characters (see Figure 859).

Figure 859 Search Locating Matching Entities

2. To locate the desired entity:
   
   a. Click on the suggestion and see which entity 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 860 Locating and Identifying the Search Object

3. Select the search object.

   The endpoint hostname report is automatically displayed in an endpoint details page (see Figure 861). For more information about the data displayed in an endpoint details page, see Viewing Endpoints Details on page 863.
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 about 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.

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.
2. Click Configuration.
   - The Alerts Configuration page opens.

Figure 862  Alerts Configuration Page

- **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.

3. Click Create New Alert.

Figure 863  Creating a New Alert
4. Enter the information for each **Create New Alert** parameter as described in Table 1, then click **Save**.

**Table 1: Create New Alert Parameters**

<table>
<thead>
<tr>
<th>Alert Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Name</td>
<td>Enter the name of the alert.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a summary description of the alert.</td>
</tr>
</tbody>
</table>
| Category        | Select the alert **Category**, then specify the desired alert type in the selected category:  
  - Authentication  
    - Failed Authentication  
    - RADIUS Failed Authentication  
    - Total Authentication  
    - WEBAUTH Authentication  
  - System  
  - TACACS  
    - TACACS Commands  
    - TACACS Failures |
| Notifications   | 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:** If you have not configured the SMTP mail server for email notifications, you will be unable to configure Alert Notifications. For the procedure, see **Messaging Setup**. |
| Filter          | To configure an Alert filter:  
  1. From the **Filter** drop-down, select the type of filter; for example, *Access Point* or *ClearPass Server*.  
  2. Specify the operator:  
    - Equals  
    - Not_Equals  
    - Starts_With  
    - Contains  
    - Not_Contains  
  3. Enter the value.  
  To create another filter, click the **Add Another** link.  
  To remove a filter, click the trashcan logo. |
| Trigger Severity| From the **Trigger Severity** drop-down, select one of the following:  
  - **Critical**  
  - **Warning** |
| Trigger Threshold| 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 | 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. |
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

You cannot edit the Watchlist trigger settings.

To modify the User Watchlist:

1. From the Insight navigation panel, choose Alerts, then select Configuration.
   - The Alerts Configuration is displayed, which shows the default User Watchlist (see Figure 864).

   **Figure 864 User Watchlist**

2. Click Watchlist, then click Modify Watchlist.
   - The Edit Alert page for the User Watchlist opens.
3. Enter the desired settings for each User Watchlist parameter as described in Table 2, then click Save.

**Table 2: Modify User Watchlist Parameters**

<table>
<thead>
<tr>
<th>Alert Field</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Name</td>
<td>Optionally, you can modify the name of the User Watchlist.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally (and recommended), enter a summary description of the User Watchlist.</td>
</tr>
<tr>
<td>Category</td>
<td>The Category is set to Alert &gt; User Watchlist. This is not an editable field.</td>
</tr>
</tbody>
</table>
### Alert Field | Action/Description
--- | ---
Notifications | 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 (for details, see **Messaging Setup**).

Filter: Username | The User Watchlist has only one filter: **Username**. From the Username drop-down, select one or more users to add to the Watchlist.

Alert Summary | When you have configured the Watchlist settings, the **Alert Summary** displays the settings for your review.

**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.
To add a user to the Watchlist, click the star icon next to the username as shown in Figure 866. The User Information page now displays the following information:

**Figure 867  User Successfully Added to Watchlist**

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.
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**
- **Creating a New Report: Settings Configuration**
- **Report Filters Configuration**
- **Specifying the Logo and Branding**
- **Report Summary Page**
- **Configured Reports Page**
- **Importing and Exporting Reports**
- **Viewing Generated Reports**
- **Regenerating Existing Reports**

**Overview**

The Reports page provides a method for creating reports with data filters and customized time ranges up to the previous two months.
**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.

> Deleting a configured report deletes both the report configuration and all related report output.

**Creating a New Report: 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.
3. Enter the appropriate information as described in Table 1, then click Next.

**Table 1: Specifying the Report Settings Parameters**

<table>
<thead>
<tr>
<th>Report Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Name</td>
<td>Enter the name of the report.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a summary description of the report.</td>
</tr>
</tbody>
</table>
| Category         | Select the report Category, then specify the desired report type in the selected category:  
  - Authentication  
  - Endpoint  
  - Guest Authentication  
  - Licensing  
  - Network  
  - OnGuard  
  - Onboard  
  - RADIUS Authentication  
  - System  
  - TACACS  
  **NOTE:** For detailed information about what report types are provided for each report category, see Insight Report Categories. |
| Notifications    | Optionally, specify report notifications. These report notification options require that you first configure the SMTP mail server for email notifications. For details, see Messaging Setup.  
  - Notify by Email. When you select this option, enter the list of email addresses |
<table>
<thead>
<tr>
<th>Report Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to be notified. When Insight Reports are sent via email to notification recipients, the recipients will receive an email with an HTML version of the report, and a zip file containing the report in CSV and PDF formats. If the zip file is larger than 2 MB, the CSV file will not be included in the zip file, but the email will include a link to download that file.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Notify by SMS.</strong> When you select this option, enter the phone numbers of each recipient (separated by commas).</td>
</tr>
<tr>
<td>Options</td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
</tbody>
</table>
|                     | - **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 | 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   | 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** settings. |
| Report Summary      | When you have configured the report settings, the **Report Summary** displays them for your review.                                                                                                                 |

**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. The complete set filters are available for each report, for maximum flexibility in defining your reports.

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.
Specify the report filter parameters as described in the following table.

**Table 2: Specifying the Filters Parameters**

<table>
<thead>
<tr>
<th>Filter Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Click the Field drop-down list and select the parameter you wish to use as a filter. The available parameters vary, according to the report type.</td>
</tr>
</tbody>
</table>
| Operator         | Select the operator to determine how Insight filters the setting in the Value field. Supported options are:  
|                  | - Equals: The field is an exact match with the value string  
|                  | - Not_Equals: The field does not exactly match the value string  
|                  | - Starts_with: The field starts with the specified value string  
|                  | - Contains: The field parameter contains the value string anywhere within the field parameter.  
|                  | - Not.Contains: The field parameter does not contain the Value parameter |
| Value            | Select the appropriate value. |
| Add Another      | Click this link to add another filter. |

**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 872 Prompt for Changing the Logo**

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:
3. To specify the logo and branding information, enter the information as described in Table 3, then click Next.

**Table 3: Specifying Logo and Branding Parameters**

<table>
<thead>
<tr>
<th>Report Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Template</td>
<td>From the drop-down, select the logo and branding template.</td>
</tr>
<tr>
<td>Page Title</td>
<td>Enter the page title.</td>
</tr>
<tr>
<td>Top Section</td>
<td>Enter the header for the top of the page.</td>
</tr>
<tr>
<td>Logo Image</td>
<td>To browse to the appropriate logo image, click Replace Image.</td>
</tr>
<tr>
<td>Bottom Section</td>
<td>Enter the footer text.</td>
</tr>
<tr>
<td>Copyright</td>
<td>Enter the copyright information. For example, &quot;Copyright 2017 NewSales, Inc.&quot;</td>
</tr>
<tr>
<td>Save Template</td>
<td>To save the new branding and logo settings, click Save Template.</td>
</tr>
</tbody>
</table>
Report Summary Page

When you complete the **Logo and Branding** section, the **Report Summary** is displayed.

**Figure 874 Report Summary**

1. Review the report summary.
   - 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.
   - 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.

**Uploading a Custom Report Template**

Starting with ClearPass 6.7, you can upload a custom report template using the **Import** option on the **Reports > Custom Reports** page.

To create a new report based on a custom report template:

1. Navigate to **Reports > Configuration**.
2. Select the **Custom** option in the **Category** drop-down list.
Configured Reports Page

To see the set of configured reports, select Reports > Configuration. From this view, you can edit or copy report settings, run or delete a configured report, and import or export reports between ClearPass servers.

**Figure 875  Configured Reports Page**

A green dot next to a report name indicates that the report generation is complete, while a yellow dot indicates that Insight is still creating the report. A red dot by the report name indicates that the report failed to generate. To display a tooltip with additional information about why a report fail to generate, hover your mouse over red dot.

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.

**Importing and Exporting Reports**

Insight allows you to import or export individual reports, or import and export multiple report definitions at once.

To export a single report definition:

1. Navigate to the Reports > Configuration page.
2. In the Configuration table, click the checkbox to the left of a report name to select that report.
3. To export the selected report definition as a JavaScript Object Notation (JSON) file, click the Export (⋮) icon to the right of the report name in the Configuration table, or click the Export button above the Configuration table.

To export multiple report definitions at once (bulk export):

1. Navigate to the Reports > Configuration page.
2. In the **Configuration** table, click the check box to the left of each report name you want to export, or click the check box in the header of the **Configuration** table to select all reports.

3. Click the **Export** button above the **Configuration** table.
   
   All selected reports are exported in a single JSON file.

   **Figure 876  Selecting Multiple Report Definitions for Bulk Export**

   ![Configuration Table with Check Boxes](image)

   To import one or more report definitions:

   1. Click the **Import Report** button.
   2. Browse to and select a JSON report definition file.
   3. If you select a file with multiple report definitions, the import process will add all reports in that file, and Insight will display a status message listing all the report definitions that have been added or updated.

   **NOTE** If you upload a report definition that uses an existing custom report template name, Insight displays a warning stating that the template name already exists, and that uploading a new report will overwrite the previous uploaded custom report configuration.

**Viewing Generated Reports**

You can view or download an existing report on the Reports page of the Insight user interface. To view a generated report:

1. From the navigation panel, click **Reports**.
2. Scroll to the **Created Reports** section.
3. To download the zip file that contains the reports in PDF and CSV formats, click the Download icon (as shown in Figure 877).

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 878).

Figure 877 Created Reports

Figure 878 Report Displayed in HTML Format
Regenerating Existing Reports

To regenerate an updated version of an existing report definition, click the run (▶) icon beside any report definition on the Reports or Reports > Configured Reports pages.

Insight Report Categories

This section provides the following information:

- Introduction
- Authentication Category Reports
- Custom Reports
- Endpoint Category Reports
- Guest Authentication Category Reports
- Licensing Reports
- Network Category Reports
- OnGuard Category Reports
- Onboard Category Report
- RADIUS Authentication Category Reports
- System Monitor 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 1 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.
Table 1: **Authentication Category Reports**

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting—Bandwidth and Session</td>
<td>This report type includes the following bandwidth and session information:</td>
</tr>
<tr>
<td>Provides the statistics using the accounting data generated during report duration. This report allows you to filter the report data by:</td>
<td>- Bandwidth Statistics: Total Bandwidth, Average Bandwidth, Maximum Bandwidth, Maximum Upstream Bandwidth, Maximum Downstream Bandwidth, Sessions, Maximum Duration, Users, Endpoints</td>
</tr>
<tr>
<td>▪ ClearPass server</td>
<td>- Upstream Bandwidth and Downstream Bandwidth Trend</td>
</tr>
<tr>
<td>▪ Network access device IP address</td>
<td>- Total Bandwidth and Average Bandwidth Trend</td>
</tr>
<tr>
<td>▪ Device category</td>
<td>- Average Session Time Trend</td>
</tr>
<tr>
<td>▪ Device family</td>
<td>- Unique Session Trend</td>
</tr>
<tr>
<td>▪ Device name</td>
<td>- Top 10 Device Categories with Most Bandwidth Consumed</td>
</tr>
<tr>
<td>▪ SSID</td>
<td>- Top 10 Device Categories with Most Sessions</td>
</tr>
<tr>
<td>▪ Endpoint IP address</td>
<td>- Top 10 Device Categories with Most Duration</td>
</tr>
<tr>
<td>▪ User name</td>
<td>- Top 10 Device Families with Most Bandwidth Consumed</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Families with Most Sessions</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Families with Most Duration</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Endpoints with Most Bandwidth Consumed</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Endpoints with Most Sessions</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Endpoints with Most Duration</td>
</tr>
<tr>
<td></td>
<td>- Top 20 Users with Most Bandwidth Consumed</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Users with Most Sessions</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Users with Most Duration</td>
</tr>
<tr>
<td></td>
<td>- Domain Summary: Provides an overview of authentications per domain.</td>
</tr>
<tr>
<td>Authentication by Authentication Source</td>
<td>This report type includes the following information:</td>
</tr>
<tr>
<td>Provides the statistics for successful and failed authentications per authentication source.</td>
<td>- Authentication Statistics</td>
</tr>
<tr>
<td></td>
<td>- Total Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>- Failed Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>- Authentication Distribution Across Authentication Source</td>
</tr>
<tr>
<td></td>
<td>- Authentication Distribution Across Authorization Source</td>
</tr>
<tr>
<td></td>
<td>- Authentication Distribution Across Authentication Source</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This report allows you to filter the report data by authentication source.</td>
<td></td>
</tr>
<tr>
<td>Authentication by ClearPass</td>
<td>This report type includes the following information:</td>
</tr>
<tr>
<td>Provides the statistics for successful and failed authentications per ClearPass servers in a cluster.</td>
<td>- Authentication Statistics</td>
</tr>
<tr>
<td></td>
<td>- Total Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>- Failed Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>- Authentication Distribution—Error Types</td>
</tr>
<tr>
<td></td>
<td>- Authentication Distribution Across Service</td>
</tr>
<tr>
<td></td>
<td>- Top 10 ClearPass with Most Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 10 ClearPass with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 10 ClearPass with Most MAC Address Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 10 ClearPass with Most Users</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This report allows you to filter the report data by ClearPass Policy Manager server.</td>
<td></td>
</tr>
<tr>
<td>Report Type</td>
<td>Report Widgets</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Authentication Overview   | 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       | 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      | 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  
   - 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. |
| Unique Failed Authentication| This report type includes the following information:  
   - Error Statistics  
   - Failed Authentication Trend |
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides statistics based on failed authentications.</td>
<td>- Authentication Distribution—Error Types</td>
</tr>
<tr>
<td></td>
<td>- Failed Authentication Distribution across Service</td>
</tr>
<tr>
<td></td>
<td>- Failed Authentication Distribution across Authentication Source</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Errors with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 20 NADs with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 10 ClearPass Servers with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Users with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Endpoints with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Services with Most Failed Authentications</td>
</tr>
<tr>
<td><strong>NOTE:</strong> 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.</td>
<td></td>
</tr>
</tbody>
</table>

**Custom Reports**

If you imported a custom report template via the Reports > Custom Reports page, you can select the Custom Reports option on the Reports > Configuration page to create a new custom report based upon that template. You can edit a custom report definition to add filters supported by that custom template type, and select raw data columns to appear in the CSV format output for that report. Note that the Custom option does not appear in the Reports > Configuration page unless you have previously uploaded a custom report template.

Log files for custom report events are separate from other Insight event log files, and are located at /var/avenda/tips/insight/admin/customreports/upload_logs.txt.

---

**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 2 contain data that can also be found in the endpoints widgets on the Endpoints Dashboard page. For additional information about the Endpoints Dashboard, see Endpoints Dashboard.
### Table 2: Endpoint Category Reports

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
</table>
| 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. |
| 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 3 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](#).
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest—Auth Trend</td>
<td>This report includes the following report widgets: Authentication Statistics, Total Authentication Trend, Authentication Trend for Today and Yesterday, Authentication Trend for Today and Same Day Week Ago, Total Authentication for One Month, Sponsor List. <strong>NOTE:</strong> This report also allows you to filter the report data by ClearPass Policy Manager host name and Network Access Device (NAD) IP address.</td>
</tr>
<tr>
<td>Guest—Auth by ClearPass</td>
<td>This report type includes the following information guest authentications 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. <strong>NOTE:</strong> This report also allows you to filter the report data by ClearPass Policy Manager host name.</td>
</tr>
<tr>
<td>Guest - Hotspot</td>
<td>This report includes the following information about hotspot user logins recorded over the selected time frame: Hotspot plan distribution (for example, free vs hourly paid access), Purchase amount distribution: purchase totals per plan type, in either dollars or the currency used to purchase the plan.</td>
</tr>
<tr>
<td>Report Type</td>
<td>Report Widgets</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Guest—Social Login</td>
<td>This report type includes the following information for guest authentication for Social Logins:</td>
</tr>
<tr>
<td></td>
<td>- Social Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>- Endpoint Distribution Across Social Providers</td>
</tr>
<tr>
<td></td>
<td>- Authentication Distribution Across Authentication Source</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This report also allows you to filter the report data by ClearPass host name and Network Access Device (NAD) IP address.</td>
</tr>
<tr>
<td>Guest Accounting—Bandwidth and Session</td>
<td>This report type includes the following bandwidth and session information:</td>
</tr>
<tr>
<td></td>
<td>- Bandwidth Statistics: Total Bandwidth, Average Bandwidth, Maximum Bandwidth, Maximum Upstream Bandwidth, Maximum Downstream Bandwidth, Sessions, Maximum Duration, Guests, Endpoints</td>
</tr>
<tr>
<td></td>
<td>- Upstream Bandwidth and Downstream Bandwidth Trend</td>
</tr>
<tr>
<td></td>
<td>- Total Bandwidth and Average Bandwidth Trend</td>
</tr>
<tr>
<td></td>
<td>- Average Session Time Trend</td>
</tr>
<tr>
<td></td>
<td>- Unique Session Trend</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Categories with Most Bandwidth Consumed</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Categories with Most Sessions</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Categories with Most Duration</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Families With Most Bandwidth Consumed</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Families With Most Sessions</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Device Families With Most Duration</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Endpoints with Most Bandwidth Consumed</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Endpoints with Most Sessions</td>
</tr>
<tr>
<td></td>
<td>- Top 20 Guests with Most Bandwidth Consumed</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Guests with Most Sessions</td>
</tr>
<tr>
<td></td>
<td>- Top 10 Guests with Most Duration</td>
</tr>
<tr>
<td>Guest Devices—Expired</td>
<td>The Guest Devices—Expired report lets you view information about expired guest devices.</td>
</tr>
<tr>
<td></td>
<td>This report type includes the following report widgets:</td>
</tr>
<tr>
<td></td>
<td>- Guest Expiry Statistics</td>
</tr>
<tr>
<td></td>
<td>- Guest Expiry List (MAC Address and Device Name)</td>
</tr>
<tr>
<td>Guest Users and Devices—Expired</td>
<td>The Guest Users and Devices—Expired report lets you view information about expired guest accounts and devices.</td>
</tr>
<tr>
<td></td>
<td>This report type includes the following report widgets:</td>
</tr>
<tr>
<td></td>
<td>- Guest Expiry Statistics</td>
</tr>
<tr>
<td></td>
<td>- Guest Expiry List (MAC Address and Visitor Name)</td>
</tr>
<tr>
<td>Guest Users—Expired</td>
<td>The Guest Users—Expired report lets you view information about expired guest accounts.</td>
</tr>
<tr>
<td></td>
<td>This report type includes the following report widgets:</td>
</tr>
<tr>
<td></td>
<td>- Guest Expiry Statistics</td>
</tr>
<tr>
<td></td>
<td>- Guest Expiry List</td>
</tr>
</tbody>
</table>

**Licensing Reports**

The licensing report category allows you to generate a report about license usage over the selected time period. Similar information can also be found in the Licensing widgets on the **Licensing Dashboard**. For additional information, see [Licensing Dashboard](#).
Table 4: Licensing Report Content

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Usage</td>
<td>This report type includes the following licensing information:</td>
</tr>
<tr>
<td></td>
<td>■ License statistics, including the total number of licenses, and the number</td>
</tr>
<tr>
<td></td>
<td>of licenses used for each license type</td>
</tr>
<tr>
<td></td>
<td>■ Number of unique endpoints on the network over the selected time period</td>
</tr>
<tr>
<td></td>
<td>■ Number of ClearPass Access licenses used over the selected time period</td>
</tr>
<tr>
<td></td>
<td>■ Number of ClearPass Guest licenses used over the selected time period</td>
</tr>
<tr>
<td></td>
<td>■ ClearPass licenses distribution (available vs used)</td>
</tr>
<tr>
<td></td>
<td>■ ClearPass license usage per host</td>
</tr>
</tbody>
</table>

Network Category Reports

The reports available in the Network category described in Table 5 contain data about network access devices and gives 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 Licensing Dashboard.

Table 5: Network Category Reports

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication by NAD</td>
<td>This report type includes the following information for Network Access Devices (NADs) using guest authentication:</td>
</tr>
<tr>
<td></td>
<td>■ Authentication Statistics</td>
</tr>
<tr>
<td></td>
<td>■ Total Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>■ Failed Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>■ Authentication Distribution Across NAD Ports</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most Authentication</td>
</tr>
<tr>
<td></td>
<td>■ Top 10 Services with Most Authentications</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most MAC Addresses</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most Users</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This report also allows you to filter the report data by NAD IP address.</td>
</tr>
<tr>
<td>Guest—Authentication by NAD</td>
<td>This report type includes the following information for Network Access Devices (NADs) using guest authentication:</td>
</tr>
<tr>
<td></td>
<td>■ Authentication Statistics</td>
</tr>
<tr>
<td></td>
<td>■ Total Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>■ Failed Authentication Trend</td>
</tr>
<tr>
<td></td>
<td>■ Authentication Distribution Across NAD Ports</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most Authentication</td>
</tr>
<tr>
<td></td>
<td>■ Top 10 Services with Most Authentications</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most MAC Addresses</td>
</tr>
<tr>
<td></td>
<td>■ Top 20 NADs with Most Guests</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This report also allows you to filter the report data by NAD IP address.</td>
</tr>
</tbody>
</table>

RADIUS—Auth by NAD

This report type includes the following information for Network Access Devices (NADs) using guest authentication:

■ Authentication Statistics
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.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication Distribution Across NAD Ports</td>
</tr>
<tr>
<td></td>
<td>Top 20 NADs with Most Authentication</td>
</tr>
<tr>
<td></td>
<td>Top 10 Services with Most Authenticizations</td>
</tr>
<tr>
<td></td>
<td>Top 20 NADs with Most Failed Authentications</td>
</tr>
<tr>
<td></td>
<td>Top 20 NADs with Most MACs</td>
</tr>
<tr>
<td></td>
<td>Top 20 NADs with Most Users</td>
</tr>
</tbody>
</table>

**NOTE:** This report also allows you to filter the report data by NAD IP address.
### OnGuard Category Reports

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
</table>
| **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  
  - Antispyware 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 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 |
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
</table>
| 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  
  - Antispyware 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 7: Onboard Report Content**

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboard Certificate</td>
<td>This report type includes the following certificate information:</td>
</tr>
<tr>
<td></td>
<td>■ Onboard statistics for numbers of revoked devices, active devices, and users</td>
</tr>
<tr>
<td></td>
<td>■ Latest Onboard Device Distribution</td>
</tr>
<tr>
<td></td>
<td>■ Active Onboard Device Distribution</td>
</tr>
<tr>
<td></td>
<td>■ Top 10 Users with Most Active Devices</td>
</tr>
<tr>
<td>Onboard Certificate - Due to Expire</td>
<td>This report type includes the following information for manually created</td>
</tr>
<tr>
<td></td>
<td>certificates due to expire within the selected time frame:</td>
</tr>
<tr>
<td></td>
<td>■ Total number of devices of each device type with certificates due to expire.</td>
</tr>
<tr>
<td></td>
<td>■ Top 10 Users with Most Active Devices</td>
</tr>
<tr>
<td>Onboard Enrollment</td>
<td>This report type provides the following information:</td>
</tr>
<tr>
<td></td>
<td>■ Total Devices Onboarded</td>
</tr>
<tr>
<td></td>
<td>■ Onboarded Devices Enrollment Trend</td>
</tr>
<tr>
<td></td>
<td>■ Onboarded Devices</td>
</tr>
<tr>
<td></td>
<td>■ Unique Users and Their Associated Total Number of Devices</td>
</tr>
<tr>
<td></td>
<td>■ Unique Onboarded Devices</td>
</tr>
</tbody>
</table>
**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](#).

**Table 8: RADIUS Authentication Category Reports**

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
</table>
| 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  
- 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 |
### System Monitor Category Reports

The reports available in the **System Monitor** 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 Monitor Dashboard**. For additional information about the System Dashboard, see [System Monitor Dashboard](#).
### Table 9: System Monitor Category Reports

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
</table>
| 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 |
| 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 10: TACACS Reports Content

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Widgets</th>
</tr>
</thead>
</table>
| 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. |

### Insight Inventory

- [About the Insight Inventory](#)
- [Sorting and Filtering Inventory Table Data](#)
- [Viewing Endpoints Details](#)

### About the Insight Inventory

Insight lists all authenticated endpoints on the network on the **Inventory** page.
View inventory information for all endpoints by navigating to **Insight > Inventory**, or click a graph widget on the **Endpoints, Posture** or **Authentication** Insight dashboards and drill down to display inventory data related to that graph.

**Figure 879  The Insight Inventory Table**

The endpoints information in the **Inventory** table is described in **Table 1**.

**Table 1: Endpoints Table Parameters**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>MAC address of the endpoint.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the endpoint.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Host name of the endpoint.</td>
</tr>
<tr>
<td>Category</td>
<td>Category assigned to the profiled endpoint device; for example, <strong>Access Points</strong>, <strong>Computer</strong>, <strong>Server Smart Device</strong>, or <strong>VoIP phone</strong>.</td>
</tr>
<tr>
<td>Family</td>
<td>The operating system (OS) family used by the endpoint device. For example, when the category is <strong>Computer</strong>, Insight can show a device OS family of <strong>Windows, Linux, or Apple Mac</strong>.</td>
</tr>
<tr>
<td>Device Name</td>
<td>The <strong>Device Name</strong> column describes a more specific device type within a device family. For example, a computer in the <strong>Windows</strong> device family may show a device type of <strong>Windows Vista/7/2008</strong> or <strong>Windows 8/10</strong>.</td>
</tr>
</tbody>
</table>

**Sorting and Filtering Inventory Table Data**

By default, each page of the **Inventory** table displays endpoints sorted by MAC address.

Click any column heading to resort the table by that column data type.

Click the filter (Ỹ) icon on the **Inventory** table header to select one or more filter options and modify the table display only selected endpoint types.

The available filter types are described in **Table 2** below.
<table>
<thead>
<tr>
<th>Column</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Category</td>
<td>The <strong>Device Category</strong> drop-down list displays a list of the categories of devices found on your network, such as a server or printer. By default, the <strong>All</strong> option is selected, and the inventory displays devices in all categories. Click this drop-down list and select any other device category to filter the table and display only devices of the selected type. The contents of this drop-down list may vary, depending upon the types of devices in your network.</td>
</tr>
<tr>
<td>Device Family</td>
<td>The <strong>Device Family</strong> drop-down list displays a list of the device families found on your network, such as a Hewlett Packard, Aruba, or Intel. By default, the <strong>All</strong> option is selected, and the inventory displays devices in all categories. Click this drop-down list and select any other device category to filter the table and display only devices of the selected type. The contents of this drop-down list may vary, depending upon the types of devices in your network, and the selected device category.</td>
</tr>
<tr>
<td>Device Name</td>
<td>The <strong>Device Name</strong> drop-down list displays a list of the device names found on your network, such as an Apple iPhone. By default, the <strong>All</strong> option is selected, and the inventory displays devices in all categories. Click this drop-down list and select any other device category to filter the table and display only devices of the selected type. The contents of this drop-down list may vary, depending upon the types of devices in your network, and the selected device category.</td>
</tr>
</tbody>
</table>
| Static IP      | Click the **Static IP** drop-down list and select one of the following options:  
  - **All**: Display endpoints with static and non-static IP addresses.  
  - **True**: Display endpoints with a static IP address.  
  - **False**: Display endpoints with a non-static IP address. |
| Conflict Status| Click the **Conflict Status** drop-down list and select one of the following options:  
  - **All**: Display all endpoints.  
  - **True**: Display endpoints with a conflict (device is profiled into two or more different categories.)  
  - **False**: Display endpoints with no conflict. |
| Fingerprint Type| Insight can obtain fingerprint information for network devices through a variety of sources (for example, obtained directly from the host, or via DHCP or SNMP) The **fingerprint** drop-down list displays a list of fingerprint information sources for the devices found on your network. By default, the **All** option is selected, and the inventory displays devices identified by all fingerprinting types. Click this drop-down list and select any other fingerprinting type to filter the table and display only devices identified by the selected fingerprinting method. **NOTE**: The contents of this drop-down list may vary, depending upon the fingerprinting methods used to identify devices on your network. |
| Posture        | Click the **Posture** option select one of the following options to filter endpoints that have a posture status as a result of having undergone a health check.  
  - **All**: Display all endpoints.  
  - **True**: Display endpoints that have posture information.  
  - **False**: Display endpoints that do not have posture information |
### Viewing Endpoints Details

The **Endpoint Details** page appears when you select any MAC address in the **Inventory** table, or when you enter and search for a search string in the Insight search bar. This data can include information in the following categories:

- **Summary**: Total number of successful authentications for that device over the selected time period.
- **Overview**: This section displays endpoint information such as the device IP address, MAC address and host name, and network details such as the AP, controller or switch port to which the endpoint is connected.
- **Device Profile**: Conflict information, and device profile data, such as the device category, family and name, and the time the device was first added or last updated.
- **Onguard**: This section displays Onguard health check data, if available.
- **Endpoint Details**: This section displays authentication details, endpoint role and policy information, the IP address of the NAD (Network Access Device), and the current authentication status.
- **Fingerprint Details**: This section displays fingerprint details and information about fingerprint information sources for that endpoint.
- **Authentication Trend**: A line chart showing the number of successful authentications during each day of the selected time period.
- **Bandwidth Usage**: A bar chart showing bandwidth used by the endpoint during each day of the selected time period.

If the endpoint is seen on the trunk port instead of an access port, the information shown in the **Switch Port** field of the **Network Details** section displays the word **(Trunk)** after the network switch port number.

### 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 the SCP or SFTP file transfer protocol.

To access the Administration page:

1. From the Insight navigation pane, click Administration.
   
   The Administration page appears.

![Administration Page](image)

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.
2. In the **File Transfer Settings** section, enter the appropriate values as described in **Table 1**.
3. When finished, click **Save**.

**Table 1: Insight File Transfer Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specify the IP address of the destination host FTP server.</td>
</tr>
</tbody>
</table>
| Protocol          | 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              | Specify the destination port number.  
The default destination port is **22**. |
| Username/Password | Enter the username and password of the host FTP server. |
| Timeout           | Specify the timeout value in seconds.  
The default value is **30 seconds**. |
| Remote Directory  | 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 opens:
Figure 882 Successful File Transfer Test

![Image](image1.png)

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 883 Specifying the Insight Database Settings

![Image](image2.png)

2. In the Database Settings section, enter the appropriate values as described in Table 2.
3. When finished, click Save.

Table 2: Insight Database Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Retention</td>
<td>Specify the number of days to retain the database. The supported range is from 1 to <strong>730</strong> days. The default value is <strong>30 days</strong>.</td>
</tr>
<tr>
<td>Report Retention</td>
<td>Specify the number of days to retain the generated reports. The supported range is from 1 to <strong>365</strong> days. The default value is <strong>60 days</strong>.</td>
</tr>
<tr>
<td>CSV Report Limit</td>
<td>Specify the number of rows for a CSV report. The supported range is from 1 to <strong>50,000</strong> rows. The default value is <strong>50000</strong> rows.</td>
</tr>
</tbody>
</table>

Managing Insight Admin Privileges

This section provides the following information:

- Overview
- Viewing the Default Insight Admin Privileges
- Defining Custom Insight Admin Privileges
- Insight User Interface 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, Administration, and Inventory) 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 displayed.

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 Policy Manager:

1. From the ClearPass Policy Manager user interface, navigate to Administration > Users and Privileges > Admin Privileges.
   - The Admin Privileges page opens.

   Figure 884  Admin Privileges Page

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 885  *Insight Read-Only Administrator Admin Privileges*

![Diagram showing admin privileges](image)

As shown in Figure 885, the default admin privileges for the Insight Read-only Administrator specifies Read-only access to all of the Insight modules:

- Dashboard
- Reports
- Alerts
- Administration
- Inventory

**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.
3. Specify the parameters in the **Basic Information** tab as described in Table 39.

**Table 39: Add Admin Privileges Parameters: Basic Information Tab**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the Admin Privileges administrator.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description of this new admin privileges administrator.</td>
</tr>
<tr>
<td>Access Type</td>
<td>Select one of the following Access Types:</td>
</tr>
<tr>
<td>Allow Passwords</td>
<td>Select this check box if you want to allow password access.</td>
</tr>
</tbody>
</table>

**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.
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 User Interface Differences for Read-Only Users**

When Insight is accessed by a user who has Read-only privileges for all five Insight modules (Dashboard, Reports, Alerts, Inventory and Administration), that user is not allowed to create or delete reports.

As shown in Figure 888, 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 888  Create New Report Button Not Present for Read-Only User**

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.
Refer to the following sections to perform various tasks using the Command Line Interface (CLI):

- Cluster Commands
- Configure Commands
- Miscellaneous Commands
- Network Commands
- Service Commands
- Show Commands
- SSH Timed Account Lockout
- System Commands

**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 1** describes the required and optional parameters for the `drop-subscriber` command:

<table>
<thead>
<tr>
<th>Parameter/Flag</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>Enter the -f parameter to force ClearPass to drop even the nodes that are down.</td>
</tr>
<tr>
<td>-i &lt;IP Address&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>-s</td>
<td>Restricts resetting the database on the dropped node. By default, Policy Manager drops the current node—if it's a Subscriber—from the cluster.</td>
</tr>
</tbody>
</table>
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`

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 2 describes the required and optional parameters for the `make-subscriber` command:
Table 2: Cluster Make-Subscriber Command Parameters

<table>
<thead>
<tr>
<th>Parameter/Flag</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-b</td>
<td>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.</td>
</tr>
<tr>
<td>-i &lt;IP address&gt;</td>
<td>Specify the Publisher's IP address. This field is mandatory.</td>
</tr>
<tr>
<td>-l</td>
<td>Restores the local log database after this operation. This field is optional.</td>
</tr>
</tbody>
</table>

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.

---

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.

---

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.

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 ClearPass 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 specify the cluster's primary and secondary NTP (Network Time Protocol) servers, the key index, key value, encryption type, and optionally, the time zone for the Publisher...
The Audit Viewer (Monitoring > Audit Viewer) tracks NTP configuration changes.

**Syntax**

```plaintext
configure date -p <ntp_server1> [-a <key-index> -v <key-value> -t <encryption-type>] [-s <ntp_server2> [-a <key-index> -v <key-value> -t <encryption-type>]] [-z <timezone>]
```

The following table describes the parameters for the `configure date` command:

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;ntp_server1&gt;</td>
<td>Specify the primary and secondary NTP server names or IP addresses. <strong>NOTE:</strong> You can specify a destination node with an IPv6 address enabled.</td>
</tr>
<tr>
<td>-p &lt;ntp_server2&gt;</td>
<td></td>
</tr>
<tr>
<td>-a &lt;key-index&gt;</td>
<td>The <strong>Key Index</strong> (also referred to as the <strong>Key ID</strong>) is a number that specifies the index for key values. The <strong>key-index</strong> value can be from 1 to 65534 inclusive. Typically an NTP client and server have to trust the same key index and key value pair for authentication to succeed.</td>
</tr>
</tbody>
</table>
| -v <key-value> | The **Key Value** is a form of shared secret, which both the client and server use for authenticating NTP messages. The **Key Value** can be:  
  - Up to 20-character printable ASCII string  
  - Up to 40-character hex value 
When entering an ASCII string for the **Key Value**, note that it **cannot** contain the following characters:  
  - & (ampersand)  
  - ; (semicolon)  
  - ` (grave accent)  
  - | (pipe)  
  - < (left angle bracket)  
  - > (right angle bracket)  
  - ( (left parenthesis)  
  - ) (right parenthesis) 
Finally, the **Key Value** ASCII string must start and end with one of the following characters:  
  - - (hyphen)  
  - ' (apostrophe)  
  - " (quote) |
| -t <encryption-type> | Select one of the two options for **Encryption Type**:  
  - SHA  
  - SHA1 
**NOTE:** In FIPS mode, **SHA** is not a supported encryption type. |
| -z <timezone> | Specify the time zone on the Publisher node. To view the list of supported time zones, enter `show all-timezones`. This field is optional. |

**Example 1**

The following example configures the **key-index**, **key-value**, and **encryption type** for the primary and secondary NTP servers:

```plaintext
[appadmin]# configure date -p ntp1.cpm.main -a 24 -v cp1234567890 -t SHA -s ntp2.cpm.main -a 16 -v cp53.56 -t SHA1
```
**Example 2**
The following example synchronizes with the primary NTP server. Note that in this example, the *key-value* is a hex code. Using a hex code for the *key-value* is supported only in the CLI, not in the user interface.

```
[appadmin]# configure date -p ntp1.cppm.main -a 96 -v 6bf60ca1876b5724831aa07c7783d391be95d6c -t SHA1
```

**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.

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 2: Configure fips-mode Command Parameters**

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>To disable <strong>FIPS</strong> mode, enter 0. Read the warning message carefully before enabling or disabling <strong>FIPS</strong> mode.</td>
</tr>
<tr>
<td>1</td>
<td>To enable <strong>FIPS</strong> mode, enter 1.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip &lt;mgmt</td>
<td>data&gt; &lt;IP address&gt;</td>
</tr>
<tr>
<td>netmask &lt;netmask&gt;</td>
<td>Specify the netmask for the IP address.</td>
</tr>
<tr>
<td>gateway &lt;gateway address&gt;</td>
<td>Specify the IP address for the network gateway.</td>
</tr>
</tbody>
</table>
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**

There are two methods for using the `configure ip6` command to configure IPv6:

**Syntax**

- `[appadmin]# configure ip6 <mgmt|data> <IPv6 address/PrefixLen> gateway <gateway address>`
- `[appadmin]# configure ip6 <mgmt|data> <IPv6 address> netmask <netmask> gateway <gateway address>`

The following table describes the parameters used in the `configure ip6` command:

**Table 4: Configure ip6 Command Parameters**

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip6 &lt;mgmt</td>
<td>data&gt; &lt;IP address&gt;</td>
</tr>
<tr>
<td>IP address/PrefixLen</td>
<td>The prefix-length in IPv6 is the equivalent of the subnet mask in IPv4.</td>
</tr>
<tr>
<td>netmask &lt;netmask&gt;</td>
<td>Specifies the netmask. For example, ffff:ffff:ffff:0000:0000:0000:0000:0000.</td>
</tr>
<tr>
<td>gateway &lt;gateway address&gt;</td>
<td>Specifies the gateway address. For example, fe90:0000:0000:0000:020c:29ff:fe7e:d3a2.</td>
</tr>
</tbody>
</table>

**Example**

- The following example configures the IPv6 management interface, IPv6 address/PrefixLength, and gateway address:
  
  ```
  ```

- The following example configures the IPv6 management interface, netmask, and gateway address:
  
  ```
  ```

**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 5: Configure mtu Command Parameters**

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtu `&lt;mgmt</td>
<td>data&gt;`</td>
</tr>
<tr>
<td><code>&lt;MTU value&gt;</code></td>
<td>Specify the MTU value in bytes. The default value is 1500 bytes.</td>
</tr>
</tbody>
</table>

**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 rellogin.*
*********************************************************
```

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 rellogin.*
*********************************************************
```

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
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 : fe80::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 ping6
- 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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`&lt;mgmt</td>
<td>data&gt;`</td>
</tr>
<tr>
<td><code>-i &lt;id&gt;</code></td>
<td>Specifies the ID of the network IP rule. If this ID is not specified, the system generates an ID automatically. <strong>NOTE:</strong> This ID determines the priority in the ordered list of rules in the routing table.</td>
</tr>
<tr>
<td><code>-s &lt;SrcAddr&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-d &lt;DestAddr&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-g &lt;ViaAddr&gt;</code></td>
<td>Specifies the via or gateway IPv6 address through which the network traffic should flow. A valid IPv6 address is allowed. This parameter is optional.</td>
</tr>
</tbody>
</table>

**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
```

---
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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-mgmt</code></td>
<td>Configures the management interface, data interface, the name of the GRE tunnel, or the VLAN number.</td>
</tr>
<tr>
<td><code>-data</code></td>
<td>Configures the management interface, data interface, the name of the GRE tunnel, or the VLAN number.</td>
</tr>
<tr>
<td><code>-greN</code></td>
<td>N specifies the GRE tunnel number ranging from 1,2,3...N.</td>
</tr>
<tr>
<td><code>-vlanN</code></td>
<td>N specifies the VLAN number.</td>
</tr>
<tr>
<td><code>-i &lt;id&gt;</code></td>
<td>Specifies the ID of the network IP rule. If this ID is not specified, the system generates an ID automatically. <strong>NOTE:</strong> This ID determines the priority in the ordered list of rules in the routing table.</td>
</tr>
<tr>
<td><code>-s &lt;SrcAddr&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-d &lt;DestAddr&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-g &lt;ViaAddr&gt;</code></td>
<td>Specifies the via or gateway IP address through which the network traffic should flow. A valid IP address is allowed. This parameter is optional.</td>
</tr>
</tbody>
</table>

**Syntax: network ip del**

```
network ip del <-i <id>>
```

The following table describes the parameter for the `network ip del` command:
### Table 3: Network IP Del Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i &lt;id&gt;</td>
<td>Specifies the ID of the rule to delete.</td>
</tr>
</tbody>
</table>

**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
```

```
===============================================
<table>
<thead>
<tr>
<th>IP Rule Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: from all lookup local</td>
</tr>
<tr>
<td>10020: from all to 10.xx.4.0/24 lookup mgmt</td>
</tr>
<tr>
<td>10040: from 10.xx.4.200 lookup mgmt</td>
</tr>
<tr>
<td>10060: from 10.xx.5.200 lookup data</td>
</tr>
<tr>
<td>32766: from all lookup main</td>
</tr>
<tr>
<td>32767: from all lookup default</td>
</tr>
</tbody>
</table>
```

**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 4: Network Nslookup Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;record-type&gt;</td>
<td>Specifies the type of DNS record. The record types available are:</td>
</tr>
<tr>
<td></td>
<td>- A</td>
</tr>
<tr>
<td></td>
<td>- AAA</td>
</tr>
<tr>
<td></td>
<td>- CNAME</td>
</tr>
<tr>
<td></td>
<td>- PTR</td>
</tr>
<tr>
<td></td>
<td>- SRV</td>
</tr>
<tr>
<td>&lt;host&gt;</td>
<td>Specifies the host or domain name to be queried.</td>
</tr>
</tbody>
</table>
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]# 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]# nslookup -q AAAA ipv6test-n1.cppmipv6.com
Server: 2001::94
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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i &lt;SrcIPv6Addr&gt;</td>
<td>Specifies the originating IPv6 address for the ping. This field is optional.</td>
</tr>
<tr>
<td>-t</td>
<td>Use this parameter to ping indefinitely. This field is optional.</td>
</tr>
<tr>
<td>&lt;host&gt;</td>
<td>Specifies the host to be pinged.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i &lt;SrcIpAddr&gt;</td>
<td>Specifies the originating IP address for the ping. This field is optional.</td>
</tr>
<tr>
<td>-t</td>
<td>Use this parameter to ping indefinitely. This field is optional.</td>
</tr>
<tr>
<td>&lt;host&gt;</td>
<td>Specifies the host to be pinged.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data[v4</td>
<td>v6]</td>
</tr>
<tr>
<td>mgmt</td>
<td>Specifies the name of network management port to reset.</td>
</tr>
</tbody>
</table>

**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 8: Network Traceroute6 Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;host&gt;</td>
<td>Specifies the name of network host. You can specify the host with an IPv6 address.</td>
</tr>
</tbody>
</table>

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 9: Network Traceroute Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;host&gt;</td>
<td>Specifies the name of the network host.</td>
</tr>
</tbody>
</table>

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
- ad netjoin
- ad netleave
- ad passwd-server
- ad testjoin
- alias
- backup
- dump certchain
- dump logs
- dump servercert
- exit
- help
- krb auth
- krb list
- ldapsearch
- quit
- restore

**ad auth**

Use the `ad auth` command to authenticate the user against Active Directory. This command manually checks against Active Directory to indicate whether or not a username and password are valid.

**Syntax**

```
ad auth -u <username> -n <NetBIOS domain name>
```

The following table describes the parameters for the `ad auth` command:

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u &lt;username&gt;</td>
<td>Specifies the username of the authenticating user. This is a mandatory parameter.</td>
</tr>
<tr>
<td>-n &lt;domain NetBIOS name&gt;</td>
<td>Specifies the domain name. This field is optional.</td>
</tr>
</tbody>
</table>

**Example**

The following example authenticates the user against Active Directory:

1. Enter the command:
   ```
   [appadmin]# ad auth -u jbrown -n sanfranedu
   
   You are prompted to enter the password.
   ```
2. Enter the password.
   
   If the username and password you provide in this command are correct, the following message is displayed:
   ```INFO – NT_STATUS_OK: Success (0x0)
   ```
   This message indicates that NT LAN Manager (NTLM) authentication (NTLM being the mechanism that ClearPass uses to authenticate users) has succeeded.

**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 2: AD Netjoin Command Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;domain-controller. domain-name&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>[domain NetBIOS name]</td>
<td>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.</td>
</tr>
<tr>
<td>[domain REALM name]</td>
<td>You can specify this argument if the derived REALM is different from the actual. This is an optional argument.</td>
</tr>
<tr>
<td>[ou=&lt;object container&gt;]</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 3: AD Netleave Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;domain NetBIOS name&gt;</td>
<td>Specifies the host to be joined to the domain. This field is mandatory.</td>
</tr>
<tr>
<td>-f</td>
<td>Forces the removal of Active Directory domain membership even if the operation fails.</td>
</tr>
</tbody>
</table>

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 Active Directory password servers.
- List the configured Active Directory password servers.
- Reset the Active Directory password servers.
When an Active Directory password server is updated in the domain server configuration, the RADIUS service is restarted.

Syntax

ad passwd-server <server> <list> <reset>

Table 4: AD passwd-server Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets the password servers. The -n parameter specifies the domain name. The -s parameter specifies one or more password server names.</td>
</tr>
<tr>
<td>list -n &lt;domain NetBIOS name&gt;</td>
<td>Lists the configured password servers.</td>
</tr>
<tr>
<td>reset -n &lt;domain NetBIOS name&gt;</td>
<td>Resets the password servers.</td>
</tr>
</tbody>
</table>

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 5: AD Netjoin Command Parameter

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;domain NetBIOS name&gt;</td>
<td>Specifies the host to be joined to the domain. This field is mandatory.</td>
</tr>
</tbody>
</table>

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 6: Alias Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;=&lt;command&gt;</td>
<td>Sets &lt;name&gt; as the alias for &lt;command&gt;.</td>
</tr>
<tr>
<td>&lt;name&gt;=</td>
<td>Removes the association.</td>
</tr>
</tbody>
</table>

### Example 1

This example set the alias "sh" for the show command:

```bash
[appadmin]# alias sh=show
```

### Example 2

This example removes the alias "sh":

```bash
[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**

```
```

The following table describes the parameters for the **backup** command:

### Table 7: Backup Command Parameters

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-f &lt;filename&gt;]</td>
<td>Specifies the backup target. If not specified, Policy Manager automatically generates a filename. This field is optional.</td>
</tr>
<tr>
<td>-c</td>
<td>Backs up ClearPass Policy Manager configuration data.</td>
</tr>
<tr>
<td>-l</td>
<td>Backs up ClearPass Policy Manager session log data.</td>
</tr>
<tr>
<td>-r</td>
<td>Backs up Insight data.</td>
</tr>
<tr>
<td>-P</td>
<td>Does not backup password fields from the configuration database. This field is optional.</td>
</tr>
<tr>
<td>-w</td>
<td>Backs up only the most recent records from the log database (the last one week).</td>
</tr>
</tbody>
</table>

### Example

```bash
[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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="">hostname:port-number</a></td>
<td>Specifies the hostname and SSL port number.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f &lt;output-file-name&gt;</td>
<td>Specifies the target for concatenated logs.</td>
</tr>
<tr>
<td>-s yyyy-mm-dd</td>
<td>Specifies the start date range. The default value is today's date. This field is optional.</td>
</tr>
<tr>
<td>-e yyyy-mm-dd</td>
<td>Specifies the end date range. The default value is today's date. This field is optional.</td>
</tr>
<tr>
<td>-n &lt;days&gt;</td>
<td>Specifies the duration in days (from today). This field is optional.</td>
</tr>
<tr>
<td>-t &lt;log-type&gt;</td>
<td>Specifies the type of log to collect. This field is optional.</td>
</tr>
<tr>
<td>-h</td>
<td>Specifies the print help for available log types.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;hostname:port-number&gt;</code></td>
<td>Specifies the hostname and SSL port number.</td>
</tr>
</tbody>
</table>

**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**

Use 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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:user@domain">user@domain</a></td>
<td>Specifies the username and domain.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-B</td>
<td>Finds the bind DN (Distinguished Name) of the LDAP directory.</td>
</tr>
<tr>
<td><a href="mailto:user@hostname">user@hostname</a></td>
<td>Specifies the username and the full qualified domain name of the host.</td>
</tr>
</tbody>
</table>
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
```
quilt
```

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
```
```

Syntax 3
```
```

The following table describes the parameters for the `restore` command:

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user@hostname:/&lt;backup-filename&gt;</td>
<td>Specifies the filepath of the the restore source.</td>
</tr>
<tr>
<td><a href="http://hostname/">http://hostname/</a>&lt;backup-filename&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;backup-filename&gt;</td>
<td></td>
</tr>
<tr>
<td>-b</td>
<td>Does not backup the current configuration data before the restore operation starts.</td>
</tr>
<tr>
<td>-c</td>
<td>Restores ClearPass Policy Manager configuration data.</td>
</tr>
<tr>
<td>-l</td>
<td>If it exists in the backup file, restores the ClearPass Policy Manager log database. This field is optional.</td>
</tr>
<tr>
<td>-i</td>
<td>Ignores version mismatch errors and attempts data migration. This field is optional.</td>
</tr>
<tr>
<td>Flag/Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-n</td>
<td>Retains local node configuration data, such as certificates, after the restore operation (default).</td>
</tr>
<tr>
<td>-N</td>
<td>Does not retain local node configuration data after the restore operation.</td>
</tr>
<tr>
<td>-r</td>
<td>Restores Insight data if it exists in the backup.</td>
</tr>
<tr>
<td>-s</td>
<td>Restores cluster server/node entries from the backup file. Node entries are in a disabled state upon restore. This field is optional.</td>
</tr>
</tbody>
</table>

**Example**

The following example restores Policy Manager configuration data from the backup file:

```bash
[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 1: Service Action Command Parameters

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| action            | 1. Choose an action:  
|                   |   - list  
|                   |   - restart  
|                   |   - start  
|                   |   - status  
|                   |   - stop  

| service-name      | 2. Choose a service:  
|                   |   - airgroup-notify  
|                   |   - cpass-admin-server  
|                   |   - cpass-async-netd  
|                   |   - cpass-carbon-server  
|                   |   - cpass-dbcn-server  
|                   |   - cpass-dbwriteserver  
|                   |   - cpass-domain-server_<NetBIOS_name>  
|                   |   - cpass-igssyslog-server  
|                   |   - cpass-igslgger-server  
|                   |   - cpass-igslrgrepo-server  
|                   |   - cpass-ipsec-service  
|                   |   - cpass-multi-master-cache-server  
|                   |   - cpass-policy-server  
|                   |   - cpass-radius-server  
|                   |   - cpass-radsec  
|                   |   - cpass-repl-server  
|                   |   - cpass-sttatsd-server  
|                   |   - cpass-sysmon-server  
|                   |   - cpass-system-auxiliary-server  
|                   |   - cpass-tacacs-server  
|                   |   - cpass-vip  
|                   |   - fias_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 ]
RadSec server [ cpass-radsec ]
Tacacs server [ cpass-tacacs-server ]
Async DB write service [ cpass-dbwriteserver ]
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 ]
Stats collection service [ cpass-sttatsd-server ]
Stats aggregation service [ cpass-carbon-server ]
ClearPass IPsec service [ cpass-ipsec-service ]
AirGroup notification service [ airgroup-notify ]
Micros Fidelio FIAS [ fias_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 syslog`
- `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 Feb 27 13:30:03 2018
```
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.

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
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: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**

```plaintext
show license
```

**Example**
The following displays an example of the **show license** command output:

```plaintext
[appadmin]# show license
-------------------------------------------
Application : ClearPass Platform
License key  : YFKV-MW62AB-Y2PZ-B7GNJX-06T4NB-WLSV-RTQUPQ-WODIFNJI-CD7N-5UR73Q
License key type : Permanent
License added on : 2018-01-24 10:15:38
Validity : <not applicable>
Customer ID : SWCKTYM7
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.

The **show ntp** command also displays information such as the NTP authentication key details corresponding to the NTP server configured (for example, Key ID and hash algorithm).

**Syntax**

```plaintext
show ntp
```

**Example**
The following displays an example of the **show ntp** command output:

```plaintext
[appadmin]# show ntp
```
NTP Server Information

Primary NTP : 10.xx.x.1
Key ID: 24
Algorithm: SHA1

Secondary NTP : 10.x.x.2
Key ID: 48
Algorithm: SHA1

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 : 6.7.1.103378
Policy Manager model number : C1000V
=======================================

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.

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 889  SSH Command Set**

```
[appadmin@123]# 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 890  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 891  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 892  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 1-10000. 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.

The SSH timed account lockout feature is disabled by default.

**Figure 893  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 894  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 895  Show SSH Command

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 ClearPass 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 factory-reset`
- `system install-image`
- `system morph-vm`
- `system patch-rollback`
- `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 resets 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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>Lists the boot images installed on the system.</td>
</tr>
<tr>
<td>-a &lt;version&gt;</td>
<td>Sets the active boot image version in A.B.C.D syntax. This field is optional.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;num_days&gt;</td>
<td>This is the cleanup interval that specifies the number of days to retain the data. This field is mandatory.</td>
</tr>
</tbody>
</table>

**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 to 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:

```
[appadmin]# system create-api-client Win.139 college52
```

**system factory-reset**

The `system factory-reset` command restores a ClearPass hardware appliance to factory defaults. This command is available only to the `appadmin` user.

The `system factory-reset` command is inherently a destructive one as it wipes out data, including any licenses on the current partition and any backups currently stored on the server. Hence, the user should create data backups outside of the target ClearPass server before running this command.

The `system factory-reset` command essentially consists of two operations:

- Resets all ClearPass configurations in the current partition only, including Policy Manager server settings, all ClearPass Guest, Onboard extensions, Active Directory domain settings, NTP settings, hostname, network settings, and date, time, and password settings.
- Cleans and resets ClearPass logs and configuration files, including those for ClearPass Guest.

When running the `system factory-reset` in a ClearPass cluster:

- If the current node is a Publisher node, running this command will drop it from the cluster. The Standby Publisher node then becomes the Publisher.
- If the current node is a Subscriber node, it will be dropped from the cluster, and will become a stand-alone node.

After successful configuration and reboot, you will be presented with the bootstrap configuration screen, where you will have to reset all the ClearPass parameters.

**Example**

The following example restores a ClearPass hardware appliance to factory defaults:

```
[appadmin]# system factory-reset
```

**system install-image**

The `system install-image` command installs a fresh image of the major product version specified in the second partition of a ClearPass hardware appliance.

This command is available only for the `appadmin` user.
The `system install-image` command is supported for ClearPass versions prior to 6.7 as well as versions 6.7 and above.

After successful execution of the `system install-image` command, the system will reboot and you will return to the installed image.

After successful configuration and reboot, you will be presented with the bootstrap configuration screen, where you will have to reset all the ClearPass parameters.

Any data present in the second partition prior to the execution of the `system install-image` command will be wiped out. Also, no licensing information from where the command is executed is carried forward.

You can apply the `system install-image` command in the following ways:

**Table 3: System Install-Image Command Methods**

<table>
<thead>
<tr>
<th>System install-image Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>system install-image http://hostname/&lt;filename&gt;</code></td>
<td>Installs the ClearPass image through <code>http</code> or <code>https</code>.</td>
</tr>
<tr>
<td><code>system install-image user@hostname:/&lt;filename&gt;</code></td>
<td>Installs the image through SCP (Secure Copy Protocol).</td>
</tr>
<tr>
<td><code>system install-image &lt;filename&gt;</code></td>
<td>Installs the image imported to the ClearPass server and available locally (offline install-image).</td>
</tr>
</tbody>
</table>

**Example**

```
[appadmin]# system install-image CPPM-x86_64-6.X.Y.Z-<any-image>.signed.tar
```

- `X.Y.Z` stands for a specific patch release version.
- `<any-image>` stands for the description of the patch.
- `signed.tar` is common nomenclature for all types of updates.

**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 migrate 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 <C1000V | C2000V | C3000V>
```

The following table describes the parameters for the `system morph-vm` command:

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vm-version&gt;</code></td>
<td>This is the updated ClearPass version of the virtual appliances. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>- C1000V</td>
</tr>
<tr>
<td></td>
<td>- C2000V</td>
</tr>
<tr>
<td></td>
<td>- C3000V</td>
</tr>
<tr>
<td></td>
<td>This field is mandatory.</td>
</tr>
</tbody>
</table>

Example

The following example converts an evaluation virtual machine to a production C3000V virtual appliance:

```
[appadmin]# system morph-vm C3000V
```

**system patch-rollback**

The `system patch-rollback` command allows a user with `appadmin` credentials to revert to the most recent ClearPass installed version. For example, if a ClearPass system is at 6.7.1 and cumulative update 6.7.x is applied, ClearPass can be reverted to 6.7.1 through the `system patch-rollback` command.

This command can also be used if there is a problem after the patch update process—for example, if an issue is identified in production that was not identified during testing, resulting in a degradation of capabilities.

Before using this command to revert from 6.7.1 to 6.7.0, you must first download the `6.7.0_source-rollback-package` from the Software Updates page and install it (see Software Updates).

**Important Points**

When issuing the `system patch-rollback` command, keep in mind the following points:

- Patch rollback is supported only for ClearPass versions 6.7 and above.
- The system patch-rollback command reverts only the most recently installed cumulative patch update within the major version. After the cumulative patch is reverted, the user will be in the patch version that was installed prior to the patch update.

**Note**

Although you can only roll back to the last version that was installed, if multiple hotfix patches are included within the cumulative patch version you are rolling back from, then you can roll back multiple hotfix patches, one at a time, to a specific hotfix within the current version. To roll back to the previously installed version, you must first roll back each intervening hotfix patch.

As best practice, users should always back up all data before proceeding with an update.

This command can also be used at the cluster level. In this case, `system patch-rollback` must be run individually on each appliance in the cluster within 24 hours after the rollback in order to maintain the cluster status.

Any custom skins that are installed in the current version are retained after the rollback to the earlier version.
System rollback events are logged in the Event Viewer.

**Syntax**

```
system patch-rollback
```

**Example**

```bash
[appadmin]# system patch-rollback
****************************************************************************************
* WARNING: This command is recommended to be executed from local console unless otherwise instructed by TAC *
* Execution through SSH console may result in system instability.
* WARNING: This command will undo software changes done by the currently installed patch. Configuration
* changes should not be affected by this action.
* As a best practice, please be sure to back-up this system before starting the operation.
* Are you sure you want to continue? y
*******************************************************************************************
INFO: Preparing for rollback
INFO: 2018022-clearpass-6.7-updates-2 will be rolled back
INFO: This will take a few minutes to complete. Please wait.
INFO: Running pre-rollback scripts
INFO: Executing rollback
INFO: Running post-rollback scripts
INFO: Please reboot now for the changes to take effect.
*******************************************************************************************
INFO: Refreshing license count information
```

For example, if ClearPass has been installed in the order 6.7.0 > 6.7.1 > 6.7.2, when the appadmin user executes the `system patch-rollback` command, the system will revert to a time just before ClearPass 6.7.2 was installed.

If, in this example, the installed 6.7.2 patch added an rpm-X, `system patch-rollback` deletes rpm-Y, and updates rpm-Z to rpm-Z+1 version. Then `system patch-rollback` deletes rpm-X, adds rpm-Y, and restores rpm-Z.

---

The `system patch-rollback` command also removes any configuration and database changes that were done as part of post-installation during the patch update.

---

The `system patch-rollback` command can also be used at the cluster level, but this command must be run individually on all cluster nodes. For patch rollback across a cluster, the appadmin user must go to each ClearPass server in the cluster to rollback the last applied patch.

**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:

```bash
[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/EAP 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 the HTTP, RADIUS/EAP, and RadSec 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/EAP Server Certificates
1: Reset Radius/EAP Server Certificate
2: Reset Http Server Certificate
3: Reset RadSec Server Certificate
4: Quit

Updating the server certificate...

Updating of server certificate complete

**system restart**

Use the *system restart* command to restart the system.

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
```

```
******************************************************************
* WARNING: This command will shut down all applications *
******************************************************************
```

Are you sure you want to continue? [y|Y]: y
**system shutdown**

Use the **system shutdown** command to shut down the current ClearPass server.

Executing this command shuts down all running applications and powers off the system.

**Syntax**

```
[appadmin]# 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>
<thead>
<tr>
<th>Parameter</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>duration_hours</td>
<td>Specify the session duration in hours. You can specify values from 0 to 12.</td>
</tr>
<tr>
<td>duration_mins</td>
<td>Specify the session duration in minutes. You can specify values from 0 to 59.</td>
</tr>
<tr>
<td>contact_id</td>
<td>Enter the username ID part of the Aruba TAC or Engineering contact.</td>
</tr>
<tr>
<td>cppm_server_ip</td>
<td>Specify the ClearPass Policy Manager server IP address.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i user@hostname:/&lt;filename&gt;</td>
<td>Installs the specified patch on the system. This field is optional.</td>
</tr>
<tr>
<td>-f</td>
<td>Reinstalls the patch in the event of a problem with the initial installation attempt. This field is optional.</td>
</tr>
<tr>
<td>-l</td>
<td>Lists the patches installed on the system. This field is optional.</td>
</tr>
</tbody>
</table>

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**
```
system upgrade <session_id>
```

**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 7: System Upgrade Command Parameters**

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-w</td>
<td>Restores last (one) week of access tracker records after the upgrade.</td>
</tr>
<tr>
<td>-l</td>
<td>Restores all access tracker records from this version.</td>
</tr>
<tr>
<td>-L</td>
<td>Does not backup or restore access tracker records from this version.</td>
</tr>
<tr>
<td>&lt;filepath&gt;</td>
<td>Enter the filepath using the syntax provided in the two examples below. This field is mandatory.</td>
</tr>
</tbody>
</table>

This command supports Secure Copy (SCP), HTTPS, HTTP, and local uploads.

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
   ```

**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 folder > Upgrade folder.
   The Upgrade page opens.
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 opens.
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.
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 1 describes the **CPPMSystemTableEntry** MIB objects.

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cppmClusterNodeType</td>
<td>ClearPass cluster node type indicating whether the node is a Publisher or Subscriber</td>
</tr>
<tr>
<td>cppmNwDataPortIPAddress</td>
<td>ClearPass server data port IP address</td>
</tr>
<tr>
<td>cppmNwDataPortMACAddress</td>
<td>ClearPass server data port MAC address</td>
</tr>
<tr>
<td>cppmNwMgmtPortIPAddress</td>
<td>ClearPass server management port IP address</td>
</tr>
<tr>
<td>cppmNwMgmtPortMACAddress</td>
<td>ClearPass server management port MAC address</td>
</tr>
</tbody>
</table>
### MIB Object Description

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cppmSystemDiskSpaceFree</td>
<td>Amount of disk space free (in bytes) in the ClearPass server</td>
</tr>
<tr>
<td>cppmSystemDiskSpaceTotal</td>
<td>Total amount of disk space available (in bytes) in the ClearPass server</td>
</tr>
<tr>
<td>cppmSystemHostname</td>
<td>ClearPass server host name</td>
</tr>
<tr>
<td>cppmSystemMemoryFree</td>
<td>Amount of memory free (in bytes) in the ClearPass server</td>
</tr>
<tr>
<td>cppmSystemMemoryTotal</td>
<td>Total amount of memory available (in bytes) in the ClearPass server</td>
</tr>
<tr>
<td>cppmSystemModel</td>
<td>Model of the ClearPass server</td>
</tr>
<tr>
<td>cppmSystemNumCPUs</td>
<td>Total number of CPUs in the ClearPass server</td>
</tr>
<tr>
<td>cppmSystemSerialNumber</td>
<td>Serial number of the ClearPass server</td>
</tr>
<tr>
<td>cppmSystemUptime</td>
<td>Amount of time the ClearPass server has been up</td>
</tr>
<tr>
<td>cppmSystemVersion</td>
<td>Product version of the ClearPass server</td>
</tr>
</tbody>
</table>

### RADIUS Server MIB Entries

**RadiusServerTableEntry**

Table 2 describes the *RadiusServerTableEntry* objects.

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radAuthRequestTime</td>
<td>Total time taken for an end-to-end RADIUS request</td>
</tr>
<tr>
<td>radPolicyEvalTime</td>
<td>Time taken for policy evaluation from the RADIUS server perspective</td>
</tr>
<tr>
<td>radServerCounterCounts</td>
<td>Total number of successful RADIUS authentications</td>
</tr>
<tr>
<td>radServerCounterFailure</td>
<td>Total number of failed RADIUS authentications</td>
</tr>
<tr>
<td>radServerCounterSuccess</td>
<td>Total number of successful RADIUS authentications</td>
</tr>
</tbody>
</table>
**RadiusServerAuthTableEntry**

*RadiusServerAuthTableEntry* exposes the following counters that refer to *authSourceName* wherever applicable (see Table 3). Counters and delays reflect details that are logged into Graphite.

**Table 3: RadiusServerAuthEntry MIB MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radAuthCounterCount</td>
<td>Total number of RADIUS authentications</td>
</tr>
<tr>
<td>radAuthCounterFailure</td>
<td>Total number of failed RADIUS authentications</td>
</tr>
<tr>
<td>radAuthCounterSuccess</td>
<td>Total number of successful RADIUS authentications</td>
</tr>
<tr>
<td>radAuthCounterTime</td>
<td>Time taken to perform RADIUS authentications</td>
</tr>
<tr>
<td>radAuthSourceName</td>
<td>Name of the RADIUS server authentication source</td>
</tr>
</tbody>
</table>

**Policy Server MIB Entries**

**PolicyServerTableEntry**

*PolicyServerTableEntry* exposes the following MIB objects (see Table 4). Counters and delays reflect details logged into Graphite.

**Table 4: PolicyServerTableEntry Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>psAuditPolicyEvalCount</td>
<td>Audit policy evaluation count</td>
</tr>
<tr>
<td>psAuditPolicyEvalTime</td>
<td>Audit policy evaluation time</td>
</tr>
<tr>
<td>psAuthCounterFailure</td>
<td>Number of failed Policy Server authentications</td>
</tr>
<tr>
<td>psAuthCounterSuccess</td>
<td>Number of successful Policy Server authentications</td>
</tr>
<tr>
<td>psAuthCounterTotal</td>
<td>Total number of Policy Server authentications</td>
</tr>
<tr>
<td>psEnforcementPolicyEvalCount</td>
<td>Enforcement policy evaluation count</td>
</tr>
<tr>
<td>psEnforcementPolicyEvalTime</td>
<td>Enforcement policy evaluation time</td>
</tr>
<tr>
<td>psPosturePolicyEvalCount</td>
<td>Posture policy evaluation count</td>
</tr>
<tr>
<td>psRestrictionPolicyEvalCount</td>
<td>Authorization restriction policy evaluation count</td>
</tr>
<tr>
<td>psRolemappingPolicyEvalCount</td>
<td>Role mapping policy evaluation count</td>
</tr>
<tr>
<td>psRolemappingPolicyEvalTime</td>
<td>Role mapping policy evaluation time</td>
</tr>
<tr>
<td>MIB Object</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>psPosturePolicyEvalTime</td>
<td>Posture policy evaluation time</td>
</tr>
<tr>
<td>psRestrictionPolicyEvalTime</td>
<td>Restriction policy evaluation time</td>
</tr>
<tr>
<td>psServicePolicyEvalCount</td>
<td>Service policy evaluation count</td>
</tr>
<tr>
<td>psServicePolicyEvalTime</td>
<td>Service policy evaluation time</td>
</tr>
<tr>
<td>psSessionlogTime</td>
<td>Policy Server session logging time</td>
</tr>
<tr>
<td>dailySuccessAuthCount</td>
<td>Total daily number of successful authentications</td>
</tr>
<tr>
<td>dailyFailedAuthCount</td>
<td>Total daily number of failed authentications</td>
</tr>
<tr>
<td>dailyTotalAuthCount</td>
<td>Total daily number of authentications</td>
</tr>
</tbody>
</table>

**PolicyServerProtoTableEntry**

*PolicyServerProtoTableEntry* exposes MIB objects for the counter values for the RADIUS, TACACS, WEBAUTH, and APPLICATION protocols.

**Table 5: PolicyServerProtoTableEntry MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>psPolicyEvalTime</td>
<td>Policy evaluation time for the protocol</td>
</tr>
<tr>
<td>psProtocolName</td>
<td>Name of the protocol</td>
</tr>
</tbody>
</table>

**PolicyServerAutzTableEntry**

*PolicyServerAutzTableEntry* exposes MIB objects for authorization counters (see Table 6).

**Table 6: PolicyServerAutzTableEntry MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>psAutzCounterCount</td>
<td>Total number of Policy Server authorizations</td>
</tr>
<tr>
<td>psAutzCounterFailure</td>
<td>Number of failed Policy Server authorizations</td>
</tr>
<tr>
<td>psAutzCounterSuccess</td>
<td>Number of successful Policy Server authorizations</td>
</tr>
<tr>
<td>psAutzCounterTime</td>
<td>Time taken to perform Policy Server authorizations</td>
</tr>
<tr>
<td>psAutzAuthSourceName</td>
<td>Name of the Policy Server authorization source</td>
</tr>
</tbody>
</table>
Web Authentication Server MIB Entries

*WebAuthProtoTableEntry* exposes MIB objects for the WebLogin, AppLogin, SamlIdp, and SamlSp web authentication protocols.

**Table 7: WebAuthProtoTableEntry MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>waAuthCounterAuthTime</td>
<td>Time taken for web authentication</td>
</tr>
<tr>
<td>waAuthCounterCount</td>
<td>Total number of web authentications</td>
</tr>
<tr>
<td>pwaAuthCounterFailure</td>
<td>Number of failed web authentications</td>
</tr>
<tr>
<td>waAuthCounterSuccess</td>
<td>Number of successful web authentications</td>
</tr>
<tr>
<td>waAuthCounterTime</td>
<td>Total time taken for web login</td>
</tr>
<tr>
<td>waPolicyEvalTime</td>
<td>Time taken to perform policy evaluation</td>
</tr>
<tr>
<td>waProtocolName</td>
<td>Name of the protocol</td>
</tr>
<tr>
<td>pwaServicePolicyEvalTime</td>
<td>Time taken to perform service policy evaluation</td>
</tr>
</tbody>
</table>

TACACS+ Server MIB Entries

*TacacsAuthTableEntry*

*TacacsAuthTableEntry* exposes MIB objects for TACACS+ authentication counters.

**Table 8: TacacsAuthTableEntry Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacAuthCounterAuthTime</td>
<td>Time taken for TACACS+ authenticizations</td>
</tr>
<tr>
<td>tacAuthCounterCount</td>
<td>Total number of TACACS+ server authentications</td>
</tr>
<tr>
<td>tacAuthCounterFailure</td>
<td>Number of failed TACACS+ server authentications</td>
</tr>
<tr>
<td>tacAuthCounterSuccess</td>
<td>Number of successful TACACS+ server authentications</td>
</tr>
<tr>
<td>tacAuthCounterTime</td>
<td>Total time taken for TACACS+ login</td>
</tr>
<tr>
<td>tacPolicyEvalTime</td>
<td>Time taken to perform policy evaluation</td>
</tr>
<tr>
<td>tacServicePolicyEvalTime</td>
<td>Time taken to perform service policy evaluation</td>
</tr>
</tbody>
</table>

*TacacsAutzTableEntry*

*TacacsAutzTableEntry* exposes MIB objects for TACACS+ authorization counters.
Table 9: TacacsAuthTableEntry Objects

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacAutzCounterCount</td>
<td>Total number of TACACS+ server authorizations</td>
</tr>
<tr>
<td>tacAutzCounterFailure</td>
<td>Number of failed TACACS+ server authorizations</td>
</tr>
<tr>
<td>tacAutzCounterSuccess</td>
<td>Number of successful TACACS+ server authorizations</td>
</tr>
<tr>
<td>tacAutzCounterTime</td>
<td>Total time taken for TACACS+ authorizations</td>
</tr>
</tbody>
</table>

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 10: TacacsAuthTableEntry Objects

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nwAppPort</td>
<td>Application port</td>
</tr>
<tr>
<td>nwAppName</td>
<td>Application name</td>
</tr>
<tr>
<td>nwTrafficTotal</td>
<td>Total network traffic in bytes</td>
</tr>
</tbody>
</table>

ClearPass SNMP Traps and OIDs

This section provides the following information:

- **Introduction**
- **Hardware Monitoring OIDs**
- **Daily Authentication Statistics OIDs**
- **Authentication Count OIDs**
- **ClearPass SNMP Traps**

**Introduction**

This section describes the traps that ClearPass Policy Manager supports as part of the ClearPass SNMP Private MIB (Management Information Base). OIDs (Object Identifiers) uniquely identify managed objects in a MIB.
hierarchy. These OIDs are in the `cppmServerInfoGroup` of the `cppmSystemTable` of the ClearPass Management Information Base (CPPM-MIB).

**Hardware Monitoring OIDs**

The hardware monitoring OIDs allow admins to monitor the fan, power, and disk status of the ClearPass C2000 and ClearPass C3000 hardware appliances using the `snmpget` and `snmpwalk` commands.

The hardware monitoring OIDs enable sending hardware traps in the event of a fan, power, or disk failure in a hardware appliance. SNMP v1, v2, and v3 queries are supported. Traps for hardware failure are not ClearPass enterprise-specific traps, but native traps sent by the Dell or HP agent running on the hardware appliance.

These OIDs monitor hardware and authentication status through SNMP polling only.

The hardware monitoring OIDs are not available for the ClearPass C1000 hardware appliance, nor are they available for virtual appliances. For a ClearPass C1000 hardware appliance or a virtual appliance, these OIDs return N/A as the value.

**Table 1: Hardware Status Monitoring OIDs**

<table>
<thead>
<tr>
<th>Trap Name</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cppmHardwareDiskStatus</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.1.1.22</td>
<td>Disk Status</td>
</tr>
<tr>
<td>cppmHardwareFanStatus</td>
<td>1.3.6.1.4.1.14823.1.6.1.1.1.1.19</td>
<td>Fan Status</td>
</tr>
<tr>
<td>cppmHardwarePowerStatus</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.1.1.20</td>
<td>Power Status</td>
</tr>
<tr>
<td>cppmHardwarePowerStatusDetails</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.1.1.1.21</td>
<td>Power Status Details</td>
</tr>
</tbody>
</table>

ClearPass Policy Manager obtains the underlying hardware configuration from the `dmidecode` (Linux) system manufacturer property. If the vendor details are not correctly set under the system manufacturer, ClearPass assumes that the underlying configuration does not correspond to the current HP/Dell hardware, which would lead to incorrect installation and set up.

**Daily Authentication Statistics OIDs**

These OIDs monitor daily authentication statistics on ClearPass. These OIDs show the total number of authentications on the ClearPass server for the given day. There are no traps associated with these OIDs.

**Table 2: Daily Authentication Statistics OIDs**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.17</td>
<td>Daily successful authentications</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.18</td>
<td>Daily failed authentications</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.19</td>
<td>Total number of authentications</td>
</tr>
</tbody>
</table>

**Authentication Count OIDs**

This section describes the SNMP trap OIDs in the `policyServerTable` of the ClearPass MIB (CPPM-MIB) that show the total number of authentications and authorizations on the ClearPass server over the past 24 hours.

Authentication counts are calculated from 00:00:00 through 23:59:59 each day.
If polls are done several times a day, by subtracting a previous poll's count from the latest poll's count, the number of authentications within a polling interval can be calculated. The authentication count traps and their OIDs are described in the following table:

**Table 3: Authentication Count OIDs**

<table>
<thead>
<tr>
<th>Trap Name</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dailyFailedAuthCount</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.18</td>
<td>Total daily number of failed authentications</td>
</tr>
<tr>
<td>dailySuccessAuthCount</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.17</td>
<td>Total daily number of successful authentications</td>
</tr>
<tr>
<td>dailyTotalAuthCount</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.2.3.1.19</td>
<td>Total daily number of authentications</td>
</tr>
</tbody>
</table>

**ClearPass SNMP Traps**

Table 4 provides the description and OID for each ClearPass SNMP trap.

**Table 4: SNMP Traps Supported by the SNMP Private MIB**

<table>
<thead>
<tr>
<th>Trap Name</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cppmActivationExpity</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1002</td>
<td>Indicates that one or more licensing activations associated with the &lt;cppmNodeApplicationName&gt; on the ClearPass Server will expire in &lt;cppmActivationDaysRemaining&gt; days</td>
</tr>
<tr>
<td>cppmClusterLicense Usage</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1016</td>
<td>Indicates the ClearPass cluster license utilization details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- &lt;clearpassServerApplicationName&gt; indicates the name of the application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- &lt;clearpassClusterLicenseTotalCount&gt; indicates the application's total cluster-wide license count.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- &lt;clearpassClusterLicenseUsageCount&gt; indicates the count of the application's used cluster-wide licenses.</td>
</tr>
<tr>
<td>cppmClusterNode AddNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1006</td>
<td>Indicates the addition of a ClearPass node to the cluster. &lt;cppmClusterServerIp&gt; indicates the IP address of the node added to the cluster.</td>
</tr>
<tr>
<td>cppmClusterNode DbldNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1009</td>
<td>Indicates that a ClearPass node in the cluster has been disabled. &lt;cppmClusterServerIp&gt; indicates the IP address of the disabled node.</td>
</tr>
<tr>
<td>cppmClusterNode DelNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1007</td>
<td>Indicates that a ClearPass node has been deleted from the cluster. &lt;cppmClusterServerIp&gt; indicates the IP address of the node removed from the cluster.</td>
</tr>
<tr>
<td>cppmClusterNode NSyncNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1010</td>
<td>Indicates the ClearPass node in the cluster that is in the out-of-sync state. &lt;cppmClusterServerIp&gt; indicates the IP address of the cluster.</td>
</tr>
<tr>
<td>Trap Name</td>
<td>OID</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cppmClusterNodePromNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1008</td>
<td>Indicates the promotion of a ClearPass node to Publisher status.</td>
</tr>
<tr>
<td>cppmClusterPwdChangedNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1011</td>
<td>Indicates that the cluster password has been changed.</td>
</tr>
<tr>
<td>cppmConfigReset</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1012</td>
<td>Indicates that the ClearPass node's configuration has been reset.</td>
</tr>
<tr>
<td>cppmConfigRestore</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1013</td>
<td>Indicates that the ClearPass node's configuration has been restored.</td>
</tr>
<tr>
<td>cppmLicenseExpiry</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1001</td>
<td>Indicates that one or more licenses associated with a ClearPass application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>will expire in &lt;cppmLicenseDaysRemaining&gt; days.</td>
</tr>
<tr>
<td>cppmLowDiskSpace</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1004</td>
<td>Indicates that the system is running low on disk space as indicated by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;cppmDiskSpaceRemaining&gt; with the units specified in &lt;cppmResourceUnit&gt;.</td>
</tr>
<tr>
<td>cppmLowMemory</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1005</td>
<td>Indicates that the system is running low on memory as indicated by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;cppmMemoryRemaining&gt; with the units specified in &lt;cppmResourceUnit&gt;.</td>
</tr>
<tr>
<td>cppmNodeCertExpiry</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1003</td>
<td>Indicates that a server certificate associated with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;cppmNodeCertApplicationName&gt; on the ClearPass Server will expire in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;cppmCertDaysRemaining&gt; days.</td>
</tr>
<tr>
<td>cppmUpdateNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1014</td>
<td>Indicates that the CPPM node's installation has been updated.</td>
</tr>
<tr>
<td>cppmUpgradeNotification</td>
<td>.1.3.6.1.4.1.14823.1.6.1.1.200.1015</td>
<td>Indicates that the CPPM node's installation has been upgraded.</td>
</tr>
</tbody>
</table>

- <cppmClusterOutOfSyncMinutes> indicates the number of minutes that the node has been out-of-sync.
- <cppmClusterServerIp> indicates the IP address of the node promoted to Publisher.
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:
- ClearPass Processes Stop and Start Events
- CPU Load Average Exceed Events
- CPU Load Average Traps
- Disk Space Threshold Traps
- Disk Utilization Threshold Exceed Events
- Network Interface Link Up and Link Down Events
- Network Interface Status Traps
- Process Status Traps
- SNMP Daemon Trap Events

ClearPass Processes Stop and Start Events

The OIDs for the start and stop events for ClearPass processes are described in the following table:

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021.8.1.2.X</td>
<td>Process Name</td>
</tr>
</tbody>
</table>

CPU Load Average Exceed Events

The OIDs for the CPU load average exceed events for 1, 5, and 15 minute threshold are described in the following table:

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021.9.1.100.1</td>
<td>Error flag for disk partition</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2021.9.1.2.1</td>
<td>Name of the partition.</td>
</tr>
</tbody>
</table>

CPU Load Average Traps

The OIDs for the CPU load average traps are described in the following tables:
CPU Load-1 Average Traps

**Table 1: CPU Load-1 Average Traps**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021.10.1.100.1</td>
<td>Error flag on the CPU load-1 average. Value of 1 indicates the load-1 has crossed its threshold; a value of 0 indicates otherwise.</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2021.10.1.12.1</td>
<td>Name of CPU load-1 average.</td>
</tr>
</tbody>
</table>

**Figure 896 CPU Load-1 Average Traps Example**

---

CPU Load-5 Average Traps

**Table 2: CPU Load-5 Average Traps**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021.10.1.100.2</td>
<td>Error flag on the CPU load-5 average. Value of 1 indicates the load-5 has crossed its threshold; a value of 0 indicates otherwise.</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2021.10.1.2.2</td>
<td>Name of CPU load-5 average.</td>
</tr>
</tbody>
</table>

**Figure 897 CPU load-5 Average Traps Example**

---

CPU Load-15 Average Traps

**Table 3: CPU Load-15 Average Traps**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021.10.1.100.3</td>
<td>Error flag on the CPU load-15 average. Value of 1 indicates the load-15 has crossed its threshold; a value of 0 indicates otherwise.</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2021.10.1.12.3</td>
<td>Name of CPU load-15 average.</td>
</tr>
</tbody>
</table>

**Figure 898 CPU Load-15 Average Traps Example**
Disk Space Threshold Traps
The OIDs for the disk space threshold s traps are described in the following table:

**Table 1: Disk Space Threshold Traps**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021.9.1.100.1</td>
<td>Error flag indicating the disk or partition is under the minimum required disk space configured for it. A value of 1 indicates that the system has reached the threshold; a value of 0 indicates otherwise.</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2021.9.1.2.1</td>
<td>Indicates the name of the partition that has met the above condition.</td>
</tr>
</tbody>
</table>

Disk Utilization Threshold Exceed Events
The OIDs for the disk utilization threshold exceed events are described in the following table:

**Table 1: Disk Utilization Threshold Exceed Events**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021.9.1.100.1</td>
<td>Error flag for the disk partition.</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.2021.9.1.2.1</td>
<td>Name of the disk partition.</td>
</tr>
</tbody>
</table>

Network Interface Status Traps
The OIDs for the network interface status traps are described in the following table:

**Table 1: Network Interface Status Traps**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.6.3.1.1.5.3</td>
<td>Indicates the link down trap with the ifAdminStatus and ifOperStatus values set to 2.</td>
</tr>
<tr>
<td>.1.3.6.1.6.3.1.1.5.4</td>
<td>Indicates the link up trap with the ifAdminStatus and ifOperStatus values set to 1.</td>
</tr>
</tbody>
</table>

In each case, the ifindex value is set to 2 for the management interface and 3 for the data port interface.

Network Interface Link Up and Link Down Events
The network interface up and down events are described in the following table:

**Table 1: Network Interface Link Up and Link Down OIDs**

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.6.3.1.1.5.3</td>
<td>Link Down.</td>
</tr>
<tr>
<td>.1.3.6.1.6.3.1.1.5.4</td>
<td>Link Up</td>
</tr>
</tbody>
</table>

SNMP Daemon Trap Events
This section contains OIDs for various trap events that are sent from ClearPass Policy Manager.
Table 1: SNMP Daemon Trap Events

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.6.3.1.1.5.1</td>
<td>Cold Start trap indicates the reinitialization of the <strong>netsnmp</strong> daemon and that its configuration file may have been altered.</td>
</tr>
<tr>
<td>.1.3.6.1.6.3.1.1.5.2</td>
<td>Warm Start trap indicates the reinitialization of the <strong>netsnmp</strong> daemon and that its configuration file has not been altered.</td>
</tr>
</tbody>
</table>

**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.

**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”
“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", "configuration", 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 HPE Passport Credentials were supplied. To find new plugins, you must provide your HPE Passport Credentials 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
Product Name: Policy Manager
License Type: <X>
User Count: <Y>”

Info Events
“Admin UI”, “INFO”, “Add License”, “Product Name: Policy Manager
License Type: <X>
User 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
Reading sysObjectld failed for device=<X>
Reading 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 sysObjectld 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 1 describes the ClearPass Policy Manager error codes:

<table>
<thead>
<tr>
<th><strong>Code</strong></th>
<th><strong>Description</strong></th>
<th><strong>Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
<td>Success</td>
</tr>
<tr>
<td>101</td>
<td>Failed to perform service classification</td>
<td>Internal Error</td>
</tr>
<tr>
<td>102</td>
<td>Failed to perform policy evaluation</td>
<td>Internal Error</td>
</tr>
<tr>
<td>103</td>
<td>Failed to perform posture notification</td>
<td>Internal Error</td>
</tr>
<tr>
<td>104</td>
<td>Failed to query authstatus</td>
<td>Internal Error</td>
</tr>
<tr>
<td>105</td>
<td>Internal error in performing authentication</td>
<td>Internal Error</td>
</tr>
<tr>
<td>106</td>
<td>Internal error in RADIUS server</td>
<td>Internal Error</td>
</tr>
<tr>
<td>201</td>
<td>User not found</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>202</td>
<td>Password mismatch</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>203</td>
<td>Failed to contact Authentication Source</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>204</td>
<td>Failed to classify request to service</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>205</td>
<td>Authentication Source not configured for service</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>206</td>
<td>Access denied by policy</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>207</td>
<td>Failed to get client MAC Address in order to perform Web authentication</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>208</td>
<td>No response from home server</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>209</td>
<td>No password in request</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>210</td>
<td>Unknown CA in client certificate</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>211</td>
<td>Client certificate not valid</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>212</td>
<td>Client certificate has expired</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>213</td>
<td>Certificate comparison failed</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>214</td>
<td>No certificate in authentication source</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>215</td>
<td>TLS session error</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>216</td>
<td>User authentication failed</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>217</td>
<td>Search failed due to insufficient permissions</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>218</td>
<td>Authentication source timed out</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>219</td>
<td>Bad search filter</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>220</td>
<td>Search failed</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>221</td>
<td>Authentication source error</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>222</td>
<td>Password change error</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>223</td>
<td>Username not available in request</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>224</td>
<td>CallingStationID not available in request</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>225</td>
<td>User account disabled</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>226</td>
<td>User account expired or not active yet</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>227</td>
<td>User account needs approval</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>228</td>
<td>User account has exceeded bandwidth limit</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>229</td>
<td>User account has exceeded session duration limit</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>230</td>
<td>User account has exceeded session count limit</td>
<td>Authentication failure</td>
</tr>
<tr>
<td>5001</td>
<td>Internal Error</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5002</td>
<td>Invalid MAC Address</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5003</td>
<td>Invalid request received</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5004</td>
<td>Insufficient parameters received</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5005</td>
<td>Query - No MAC address record found</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5006</td>
<td>Query - No supported actions</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5007</td>
<td>Query - Cannot fetch MAC address details</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5008</td>
<td>Request: MAC address not online</td>
<td>Command and Control</td>
</tr>
<tr>
<td>5009</td>
<td>Request: No MAC address record found</td>
<td>Command and Control</td>
</tr>
<tr>
<td>6001</td>
<td>Unsupported TACACS parameter in request</td>
<td>TACACS Protocol</td>
</tr>
<tr>
<td>6002</td>
<td>Invalid sequence number</td>
<td>TACACS Protocol</td>
</tr>
<tr>
<td>6003</td>
<td>Sequence number overflow</td>
<td>TACACS Protocol</td>
</tr>
<tr>
<td>6101</td>
<td>Not enough inputs to perform authentication</td>
<td>TACACS Authentication</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>6102</td>
<td>Authentication privilege level mismatch</td>
<td>TACACS Authentication</td>
</tr>
<tr>
<td>6103</td>
<td>No enforcement profiles matched to perform authentication</td>
<td>TACACS Authentication</td>
</tr>
<tr>
<td>6201</td>
<td>Authorization failed as session is not authenticated</td>
<td>TACACS Authorization</td>
</tr>
<tr>
<td>6202</td>
<td>Authorization privilege level mismatch</td>
<td>TACACS Authorization</td>
</tr>
<tr>
<td>6203</td>
<td>Command not allowed</td>
<td>TACACS Authorization</td>
</tr>
<tr>
<td>6204</td>
<td>No enforcement profiles matched to perform command authorization</td>
<td>TACACS Authorization</td>
</tr>
<tr>
<td>6301</td>
<td>New password entered does not match</td>
<td>TACACS Change Password</td>
</tr>
<tr>
<td>6302</td>
<td>Empty password</td>
<td>TACACS Change Password</td>
</tr>
<tr>
<td>6303</td>
<td>Change password allowed only for local users</td>
<td>TACACS Change Password</td>
</tr>
<tr>
<td>6304</td>
<td>Internal error in performing change password</td>
<td>TACACS Change Password</td>
</tr>
<tr>
<td>9001</td>
<td>Wrong shared secret</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9002</td>
<td>Request timed out</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9003</td>
<td>Phase 2 PAC failure</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9004</td>
<td>Client rejected after PAC provisioning</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9005</td>
<td>Client does not support posture request</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9006</td>
<td>Received error TLV from client</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9007</td>
<td>Received failure TLV from client</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9008</td>
<td>Phase 2 PAC not found</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9009</td>
<td>Unknown Phase 2 PAC</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9010</td>
<td>Invalid Phase 2 PAC</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9011</td>
<td>PAC verification failed</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9012</td>
<td>PAC binding failed</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9013</td>
<td>Session resumption failed</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9014</td>
<td>Cached session data error</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9015</td>
<td>Client does not support configured EAP methods</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9016</td>
<td>Client did not send Cryptobinding TLV</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9017</td>
<td>Failed to contact OCSP Server</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9018</td>
<td>RADIUS protocol error</td>
<td>RADIUS Protocol</td>
</tr>
<tr>
<td>9019</td>
<td>Client sent conflicting identities</td>
<td>RADIUS Protocol</td>
</tr>
</tbody>
</table>
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**
- **Web Based Authentication Use Case**
- **MAC Authentication Use Case**
- **TACACS+ Use Case**
- **Single Port Use Case**

**802.1X Wireless Use Case**

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

**Figure 899  Flow of Control, Basic 802.1X Configuration Use Case**
Policy Manager ships with fourteen preconfigured services. In this use case, you select a service that supports 802.1X wireless requests. Follow the steps below to configure this basic 802.1X service that uses [EAP FAST], one of the pre-configured Policy Manager authentication methods, and **Active Directory Authentication Source (AD)**, an external authentication source within your existing enterprise.

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

Policy Manager tests client identity against role-mapping rules, appending any match (multiple roles acceptable) to the request for use by the enforcement policy. In the event of role-mapping failure, Policy Manager assigns a default role. This use case create the role mapping policy **RMP_DEPARTMENT** that distinguishes clients by department and the corresponding roles **ROLE_ENGINEERING** and **ROLE_FINANCE**, to which it maps.

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

For purposes of posture evaluation, you can configure a posture policy (internal to Policy Manager), a posture server (external), or an audit server (internal or external). Each of the first three use cases demonstrates one of these options; here, the posture server.

### Configuring a Service

1. Navigate to **Configuration > Services**.
2. Click the ✚ **Add** icon to add a service. The **Configuration > Services > Add** window opens.
3. If it is not already selected, click the **Service** tab and define basic service information.
   a. Enter a name for the service in the **Name** field.
   b. Click the **Type** drop-down list and select **802.1X Wireless**.
   c. (Optional) click the **Monitor Mode** checkbox to allow handshakes to occur (for monitoring purposes), but without enforcement.
   d. Click **Next** to display the **Authentication** tab.
4. Configure authentication.
   a. In the **Authentication Methods** field, select **[EAP Fast]**.
   b. In the Authentication Sources field, click the Select to Add drop-down list and select the following sources.
      - [Local User Repository] [Local SQL DB]
      - [Guest User Repository] [Local SQL DB]
      - [Guest Device Repository] [Local SQL DB]
      - [Endpoints Repository] [Local SQL DB]
      - [Onboard Devices Repository] [Local SQL DB]
      - [Admin User Repository] [Local SQL DB]
      - [Active Directory]
   c. (Optional) Select **Strip Username Rules** to pre-process the user name (to remove prefixes and suffixes) before sending it to the authentication source.

### Creating a New Role Mapping Policy
To create a new Role Mapping policy:

1. Click the **Roles** tab.
2. Click **Add new Role Mapping Policy**. The Role Mappings page opens.

**Figure 900  Role Mapping Navigation and Settings**

3. Add a new role, navigate to the **Policy** tab. Enter the **Policy Name**, For example, ROLE_ENGINEER and click **Save**. Repeat the same step for ROLE_FINANCE. The following figure displays the **Policy** tab:

**Figure 901  Policy Tab**

4. Click the **Next** button in the **Rules Editor**.
5. Create rules to map client identity to a role. From the **Mapping Rules** tab, select the **Rules Evaluation Algorithm** radio button. The following figure displays the **Mapping Rules** tab:
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 903 Roles Tab**

10. Select **Role Mapping Policy**, for example, RMP_DEPARTMENT. Click **Next**.
11. Add a **Microsoft NPS** external posture server to the 802.1X service. Click the **Posture** tab. The following figure displays the **Posture** tab:

**Figure 904  Posture Tab**

12. Click **Add new Posture Server** to add a new posture server.

13. Configure the following posture settings examples:
   - **Name** (freeform): **PS_NPS**
   - **Server Type** radio button: **Microsoft NPS**
   - **Default Posture Token** (selector): **UNKNOWN**

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

**Figure 905  Posture Server Tab**

14. Click **Next**.

15. Configure connection settings in the **Primary/ Backup Server** tabs by entering the connection information for the RADIUS posture server. The following figure displays the **Primary Server** tab:
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 907 Posture Tab**

18. Click the **Next** button. Assign an enforcement policy.

19. Enforcement policies contain dictionary-based rules for evaluation of Role, Posture Tokens, and System Time to evaluation profiles. Policy Manager applies all matching enforcement profiles to the request. In the case of no match, Policy Manager assigns a default enforcement profile. The following figure displays the **Enforcement** tab:

**Table 40: Enforcement Policy Navigation and Settings**
20. From the **Enforcement** tab, select the **Enforcement Policy**. For instructions about how to build an enforcement policy, refer to [Configuring Enforcement Policies](#).

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 908 Flow-of-Control of Web-Based Authentication for Guests**

**Configuring a Service**

Perform the following steps to configure Policy Manager for WebAuth-based Guest access.

1. Prepare the switch to pre-process WebAuth requests for the Policy Manager 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 1: Service Navigation and Settings

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new Service:</td>
<td><img src="image" alt="Service Navigation and Settings" /></td>
</tr>
<tr>
<td>- Services &gt;</td>
<td></td>
</tr>
<tr>
<td>- Add Service &gt;</td>
<td></td>
</tr>
<tr>
<td>Name the Service and select a pre-configured Service Type:</td>
<td><img src="image" alt="Service Navigation and Settings" /></td>
</tr>
<tr>
<td>- Service (tab) &gt;</td>
<td></td>
</tr>
<tr>
<td>- Type (selector): Aruba Web-Based Authentication &gt;</td>
<td></td>
</tr>
<tr>
<td>- Name/Description (freeform) &gt;</td>
<td></td>
</tr>
<tr>
<td>- Upon completion, click Next.</td>
<td></td>
</tr>
</tbody>
</table>

3. Set up the Authentication.
   b. Source: Administrators typically configure Guest Users in the local Policy Manager database.

4. Configure a Posture Policy.

For purposes of posture evaluation, you can configure a Posture Policy (internal to Policy Manager), a Posture Server (external), or an Audit Server (internal or external). Each of the first three use cases demonstrates one of these options. This use case demonstrates the Posture Policy.

As of the current version, Policy Manager ships with five pre-configured posture plugins that evaluate the health of the client and return a corresponding posture token.

To add the internal posture policy `IPP_UNIVERSAL_XP`, which (as you will configure it in this Use Case, checks any Windows® XP clients to verify the most current Service Pack).
Table 2: Local Policy Manager Database Navigation and Settings

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the local Policy Manager database:</td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td>- Authentication (tab) &gt;</td>
<td>- Strip Username Rules (check box) &gt;</td>
</tr>
<tr>
<td>- Sources (Select drop-down list): [Local User Repository] &gt;</td>
<td>- Enter an example of preceding or following separators (if any), with the phrase &quot;user&quot; representing the username to be returned. For authentication, Policy Manager strips the specified separators and any paths or domains beyond them.</td>
</tr>
<tr>
<td>- Add &gt;</td>
<td>- Upon completion, click Next (until you reach Enforcement Policy).</td>
</tr>
</tbody>
</table>

For authentication, Policy Manager strips the specified separators and any paths or domains beyond them.
Table 3: Posture Policy Navigation and Settings

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Posture Policy:</td>
<td>Create a Posture Policy:</td>
</tr>
<tr>
<td>- Posture (tab) &gt;</td>
<td>- Posture (tab) &gt;</td>
</tr>
<tr>
<td>- Enable Validation Check (check box) &gt;</td>
<td>- Enable Validation Check (check box) &gt;</td>
</tr>
<tr>
<td>- Add new Internal Policy (link) &gt;</td>
<td>- Add new Internal Policy (link) &gt;</td>
</tr>
</tbody>
</table>

Name the Posture Policy and specify a general class of operating system:
- **Policy** (tab) >
- **Policy Name** (freeform): \( \text{IPP\_UNIVERSAL} \)
- **Host Operating System** (radio buttons): \( \text{Windows} \)>
- When finished working in the **Policy** tab, click **Next** to open the Posture Plugins tab

![Posture Policy Navigation and Settings](image_url)
### Navigation

Select a Validator:
- **Posture Plugins** (tab) >
- Enable **Windows Health System Validator** >
- Configure (button) >

### Setting

Configure the Validator:
- **Windows System Health Validator** (popup) >
- Enable all Windows operating systems (check box) >
- Save (button) >
- 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.

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

The following fields deserve special mention:

- **Default Posture Token.** Value of the posture token to use if health status is not available.
- **Remediate End-Hosts.** When a client does not pass posture evaluation, redirect to the indicated server for remediation.
- **Remediation URL.** URL of remediation server.

5. Create an Enforcement Policy.

Because this Use Case assumes the Guest role, and the Aruba Web Portal agent has returned a posture token, it does not require configuration of Role Mapping or Posture Evaluation.

The SNMP_POLICY selected in this step provides full guest access to a Role of [Guest] with a Posture of Healthy, and limited guest access.

**Table 4: Enforcement Policy Navigation and Settings**

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new Enforcement Policy:</td>
<td><img src="image" alt="SNMP_POLICY Configuration" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Enforcement Policy Details" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Enforcement Profiles" /></td>
</tr>
</tbody>
</table>

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-holds.

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 909  Flow-of-Control of MAC Authentication for Network Devices**
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.
3. **Table 1: MAC Authentication Service Navigation and Settings**

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new Service:</td>
<td><img src="image_url" alt="Image" /></td>
</tr>
<tr>
<td>• Services &gt;</td>
<td><img src="image_url" alt="Image" /></td>
</tr>
<tr>
<td>• Add Service (link) &gt;</td>
<td><img src="image_url" alt="Image" /></td>
</tr>
</tbody>
</table>

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

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. You can also select any other supported type of authentication source.
### Table 2: Authentication Method Navigation and Settings

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Settings</th>
</tr>
</thead>
</table>
| 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) |

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.

   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 3: Audit Server Navigation and Settings

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Settings</th>
</tr>
</thead>
</table>
| Configure the Audit Server:  
  - Audit (tab) >  
  - Audit End Hosts (enable) >  
  - Audit Server (selector): NMAP  
  - Trigger Conditions (radio button): For MAC authentication requests  
  - Reauthenticate client (check box): Enable |

   Upon completion of the audit, Policy Manager caches Role (Nmap and Nessus) and Posture (Nessus), then resets the connection (or the switch reauthenticates after a short session timeout), triggering a new request, which follows the same path until it reaches Role Mapping/Posture/Audit; this appends cached information for this client to the request for passing to Enforcement.

6. Select the Enforcement Policy Sample_Allow_Access_Policy:
Table 4: Enforcement Policy Navigation and Settings

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the Enforcement Policy:</td>
<td></td>
</tr>
<tr>
<td>■ Enforcement (tab) &gt;</td>
<td></td>
</tr>
<tr>
<td>■ Use Cached Results (check box): Select Use cached Roles and Posture attributes from previous sessions &gt;</td>
<td></td>
</tr>
<tr>
<td>■ Enforcement Policy (selector): UnmanagedClientPolicy</td>
<td></td>
</tr>
<tr>
<td>■ When you are finished with your work in this tab, click Save.</td>
<td></td>
</tr>
</tbody>
</table>

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 911** *Administrator connections to Network Access Devices via TACACS*
Configuring the Service

Perform the following steps to configure Policy Manager for TACACS+-based access:

1. Navigate to Configuration > Services.

2. Click the Add icon to add a service. The Configuration > Services > Add window opens.

3. If it is not already selected, click the Service tab and define basic service information.
   a. Enter a name for the service in the Name field.
   b. Click the Type drop-down list and select the preconfigured service type that matches your Policy Manager Admin Network Login Service.
   c. Click Next to display the Authentication tab.

4. Define the Authentication settings for the service. Authentication methods can be left to their default values, as the Policy Manager TACACS+ service authenticates TACACS+ requests internally.
   a. In the Authentication Sources section, click the Select to Add drop-down list.
   b. Select AD (Active Directory). For this use case example, Network Access Device authentication data will be stored in the Active Directory.

5. Click the Enforcement tab and select an Enforcement Policy.
a. Click the Enforcement Policy drop-down list and select the Enforcement Policy [Admin Network Login Policy] that distinguishes the two allowed roles (Net Admin Limited and Device SuperAdmin).

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

**Single Port Use Case**

This Service supports all three types of connections on a single port.

The following figure illustrates both the overall flow of control for this hybrid service, in which complementary switch and Policy Manager configurations allow all three types of connections on a single port:

*Figure 912  Flow of the Multiple Protocol Per Port Case*
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 958
- Variables on page 968
- Operators on page 969

### Namespaces

Multiple namespaces are displayed in the rules-editing interfaces, depending upon what you are editing.

For detailed information about the available namespaces, see the following topics:

- Application Namespace
- Audit Namespaces
- Authentication Namespaces
- Authorization Namespaces
- Certificate Namespaces
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 are provided with ClearPass Policy Manager. 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 Service Flow Control for more information.

The Avenda Systems:Audit namespace appears when editing post-audit rules for Nessus and NMAP audit servers.

The following table displays the Audit Namespace attributes:

<table>
<thead>
<tr>
<th><strong>Table 1:</strong> Audit Namespace Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute Name</strong></td>
</tr>
</tbody>
</table>
| 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>
<thead>
<tr>
<th>Attribute Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>InnerMethod</td>
<td>CHAP</td>
</tr>
<tr>
<td></td>
<td>EAP-GTC</td>
</tr>
<tr>
<td></td>
<td>EAP-MD5</td>
</tr>
<tr>
<td></td>
<td>EAP-MSCHAPv2</td>
</tr>
<tr>
<td></td>
<td>EAP-TLS</td>
</tr>
<tr>
<td></td>
<td>MSCHAP</td>
</tr>
<tr>
<td></td>
<td>PAP</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The EAP-MD5 authentication type is not supported if you use the ClearPass Policy Manager in the FIPS mode.</td>
<td></td>
</tr>
<tr>
<td>OuterMethod</td>
<td>CHAP</td>
</tr>
<tr>
<td></td>
<td>EAP-FAST</td>
</tr>
<tr>
<td></td>
<td>EAP-MD5</td>
</tr>
<tr>
<td></td>
<td>EAP-PEAP</td>
</tr>
<tr>
<td></td>
<td>EAP-TLS</td>
</tr>
<tr>
<td></td>
<td>EAP-TTLS</td>
</tr>
<tr>
<td></td>
<td>MSCHAP</td>
</tr>
<tr>
<td></td>
<td>PAP</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The EAP-MD5 authentication type is not supported if you use the ClearPass Policy Manager in the FIPS mode.</td>
<td></td>
</tr>
<tr>
<td>Phase1PAC</td>
<td><strong>None:</strong> No PAC was used to establish the outer tunnel in the EAP-FAST authentication method</td>
</tr>
<tr>
<td></td>
<td><strong>Tunnel:</strong> A tunnel PAC was used to establish the outer tunnel in the EAP-FAST authentication method</td>
</tr>
<tr>
<td></td>
<td><strong>Machine:</strong> A machine PAC was used to establish the outer tunnel in the EAP-FAST authentication method; machine PAC is used for machine authentication (see EAP-FAST in Adding and Modifying Authentication Methods).</td>
</tr>
<tr>
<td>Phase2PAC</td>
<td><strong>None:</strong> No PAC was used instead of an inner method handshake in the EAP-FAST authentication method</td>
</tr>
<tr>
<td></td>
<td><strong>UserAuthPAC:</strong> A user authentication PAC was used instead of the user authentication inner method handshake in the EAP-FAST authentication method</td>
</tr>
<tr>
<td></td>
<td><strong>PosturePAC:</strong> A posture PAC was used instead of the posture credential handshake in the EAP-FAST authentication method</td>
</tr>
<tr>
<td>Posture</td>
<td><strong>Capable:</strong> The client is capable of providing posture credentials</td>
</tr>
<tr>
<td></td>
<td><strong>Collected:</strong> Posture credentials were collected from the client</td>
</tr>
<tr>
<td></td>
<td><strong>Not-Capable:</strong> The client is not capable of providing posture credentials</td>
</tr>
<tr>
<td></td>
<td><strong>Unknown:</strong> It is not known whether the client is capable of providing credentials</td>
</tr>
<tr>
<td>Status</td>
<td><strong>None:</strong> No authentication took place</td>
</tr>
<tr>
<td></td>
<td><strong>User:</strong> The user was authenticated</td>
</tr>
<tr>
<td></td>
<td><strong>Machine:</strong> The machine was authenticated</td>
</tr>
<tr>
<td></td>
<td><strong>Failed:</strong> Authentication failed</td>
</tr>
<tr>
<td></td>
<td><strong>AuthSource-Unreachable:</strong> The authentication source was unreachable</td>
</tr>
<tr>
<td>MacAuth</td>
<td><strong>NotApplicable:</strong> Not a MAC Auth request</td>
</tr>
<tr>
<td></td>
<td><strong>Known Client:</strong> Client MAC address was found in an authentication source</td>
</tr>
<tr>
<td></td>
<td><strong>Unknown Client:</strong> Client MAC address was not found in an authentication source</td>
</tr>
</tbody>
</table>
### 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](#) 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](#)).

  **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.**

---

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username as received from the client (after the strip user name rules are applied).</td>
</tr>
<tr>
<td>Full-Username</td>
<td>The username as received from the client (before the strip user name rules are applied).</td>
</tr>
<tr>
<td>Source</td>
<td>The name of the authentication source used to authenticate the user.</td>
</tr>
</tbody>
</table>
**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 1: Certificate Namespace Attributes**

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

### 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 1: Connection Namespace Pre-defined Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src-IP-Address</td>
<td>Src-IP-Address and Src-Port are the IP address and port from which the request (RADIUS, TACACS+, etc.) originated.</td>
</tr>
<tr>
<td>Src-Port</td>
<td></td>
</tr>
<tr>
<td>Dest-IP-Address</td>
<td>Dst-IP-Address and Dst-Port are the IP address and port at which Policy Manager received the request (RADIUS, TACACS+, etc.).</td>
</tr>
<tr>
<td>Dest-Port</td>
<td></td>
</tr>
<tr>
<td>NAD-IP-Address</td>
<td>IP address of the network device from which the request originated.</td>
</tr>
</tbody>
</table>
### Attribute Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-Mac-Address</td>
<td>MAC address of the client.</td>
</tr>
<tr>
<td>Client-Mac-Address-Colon</td>
<td>Client MAC address in different formats.</td>
</tr>
<tr>
<td>Client-Mac-Address-Dot</td>
<td></td>
</tr>
<tr>
<td>Client-Mac-Address-Hyphen</td>
<td></td>
</tr>
<tr>
<td>Client-Mac-Address-Nodelim</td>
<td></td>
</tr>
<tr>
<td>Client-IP-Address</td>
<td>IP address of the client (if known).</td>
</tr>
</tbody>
</table>

## Date Namespaces

The date namespace has three pre-defined attributes:

- Day-of-Week
- Date-of-Year
- Time-of-Day

For Day-of-Week, the supported operators are BELONG_TO and NOT_BELONGS_TO, and the value field shows a multi-select list box with days from Monday through Sunday.

The Time-of-Day attribute shows a time icon in the value field.

The Date-of-Year attribute shows a date, month and year icon in the value field.

The operators supported for Date-of-Year and Time-of-Day attributes are the similar to the ones supported for the integer data type.

### Date Namespace Editing Contexts

- Enforcement policies
- Filter rules for Access Tracker and Activity Reports
- Role mapping policies
- Service rules

## Device Namespaces

The Device namespace has four pre-defined attributes:

- Location
- OS-Version
- Device-Type
- Device-Vendor

Custom attributes also appear in the attribute list if they are defined as custom tags for the device.

These attributes can be used only if you have pre-populated the values for these attributes when a network device is configured.
Endpoint Namespaces

Use these attributes to look for attributes of authenticating endpoints, which are present in the Policy Manager endpoints list. The Endpoint namespace has the following attributes:

- Disabled By
- Disabled Reason
- Enabled By
- Enabled Reason
- Info URL

Guest User Namespaces

The GuestUser namespace has the attributes associated with the guest user (resident in the Policy Manager guest user database) who authenticated in this session. This namespace is only applicable if a guest user is authenticated. The GuestUser namespace has six pre-defined attributes:

- Company-Name
- Designation
- Email
- Location
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the guest user.

These attributes can be used only if you have pre-populated the values for these attributes when a guest user is configured in Policy Manager.

Host Namespaces

The Host namespace has the following predefined attributes:

- Name*
- OSTYPE*
- FQDN*
- UserAgent**
- CheckType**
- UniqueID
- AgentType*
- InstalledSHAs*

* Only populated when request is originated by a Microsoft NAP-compatible agent.

** Only present if Policy Manager acts as a Web authentication portal.

Local User Namespaces

The LocalUser namespace has the attributes associated with the local user (resident in the Policy Manager local user database) who authenticated in this session. This namespace is only applicable if a local user is authenticated.
The LocalUser namespace has four pre-defined attributes:
- Designation
- Email
- Phone
- Sponsor

Custom attributes also appear in the attribute list if they are defined as custom tags for the local user.

These attributes can be used only if you have pre-populated the values for these attributes when a local user is configured in Policy Manager.

**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 710 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 1: Policy Manager Variables Supported by ClearPass

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{attribute-name}</td>
<td>\textit{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 184.</td>
</tr>
<tr>
<td>%{Radius:IETF:MAC-Address-Hyphen}</td>
<td>MAC address of client in aa-bb-cc-dd-ee-ff format</td>
</tr>
<tr>
<td>%{RadiusS:IETF:MAC-Address-Dot}</td>
<td>MAC address of client in aabb.ccdd.eeff format</td>
</tr>
<tr>
<td>%{Radius:IETF:MAC-Address-NoDelim}</td>
<td>MAC address of client in aabbcdddeeff format</td>
</tr>
</tbody>
</table>
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 1: Attribute Operators**

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>- BELONGS_TO</td>
</tr>
<tr>
<td></td>
<td>- NOT_BELONGS_TO</td>
</tr>
<tr>
<td></td>
<td>- BEGINS_WITH</td>
</tr>
<tr>
<td></td>
<td>- NOT_BEGINS_WITH</td>
</tr>
<tr>
<td></td>
<td>- CONTAINS</td>
</tr>
<tr>
<td></td>
<td>- NOT_CONTAINS</td>
</tr>
<tr>
<td></td>
<td>- ENDS_WITH</td>
</tr>
<tr>
<td></td>
<td>- NOT_ENDS_WITH</td>
</tr>
<tr>
<td></td>
<td>- EQUALS</td>
</tr>
<tr>
<td></td>
<td>- NOT_EQUALS</td>
</tr>
<tr>
<td></td>
<td>- EQUALS_IGNORE_CASE</td>
</tr>
<tr>
<td></td>
<td>- NOT_EQUALS_IGNORE_CASE</td>
</tr>
<tr>
<td></td>
<td>- EXISTS</td>
</tr>
<tr>
<td></td>
<td>- NOT_EXISTS</td>
</tr>
<tr>
<td></td>
<td>- MATCHES_REGEX</td>
</tr>
<tr>
<td></td>
<td>- NOT_MATCHES_REGEX</td>
</tr>
<tr>
<td>Integer</td>
<td>- BELONGS_TO</td>
</tr>
<tr>
<td></td>
<td>- NOT_BELONGS_TO</td>
</tr>
<tr>
<td></td>
<td>- EQUALS</td>
</tr>
<tr>
<td></td>
<td>- NOT_EQUALS</td>
</tr>
<tr>
<td></td>
<td>- EXISTS</td>
</tr>
<tr>
<td></td>
<td>- NOT_EXISTS</td>
</tr>
<tr>
<td></td>
<td>- GREATER_THAN</td>
</tr>
<tr>
<td></td>
<td>- GREATER_THAN_OR_EQUALS</td>
</tr>
<tr>
<td></td>
<td>- LESS_THAN</td>
</tr>
<tr>
<td></td>
<td>- LESS_THAN_OR_EQUALS</td>
</tr>
<tr>
<td>Time or Date</td>
<td>- EQUALS</td>
</tr>
<tr>
<td></td>
<td>- NOT_EQUALS</td>
</tr>
<tr>
<td></td>
<td>- GREATER_THAN</td>
</tr>
<tr>
<td></td>
<td>- GREATER_THAN_OR_EQUALS</td>
</tr>
<tr>
<td></td>
<td>- LESS_THAN</td>
</tr>
<tr>
<td></td>
<td>- LESS_THAN_OR_EQUALS</td>
</tr>
<tr>
<td></td>
<td>- IN_RANGE</td>
</tr>
</tbody>
</table>
## Attribute Type

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day</td>
<td>BELONGS_TO</td>
</tr>
<tr>
<td></td>
<td>NOT_BELONGS_TO</td>
</tr>
<tr>
<td>List (Example: Role)</td>
<td>EQUALS</td>
</tr>
<tr>
<td></td>
<td>NOT_EQUALS</td>
</tr>
<tr>
<td></td>
<td>MATCHES_ALL</td>
</tr>
<tr>
<td></td>
<td>NOT_MATCHES_ALL</td>
</tr>
<tr>
<td></td>
<td>MATCHES_ANY</td>
</tr>
<tr>
<td></td>
<td>NOT_MATCHES_ANY</td>
</tr>
<tr>
<td></td>
<td>MATCHES_EXACT</td>
</tr>
<tr>
<td></td>
<td>NOT_MATCHES_EXACT</td>
</tr>
<tr>
<td>Group (Example: Calling-Station-Id, NAS-IP-Address)</td>
<td>BELONGS_TO_GROUP</td>
</tr>
<tr>
<td></td>
<td>NOT_BELONGS_TO_GROUP</td>
</tr>
</tbody>
</table>

The following table describes all operator types:

**Table 41: Operator Descriptions**

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEGINS_WITH</td>
<td>For string data type, true if the run-time value of the attribute begins with the configured value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Radius:IETF:NAS-Identifier BEGINS_WITH &quot;SJ-&quot;</td>
</tr>
<tr>
<td>BELONGS_TO</td>
<td>For string data type, true if the run-time value of the attribute matches a set of configured string values.</td>
</tr>
<tr>
<td>Example:</td>
<td>Radius:IETF:Service-Type BELONGS_TO Login-User, Framed-User, Authenticate-Only</td>
</tr>
<tr>
<td></td>
<td>For integer data type, true if the run-time value of the attribute matches a set of configured integer values.</td>
</tr>
<tr>
<td>Example:</td>
<td>Radius:IETF:NAS-Port BELONGS_TO 1,2,3</td>
</tr>
<tr>
<td></td>
<td>For day data type, true if run-time value of the attribute matches a set of configured days of the week.</td>
</tr>
<tr>
<td>Example:</td>
<td>Date:Day-of-Week BELONGS_TO MONDAY, TUESDAY, WEDNESDAY</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>BELONGS_TO_GROUP</td>
<td>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).</td>
</tr>
<tr>
<td>Example:</td>
<td>Radius:IETF:Calling-Station-Id BELONGS_TO_GROUP Printers.</td>
</tr>
<tr>
<td>CONTAINS</td>
<td>For string data type, true if the run-time value of the attribute is a substring of the configured value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Radius:IETF:NAS-Identifier CONTAINS &quot;VPN&quot;</td>
</tr>
<tr>
<td>ENDS_WITH</td>
<td>For string data type, true if the run-time value of the attribute ends with the configured value.</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Example:</strong> Radius:IETF:NAS-Identifier ENDS_WITH &quot;DEVICE&quot;</td>
<td><strong>EQAULS</strong></td>
</tr>
<tr>
<td></td>
<td>True if the run-time value of the attribute matches the configured value. For string data type, this is a case-sensitive comparison. <strong>Example:</strong> Radius:IETF:NAS-Identifier EQUALS &quot;SJ-VPN-DEVICE&quot;</td>
</tr>
<tr>
<td></td>
<td><strong>EQUALS_IGNORE_CASE</strong></td>
</tr>
<tr>
<td></td>
<td>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. <strong>Example:</strong> Radius:IETF:NAS-Identifier EQUALS_IGNORE_CASE &quot;sj-vpn-device&quot;</td>
</tr>
<tr>
<td></td>
<td><strong>EXISTS</strong></td>
</tr>
<tr>
<td></td>
<td>For string data type, true if the run-time value of the attribute exists. This is a unary operator. <strong>Example:</strong> Radius:IETF:NAS-Identifier EXISTS</td>
</tr>
<tr>
<td></td>
<td><strong>GREATER_THAN</strong></td>
</tr>
<tr>
<td></td>
<td>For integer, time and date data types, true if the run-time value of the attribute is greater than the configured value. <strong>Example:</strong> Radius:IETF:NAS-Port GREATER_THAN 10</td>
</tr>
<tr>
<td></td>
<td><strong>GREATER_THAN_OR_EQUALS</strong></td>
</tr>
<tr>
<td></td>
<td>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. <strong>Example:</strong> Radius:IETF:NAS-Port GREATER_THAN_OR_EQUALS 10</td>
</tr>
<tr>
<td></td>
<td><strong>IN_RANGE</strong></td>
</tr>
<tr>
<td></td>
<td>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. <strong>Example:</strong> Date:Date-of-Year IN_RANGE 2007-06-06,2007-06-12</td>
</tr>
<tr>
<td></td>
<td><strong>LESS_THAN</strong></td>
</tr>
<tr>
<td></td>
<td>For integer, time and date data types, true if the run-time value of the attribute is less than the configured value. <strong>Example:</strong> Radius:IETF:NAS-Port LESS_THAN 10</td>
</tr>
<tr>
<td></td>
<td><strong>LESS_THAN_OR_EQUALS</strong></td>
</tr>
<tr>
<td></td>
<td>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. <strong>Example:</strong> Radius:IETF:NAS-Port LESS_THAN_OR_EQUALS 10</td>
</tr>
<tr>
<td></td>
<td><strong>MATCHES_ALL</strong></td>
</tr>
<tr>
<td></td>
<td>For list data types, true if all of the run-time values in the list are found in the configured values. <strong>Example:</strong> Tips:Role MATCHES_ALL HR,ENG,FINANCE. In this example, if the run-time values of Tips:Role are HR,ENG,FINANCE,MGR,ACCT the condition evaluates to true.</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MATCHES ANY</td>
<td>For list data types, true if any of the run-time values in the list match one of the configured values. <strong>Example:</strong> Tips:Role MATCHES_ANY HR, ENG, FINANCE</td>
</tr>
<tr>
<td>MATCHES EXACT</td>
<td>For list data types, true if all of the run-time values of the attribute match all of the configured values. <strong>Example:</strong> 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.</td>
</tr>
<tr>
<td>MATCHES REGEX</td>
<td>For string data type, true if the run-time value of the attribute matches the regular expression in the configured value. <strong>Example:</strong> Radius:IETF:NAS-Identifier MATCHES_REGEX sj-device[1-9]-dev*</td>
</tr>
</tbody>
</table>

**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 opens.

   **Figure 913 Applications Dictionaries Page**

2. To see the application attributes, click the name of an application.
   - The **Application Attributes** dialog box opens.
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.**